МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ФАХОВИЙ КОЛЕДЖ ІНЖЕНЕРІЇ, УПРАВЛІННЯ ТА ЗЕМЛЕВПОРЯДКУВАННЯ
НАЦІОНАЛЬНОГО АВІАЦІЙНОГО УНІВЕРСИТЕТУ»

ОСВІТНЬО–ПРОФЕСІЙНА ПРОГРАМА
Кібербезпека

фахової передвищої освіти

ГАЛУЗЬ ЗНАНЬ 12 Інформаційні технології

СПЕЦІАЛЬНІСТЬ 125 Кібербезпека та захист інформації

КВАЛІФІКАЦІЯ Фаховий молодший бакалавр з кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО
Педагогічною радою Коледжу
протокол №_____від_____

Освітньо-професійна програма вводиться в дію з _____
(наказ від _____№___)
В.о. директора
_____ **Юрій ШМЕЛЬОВ**

Київ 2024р.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

ПЕРЕДМОВА

Освітньо-професійна програма розроблена робочою групою у складі:

Відповідальний за розробку освітньо-професійної програми

Пономаренко Андрій Васильович	викладач вищої категорії циклової комісії Кібербезпеки, інженерії програмного забезпечення та комп'ютерного дизайну

Члени робочої групи:

Краліна Ганна Сергіївна	викладач вищої категорії циклової комісії Кібербезпеки, інженерії програмного забезпечення та комп'ютерного дизайну
Рябчук Наталія Анатоліївна	викладач-методист циклової комісії Кібербезпеки, інженерії програмного забезпечення та комп'ютерного дизайну, завідувач відділення комп'ютерної інженерії та кібербезпеки
Осіпова Дар’я Олексіївна	здобувач освіти навчальної групи 313-КБ

1. Опис освітньо-професійної програми зі спеціальності 125 Кібербезпека та захист інформації галузі знань 12 Інформаційні технології

1 – Загальна інформація		
1.1	**Повна назва закладу фахової передвищої освіти**	Відокремлений структурний підрозділ «Фаховий коледж інженерії, управління та землевпорядкування Національного авіаційного університету»
1.2	**Освітньо-професійний ступінь**	Фаховий молодший бакалавр
1.3	**Освітня кваліфікація**	Фаховий молодший бакалавр з кібербезпеки та захисту інформації
1.4	**Професійна кваліфікація**	Не надається
1.5	**Кваліфікація в дипломі**	Освітньо-професійний ступінь – фаховий молодший бакалавр Спеціальність – 125 Кібербезпека та захист інформації Освітньо-професійна програма – Кібербезпека
1.6	**Рівень кваліфікації згідно з Національною рамкою кваліфікацій**	Освітньо-професійний ступінь фахового молодшого бакалавра відповідає 5 рівню Національної рамки кваліфікацій
1.7	**Офіційна назва освітньо-професійної програми**	Кібербезпека
1.8	**Обсяг кредитів ЄКТС, необхідний для здобуття ступеня фахового молодшого бакалавра**	180 кредитів ЄКТС, термін навчання: -3 роки 10 місяців на основі БЗСО; -2 роки 10 місяців на основі ПЗСО
1.9	**Наявність акредитації**	Не акредитована, акредитація передбачається у 2025 році
1.10	**Термін дії освітньо-професійної програми**	Рік вступу – 2024 та наступні до нової редакції освітньо-професійної програми
1.11	**Вимоги до осіб, які можуть розпочати навчання за програмою**	- базова середня освіта (з одночасним виконанням освітньої програми профільної середньої освіти, тривалість здобуття якої становить два роки); - повна загальна середня освіта (профільна середня освіта); - фахова передвища освіта. Умови вступу визначаються Правилами прийому до ВСП КІУтЗ НАУ, затвердженими Педагогічною радою коледжу.
1.12	**Мова(и) викладання**	Українська
1.13	**Інтернет-адреса постійного розміщення освітньо-професійної програми**	www.kitu.nau.edu.ua
2 – Мета освітньо-професійної програми		
2.1.	Метою освітньо-професійної програми є підготовка висококваліфікованих та конкурентноспроможних фахівців за освітньо-професійним ступенем «фаховий молодший бакалавр» у сфері інформаційної та/або кібербезпеки, здатних успішно розв’язувати типові	

	задачі та практичні проблеми, пов'язані з використанням сучасного програмного та програмно-апаратного забезпечення для забезпечення кіберзахисту.	
3– Характеристика освітньо-професійної програми		
3.1	**Предметна область**	***Об'єкт вивчення*:** об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології. А також технології забезпечення безпеки інформації та процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. ***Цілі навчання*:** формування здатності використовувати та впроваджувати технології інформаційної та/або кібербезпеки. ***Теоретичний зміст предметної області:*** знання щодо 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 виявлення, управління та ідентифікації ризиків; методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; методів та засобів технічного та криптографічного захисту інформації; сучасних інформаційно-комунікаційних технологій; сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; автоматизованих систем проектування. ***Методи, методики та технології:*** створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. ***Інструменти та обладнання:*** засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу,

		обробки, відображення та захисту даних (інформаційних потоків).
4 – Придатність випускників до працевлаштування та подальшого навчання		
4.1.	**Придатність до працевлаштування**	Випускники можуть обіймати первинні посади відповідно до Національного класифікатора професій України (ДК 003:2010): 3439(24771) Фахівець із організації інформаційної безпеки. International Standard Classification of Occupations 2008 (ISCO08): 2529 Security specialist (ICT). 3439 Інспектор з організації захисту секретної інформації 3439 Фахівець з режиму секретності 3439 Фахівець із організації захисту інформації з обмеженим доступом 3439 Фахівець із організації інформаційної безпеки
4.2.	**Академічні права випускників**	Подальше продовження навчання за початковим рівнем (короткий цикл) та/або першим (бакалаврським) рівнем вищої освіти, набуття додаткових кваліфікацій в системі освіти дорослих, у тому числі післядипломної освіти. Робота за фахом.
5 – Викладання та оцінювання		
5.1.	**Викладання та навчання**	Студентоцентроване навчання, технології проблемного і диференційованого, інтенсифікації та індивідуалізації навчання, програмованого та розвивального навчання, інформаційна технологія, ініціативне самонавчання, навчання на основі досліджень. Викладання проводиться у вигляді лекцій, практичних занять, лабораторних робіт, роботи в малих групах, проведення індивідуальних занять, проходження практики, консультацій з викладачами, самонавчання через електронне модульне середовище навчального процесу.
5.2.	**Оцінювання**	Заліки, екзамени, звіти з практичних та лабораторних робіт, звіти з практик, есе, презентації, поточний контроль, курсове проєктування, атестація (захист кваліфікаційної роботи). Оцінювання навчальних досягнень здобувачів освіти здійснюється за 100 бальною шкалою ЄКТС (ECTS).
6 – Перелік компетентностей випускника		
6.1.	**Інтегральна компетентність (ІК)**	Здатність вирішувати типові спеціалізовані задачі та практичні проблеми в галузі забезпечення інформаційної безпеки і кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

6.2.	**Загальні компетентності (ЗК)**	**ЗК01**. Здатність застосовувати знання у практичних ситуаціях. **ЗК02**. Знання та розуміння предметної області та розуміння професійної діяльності. **ЗК03**. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. **ЗК04**. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. **ЗК05.** Здатність до пошуку, оброблення та аналізу інформації з різних джерел. **ЗК06**. 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. **ЗК07**. 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. **ЗК08**. Здатність вчитися і оволодівати сучасними знаннями. **ЗК09**. Навички використання інформаційних і комунікаційних технологій. **ЗК10**. Здатність працювати в команді. **ЗК11**. Здатність діяти на основі етичних міркувань (мотивів), прагнення до збереження навколишнього середовища. **ЗК12**. Здатність діяти соціально відповідально та свідомо.
6.3.	**Спеціальні компетентності (СК)**	**СК01**. 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. **СК02**. Здатність до використання інформаційнокомунікаційних технологій, сучасних методів і моделей інформаційної безпеки. **СК03**. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту

		інформації в інформаційно-телекомунікаційних (автоматизованих) системах. **СК04**. Здатність забезпечувати неперервність бізнесу згідно зі встановленою політикою безпеки. **СК05**. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки. **СК06**. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. **СК07**. Здатність забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). **СК08**. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. **СК09**. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою. **СК10**. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. **СК11**. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем. **СК12**. Знання теоретичних та практичних принципів та інструментальних засобів в професійній галузі та уміння їх застосовувати.
7 – Зміст підготовки здобувачів фахової передвищої освіти, сформульований у термінах результатів навчання (РН)		
7.1.	**РН01**. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. **РН02**. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. **РН03**. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. **РН04**. Аналізувати, аргументувати, приймати рішення при розв'язанні типових спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.	

	РН05. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. **РН06**. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. **РН07**. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. **РН08**. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. **РН09**. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. **РН10**. Розробляти моделі загроз та порушника. **РН11**. Аналізувати проекти ІТС, базуючись на стандартизованих технологіях та протоколах передачі даних. **РН12**. Вирішувати завдання захисту програм та інформації, що обробляється в ІТС програмно-апаратними засобами, та давати оцінку якості прийнятих рішень. **РН13**. Реалізовувати комплексні системи захисту інформації в АС організації (підприємства) відповідно до вимог нормативно-правових документів. **РН14**. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. **РН15**. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в ІТС. **РН16**. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в ІТС. **РН17**. Вирішувати задачі управління процедурами ідентифікації, аутентифікації, авторизації процесів і користувачів в ІТС згідно встановленої політики інформаційної і\або кібербезпеки. **РН18**. Здійснювати протидію отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. **РН19**. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах. **РН20**. Брати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації. **РН21**. 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 зі встановленою політикою інформаційної і\або кібербезпеки. **РН22**. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. **РН23**. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. **РН24**. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. **РН25**. Здійснювати аналіз ризиків обробки інформації в ІТС.

	РН26. Вирішувати задачі аналізу програмного коду на наявність можливих уразливостей.	
8. Ресурсне забезпечення реалізації освітньо-професійної програми		
8.1.	**Кадрове забезпечення**	Відповідно ліцензійних вимог, затверджених Постановою Кабінету міністрів України від 30.12.2015 р. № 1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти», навчальні дисципліни та інші освітні компоненти освітньої програми викладаються та забезпечуються педагогічними працівниками, академічна та /або професійна кваліфікація яких відповідає змісту зазначених навчальних дисциплін загальної та професійної підготовки й інших освітніх компонентів освітньої програми.
8.2.	**Матеріально-технічне забезпечення**	Матеріально-технічна база коледжу відповідає ліцензійним вимогам та вимогам освітньо-професійної програми. Спеціалізовані кабінети: історії, філологічних дисциплін, іноземних мов, математичних дисциплін, комп'ютерних мереж, програмування, інформаційної безпеки. Спеціалізовані комп'ютерні лабораторії: архітектури комп'ютерів, операційних систем та системного програмного забезпечення, мережевого обладнання та технологій, технологій програмування. Актова зала, стадіон, спортивна зала.
8.3	**Інформаційне та навчальнометодичне забезпечення**	Бібліотека коледжу, електронна бібліотека, фахові періодичні видання, авторські методичні посібники викладачів, бібліотека НАУ.
9 – Академічна мобільність		
9.1.	**Національна кредитна мобільність**	Угода щодо підвищення кваліфікації (стажування) педагогічних працівників у Національному авіаційному університеті. Планується підписання двосторонніх договорів з провідними коледжами України
9.2.	**Міжнародна кредитна мобільність**	Планується підписання двосторонніх договорів з провідними коледжами Європейського союзу
9.3.	**Навчання іноземних здобувачів фахової передвищої освіти**	Планується розширення провадження освітньої діяльності для підготовки іноземних громадян та осіб без громадянства

2. Перелік освітніх компонентів і логічна послідовність їх виконання

2.1. Перелік компонентів ОПП

Код о/к	Освітні компоненти освітньо-професійної програми (навчальні дисципліни, курсові проєкти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумкового контролю
1	2	3	4
Обов'язкові освітні компоненти ОПП			
Обов'язкові освітні компоненти, що формують загальні компетентності			
ОК1	Історія та культура України	3	залік
ОК2	Основи правознавства	3	залік
ОК3	Економічна теорія	3	залік
ОК4	Вища фізика	4	екзамен
ОК5	Українська мова (за професійним спрямуванням)	3	залік
ОК6	Іноземна мова (за професійним спрямуванням)	6	екзамен
ОК7	Фізичне виховання	4	залік
ОК8	Вища математика	10	екзамен
ОК9	Комп`ютерна дискретна математика	3	залік
ОК10	Теорія ймовірностей і математична статистика	3	залік
Обов'язкові освітні компоненти, що формують спеціальні компетентності			
ОК11	Вступ до спеціальності	3	залік
ОК12	Основи інформаційної безпеки держави	3	екзамен
ОК13	Інформаційні технології та основи програмування	5	екзамен
ОК14	Операційні системи та системне програмне забезпечення	5	екзамен
ОК15	Стандарти інформаційної безпеки	5	екзамен
ОК16	Комп`ютерна схемотехніка	4	залік
ОК17	Організація комп`ютерних мереж	4	залік
ОК18	Інтернет-технології	4	залік
ОК19	Архітектура апаратного забезпечення комп`ютера	6	екзамен, КР
ОК20	Безпека програм та даних	5	залік
ОК21	Мікропроцесорна техніка	5	залік
ОК22	Основи системного аналізу	4	залік
ОК23	Технології програмування	7	екзамен, КП
ОК24	Прикладна криптографія	4	екзамен
ОК25	Управління ресурсами інформаційних систем	3	залік
ОК26	Захищені комп'ютерні системи та мережі	7	екзамен, КП
ОК27	Системи розмежування доступу	4	залік
ОК28	Комплексні системи захисту інформації	3	екзамен

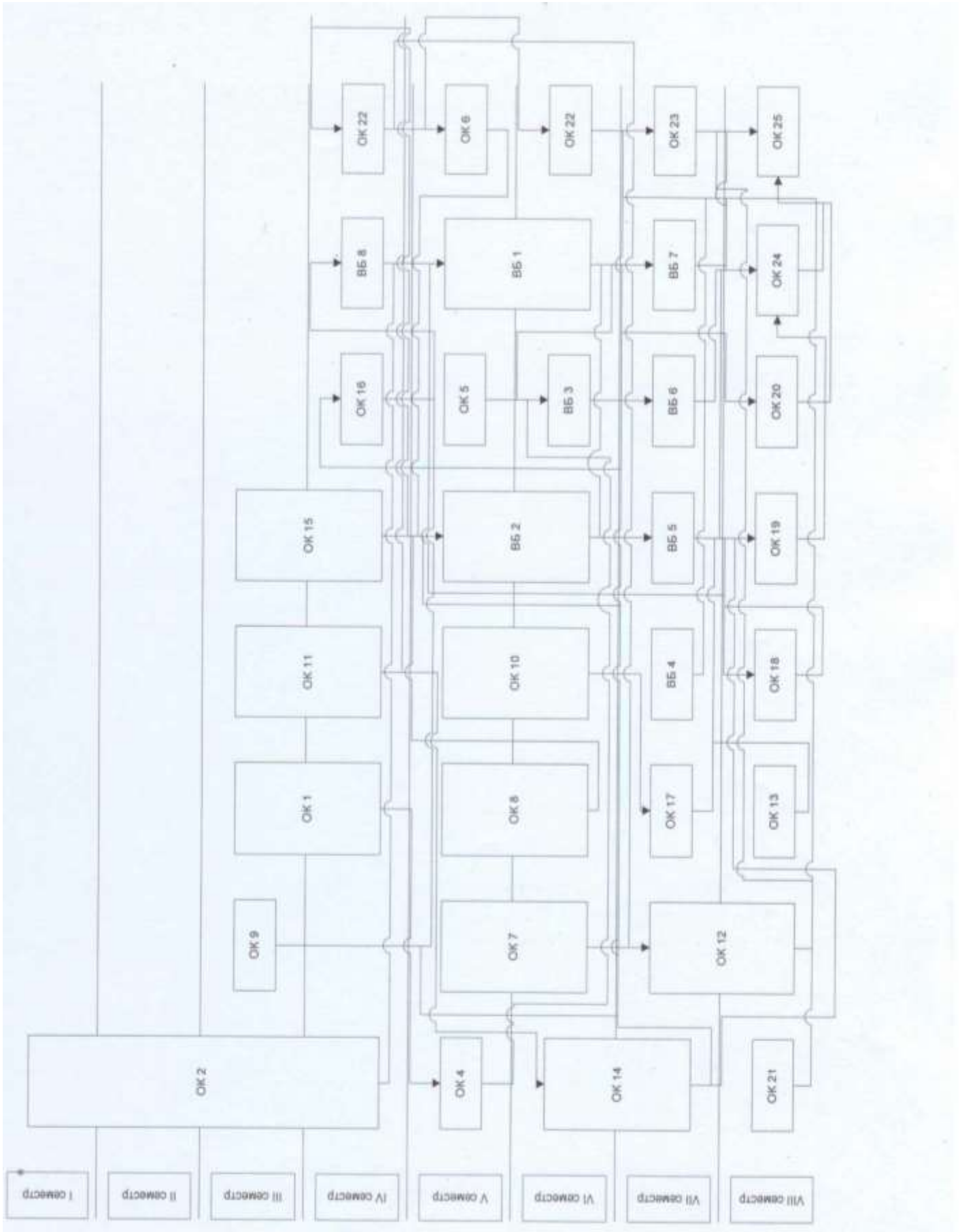
ОК29	Основи охорони праці та БЖД	3	залік
ОК30	Практика навчальна	6	залік
ОК31	Практика технологічна	9	екзамен
ОК32	Практика виробнича	12	екзамен
ОК33	Атестація (комплексний кваліфікаційний екзамен)	3	
Загальний обсяг обов'язкових освітніх компонентів:		**156**	
Вибіркові освітні компоненти ОПП (за вибором здобувача фахової передвищої освіти)			
Вибіркові освітні компоненти ОПП, що формують загальні компетентності			
ВК1	Вибірковий компонент 1	4	залік
	Вибірковий компонент 1		
	Вибірковий компонент 1		
ВК2	Вибірковий компонент 2	4	залік
	Вибірковий компонент 2		
	Вибірковий компонент 2		
Загальний обсяг вибіркових освітніх компонентів:		8	
Вибіркові освітні компоненти ОПП, що формують спеціальні компетентності			
ВК3	Вибірковий компонент 3	4	залік
	Вибірковий компонент 3		
	Вибірковий компонент 3		
ВК4	Вибірковий компонент 4	4	залік
	Вибірковий компонент 4		
	Вибірковий компонент 4		
ВК5	Вибірковий компонент 5	4	залік
	Вибірковий компонент 5		
	Вибірковий компонент 5		
ВК6	Вибірковий компонент 6	4	залік
	Вибірковий компонент 6		
	Вибірковий компонент 6		
Загальний обсяг вибіркових освітніх компонентів:		16	
Загальний обсяг вибіркових освітніх компонентів:		**24**	
ЗАГАЛЬНИЙ ОБСЯГ ОПП:		**180**	

Каталог вибіркових освітніх компонент

Освітні компоненти вибіркового блоку, що формують загальні компетентності
ВК1 Екологія ВК1 Філософія ВК1 Етика та естетика
ВК2 Інформаційно-психологічні впливи у кіберпросторі ВК2 Групова динаміка та комунікації ВК2 Основи психології
Освітні компоненти вибіркового блоку, що формують спеціальні компетентності

ВК3 Системи технічного захисту інформації ВК3 Технології штучного інтелекту ВК3 Випробовування систем захисту інформації
ВК4 Бази даних ВК4 Інформаційні системи і технології ВК4 Технічні засоби охорони об’єктів
ВК5 Економіка в галузі інформаційної безпеки ВК5 Оцінка та управління ризиками ВК5 Основи менеджменту та маркетингу
ВК6 Основи секретного діловодства ВК6 Теорія інформації та кодування ВК6 Управління проєктами захисту інформації

2.2. Структурно-логічна схема ОПП



3. Форма атестації здобувачів фахової передвищої освіти

Атестація випускників освітньо-професійної програми Кібербезпека спеціальності 125 Кібербезпека та захист інформації здійснюється у формі комплексного кваліфікаційного екзамену за фахом.

Вимоги до комплексного кваліфікаційного екзамену:

- комплексний кваліфікаційний екзамен за фахом проводиться в два етапи: комплекс тестів та письмові за білетами, які містять теоретичні питання та практичні завдання, спрямовані на виявлення здатності студента вирішувати конкретні практичні ситуації, які виникають при проектуванні та розробці програмного забезпечення автоматизованих систем.
- програма комплексного кваліфікаційного екзамену за фахом складається з розділів, що інтегрують питання по визначенню цілей, теоретичних основ та прикладних питань спеціальності, форм та методів діяльності фахового молодшого бакалаврів з кібербезпеки (Захищені комп'ютерні системи та мережі; Управління ресурсами інформаційних систем; Безпека програм та даних; Основи системного аналізу).

4. Вимоги до системи внутрішнього забезпечення якості фахової передвищої освіти

Якість освітньо-професійної програми визначається внутрішньою системою забезпечення якості фахової передвищої освіти та освітньої діяльності ВСП КІУтЗ НАУ, яка функціонує згідно з Положенням про систему забезпечення якості освітньої діяльності та якості освіти у Відокремленому структурному підрозділі «Фаховий коледж інженерії, управління та землевпорядкування Національного авіаційного університету», ухваленого Педагогічною радою (протокол від 08.03.2023 р. № 3), і відповідає вимогам Закону України «Про вищу освіту» (Розділ V. Забезпечення якості вищої освіти, ст.16) та Закону України «Про фахову передвищу освіту» (Розділ IV. Забезпечення якості фахової передвищої освіти, ст.17), й передбачає здійснення таких процедур і заходів:

1) визначення принципів та процедур забезпечення якості фахової передвищої освіти;
2) розроблення освітньо-професійних програм, здійснення моніторингу та періодичного перегляду освітніх програм;
3) щорічне оцінювання здобувачів фахової передвищої освіти і педагогічних працівників коледжу та регулярне оприлюднення результатів таких

оцінювань на офіційному веб-сайті закладу освіти, на інформаційних стендах та в будь-який інший спосіб;

4) забезпечення підвищення кваліфікації педагогічних працівників;

5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів, за кожною освітньою програмою;

6) забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;

7) забезпечення публічності інформації про освітні програми, умови і процедури присвоєння ступеня фахової передвищої освіти та кваліфікацій;
8) забезпечення дотримання академічної доброчесності працівниками закладу освіти та здобувачами фахової передвищої освіти;

8) інших процедур і заходів, які забезпечують належний рівень якості фахової передвищої освіти.

Система забезпечення якості освітньої діяльності та якості фахової передвищої освіти закладу фахової передвищої освіти (внутрішня система забезпечення якості освіти) за поданням закладу може оцінюватися центральним органом виконавчої влади із забезпечення якості освіти або акредитованими ним незалежними установами оцінювання та забезпечення якості фахової перед вищої освіти на предметії відповідності вимогам до системи забезпечення якості фахової передвищої освіти, що затверджуються центральним органом влади у сфері освіти і науки за поданням центрального органу виконавчої влади із забезпечення якості освіти.

6. Матриця відповідності компетентностей випускника компонентам освітньо-професійної програми

Компоненти ОП / Компетентності (ЗК, ФК)	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22
ЗК1			+		+	+	+			+	+	+	+			+	+	+	+	+	+	+
ЗК2		+	+		+	+		+	+	+	+	+				+	+	+	+	+	+	+
ЗК3		+	+							+	+	+		+								+
ЗК4			+						+	+	+	+		+	+	+	+	+			+	+
ЗК5		+	+		+				+						+			+		+	+	+
ЗК6	+	+					+	+	+												+	+
ЗК7	+	+		+			+	+														
ЗК8		+	+		+									+	+			+	+	+	+	
ЗК9										+					+	+	+	+			+	
ЗК10				+														+			+	
ЗК11	+							+														
ЗК12	+						+	+	+								+					
СК1			+				+	+	+								+	+				+
СК2								+		+	+	+			+	+	+	+		+	+	+
СК3						+					+	+	+			+	+				+	+
СК4									+						+	+	+	+		+		
СК5										+	+	+		+	+	+	+	+	+			+
СК6											+						+				+	
СК7										+	+		+	+				+	+	+	+	+
СК8							+		+		+				+	+	+	+		+	+	+
СК9			+				+	+	+			+				+		+			+	+
СК10											+								+	+	+	+
СК11										+	+	+			+	+	+	+		+	+	
СК12						+	+		+		+	+			+		+		+	+	+	+

7. Матриця відповідності результатів навчання освітнім компонентам освітньо-професійної програми

Освітні компоненти / РН	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22
РН-1		+	+					+													+	
РН-2									+						+			+			+	+
РН-3			+		+												+	+	+	+	+	+
РН-4					+	+			+	+	+				+			+			+	+
РН-5				+				+						+							+	+
РН-6	+				+			+	+						+	+	+		+		+	+
РН-7							+	+	+								+					+
РН-8	+	+	+				+	+	+	+	+				+	+	+	+		+	+	+
РН-9										+	+	+			+	+		+				+
РН-10											+				+		+				+	+
РН-11			+								+				+	+		+				
РН-12									+	+	+	+		+	+					+		
РН-13						+	+	+	+			+				+			+	+	+	+
РН-14			+			+				+	+	+	+	+					+	+	+	+
РН-15						+				+	+	+	+	+		+	+	+				+
РН-16										+	+	+		+	+	+	+	+	+	+	+	+
РН-17															+	+	+	+				+
РН-18											+					+	+				+	+
РН-19										+	+	+				+	+					+
РН-20							+		+			+			+			+				+
РН-21									+	+	+				+			+				+
РН-22											+				+			+				
РН-23											+						+	+				
РН-24								+	+						+						+	+
РН-25																						
РН-26										+			+	+					+	+	+	+

8. Матриця відповідності результатів навчання та компетентностей

Освітні компоненти / РН	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22
РН-1		+	+					+													+	
РН-2									+						+			+			+	+
РН-3			+		+												+	+	+	+	+	+
РН-4					+	+			+	+	+				+			+			+	+
РН-5				+				+						+							+	+
РН-6	+				+			+	+						+	+	+		+		+	+
РН-7							+	+	+								+					+
РН-8	+	+	+				+	+	+	+	+				+	+	+	+		+	+	+
РН-9										+	+	+			+	+		+				+
РН-10											+				+		+				+	+
РН-11			+								+				+	+		+				
РН-12									+	+	+	+		+	+					+		
РН-13						+	+	+	+			+				+			+	+	+	+
РН-14			+			+				+	+	+	+	+					+	+	+	+
РН-15						+				+	+	+	+	+		+	+	+				+
РН-16										+	+	+		+	+	+	+	+	+	+	+	+
РН-17															+	+	+	+				+
РН-18											+					+	+				+	+
РН-19										+	+	+				+	+					+
РН-20							+		+			+			+			+				+
РН-21									+	+	+				+			+				+
РН-22											+				+			+				
РН-23											+						+	+				
РН-24								+	+						+						+	+
РН-25																						
РН-26										+			+	+					+	+	+	+