МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КОЛЕДЖ ІНЖЕНЕРІЇ ТА УПРАВЛІННЯ
НАЦІОНАЛЬНОГО АВІАЦІЙНОГО УНІВЕРСИТЕТУ

ОСВІТНЬО –ПРОФЕСІЙНА ПРОГРАМА

«КІБЕРБЕЗПЕКА»

Освітньо – кваліфікаційний рівень **МОЛОДШИЙ СПЕЦІАЛІСТ**

Спеціальність **125 КІБЕРБЕЗПЕКА**

Галузь знань **12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ**

Освітня кваліфікація **МОЛОДШИЙ СПЕЦІАЛІСТ З КІБЕРБЕЗПЕКИ**

Затверджено Вченою радою
Голова Вченої ради
_____ В. Ісаєнко
(протокол № 9 від 19.12. 2018 р.)

Освітньо-професійна програма
вводиться в дію наказом ректора
Ректор _____ В. Ісаєнко
(наказ № 625/од від 27.12. 2018 р.)

КИЇВ 2018

ПЕРЕДМОВА

РОЗРОБЛЕНО ПРОЕКТНОЮ ГРУПОЮ

СПЕЦІАЛЬНОСТІ 125 КІБЕРБЕЗПЕКА

у складі:

КЕРІВНИК ПРОЕКТНОЇ ГРУПИ:

КРАСОВСЬКА Євгенія Вікторівна – кандидат технічних наук, викладач КІтУ НАУ

_____

(підпис)

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

ПОНОМАРЕНКО Олександр Васильович – кандидат технічних наук, доцент кафедри компютерних систем та мереж, директор КІтУ НАУ

_____

ЛЕЩИНСЬКИЙ Олег Львович – кандидат фізико-математичних наук, доцент кафедри економічної кібернетики, заступник директора з виробничої роботи КІтУ НАУ

_____

(підпис)

ДІЄ ЯК ТИМЧАСОВА ДО ВВЕДЕННЯ СТАНДАРТУ

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

ПОГОДЖЕНО
Науково-методичною радою коледжу
протокол № 3
від "26" 10 2018 р
Голова Науково-методичної ради КІтУ НАУ
_____ О. Пономаренко

ПОГОДЖЕНО
Педагогічною радою коледжу
протокол № 3
від "25" 10 2018 р
Голова Педагогічної ради КІтУ НАУ
_____ О. Пономаренко

ПОГОДЖЕНО
Проектною групою КІтУ НАУ
протокол засідання № 2
від "24" 10 2018 р
Керівник проектної групи
_____ Є. Красовська

ДІЄ ЯК ТИМЧАСОВА ДО ВВЕДЕННЯ СТАНДАРТУ

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

ПОГОДЖЕНО
Науково-методичною радою коледжа
протокол № 2
від "25" 10 2018 р
Голова Науково-методичної ради КІтУ НАУ
_____ О. Пономаренко

ПОГОДЖЕНО
Педагогічною радою коледжу
протокол № 2
від "25" 10 2018 р
Голова Педагогічної ради КІтУ НАУ
_____ О. Пономаренко

ПОГОДЖЕНО
Проектною групою КІтУ НАУ
протокол засідання № 2
від "25" 10 2018 р
Керівник проектної групи
_____ Є. Красовська

1. Профіль освітньо-професійної програми

Розділ 1. Загальна інформація		
1.1.	Повна назва вищого навчального закладу та структурного підрозділу	Національний авіаційний університет Коледж інженерії та управління Національного авіаційного університету
1.2.	Ступінь фахової передвищої освіти та назва кваліфікації мовою оригіналу	Молодший спеціаліст Фахівець з кібербезпеки
1.3.	Офіційна назва освітньо-професійної програми	Освітньо-професійна програма «Кібербезпека» фахової передвищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології»
1.4.	Тип диплому та обсяг освітньо-професійної програми	Диплом молодшого спеціаліста, одиничний, 180 кредитів ЄКТС, термін навчання 3 роки 10 місяців
1.5.	Наявність акредитації	
1.6.	Цикл/рівень	НРК України– 5 рівень, FQ-EHEA – короткий цикл, EQF LLL – 5 рівень
1.7.	Передумови	Особа має право здобути ступінь молодшого спеціаліста за умови наявності в неї базової або повної загальної середньої освіти
1.8.	Мова(и) викладання	Українська
1.9.	Термін дії освітньо-професійної програми	До прийняття стандарту
1.10	Інтернет-адреса постійного розміщення опису освітньо-професійної програми	www.kitu.nau.edu.ua
Розділ 2. Мета освітньо-професійної програми		
2.1.	Чітке та коротке формулювання (в одному - двох реченнях)	Формування особистості фахівця, здатного розв'язувати складні спеціалізовані задачі та практичні проблеми, що можуть виникати в процесі розробки та експлуатації програмного та апаратного забезпечення комп'ютерних систем та мереж. Надати теоретичні знання та практичні уміння і навички, достатні для успішного виконання професійних обов'язків за спеціальністю «Кібербезпека» та підготувати студентів для подальшого навчання за обраною спеціальністю
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 молодшого спеціаліста, прикладна орієнтація.
3.3.	Основний фокус освітньо-професійної програми та спеціалізації	Спеціальна освіта в галузі інформаційних технологій спеціальність «Кібербезпека».

3.4.	Особливості освітньо-професійної програми	Вимагає спеціальної практики.
Розділ 4. Придатність випускників до працевлаштування та подальшого навчання		
4.1.	Придатність до працевлаштування	Фахівець може займати первинні посади (за ДК 003:2010): 3439 (24771). Фахівець із організації інформаційної безпеки. 2131.2 – Адміністратор бази даних 2131.2 – Адміністратор даних 2131.2 – Адміністратор доступу 2131.2 – Аналітик з комп'ютерних комунікацій 2131.2 – Аналітик з комп'ютерних систем 2131.2 – Аналітик з комп'ютерного банку даних International Standard Classification of Occupations 2008 (ISCO-08): 2529 Security specialist (ICT).
4.2.	Подальше навчання	Продовження навчання здобувачів вищої освіти для отримання освітнього ступеня бакалавр
Розділ 5. Викладання та оцінювання		
5.1.	Викладання та навчання	Студентоцентроване навчання, технологія проблемного і диференційованого навчання, технологія інтенсифікації та індивідуалізації навчання, технологія програмованого навчання, інформаційна технологія, технологія розвивального навчання, самонавчання, навчання на основі досліджень. Викладання проводиться у вигляді: лекції, мультимедійної лекції, інтерактивної лекції, семінарів, практичних занять, лабораторних робіт, самостійного навчання на основі підручників та конспектів, консультації з викладачами, підготовка кваліфікаційної роботи молодшого спеціаліста (проекту).
5.2.	Оцінювання	Письмові екзамени, практика, есе, презентації, поточний контроль, проектна робота, захист дипломного проекту.
Розділ 6. Програмні компетентності		
6.1.	Інтегральні компетентності	Здатність розв'язувати складні 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'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.	Фахові компетентності (ФК)	ФК 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. ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки. ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. ФК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики безпеки. ФК 5. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки. ФК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.

		ФК 7. Здатність забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) ФК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку ФК 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою. ФК 10. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. ФК 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем. ФК 12. Знання теоретичних та практичних принципів та інструментальних засобів в професійній галузі та уміння їх застосовувати. □
	Розділ 7. Програмні результати навчання	
7.1.	Програмні результати навчання	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 проблему 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 складних 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, 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 проекти 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. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки 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 встановленої політики 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	Педагогічний склад, задіяний до викладання циклу дисциплін професійної підготовки
8.2.	Матеріально-технічне забезпечення	Матеріально-технічна база коледжу володіє достатнім аудиторним фондом. Усі лабораторні та практичні заняття не за профільними дисциплінами проводяться на базі аудиторного фонду та матеріально-технічної бази коледжу.
8.3	Інформаційне та навчально-методичне забезпечення	Використання електронної бібліотеки коледжу та авторських методичних розробок викладацького складу.

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

2.1. Перелік компонент ОПП

Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОПП			
ОК 01	Історія та культура України	3	залік
ОК 02	Іноземна мова	4	залік
ОК 03	Фізичне виховання	3	залік
ОК 04	Українська мова	3	залік
ОК 05	Філософія	3	залік
ОК 06	Дискретна математика	3,5	залік
ОК 07	Вища математика	17	екзамен
ОК 08	Фізика (вибрані розділи)	10	екзамен
ОК 09	Стандарти інформаційної безпеки	3	залік
ОК 10	Комп'ютерна графіка	7	залік
ОК 11	Інформаційні технології та основи програмування	11,5	екзамен
ОК 12	Захищені комп'ютерні системи та мережі	9	екзамен, курсове проектування
ОК 13	Інформаційно-психологічні впливи у кіберпросторі	4	залік
ОК 14	Технології програмування	8,5	екзамен, курсове проектування
ОК 15	Операційні системи та системне програмне забезпечення	6	екзамен
ОК 16	Основи інформаційної безпеки держави	4	екзамен
ОК 17	Основи системного аналізу	3,5	екзамен
ОК 18	Управління ресурсами інформаційних систем	3,5	екзамен
ОК 19	Оцінка та управління ризиками	3	залік
ОК 20	Технології штучного інтелекту	3	залік
ОК 21	Основи охорони праці	3	екзамен
ОК 22	Навчальна практика	10	
ОК 23	Технологічна практика	7	
ОК 24	Переддипломна практика	7	
ОК 25	Дипломне проектування	5	
Загальний обсяг обов'язкових компонент:		**144,5**	
Вибіркові компоненти ОПП			
Вибірковий блок 1			
ВБ 1.1	Англійська мова (за професійним спрямуванням)	8	екзамен
ВБ 1.2	Архітектура апаратного забезпечення комп'ютера	5	екзамен, курсове проектування

ВБ 1.3	Організація секретного діловодства	3	залік
ВБ 1.4	Бази даних та основи SQL	4	залік
ВБ 1.5	Сучасні системи розмежування доступу	4,5	залік
ВБ 1.6	Економіка в галузі інформаційної безпеки	3,5	залік
ВБ 1.7	Випробування систем захисту інформації	3,5	залік
ВБ 1.8	Інтернет-технології	4	залік
Вибірковий блок 2			
ВБ 2.1	Іноземна мова (за професійним спрямуванням)	8	екзамен
ВБ 2.2	Апаратні компоненти операційних систем	5	екзамен,
ВБ 2.3	Особливості організації конфіденційного діловодства	3	залік
ВБ 2.4	Бази даних та знань	4	залік
ВБ 2.5	Системи контролю і керування доступом	4,5	залік
ВБ 2.6	Економічна безпека діяльності підприємств	3,5	залік
ВБ 2.7	Спеціальне системне програмне забезпечення	3,5	залік
ВБ 2.8	Захищені мережеві протоколи	4	залік
Загальний обсяг вибіркових компонент		**35,5**	
Загальний обсяг освітньо-професійної програми		**180**	

3. Форма атестації здобувачів вищої освіти

Атестація випускників освітньо-професійної програми «Кібербезпека» спеціальності 125 «Кібербезпека» проводиться у формі публічного захисту (демонстрації) дипломного проекту та завершується видачею документу встановленого зразка про присудження освітньо-кваліфікаційного рівня молодшого спеціаліста із присвоєнням кваліфікації: Фахівець з кібербезпеки за спеціальністю 125 «Кібербезпека».

Атестація здійснюється відкрито і публічно.