МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Відокремлений структурний підрозділ «Фаховий коледж інженерії та управління Національного авіаційного університету»

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

КІБЕРБЕЗПЕКА

фахової передвищої освіти

Галузь знань 12 Інформаційні технології

Спеціальність 125 Кібербезпека

Кваліфікація Фаховий молодший бакалавр з кібербезпеки

Освітньо-професійна програма
затверджена Педагогічною радою коледжу
протокол № 11 від 30.06.2022 р.
Вводиться в дію наказом директора
В.о. директора
_____ Віктор ПАРАНІЧ
Наказ № 50/1-од від 18.07.2022 р.

КИЇВ

1.Профіль освітньо-професійної програми

Розділ 1. Загальна інформація		
1.1	**Повна назва закладу освіти та структурного підрозділу**	Відокремлений структурний підрозділ «Фаховий коледж інженерії та управління Національного авіаційного університету»
1.2	**Освітньо-професійний ступінь**	Фаховий молодший бакалавр
1.3	**Офіційна назва освітньо-професійної програми**	**КІБЕРБЕЗПЕКА**
1.4	**Тип диплому та обсяг освітньо-професійної програми**	Диплом фахового молодшого бакалавра,одиничний, 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
1.7	**Професійна кваліфікація**	Не надається
1.8	**Кваліфікація в дипломі**	Освітньо-професійний ступінь –фаховий молодший бакалавр Спеціальність – 125 Кібербезпека 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 освітньо-професійної програми 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 – 2022 та наступні до нової редакції освітньо-професійної програми
1.14	**Інтернет-адреса постійного розміщення опису освітньо-професійної програми**	www.kitu.nau.edu.ua

Розділ 2. Опис предметної області		
2.1	***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 фахівців, здатних використовувати і впроваджуватитехнології інформаційної та/або кібербезпеки. ***Теоретичний зміст предметної області.*** ***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 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:*** Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки. ***Інструменти та обладнання:*** - системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; - сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.	
Розділ 3. Характеристика освітньо-професійної програми		
3.1	**Предметна область (галузь знань, спеціальність, спеціалізація (за наявності))**	Галузь знань 12 Інформаційні технології Спеціальність 125 Кібербезпека
3.2	**Орієнтація освітньо-професійної програми**	Освітньо-професійна програма фахового молодшого бакалавра базується на загально-наукових та практичних результатах в кібербезпеці і має прикладну орієнтацію.
3.3	**Основний фокус освітньо-професійної програми та спеціалізації**	Спеціальна освіта в галузі інформаційних технологій
3.4	**Особливості освітньо-професійної програми**	Вимагає спеціальної практики з метою забезпечення умов підготовки фахівців в реальному середовищі майбутньої професійної діяльності.

Розділ 4. Придатність випускників до працевлаштування та подальшого навчання		
4.1	**Працевлаштування випускників**	Фахівець може займати первинні посади (за ДК 003:2010): 3439 (24771). Фахівець із організації інформаційної безпеки 2131.2 – Адміністратор бази даних2131.2 – Адміністратор даних 2131.2 – Адміністратор доступу International Standard Classification of Occupations 2008 (ISCO-08): 2529 Security specialist (ICT).
4.2	**Академічні права випускників**	Продовження навчання за початковим (короткий цикл) або першим (бакалаврський) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі освіти дорослих.
Розділ 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 підручників та конспектів, консультацій з викладачами, підготовки кваліфікаційної роботи (проєкту).
5.2	**Оцінювання**	Заліки, екзамени, звіти з практики, есе, презентації, поточний контроль, проєктна робота, захист кваліфікаційної роботи (проєкту). Оцінювання навчальних досягнень здобувачів освіти здійснюється за 100 бальною шкалою ЄКТС (ECTS) та національною 4-х бальною шкалою («відмінно», «добре», «задовільно», «незадовільно») системами.
Розділ 6. Програмні компетентності		
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.

		ЗК 3. 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'язкияк 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. СК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоївта 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.
Розділ 7. Програмні результати навчання (ПРН)		
7.1	ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. ПРН 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. ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або	

	кібербезпеки. ПРН 8. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. ПРН 9. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. ПРН 10. Розробляти моделі загроз та порушника. ПРН 11. Аналізувати проєкти ІТС, базуючись на стандартизованих технологіях та протоколах передачі даних. ПРН 12. Вирішувати завдання захисту програм та інформації, що обробляється в ІТС програмно-апаратними засобами, та давати оцінку якості прийнятих рішень. ПРН 13. Реалізовувати комплексні системи захисту інформації в АС організації (підприємства) відповідно до вимог нормативно-правових документів. ПРН 14. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. ПРН 15. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в ІТС. ПРН 16. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в ІТС. ПРН 17. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в ІТС згідно встановленої політики інформаційної і\або кібербезпеки. ПРН 18. Здійснювати протидію отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. ПРН 19. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах. ПРН 20. Брати участь у розробці та впровадженні стратегії інформаційноїбезпеки та/або кібербезпеки відповідно до цілей і завдань організації. ПРН 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. ПРН 22. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. ПРН 23. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. ПРН 24. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. ПРН 25. Здійснювати аналіз ризиків обробки інформації в ІТС. ПРН 26. Вирішувати задачі аналізу програмного коду на наявність можливих вразливостей.	
Розділ 8. Ресурсне забезпечення реалізації 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. 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 «КІтУ НАУ» та НАУ.
Розділ 9. Академічна мобільність		
	Національна кредитна мобільність	Планується підписання двосторонніх договорів з провідними коледжами України
	Міжнародна кредитна мобільність	Планується підписання двосторонніх договорів з провідними коледжами Європейського союзу
	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 проєкти (роботи), практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумкового контролю/КП, КР
1	2	3	4
Обов'язкові компоненти ОПП			
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
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	
Загальний обсяг обов'язкових компонентів:		**133**	
Вибіркові компоненти ОПП (за вибором здобувача фахової передвищої освіти)			
Вибірковий блок ВБ 1			
ВБ 1.1	Економікс	3	Залік
	Екологія		
ВБ 1.2	Основи правознавства	3	Залік
	Основи конституційного права		
ВБ 1.3	Інженерна та комп`ютерна графіка	4	Залік
	Інформаційні системи і технології		
ВБ 1.4	Філософія	3	Залік
	Етика та естетика		
ВБ 1.5	Бази даних	4	Залік
	Метрологія та вимірювання		
ВБ 1.6	Економіка в галузі інформаційної безпеки	4	Залік
	Технічні засоби охорони об'єктів		
ВБ 1.7	Соціологія	3	Залік
	Основи психології		

ВБ 1.8	Оцінка та управління ризиками	4	Залік
	Основи менеджменту та маркетингу		
Загальний обсяг вибіркових компонентів ВБ 1:		***28***	
Вибірковий блок ВБ 2			
ВБ 2.1	Інтернет-технології	4	Залік
	Системи технічного захисту інформації		
ВБ 2.2	Технології штучного інтелекту	4	Залік
	Цифрова схемотехніка		
ВБ 2.3	Інформаційно-психологічні впливи у кіберпросторі	4	Залік
	Теорія електричних кіл і систем		
ВБ 2.4	Випробування систем захисту інформації	4	Залік
	Основи електроніки і схемотехніки		
ВБ 2.5	Організація секретного діловодства	3	Залік
	Телекомунікаційні системи та мережі		
Загальний обсяг вибіркових компонентів ВБ 2:		***19***	
Загальний обсяг вибіркових компонент:		***47***	
Загальний обсяг освітньо-професійної програми		**180**	

3. Форма атестації здобувачів освіти

Атестація випускників освітньо-професійної програми Кібербезпека спеціальності 125 Кібербезпека проводиться у формі публічного захисту (демонстрації) кваліфікаційної роботи та завершується видачею документа встановленого зразка про присудження освітньо-професійого 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 «КІтУ НАУ»

Якість освітньо-професійної програми визначається внутрішньою системою забезпечення якості фахової передвищої освіти та освітньої діяльності ВСП «КІтУ НАУ», яка функціонує згідно з Положенням про систему забезпечення якості вищої та фахової передвищої освіти в Відокремленому структурному підрозділі «Фаховий коледж інженерії та управління Національного авіаційного університету», ухваленого Педагогічною радою (протокол від 25.02.2021 р. № 4), 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;

9) 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.