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

Освітньо-професійна програма
затверджена Педагогічною радою коледжу
протокол № 3 від 27.04. 2023 р.
Вводиться в дію наказом в.о. директора
В.о. директора
_____/ Віктор ПАРАНІЧ
Наказ № 35/09 від 08.05. 2023 р.

КИЇВ

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

1 - Загальна інформація		
1.1	**Повна назва закладу освіти та структурного підрозділу**	Відокремлений структурний підрозділ «Фаховий коледж інженерії, управління та землевпорядкування Національного авіаційного університету»
1.2	**Освітньо-професійний ступінь**	Фаховий молодший бакалавр
1.3	**Офіційна назва освітньо-професійної програми**	**КІБЕРБЕЗПЕКА**
1.4	**Обсяг кредитів ЄКТС, необхідний для здобуття ступеня фахового молодшого бакалавра**	180 кредитів ЄКТС. Термін навчання: - 2 роки 10 місяців на основі ПЗСО (профільної середньої освіти); - 3 роки 10 місяців на основі БЗСО
1.5	**Наявність акредитації**	Не акредитована, передбачається акредитація у 2024 році
1.6	**Освітня кваліфікація**	Фаховий молодший бакалавр з кібербезпеки та захисту інформації
1.7	**Професійна кваліфікація**	Не надається
1.8	**Кваліфікація в дипломі**	Освітньо-професійний ступінь - фаховий молодший бакалавр Спеціальність – 125 Кібербезпека та захист інформації Освітньо-професійна програма – Кібербезпека
1.9	**Цикл/ рівень**	НРК України – 5 рівень, ЄРК – 5 рівень, РК ЄПВО – короткий цикл
1.10	**Вимоги до осіб, які можуть розпочати навчання за програмою**	Повна загальна середня освіта. Вступ на навчання на освітньо-професійну програму на основі базової середньої освіти зобов'язує здобувачів фахової передвищої освіти одночасно виконати програму профільної середньої освіти професійного спрямування, тривалість здобуття якої становить два роки. Освітня програма профільної середньої освіти професійного спрямування, що відповідає галузі знань та /або спеціальності, інтегрується з освітньо-професійною програмою фахового молодшого бакалавра. Мінімум 50% обсягу ОПП спрямовується на досягнення результатів навчання за спеціальністю.
1.11	**Форми здобуття освіти**	Інституційна очна (денна), заочна
1.12	**Мова (и) викладання**	Українська
1.13	**Термін дії освітньо-професійної програми**	Рік вступу – 2023 та наступні до нової редакції освітньо-професійної програми
1.14	**Інтернет-адреса постійного розміщення опису ОПП**	www.kitu.nau.edu.ua

<table>
<tr><th colspan="3">2 – Мета освітньо-професійної програми</th></tr>
<tr><td colspan="3">Метою освітньо-професійної програми є підготовка висококваліфікованих та конкурентоспроможних фахівців за освітньо-професійним ступенем «фаховий молодший бакалавр» у сфері інформаційних технологій у напрямку забезпечення кібербезпеки, здатних розв’язувати типові спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та\або кібербезпеки із використанням сучасного програмного та програмно-апаратного забезпечення (засобів) кіберзахисту.</td></tr>
<tr><th colspan="3">3 – Характеристика освітньо-професійної програми</th></tr>
<tr><td>3.1</td><td>Предметна область</td><td>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: підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки.
Теоретичний зміст предметної області складають 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.</td></tr>
</table>

		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).
3.2	**Орієнтація освітньо-професійної програми**	Освітньо-професійна програма фахового молодшого бакалавра базується на загальнонаукових та практичних результатах в кібербезпеці і має прикладну орієнтацію напрямку інтеграції програмно-апаратних засобів виявлення, моніторингу та забезпечення інформаційної безпеки, сучасних інформаційних технологій захисту інформації в інформаційно-комунікаційних системах, технологій збереження даних в кіберпросторі та інтелектуалізації функцій протидії кіберзлочинності.
3.3	**Основний фокус освітньо- професійної програми та спеціалізації**	Спеціальна освіта в галузі 12 «Інформаційні технології», спеціальності 125 «Кібербезпека» Освітня програма здобуття фахової передвищої освіти в галузі інформаційних технологій спеціальності «Кібербезпека» сфокусована на здатності організовувати й підтримувати комплекс заходів щодо забезпечення інформаційної безпеки з урахуванням їхньої обґрунтованості, технічної реалізації, економічної доцільності, можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації. Ключові слова: інформаційні технології, кібербезпека, автоматизація, система керування, система автоматизації, комп'ютеризовані системи управління, процеси керування, інформаційно-комунікаційні системи, проектування, системи технічного захисту, комп'ютерні мережі, криптографія, шифрування, кодування.
3.4	**Особливості освітньо-професійної програми**	Програма передбачає обов'язковою умовою проходження навчальної та виробничої практики на спеціалізованих підприємствах, що експлуатують або розробляють інформаційні технології, системи технічного та програмного захисту інформації. з метою забезпечення умов підготовки фахівців в реальному середовищі майбутньої професійної діяльності.
4 – Придатність випускників до працевлаштування та подальшого навчання		
4.1	**Працевлаштування випускників**	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**	Продовження навчання за початковим рівнем (короткий цикл) та/або першим (бакалаврським) рівнем вищої освіти та набуття додаткових кваліфікацій в системі освіти дорослих, в тому числі післядипломної освіти.
5 – Викладання та оцінювання		
5.1	**Викладання та навчання**	Студентоцентроване навчання, технологія проблемного і диференційованого навчання, технології інтенсифікації та індивідуалізації, програмованого навчання, інформаційна технологія, технологія розвивального навчання, самонавчання, навчання на основі досліджень. Викладання проводиться у вигляді лекцій, інтерактивних лекцій, семінарів, практичних занять, лабораторних робіт, самостійного навчання на основі консультацій з викладачами, підручників, навчальних посібників, конспектів лекцій, методичних рекомендацій, електронних навчальних курсів, розроблених педагогічним складом коледжу, періодичних наукових видань та мережі Internet. або командного вирішення ситуаційних завдань, кейсів з метою розвитку креативного мислення та вміння працювати у команді; майстер-класів, відкритих лекцій, тренінгів, ділових ігор з провідними фахівцями галузі; підготовки кваліфікаційної роботи (проекту).
5.2	**Оцінювання**	Види контролю: поточний, тематичний, періодичний, підсумковий, самоконтроль. Форми контролю: диференційовані заліки, екзамени, звіти з практики, презентації, участь у семінарах, поточний контроль, есе, реферати, курсове проектування, захист кваліфікаційного проекту. Оцінювання навчальних досягнень здобувачів освіти здійснюється за 100 бальною шкалою ЄКТС (ECTS).
6 – Перелік компетентностей випускника		
6.1	**Інтегральна компетентність (ІК)**	Здатність розв’язувати 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)**	**ЗК**1. Здатність застосовувати знання у практичних ситуаціях. **ЗК**2. Знання та розуміння предметної області та розуміння професійної діяльності.

		ЗК3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. **ЗК**4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. **ЗК**5. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. **ЗК**6. 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. **ЗК**7. 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. **ЗК**8. Здатність вчитися і оволодівати сучасними знаннями. **ЗК**9. Навички використання інформаційних і комунікаційних технологій. **ЗК**10. Здатність працювати в команді. **ЗК**11. Здатність діяти на основі етичних міркувань (мотивів), прагнення до збереження навколишнього середовища. **ЗК**12. Здатність діяти соціально відповідально та свідомо.
6.3	**Спеціальні (фахові компетентності (СК)**	**СК**1. 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. **СК**2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки. **СК**3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. **СК**4. Здатність забезпечувати неперервність бізнесу згідно зі встановленою політикою безпеки. **СК**5. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки.

		СК6. Здатність відновлювати штатне функціонування інформаційних, інформаційно- телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. **СК**7. Здатність забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). **СК**8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. **СК**9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою. **СК**10. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. **СК**11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем. **СК**12. 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		**РН**1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. **РН**2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. **РН**3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. **РН**4. 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. **РН**5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. **РН**6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. **РН**7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. **РН**8. Впроваджувати процеси, що базуються на національних та міжнародних

	стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. **РН**9. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. **РН**10. Розробляти моделі загроз та порушника. **РН**11. Аналізувати проекти ІТС, базуючись на стандартизованих технологіях та протоколах передачі даних. **РН**12. Вирішувати завдання захисту програм та інформації, що обробляється в ІТС програмно-апаратними засобами, та давати оцінку якості прийнятих рішень. **РН**13. Реалізовувати комплексні системи захисту інформації в АС організації (підприємства) відповідно до вимог нормативно-правових документів. **РН**14. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. **РН**15. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в ІТС. **РН**16. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в ІТС. **РН**17. Вирішувати задачі управління процедурами ідентифікації, аутентифікації, авторизації процесів і користувачів в ІТС згідно встановленої політики інформаційної і\або кібербезпеки. **РН**18. Здійснювати протидію отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. **РН**19. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах. **РН**20. Брати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації. **РН**21. 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. **РН**22. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. **РН**23. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. **РН**24. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. **РН**25. Здійснювати аналіз ризиків обробки інформації в ІТС. **РН**26. Вирішувати задачі аналізу програмного коду на наявність можливих уразливостей.	
8 – Ресурсне забезпечення реалізації освітньо-професійної програми		
8.1	**Кадрове забезпечення**	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 характеризується достатнім аудиторним фондом. В наявності достатній лекційний аудиторний фонд з мультимедійним обладнанням, спеціалізовані кабінети, комп'ютерні лабораторії. Освітній процес підготовки фахових молодших бакалаврів з кібербезпеки забезпечується спеціалізованими кабінетами: інформаційної безпеки, мережевих технологій, програмування та спеціалізованими комп'ютерними лабораторіями: технологій програмування, мережевого обладнання та технологій, програмування для Інтернет, комп'ютерної графіки та інформаційних систем.
8.3	**Інформаційне та навчально- методичне забезпечення**	Використання електронної бібліотеки коледжу та авторських методичних розробок викладацького складу. Бібліотека ВСП «КІУтЗ НАУ» та НАУ.
9 – Академічна мобільність		
9.1	**Національна кредитна мобільність**	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 компонентів освітньо-професійної програми та їх логічна послідовність

2.1 Перелік компонентів ОПП

Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумкового контролю, КП, КР
1	*2*	*3*	*4*
Обов'язкові освітні компоненти ОПП			
Обов’язкові освітні компоненти, що формують загальні компетентності			
ОК 1	Історія та культура України	3	Залік
ОК 2	Українська мова за професійним спрямуванням	3	Залік
ОК 3	Іноземна мова за професійним спрямуванням	6	Екзамен
ОК 4	Фізичне виховання	4	Залік
ОК 5	Вища математика	10	Екзамен
ОК 6	Вища фізика	8	Залік
ОК 7	Основи охорони праці та БЖД	3	Залік
Обсяг обов’язкових освітніх компонентів (загальні комп.):		***37***	
Обов’язкові освітні компоненти, що формують спеціальні компетентності			
ОК 8	Основи інформаційної безпеки держави	4	Екзамен
ОК 9	Стандарти інформаційної безпеки	4	Екзамен
ОК 10	Інформаційні технології та основи програмування	9	Екзамен
ОК 11	Операційні системи та системне програмне забезпечення	6	Екзамен
ОК 12	Архітектура апаратного забезпечення комп`ютера	8	Екзамен/КР
ОК 13	Комп`ютерна дискретна математика	6	Екзамен
ОК 14	Технології програмування	8	Екзамен/КП
ОК 15	Основи системного аналізу	5	Екзамен
ОК 16	Системи розмежування доступу	5	Залік
ОК 17	Захищені комп`ютерні системи та мережі	8	Екзамен/КП
ОК 18	Управління ресурсами інформаційних систем	5	Екзамен
ОК 19	Практика навчальна	7	Залік
ОК 20	Практика технологічна	8	Залік
ОК 21	Практика переддипломна (виробнича)	8	Залік
ОК 22	Атестація (Кваліфікаційна робота)	5	
Обсяг обов’язкових освітніх компонентів спец. комп.):		***96***	
Загальний обсяг обов'язкових компонентів ОПП:		**133**	
Вибіркові компоненти ОПП (за вибором здобувача фахової передвищої освіти)			
Вибірковий блок ВБ1 (вибір 4 ОК з каталогу)			
ВБ 1.1	Освітній компонент каталогу ВБ 1	3	Залік
ВБ 1.2	Освітній компонент каталогу ВБ 1	3	Залік
ВБ 1.3	Освітній компонент каталогу ВБ 1	3	Залік
ВБ 1.4	Освітній компонент каталогу ВБ 1	3	Залік
Загальний обсяг вибіркових компонентів ВБ 1:		***12***	
Вибірковий блок ВБ 2 (вибір 4 ОК з каталогу)			
ВБ 2.1	Освітній компонент каталогу ВБ 2	4	Залік

ВБ 2.2	Освітній компонент каталогу ВБ 2	4	Залік
ВБ 2.3	Освітній компонент каталогу ВБ 2	4	Залік
ВБ 2.4	Освітній компонент каталогу ВБ 2	4	Залік
Загальний обсяг вибіркових компонентів ВБ 2:		***16***	
Вибірковий блок ВБ 3 (вибір 5 ОК з каталогу)			
ВБ 3.1	Освітній компонент каталогу ВБ 3	4	Залік
ВБ 3.2	Освітній компонент каталогу ВБ 3	4	Залік
ВБ 3.3	Освітній компонент каталогу ВБ 3	4	Залік
ВБ 3.4	Освітній компонент каталогу ВБ 3	4	Залік
ВБ 3.5	Освітній компонент каталогу ВБ 3	3	Залік
Загальний обсяг вибіркових компонентів ВБ 3:		***19***	
Загальний обсяг вибіркових компонент ОПП		**47**	
Загальний обсяг ОПП (кредитів ЄКТС)		**180**	

2.2 Каталог вибіркових освітніх компонентів ОПП (по блоках)

№ вибіркового блоку	Освітні компоненти вибіркового блоку
ВБ 1	**ВБ** 1.1.Економікс **ВБ** 1.1 Екологія
	ВБ 1.2 Основи правознавства **ВБ** 1.2 Основи конституційного права
	ВБ 1.3 Філософія **ВБ** 1.3 Етика та естетика
	ВБ 1.4 Соціологія **ВБ** 1.4 Основи психології
ВБ 2	**ВБ** 2.1 Інженерна та комп`ютерна графіка **ВБ** 2.1. Інформаційні системи і технології
	ВБ 2.2 Бази даних **ВБ** 2.2 Метрологія та вимірювання
	ВБ 2.3 Економіка в галузі інформаційної безпеки **ВБ** 2.3 Технічні засоби охорони об’єктів
	ВБ 2.4 Оцінка та управління ризиками **ВБ** 2.4 Основи менеджменту та маркетингу
ВБ 3	**ВБ** 3.1 Інтернет-технології **ВБ** 3.1 Системи технічного захисту інформації
	ВБ 3.2.Технології штучного інтелекту **ВБ** 3.2 Цифрова схемотехніка
	ВБ 3.3 Інформаційно-психологічні впливи у кіберпросторі **ВБ** 3.3 Теорія електричних кіл і систем
	ВБ 3.4 Випробування систем захисту інформації **ВБ** 3.4 Основи електроніки і схемотехніки
	ВБ 3.5 Організація секретного діловодства **ВБ** 3.5 Телекомунікаційні системи та мережі

2.3. Структурно-логічна схема ОПП

№	Код н/д	Компоненти ОПП (навчальні дисципліни, курсові роботи, практики, тощо)	І курс		ІІ курс		ІІІ курс		IV курс	
			семестр							
			1	2	3	4	5	6	7	8
1	Освітні компоненти, що належать до циклу дисциплін повної загальної середньої освіти	Українська мова	+	+	+	+				
2		Українська література	+	+	+	+				
3		Зарубіжна література	+							
4		Іноземна мова	+	+	+	+				
5		Історія України		+	+					
6		Всесвітня історія	+							
7		Громадянська освіта		+						
8		Математика (алгебра і початки аналізу та геометрія)	+	+	+	+				
9		Біологія і екологія	+	+						
10		Географія		+						
11		Фізика і астрономія	+	+	+	+				
12		Хімія	+	+						
13		Фізична культура	+	+	+	+				
14		Захист України	+	+						
15		Захист України (МП)		+						
16		Інформатика	+	+						
17		Технології			+					
18	ОК8	Основи інформаційної безпеки держави			+					
19	ОК10	Інформаційні технології та основи програмування			+	+				
20	ВБ1	Економікс (або Екологія)			+					
21	ОК11	Операційні системи та системне програмне забезпечення			+	+				
22	ОК9	Стандарти інформаційної безпеки				+				
23	ВБ3	Інтернет-технології (або Системи технічного захисту інформації)				+				
24	ВБ1	Основи правознавства (або Основи конституційного права)				+				
25	ОК1	Історія та культура України				+				
26	ОК12	Архітектура апаратного забезпечення комп`ютера					+	+		
27	ОК13	Комп`ютерна дискретна математика					+			
28	ОК5	Вища математика					+	+		
29	ОК6	Вища фізика					+	+		
30	ВБ2	Інженерна та комп`ютерна графіка (або Інформаційні системи і технології)					+	+		
31	ВБ1	Філософія (або Етика та естетика)					+			
32	ОК4	Фізичне виховання					+	+		
33	ОК3	Іноземна мова (за професійним спрямуванням)					+	+		
34	ОК2	Українська мова (за професійним спрямуванням)						+		
35	ВБ3	Організація секретного діловодства (або Телекомунікаційні системи та мережі)						+		
36	ОК14	Технології програмування						+	+	
37	ОК15	Основи системного аналізу							+	
38	ОК16	Системи розмежування доступу							+	
39	ВБ2	Бази даних (або Метрологія та вимірювання)							+	
40	ВБ3	Випробування систем захисту інформації (або Основи електроніки і схемотехніки)							+	
41	ОК7	Основи охорони праці та БЖД							+	

42	ОК17	Захищені комп`ютерні системи та мережі							+	+
43	ОК18	Управління ресурсами інформаційних систем								+
44	ВБ2	Оцінка та управління ризиками (або Основи менеджменту та маркетингу)								+
45	ВБ3	Технології штучного інтелекту (або Цифрова схемотехніка)								+
46	ВБ3	Інформаційно-психологічні впливи у кіберпросторі (або Теорія електричних кіл і систем)								+
47	ВБ2	Економіка в галузі інформаційної безпеки (або Технічні засоби охорони об’єктів)								+
48	ВБ1	Соціологія (або Основи психології)								+
49	ОК19	Практика навчальна				+		+		
50	ОК20	Практика технологічна						+		
51	ОК21	Практика виробнича								+
52	ОК22	Атестація (Захист кваліфікаційної роботи)								+

3. Форма атестації здобувачів освіти

Атестація випускників освітньо-професійної програми Кібербезпека спеціальності 125 Кібербезпека та захист інформації проводиться у формі публічного захисту (демонстрації) кваліфікаційної роботи та завершується видачею документа встановленого зразка про присудження освітньо-професійного ступеня фахового молодшого бакалавра із присвоєнням кваліфікації «Фаховий молодший бакалавр з кібербезпеки».

Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації. Атестація здійснюється відкрито і публічно. Кваліфікаційна робота розміщується в репозитарії коледжу. Оприлюднення кваліфікаційних робіт, що містять інформацію з обмеженим доступом, здійснюється відповідно до вимог чинного законодавства.

4. Система внутрішнього забезпечення якості фахової передвищої освіти ВСП «КІУтЗ НАУ»

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», затвердженого Педагогічною радою (протокол від 08.03.2023 р. № 2), 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 та оприлюднення політики, принципів та процедур забезпечення якості фахової передвищої освіти, що інтегровані до загальної системи управління коледжем, узгоджені з його стратегією, передбачають залучення внутрішніх та зовнішніх зацікавлених сторін;

2) визначення і послідовне дотримання процедур розроблення освітньо-професійних програм, які забезпечують відповідність їх змісту стандартам фахової передвищої освіти, декларованим цілям, урахування позицій заінтересованих сторін, чітке визначення кваліфікацій, що присуджуються та/або присвоюються, які мають бути узгоджені з Національною рамкою кваліфікацій;

3) розроблення освітньо-професійних програм та здійснення (за участю здобувачів освіти) їх моніторингу та періодичного перегляду освітньо-професійних програм з метою гарантування досягнення встановлених для них цілей та їх відповідності потребам здобувачів фахової передвищої освіти і суспільства, включаючи опитування здобувачів фахової передвищої освіти;

4) забезпечення дотримання вимог правової визначеності, оприлюднення та послідовного дотримання нормативних документів коледжу, що регулюють усі

стадії підготовки здобувачів фахової передвищої освіти (прийом на навчання, організація освітнього процесу, визнання результатів навчання, переведення, відрахування, атестація тощо);

5) 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 чи інший спосіб;

6) визначення та послідовне дотримання вимог щодо компетентності педагогічних (науково-педагогічних) працівників, застосовування чесних і прозорих правил прийняття на роботу та безперервного професійного розвитку персоналу/забезпечення підвищення кваліфікації педагогічних працівників;

7) забезпечення необхідного фінансування освітньої та викладацької діяльності, а також адекватних та доступних освітніх ресурсів і підтримки здобувачів фахової передвищої освіти, самостійної роботи студентів, за кожною освітньою програмою;

8) забезпечення збирання, аналізу і використання відповідної інформації для ефективного управління освітньо-професійними програмами та діяльністю закладу, та наявності інформаційних систем ефективного управління освітнім процесом;

9) забезпечення публічної, зрозумілої, точної, об’єктивної, своєчасної та легкодоступної інформації про діяльність коледжу та освітньо-професійні програми, умови і процедури присвоєння ступеня фахової передвищої освіти та кваліфікацій;

10) забезпечення дотримання академічної доброчесності працівниками коледжу та здобувачами освіти, створення і забезпечення функціонування ефективної системи запобігання та виявлення академічного плагіату, порушень академічної доброчесності, притягнення порушників до академічної відповідальності;

11) періодичне проходження процедури зовнішнього забезпечення якості фахової передвищої освіти;

12) залучення здобувачів фахової передвищої освіти та роботодавців як повноправних партнерів до процедур і заходів забезпечення якості освіти;

13) забезпечення студентоорієнтованого навчання в освітньому процесі;

14) здійснення інших процедур і заходів, які забезпечують належний рівень якості фахової передвищої освіти, визначених законодавством, установчими документами коледжу або відповідно до них.

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 предмет її відповідності вимогам до системи забезпечення якості фахової передвищої освіти, що затверджуються центральним органом влади у сфері освіти і науки.

6. Матриця відповідності програмних компетентностей компонентам ОПП

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 забезпечення програмних результатів навчання (РН) відповідними компонентами ОПП

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										+			+	+					+	+	+	+