Проект
(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Безпека інформаційних і комунікаційних систем»

Другого (магістерського) рівня вищої освіти

за спеціальністю __125 «Кібербезпека»_____

галузі знань ____12 Інформаційні технології_____

СМЯ НАУ ОПП 09.01.09 – 03 – 2021

Освітньо-професійна програма
Затверджена Вченою радою Університету
Протокол №_____ від _____2021 р.

Вводиться в дію наказом ректора
Ректор
_____Луцький М.Г.
Наказ №_____ від _____2021 р.

КИЇВ

ДІЄ ЯК ТИМЧАСОВА ДО ВВЕДЕННЯ СТАНДАРТУ ВИЩОЇ ОСВІТИ УКРАЇНИ

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

ПОГОДЖЕНО
Радою з якості Національного авіаційного університету
протокол №_____
від «_____»_____20___ р.
Голова Ради з якості НАУ

_____

ПОГОДЖЕНО
Вченою радою Факультету кібербезпеки, комп'ютерної та програмної інженерії
протокол №_____
від «_____»_____20___ р.
Голова вченої ради факультету

_____ Нестеренко К.С.

ПОГОДЖЕНО
Кафедрою комп'ютеризованих систем захисту інформації
протокол засідання №_____
від «_____»_____20___ р.
Завідувач кафедри

_____ Казмірчук С.В

ПОГОДЖЕНО
Студентською радою Факультету кібербезпеки, комп'ютерної та програмної інженерії протокол №_____
від «_____»_____20___ р.
Голова студентської ради

_____

ПЕРЕДМОВА

Розроблено робочою групою освітньо-професійної програми (спеціальності 125 «Кібербезпека», рік вступу – 2021-й та наступні до нової редакції освітньої програми)

у складі:

ГАРАНТ ОСВІТНЬОЇ ПРОГРАМИ:

Казмірчук Світлана Володимирівна – д.т.н., доц., завідувач кафедри комп'ютеризованих систем захисту інформації

_____
підпис гаранта

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

Ільєнко Анна Вадимівна – к.т.н., доц., доцент кафедри комп'ютеризованих систем захисту інформації

_____
підпис члена робочої групи

Єлізаров Анатолій Борисович – к.т.н., доц., доцент кафедри комп'ютеризованих систем захисту інформації

_____
підпис члена робочої групи

Дубчак Олена Вікторівна – старший викладач кафедри комп'ютеризованих систем захисту інформації

_____
підпис члена робочої групи

Кваша Діана Сергіївна – здобувачка вищої освіти

_____
підпис здобувача вищої освіти

ЗОВНІШНІ СТЕЙКХОЛДЕРИ:

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 комп'ютеризованих систем захисту інформації
1.2.	Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Освітній ступінь Магістр Магістр з кібербезпеки
1.3.	Офіційна назва освітньо-професійної програми	Безпека інформаційних і комунікаційних систем
1.4.	Тип диплому та обсяг освітньо-професійної програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 рік 4 місяці
1.5.	Акредитаційна інституція	Акредитаційна комісія, Міністерство освіти і науки України, сертифікат УД № 11005810 від 12.11.2018р.
1.6.	Період акредитації	Термін дії сертифікату до 01.07.2023 р.
1.7.	Цикл/рівень	НРК України – 7 рівень; FQ-EHEA – другий цикл; EQF-LLL – 7 рівень
1.8.	Передумови	Вища освіта зі ступенем бакалавр
1.9.	Форма навчання	Інституційна з елементами дистанційної: очна, заочна
1.10	Мова(и) викладання	Українська
1.11	Інтернет-адреса постійного розміщення опису освітньої програми	http://www.nau.edu.ua http://www.kszi.nau.edu.ua
Розділ 2. Ціль освітньо-професійної програми		
2.1.	Ціль освітньої-професійної програми «Безпека інформаційних і комунікаційних систем» полягає в підготовці висококваліфікованих, конкурентоспроможних фахівців за другим (магістерським) рівнем у галузі 125 Кібербезпека та забезпечення студентів фундаментальної підготовки у вигляді поглиблених теоретичних і практичних знань, умінь та навичок, достатніх для ефективного виконання завдань інноваційного характеру відповідного рівня професійної діяльності в галузі захисту інформації; оволодіння студентами знаннями, вміннями та навичками з проектування, експлуатації, адміністрування та інформаційного захисту комп'ютерних систем, локальних і корпоративних інформаційно-обчислювальних мереж та системного програмного забезпечення.. ОП «Безпека інформаційних і комунікаційних систем» 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 освіти, досліджень і практики, так і надання високоякісних освітніх та науково-дослідних послуг громадянам України та іноземцям при підготовці фахівців авіаційно-космічної галузі. У ОП немає аналогів серед ЗВО України щодо врахування галузевого контексту функціонування авіаційного сектору.	
Розділ 3. Характеристика освітньо-професійної програми		
3.1	Предметна область (об’єкт діяльності, теоретичний зміст)	Об’єкти професійної діяльності випускників: – об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою об’єктів, що підлягають захисту. Цілі навчання підготовка професіоналів, здатних використовувати і впроваджувати технології та застосовувати засоби інформаційної та/або кібербезпеки. Теоретичний зміст предметної діяльності. Знання: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проектування. Методи, методики та технології: методи, методики та технології забезпечення інформаційної та/або кібербезпеки. Інструменти та обладнання: системи розробки, забезпечення, моніторингу та контролю інформаційної та/або кібербезпеки; сучасне програмно-апаратне забезпечення інфокомунікаційних технологій.
3.2.	Орієнтація освітньо-професійної програми	Програма має прикладну орієнтацію. Базується на загальновідомих положеннях,

		результатах сучасних наукових досліджень та нових знаннях в галузі кібербезпеки, необхідних для майбутньої професійної діяльності магістрів, здатних вирішувати певні проблеми і задачі за умови оволодіння системою компетентностей.
3.3.	Основний фокус освітньо-професійної програми	Спеціальна освіта та професійна підготовка в галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека Ключові слова: кібербезпека, криптосистема, технології забезпечення безпеки інформації
3.4.	Особливості освітньо-професійної програми	Освітньо-професійна програма розроблена на основі студентоцентрованого підходу, який реалізується через індивідуалізацію освіти. З метою підготовки до роботи в реальному середовищі майбутньої професійної діяльності та отримання випускниками освітньої кваліфікації магістр з кібербезпеки, програма забезпечує підготовку професіоналів, здатних: – виявляти та оцінювати ознаки стороннього кібервпливу; – моделювати можливі ситуації стороннього кібервпливу та попереджати їх можливі наслідки; – організовувати і підтримувати комплекс заходів щодо забезпечення інформаційної та/або кібербезпеки; – проводити дослідження у напрямах забезпечення інформаційної та/або кібербезпеки національних інтересів України й обґрунтовувати шляхи підвищення їх ефективності; – забезпечити криптографічний захист інформаційних ресурсів тощо. З метою передачі передового досвіду майбутньому фахівцю, висвітлення в навчальному процесі останніх досягнень науки і техніки, правил ведення успішного бізнесу програма передбачає: - реалізацію процесного підходу при конструюванні змісту профільно-орієнтованих навчальних дисциплін, студентської мобільності, академічної співпраці та молодіжних обмінів; - залучення до викладацької діяльності керівників та професіоналів, які працюють як в системі професійної освіти, так й на виробництві в галузі інформаційних технологій та телекомунікацій, а також представників бізнесу.
Розділ 4. Придатність випускників до працевлаштування та подальшого навчання		
4.1.	Придатність до працевлаштування	Професійна діяльність в галузі інформаційних технологій, установах, організаціях різних форм власності на посадах визначених чинною редакцією Національного класифікатора

		України: Класифікатор професій (ДК 003:2010), які здобули освіту за освітньою програмою «Безпека інформаційних і комунікаційних систем» можуть обіймати такі первинні посади, як: – програміст/тестувальник програмного забезпечення систем інформаційної та кібербезпеки; – адміністратор комп'ютерних систем і мереж; – адміністратор інформаційної та кібербезпеки; – аудитор/пентестер безпеки інформаційно-комунікаційних систем; – розробник засобів захисту інформації; – провідний спеціаліст/керівник служби технічного захисту інформації тощо.
4.2.	Подальше навчання	Програма орієнтована на продовження освіти й отримання вищих кваліфікаційних рівнів і наукових ступенів, що відповідає восьмому кваліфікаційному рівню Національної рамки кваліфікацій, з присудженням першого наукового ступеня третього рівня вищої освіти – доктора філософії; набуття додаткових кваліфікацій в системі післядипломної освіти
Розділ 5. Викладання та оцінювання		
5.1.	Викладання та навчання (методи, методики, технології, інструменти та обладнання)	Ґрунтуються на принципах студентоцентризму та індивідуально-особистісного підходу; реалізуються через навчання на основі досліджень, посилення практичної орієнтованості та творчої спрямованості у формі комбінації лекцій, практичних занять, самостійної навчальної і дослідницької роботи, розв’язування прикладних задач, виконання проектів, навчальних та виробничих практик, курсових робіт, дипломної роботи.
5.2.	Оцінювання	Накопичувальна бально-рейтингова система, що передбачає оцінювання студентів за усі види аудиторної та позааудиторної освітньої діяльності у вигляді вхідного, поточного, рубіжного та/або семестрового контролю та атестації.
Розділ 6. Програмні компетентності		
6.1.	Інтегральна компетентність	Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної та\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов
6.2.	Загальні компетентності (ЗК)	ЗК 1. Знання та розуміння предметної області та розуміння професії. ЗК 2. Здатність професійно спілкуватися державною та

		іноземною мовами як усно, так і письмово. ЗК 3. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК 4.Здатність до пошуку оброблення та аналізу інформації. ЗК 5.Здатність до здобування нових знань, накопичення наукових та педагогічних вмінь і навичок та їх застосування в практичних ситуаціях
6.3.	Фахові компетентності (ФК)	ФК 1. Здатність проектувати, розробляти, впроваджувати і супроводжувати програмні та програмно-апаратні комплекси і системи засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних системах . ФК2. Здатність до використання та впровадження сучасних інформаційних технологій та систем у сфері інформаційної безпеки та/або кібербезпеки ФК3. Здатність застосовувати відповідні математичні, наукові і технічні методи, а також спеціалізоване програмне забезпечення для вирішення завдань в сфері інформаційної та кібербезпеки ФК 4. Здатність до проектування, впровадження, супроводження інформаційних мереж і ресурсів, з метою забезпечення захисту інформації та безперервного функціонування з використанням сучасних технологій інформаційної безпеки та/або кібербезпеки. ФК 5. Здатність розробляти та впроваджувати систему управління інформаційними ресурсами, розробляти моделі загроз й моделі порушника та процедури виявлення кібервпливу, а також забезпечувати штатне функціонування системи інформаційної безпеки та/або кібербезпеки організації з використанням сучасних технологій. ФК 6. Здатність розробляти, впроваджувати, та супроводжувати інформаційні процеси з використанням методів та засобів криптографічного захисту інформації. ФК 7. Здатність виявляти і описувати ефективність рішень в сфері інформаційної безпеки та/або кібербезпеки на основі використання аналітичних методів і методів моделювання ФК 8. Здатність проводити науково-освітню діяльність і наукові дослідження в сфері безпеки інформаційно-комунікаційних систем і технологій у відповідність вітчизняним та світовим стандартам галузі інформаційної безпеки та/або кібербезпеки.

Розділ 7. Програмні результати навчання		
7.1.	Програмні результати навчання (ПРН)	**ПРН 1.** Вміння спілкуватись, включаючи усну та письмову комунікацію українською мовою та однією з іноземних мов (англійською, німецькою, італійською, французькою, іспанською). **ПРН 2.** Вміння представляти отримані знання та навички з теорії та практики галузі інформаційної безпеки та/або кібербезпеки в усній та/або письмових формах перед фаховою і нефаховою аудиторією. **ПРН 3.** – розуміння шляхів самостійного освоєння нових методів дослідження, нового наукового й науково-виробничого профілю діяльності; – здійснювати науково-дослідну роботу в професійній області, зокрема під час розробки нових технологій інформаційної та/або кібербезпеки; – використовувати методи загальнонаукового аналізу у сфері інформаційної та кібербезпеки та демонструвати можливості сучасних природничо-наукових методів дослідження у практиці забезпечення інформаційної та/або кібербезпеки; – здійснювати розробку планів і програм проведення наукових досліджень і технічних розробок, підготовка окремих завдань для виконавців в сфері забезпечення інформаційної та/або кібербезпеки. **ПРН 4.** – вміти проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної та/або кібербезпеки; – вирішувати задачі практичного застосування в своїй професійній діяльності криптографічних алгоритмів, протоколів та криптосистем для забезпечення належного рівня інформаційної та кібербезпеки в інформаційно-телекомунікаційних системах; – розробляти та впроваджувати криптографічні системи і використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах. **ПРН 5.** – здійснювати організацію функціонування інформаційно-комунікаційної систем: формувати опис автоматизованої системи та середовища її функціонування, визначати склад апаратного та програмного забезпечення, здійснювати аналіз обчислювальних процесів та технологій обробки

		інформації, аналіз складу та характеристик існуючої системи захисту з використанням засобів Cisco. – знати спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки інформаційних мереж; – вміти проектувати захищені (з урахуванням загроз) інформаційні мережі з використанням сучасних методів та технологій забезпечення інформаційної безпеки та/або кібербезпеки. **ПРН 6.** Вміння реалізовувати математичні та комп'ютерні моделі для побудови, експлуатації та оцінки захищеності інформаційної системи шляхом використання спеціалізованих програмних та апаратних засобів забезпечення інформаційної та кібербезпеки. **ПРН 7.** Вміння здійснювати розробку проектів зі створення і впровадження систем забезпечення інформації та кібербезпеки, а саме засобів захисту інформації, розробляти програми та методики випробувань. **ПРН 8.** – здатність управляти проектами з забезпечення інформаційної та кібербезпеки, моделювати системи та процеси захисту інформації, здійснювати аналіз об’єктів захисту, приймати експертні рішення; – здатність організовувати та проводити роботи щодо розробки та оцінки поточного стану системи інформаційної безпеки, встановлення рівня її відповідності певним критеріям та надання результатів у вигляді рекомендації; – здатність володіти новітніми технологіями розроблення програмних та програмно-апаратних засобів захисту інформації при вирішенні прикладних задач інформації та кібербезпеки. **ПРН 9.** – здатність здійснювати виявлення стороннього кібервпливу; – здатність здійснювати протидію несанкціонованому проникненню протиборчих сторін у власні інформаційні системи, забезпечуючи стійкість їхньої роботи, а також відновлення нормального функціонування після здійснення кібервпливу; – здатність обґрунтовувати комплекс завдань із проектування систем кіберзахисту; – здатність здійснювати поточний аналіз стану захищеності кіберпростору; – здатність здійснювати моделювати можливі ситуації кібервпливу та здійснювати прогнозування впливів на кіберінфраструктуру;

		– здатність розробляти та впроваджувати програмні моделі реалізації методів оцінці захищеності інформаційних і комунікаційних систем.
Розділ 8. Ресурсне забезпечення реалізації програми		
8.1.	Кадрове забезпечення	Всі науково-педагогічні працівники, що забезпечують освітньо- професійну програму за кваліфікацією відповідають профілю і напряму дисциплін, що викладаються, мають необхідний стаж педагогічної роботи та досвід практичної роботи. В процесі організації навчального процесу залучаються професіонали з досвідом дослідницької, управлінської, інноваційної, творчої та фахової роботи, іноземні лектори.
8.2.	Матеріально-технічне забезпечення	Навчальні приміщення, комп'ютерні робочі місця, мультимедійні класи дозволяють повністю забезпечити освітній процес протягом усього циклу підготовки за освітньою програмою.
8.3.	Інформаційне та навчально-методичне забезпечення	Офіційний веб-сайт www.nau.edu.ua містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти. Матеріали навчально-методичного забезпечення освітньої програми викладені в репозитарії НАУ за посиланням: http://er.nau.edu.ua/handle/NAU/9162 Всі ресурси науково-технічної бібліотеки доступні через сайт університету: http://www.lib.nau.edu.ua Читальний зал забезпечений бездротовим доступом до мережі Інтернет. Електронний репозитарій наукової бібліотеки НАУ: http://er.nau.edu.ua
Розділ 9. Академічна мобільність		
9.1.	Національна кредитна мобільність	У рамках двосторонніх договорів між Національним авіаційним університетом та вітчизняними закладами вищої освіти.
9.2.	Міжнародна кредитна мобільність	У рамках Еразмус+К1 договір про співробітництво між НАУ та навчальними закладами ЕС
9.3.	Навчання іноземних здобувачів вищої освіти	Основні навчальні модулі забезпечені навчально-методичним комплексами для іноземних здобувачів вищої освіти.

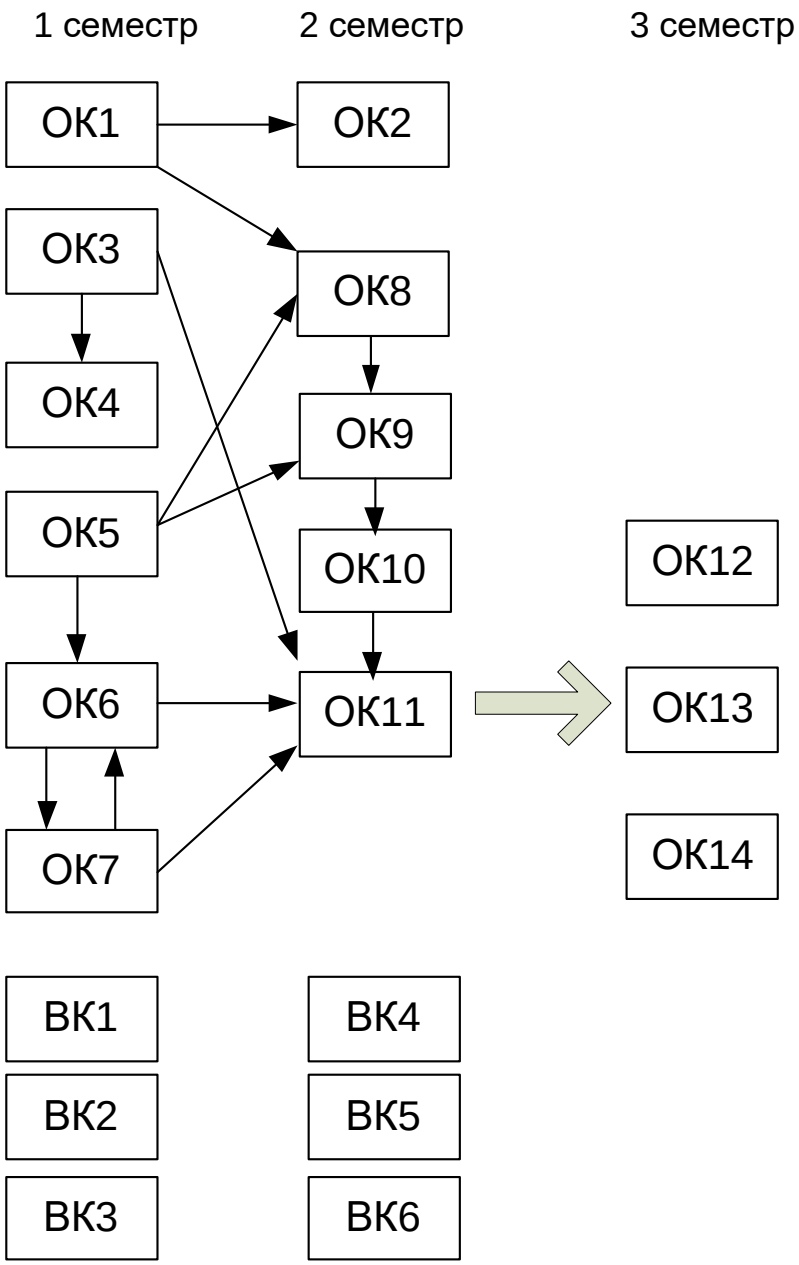
2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

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

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				
ОК1.	Ділова іноземна мова	3,5	Екзамен	1
ОК2.	Наукові комунікації у фаховій діяльності	3,5	Диф.залік	2
ОК3.	Методологія прикладних досліджень у сфері кібербезпеки	2,5	Диф.залік	1
ОК4.	Курсовий проєкт з дисципліни Методологія прикладних досліджень у сфері кібербезпеки	1,5	Захист	1
ОК5.	Методи побудови та аналізу криптосистем	3,5	Екзамен	1
ОК6.	Моделювання та оптимізація безпекових процесів авіаційної галузі	3,5	Екзамен	1
ОК7.	Автоматизоване проектування технічних засобів захисту інформації	3,5	Диф.залік	1
ОК8.	Захист комунікаційних мереж засобами Cisco	6,0	Екзамен	2
ОК9.	Технології створення та застосування систем захисту кібернетичного простору	6,0	Екзамен	2
ОК10	Курсова робота з дисципліни Технології створення та застосування систем захисту кібернетичного простору	1,0	Захист	2
ОК11.	Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	4,5	Диф.залік	2
ОК12.	Переддипломна практика	6,0	Диф.залік	3
ОК13.	Єдиний державний кваліфікаційний іспит	3,0		3
ОК14.	Кваліфікаційна робота	18,0		3
Загальний обсяг обов'язкових компонент:		**66 кредитів ЄКТС**		
Вибіркові компоненти *				
ВК 1.		4,0	Диф.залік	1
ВК 2.		4,0	Диф.залік	1
ВК 3.		4,0	Диф.залік	1
ВК 4.		4,0	Диф.залік	2
ВК 5.		4,0	Диф.залік	2
ВК 6.		4,0	Диф.залік	2
Загальний обсяг вибіркових компонент		**24 кредити ЄКТС**		
Загальний обсяг		**90 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. Вибіркові компоненти обираються здобувачами вищої освіти із каталогів рекомендованих та альтернативних вибіркових дисциплін.*

2.2. Структурно-логічна схема освітньо-професійної програми



3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здобувачів ОС «Магістр» здійснюється у формі єдиного державного кваліфікаційного іспиту та публічного захисту кваліфікаційної магістерської роботи і завершується видачею документу встановленого зразку про присудження їм освітнього ступеня «Магістр» із присвоєнням освітньої кваліфікації: Магістр з кібербезпеки, за спеціальністю 125 «Кібербезпека».
Єдиний державний кваліфікаційний іспит	Єдиний державний кваліфікаційний іспит повинен виявляти рівень засвоєння студентом навчального матеріалу, передбаченого навчальними програмами окремих дисциплін, та вміння випускника використовувати знання, набуті в процесі теоретичної підготовки, для вирішення професійних та соціально-виробничих завдань, з якими може зустрітись і які повинен уміти вирішувати майбутній фахівець під час своєї професійної діяльності, а також його підготовленість до продовження навчання за більш високими освітніми ступенями або в системі післядипломного навчання з урахуванням загальних вимог, передбачених стандартами вищої освіти.
Вимоги до кваліфікаційної роботи (за наявності)	Кваліфікаційна магістерська робота 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 магістерська робота не повинна містити академічного плагіату, у тому числі некоректних текстових запозичень, фабрикації та фальсифікації. Кваліфікаційна магістерська робота має бути розміщена на сайті Університету або його структурного підрозділу, або у репозитарії. Публічний захист кваліфікаційної магістерської 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	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ВК 1	…	ВК 6
ІК	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		
ЗК1			+	+	+	+		+	+			+	+	+	+		
ЗК2		+	+									+	+	+	+		
ЗК3				+	+	+	+	+				+	+	+	+		
ЗК4			+	+	+	+	+		+			+	+	+	+		
ЗК5			+	+	+							+	+	+	+		
ФК1						+	+	+	+	+	+	+	+	+	+		
ФК2						+		+	+	+	+	+	+	+	+		
ФК3						+			+	+	+	+	+	+	+		
ФК4							+	+			+	+	+	+	+		
ФК5								+			+	+	+	+	+		
ФК6					+						+	+	+	+	+		
ФК7						+	+				+	+	+	+	+		
ФК8											+	+	+	+	+		

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

Компоненти / Програмні результати навчання	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ВК 1	…	ВК 6
ПРН1	+	+									+	+	+	+			
ПРН2		+	+	+							+	+	+	+			
ПРН3			+	+							+	+	+	+			
ПРН4					+			+	+	+	+	+	+	+			
ПРН5								+	+	+	+	+	+	+			
ПРН6						+	+		+	+	+	+	+	+			
ПРН7							+				+	+	+	+			
ПРН8							+	+	+	+	+	+	+	+			
ПРН9									+	+	+	+	+	+			

(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				