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

КВАЛІФІКАЦІЯ Фаховий молодший бакалавр з кібербезпеки

ЗАТВЕРДЖЕНО
Педагогічною радою Коледжу
протокол №7 від 04.06.2024р.

Освітньо-професійна програма
вводиться в дію з 06.06.2024р.
(наказ від 06.06.2024р. №43-од)
В.о. директора
_____ **Ніна ГРИШКО**

Київ 2024р.

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

ПОГОДЖЕНО
Методичною радою ВСП КІУтЗ НАУ
протокол №10
від "16" травня 2024 р
Голова Науково-методичної ради
ВСП КІУтЗ НАУ
_____Альона ХЕБДА

ПОГОДЖЕНО
Цикловою комісією Кібербезпеки, інженерії програмного забезпечення та комп'ютерного дизайну ВСП КІУтЗ НАУ
протокол №10/61
від "15" 05 2024 р
Голова циклової комісії
_____Дар'я ГРИГОР'ЄВА

ПЕРЕДМОВА

Освітньо-професійна програма «Кібербезпека» ступеня фаховий молодший бакалавр, галузь знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека.

Освітньо-професійна програма є нормативним документом, який регламентує нормативні, компетентнісні, кваліфікаційні, організаційні, навчальні та методичні вимоги до підготовки фахових молодших бакалаврів у галузі 12 Інформаційні технології за спеціальністю 125 Кібербезпека (освітня кваліфікація: «Фаховий молодший бакалавр з кібербезпеки»).

Освітньо-професійна програма заснована на компетентнісному підході до підготовки спеціаліста в галузі 12 Інформаційні технології за спеціальністю 125 Кібербезпека (освітня кваліфікація: «Фаховий молодший бакалавр з кібербезпеки») у структурі фахової передвищої освіти.

Розроблено робочою групою у складі:

Керівник робочої проєктної групи:	Андрій ПОНОМАРЕНКО, викладач вищої категорії, викладач циклової комісії кібербезпеки, інженерії програмного забезпечення та комп'ютерного дизайну КІУтЗ КАІ
Члени робочої проєктної групи:	Ганна КРАЛІНА, викладач вищої категорії, викладач циклової комісії Кібербезпеки, інженерії програмного забезпечення та комп'ютерного дизайну Відокремленого структурного підрозділу «Фаховий коледж інженерії, управління та землевпорядкування Національного авіаційного університету»
	Наталія РЯБЧУК, викладач вищої категорії, викладач циклової комісії Кібербезпеки, інженерії програмного забезпечення та комп'ютерного дизайну Відокремленого структурного підрозділу «Фаховий коледж інженерії, управління та землевпорядкування Національного авіаційного університету»
	Дар'я ОСІПОВА, студентка групи 313-КБ Відокремленого структурного підрозділу «Фаховий коледж інженерії, управління та землевпорядкування Національного авіаційного університету»

1. Опис освітньо-професійної програми «Кібербезпека» галузі знань 12 Інформаційні технології зі спеціальності 125 Кібербезпека

1 – Загальна інформація	
Повна назва закладу освіти та структурного підрозділу	Відокремлений структурний підрозділ «Фаховий коледж інженерії, управління та землевпорядкування Національного авіаційного університету»
Освітньо-професійний ступінь	Фаховий молодший бакалавр
Освітня кваліфікація	Фаховий молодший бакалавр з кібербезпеки
Професійна кваліфікація	Не надається
Кваліфікація в дипломі	Освітньо-професійний ступінь - фаховий молодший бакалавр Спеціальність – 125 Кібербезпека Освітньо-професійна програма – Кібербезпека
Рівень кваліфікації згідно з Національною рамкою кваліфікацій	Освітньо-професійний ступінь фахового молодшого бакалавра відповідає 5 рівню Національної рамки кваліфікацій
Офіційна назва освітньо-професійної програми	Кібербезпека
Обсяг кредитів ЄКТС, необхідний для здобуття ступеня фахового молодшого бакалавра	180 кредитів ЄКТС, термін навчання –3 роки 10 місяців Обсяг освітньо-професійної програми фахового молодшого бакалавра на основі повної загальної середньої освіти (профільної середньої освіти) становить 180 кредитів ЄКТС. На основі базової середньої освіти здобувачі фахової передвищої освіти зобов'язані одночасно виконати освітню програму профільної середньої освіти, 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 освітньопрофесійної програми має бути спрямовано на досягнення результатів навчання за спеціальністю, визначених Стандартом фахової передвищої освіти. Обсяг освітньо-професійної програми фахового молодшого бакалавра на основі професійної (професійно-технічної) освіти, фахової передвищої освіти або вищої освіти визначається закладом фахової передвищої освіти з урахуванням визнання раніше здобутих результатів навчання. Обсяг такої програми становить не менше 50 % загального обсягу освітньо-професійної програми на основі профільної середньої освіти.
Наявність акредитації	Не акредитована, передбачається акредитація у 2025 році
Термін дії освітньо-професійної програми	Рік вступу – 2022 та наступні до нової редакції освітньо-професійної програми
Цикл/ рівень	НРК України – 5 рівень, ЄРК – 5 рівень, РК ЄПВО – короткий цикл

Вимоги до осіб, які можуть розпочати навчання за програмою	Особа може здобувати фахову передвищу освіту за освітньо-професійною програмою «Кібербезпека» на основі базової середньої освіти, повної середньої освіти, професійної (професійно-технічної) освіти, фахової передвищої освіти або вищої освіти. Особи, які здобувають фахову передвищу освіту на основі базової середньої освіти, зобов'язані одночасно виконати освітню програму профільної середньої освіти професійного спрямування. Вимоги визначаються правилами прийому на освітньо-професійну програму фахового молодшого бакалавра
Мова (и) викладання	Українська
Інтернет-адреса постійного розміщення опису ОПП	https://kiutz.nau.edu.ua/
2 – Мета освітньо-професійної програми	
Метою освітньо-професійної програми є підготовка висококваліфікованих та конкурентоспроможних 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	
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	
Придатність до працевлаштування	Фаховий молодший бакалавр з кібербезпеки та захисту інформації може виконувати зазначену в Національному класифікаторі професій ДК003:2010 (зі змінами) професійну роботу та обіймати відповідну первинну посаду: 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
Академічні права випускників	Подальше продовження навчання за першим (бакалаврським) рівнем вищої освіти, набуття додаткових кваліфікацій в системі освіти дорослих, у тому числі післядипломної освіти.
5 – Викладання та оцінювання	
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.
Оцінювання	Заліки, екзамени, звіти з практичних та лабораторних робіт, звіти з практик, презентації, поточний контроль, курсове проєктування, атестація. Оцінювання навчальних досягнень здобувачів освіти здійснюється за 100 бальною шкалою ЄКТС (ECTS).
6 – Перелік компетентностей випускника	
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.

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. **ЗК8**. Здатність працювати в команді.
Спеціальні компетентності (СК)	**СК01**. Здатність застосовувати законодавчу та нормативноправову 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 розробки та використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. **СК04**. Здатність забезпечувати працездатність інформаційнокомунікаційних систем згідно зі встановленою політикою безпеки. **СК05**. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. **СК06**. Здатність відновлювати штатне функціонування інформаційних, інформаційно- телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. **СК07**. Здатність впроваджувати та 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 та криптографічного захисту інформації на об'єктах інформаційної діяльності. **СК11**. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. **СК12**. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

7 – Зміст підготовки здобувачів фахової передвищої освіти, сформульований у термінах результатів навчання (РН)

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 інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних.

РН12. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку якості прийнятих рішень.

РН13. Реалізовувати комплексні системи захисту інформації в автоматизованих системах 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 інформаційно-телекомунікаційних системах.

РН16. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.

РН17. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки. **РН18**. Реалізовувати заходи з протидії 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 відновлення функціонування інформаційних та інформаційно-телекомунікаційних (автоматизованих) систем після здійснення кібератак, збоїв та відмов різних класів та походження. **РН22.** Організовувати процес свого навчання та самоосвіти. **РН23.** Розуміти фундаментальні принципи буття людини, природи, суспільства.

8. Ресурсне забезпечення реалізації освітньо-професійної програми	
Кадрове забезпечення	Відповідно до 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.
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. Соціальна інфраструктура включає спортивний зал, тренажерну залу, їдальню, гуртожиток; студенти мають доступ до мережі Інтернет.
Інформаційне та навчально- методичне забезпечення	Забезпеченість бібліотеки та читального залу підручниками та навчальними посібниками (зокрема й електронними), фаховими періодичними виданнями відповідного профілю; офіційний веб-сайт; наявність комплексів навчально-методичних матеріалів навчальних дисциплін, зокрема електронних для дистанційного навчання; точки бездротового доступу до мережі Інтернет; віртуальне навчальне середовище; корпоративна пошта. Коледжем обрані такі платформи для організації дистанційного навчання: Google Classroom, Meet.
9 – Академічна мобільність	
Національна кредитна мобільність	Планується підписання двосторонніх договорів з провідними коледжами України

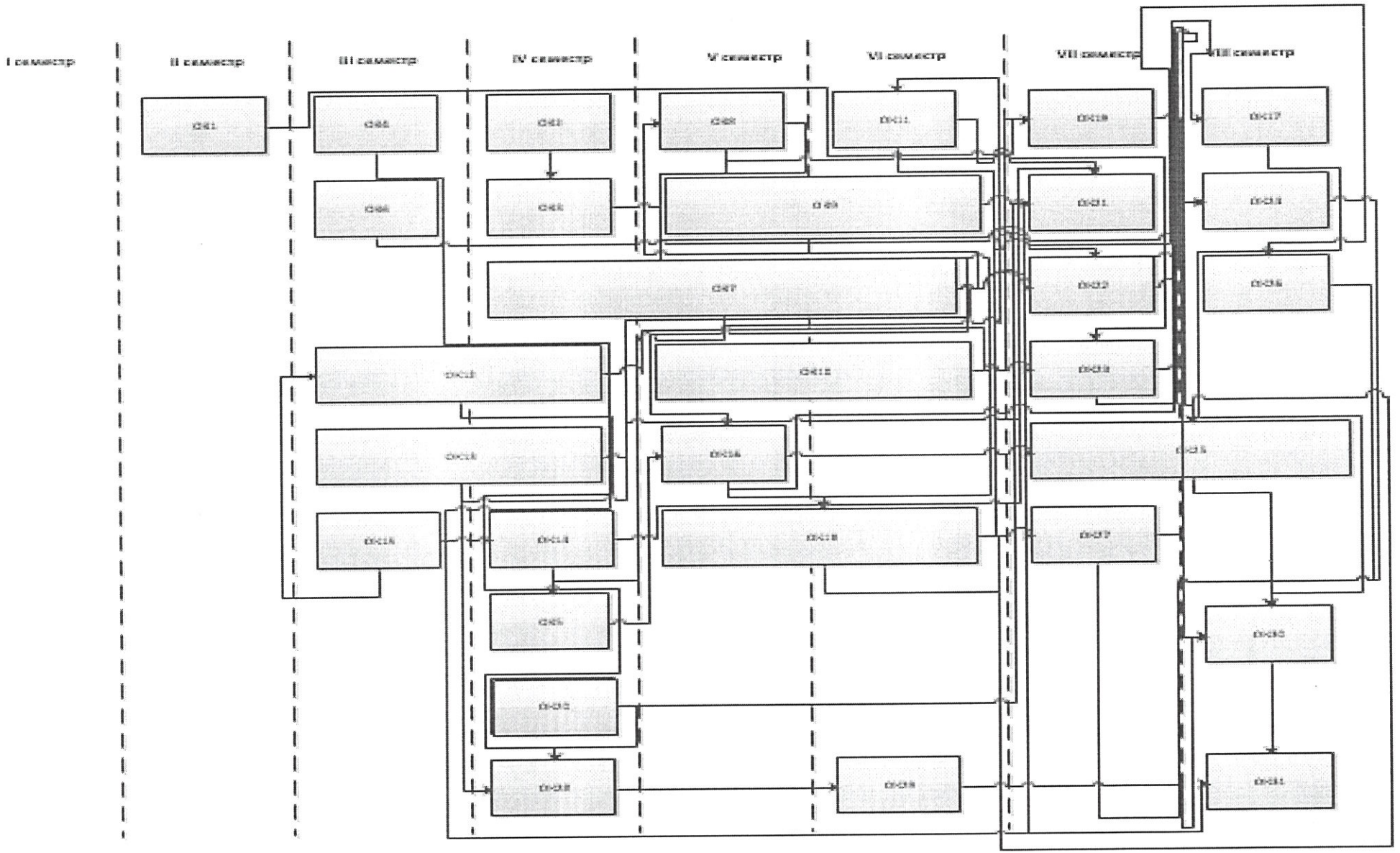
Міжнародна кредитна мобільність	Регламентовано Положенням про академічну мобільність у Відокремленому структурному підрозділі «Фаховий коледж інженерії, управління та землевпорядкування Національного авіаційного університету»
Навчання іноземних здобувачів фахової передвищої освіти	

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
Обов'язкові освітні компоненти ОПП			
Обов'язкові освітні компоненти, що формують загальні компетентності			
ОК 1	Основи екології	3	Залік
ОК 2	Історія та культура України	3	Залік
ОК 3	Основи правознавства	3	Залік
ОК 4	Українська мова за професійним спрямуванням	3	Залік
ОК 5	Фізика (електрика)	4	Залік
ОК 6	Економічна теорія	3	Залік
ОК 7	Вища математика	10	Залік
ОК 8	Комп`ютерна дискретна математика	4	Екзамен
ОК 9	Іноземна мова за професійним спрямуванням	6	Залік/екзамен
ОК 10	Фізичне виховання	4	Залік
ОК 11	Теорія ймовірностей та математична статистика	4	Залік
Обсяг обов'язкових освітніх компонентів (загальні комп.):		*47*	
Обов'язкові освітні компоненти, що формують спеціальні компетентності			
ОК 12	Інформаційні технології та основи програмування	8	Екзамен
ОК 13	Операційні системи та системне програмне забезпечення	8	Залік/екзамен
ОК 14	Стандарти інформаційної безпеки	6	Екзамен
ОК 15	Основи інформаційної безпеки держави	5	Екзамен
ОК 16	Комп'ютерна схемотехніка та мікропроцесорна техніка	6	Екзамен
ОК 17	Організація комп'ютерних мереж	5	Екзамен
ОК 18	Архітектура апаратного забезпечення комп`ютера	9	Залік/екзамен/КР
ОК 19	Основи охорони праці та БЖД	3	Залік
ОК 20	Інтернет технології	4	Залік
ОК 21	Безпека програм та даних	4	Залік
ОК 22	Основи системного аналізу	4	Залік
ОК 23	Технології програмування	6	Екзамен/КП
ОК 24	Управління ресурсами інформаційних систем	3	Залік
ОК 25	Захищені комп`ютерні системи та мережі	6	Залік/екзамен/КП
ОК 26	Системи розмежування доступу	3	Залік
ОК 27	Комплексні системи захисту інформації	4	Екзамен
ОК 28	Практика навчальна	6	Залік
ОК 29	Практика технологічна	9	Залік
ОК 30	Практика виробнича	9	Залік

ОК 31	Атестація (Комплексний кваліфікаційний екзамен)	1	
Обсяг обов'язкових освітніх компонентів спец. комп.):		***109***	
Загальний обсяг обов'язкових компонентів ОПП:		**156**	
Вибіркові освітні компоненти ОПП (за вибором здобувача фахової передвищої освіти)			
Вибіркові освітні компоненти ОПП, що формують загальні компетентності			
ВК1	Вибірковий компонент 1.1	3	Залік
	Вибірковий компонент 1.2		
ВК2	Вибірковий компонент 2.1	3	Залік
	Вибірковий компонент 2.2		
ВК3	Вибірковий компонент 3.1	3	Залік
	Вибірковий компонент 3.2		
Загальний обсяг вибіркових освітніх компонентів:		***9***	
Вибіркові освітні компоненти ОПП, що формують спеціальні компетентності			
ВК4	Вибірковий компонент 4.1	3	Залік
	Вибірковий компонент 4.2		
ВК5	Вибірковий компонент 5.1	3	Залік
	Вибірковий компонент 5.2		
ВК6	Вибірковий компонент 6.1	3	Залік
	Вибірковий компонент 6.2		
ВК7	Вибірковий компонент 7.1	3	Залік
	Вибірковий компонент 7.2		
ВК8	Вибірковий компонент 8.1	3	Залік
	Вибірковий компонент 8.2		
Загальний обсяг вибіркових освітніх компонентів:		***15***	
Загальний обсяг вибіркових освітніх компонентів:		**24**	
ЗАГАЛЬНИЙ ОБСЯГ ОПП:		**180**	

2.2 Структурно-логічна схема освітньо-професійної програми



3. Форма атестації здобувачів освіти

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

4. Вимоги до системи внутрішнього забезпечення якості фахової передвищої освіти

Система забезпечення закладами фахової передвищої освіти якості освітньої діяльності та якості фахової передвищої освіти (внутрішня система забезпечення якості освіти) включає:

1) визначення та оприлюднення політики, принципів та процедур забезпечення якості фахової передвищої освіти, що інтегровані до загальної системи управління закладом фахової передвищої освіти, узгоджені з його стратегією і передбачають залучення внутрішніх та зовнішніх зацікавлених сторін;

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

3) здійснення за участю здобувачів освіти 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 перед вищої освіти;

4) забезпечення дотримання вимог правової визначеності, оприлюднення та послідовного дотримання нормативних документів закладу фахової передвищої освіти, що регулюють усі стадії підготовки здобувачів фахової перед вищої освіти (прийом на навчання, організація освітнього процесу, визнання результатів навчання, переведення, відрахування, атестація тощо);

5) забезпечення релевантності, надійності, прозорості та об'єктивності оцінювання, що здійснюється у рамках освітнього процесу;

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;

7) забезпечення необхідного фінансування освітньої та викладацької діяльності, а також адекватних та доступних освітніх ресурсів і підтримки здобувачів фахової перед вищої освіти за кожною освітньо-професійною програмою;

8) забезпечення збирання, аналізу і використання відповідної інформації для ефективного управління освітньо-професійними програмами та іншою діяльністю закладу;

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

10) забезпечення дотримання академічної доброчесності працівниками закладу фахової перед вищої освіти та здобувачами фахової перед вищої освіти, у тому числі створення і забезпечення функціонування ефективної системи запобігання та виявлення академічного плагіату та інших порушень академічної доброчесності, притягнення порушників до академічної відповідальності;

11) періодичне проходження процедури зовнішнього забезпечення якості фахової перед вищої освіти;

11) періодичне проходження процедури зовнішнього забезпечення якості фахової перед вищої освіти;

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

13) забезпечення дотримання студентоорієнтованого навчання в освітньому процесі;

14) здійснення інших процедур і заходів, визначених законодавством, установчими документами закладів фахової перед вищої освіти або відповідно до них.

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

5. Матриця відповідності компетентностей випускника компонентам освітньо-професійної програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31
ЗК01						+					+																	+	+	+	+
ЗК02												+	+	+	+		+	+			+	+		+	+		+				
ЗК03				+					+																						
ЗК04													+	+			+	+			+	+	+	+		+			+	+	+
ЗК05											+			+	+							+		+			+	+	+	+	+
ЗК06			+																												
ЗК07	+	+								+																					
ЗК08				+		+	+						+													+	+			+	
ЗК09												+											+								
ЗК10																							+			+					
ЗК11	+																														
ЗК12			+																												
СК01															+																
СК02														+		+	+	+		+				+	+		+		+	+	+
СК03					+		+	+				+	+			+		+					+	+	+	+	+		+	+	+
СК04					+											+	+	+						+	+	+	+			+	
СК05								+						+	+	+					+				+	+	+	+	+	+	+
СК06					+								+			+	+	+							+						
СК07																	+							+	+	+	+	+	+	+	+
СК08															+				+												
СК09														+	+									+	+	+	+	+	+	+	+
СК10																+	+			+				+	+	+	+		+	+	+
СК11																	+	+							+		+		+	+	+
СК12																	+	+		+	+	+								+	+

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

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ОК14	ОК15	ОК16	ОК17	ОК18	ОК19	ОК20	ОК21	ОК22	ОК23	ОК24	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31
РН01				+					+																						
РН02		+	+			+							+		+				+												
РН03			+					+				+				+				+								+	+	+	+
РН04							+	+			+	+	+				+	+	+									+	+	+	+
РН05												+	+	+	+	+	+	+		+	+				+	+	+				
РН06					+	+	+				+	+	+					+				+	+			+	+	+	+	+	+
РН07			+											+	+										+						
РН08														+											+		+				+
РН09													+				+			+		+				+					
РН10												+	+							+	+		+		+				+	+	+
РН11								+					+			+	+	+				+		+		+		+	+	+	
РН12												+	+									+	+		+		+	+	+	+	
РН13													+			+	+							+	+		+			+	
РН14													+											+	+		+	+	+	+	
РН15					+		+														+				+				+	+	
РН16													+							+	+				+		+	+		+	
РН17												+	+							+	+		+		+	+				+	
РН18												+	+							+	+		+		+	+	+				
РН19												+	+				+				+		+		+			+	+		
РН20													+							+		+					+		+		
РН21																									+		+				
РН22																					+				+						
РН23																								+			+				
РН24			+											+	+														+		
РН25																								+	+						
РН26																					+	+	+					+			
РН27	+									+																					

7. Матриця відповідності результатів навчання та компетентностей

	ЗК01	ЗК02	ЗК03	ЗК04	ЗК05	ЗК06	ЗК07	ЗК08	ЗК09	ЗК10	ЗК11	ЗК12	СК01	СК02	СК03	СК04	СК05	СК06	СК07	СК08	СК09	СК10	СК11	СК12
РН01			+										+											+
РН02	+	+				+	+			+			+											
РН03		+		+	+															+			+	+
РН04				+								+											+	+
РН05				+				+						+										
РН06	+	+											+	+										
РН07												+	+											
РН08													+							+				
РН09																							+	+
РН10									+								+		+	+				+
РН11					+																+			
РН12					+														+	+		+		
РН13													+	+	+	+			+					
РН14															+	+			+					
РН15	+															+	+					+		
РН16																+		+	+					
РН17																+			+		+	+		
РН18								+									+		+		+			
РН19									+						+		+					+		
РН20										+										+	+	+		
РН21																		+	+				+	
РН22																		+		+				
РН23	+			+													+			+				
РН24								+					+							+				
РН25								+									+				+		+	
РН26															+		+							
РН27											+													