(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Управління інформаційною безпекою»
(найменування освітньої програми)
Першого (бакалаврського) рівня вищої освіти

за спеціальністю 125 Кібербезпека
(шифр та найменування спеціальності)
галузі знань 12 Інформаційні технології
(шифр та найменування галузі)

СМЯ НАУ 09.01.08 – 03 – 2021

Освітньо-професійна програма
Затверджена Вченою радою
протокол № 5 від 11.05.2021р.

Вводиться в дію наказом ректора
Ректор
_____ М. Луцький
наказ №326 від 01.06. 2021р.

Стандарт вищої освіти України: перший (бакалаврський) рівень, галузь знань 12 – Інформаційні технології, спеціальність 125 – Кібербезпека. Затверджено і введено в дію наказом Міністерства освіти і науки України від 04.10.2018 р. № 1047

ЛИСТ ПОГОДЖЕННЯ

освітньо-професійної програми

ПОГОДЖЕНО

Науково-методичною радою

протокол № 4

від "17" 05 2021 р.

Голова НМР НАУ,

Проректор з навчальної роботи

_____ А. Полухін

ПОГОДЖЕНО

Вченою радою Факультету кібербезпеки, комп'ютерної та програмної інженерії

протокол № 6

від "14" 05 2021 р.

Голова Вченої ради

Факультету кібербезпеки, комп'ютерної та програмної інженерії

_____ К. Нестеренко

ПОГОДЖЕНО

Кафедрою безпеки інформаційних технологій

протокол засідання № 40

від "5" 05 2021 р.

Завідувач кафедри

_____ О. Корченко

ПОГОДЖЕНО

Студентською радою Факультету кібербезпеки, комп'ютерної та програмної інженерії

протокол № 21/5-н-ФКІПІ

від "11" травня 2021 р.

Голова Студентської ради

Факультету кібербезпеки, комп'ютерної та програмної інженерії

_____ В. Прощаваєв

ПЕРЕДМОВА

Розроблено робочою групою освітньо-професійної програми (спеціальності 125 Кібербезпека) у складі:

ГАРАНТ ОСВІТНЬОЇ ПРОГРАМИ:

ХОХЛАЧОВА Ю.Є., к.т.н., доц., доцент кафедри безпеки інформаційних технологій

(підпис)

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

ЗАРІЦЬКИЙ О.В., д.т.н., доцент кафедри безпеки інформаційних технологій

(підпис)

ІВАНЧЕНКО І.С., к.т.н., доц., доцент кафедри безпеки інформаційних технологій

(підпис)

СИДОРЕНКО В.М., к.т.н., доцент кафедри безпеки інформаційних технологій

(підпис)

ПІНДЕЛЬ К.О., студентка кафедри безпеки інформаційних технологій, групи АМ-475

(підпис)

ЗОВНІШНІЙ СТЕЙКХОЛДЕР
ЄВСЕЄВ С.П., д.т.н., проф.,
завідувач кафедри кібербезпеки та інформаційних технологій Харківського національного економічного університету ім. С. Кузнеця

(підпис)

Рецензії-відгуки зовнішніх стейкхолдерів (додаються).

Рівень документа – 3б
Плановий термін між ревізіями – 1 рік
Контрольний примірник

1. Профіль освітньо-професійної програми

Розділ 1. Загальна інформація		
1.1.	Повна назва закладу вищої освіти та структурного підрозділу	Національний авіаційний університет, Факультет кібербезпеки, комп'ютерної та програмної інженерії, кафедра безпеки інформаційних технологій
1.2.	Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр Бакалавр з кібербезпеки
1.3.	Офіційна назва освітньо-професійної програми та спеціалізації (за наявності)	Управління інформаційною безпекою
1.4.	Тип диплому та обсяг освітньо-професійної програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання: 3 роки 10 місяців (денна форма навчання), 4 роки 6 місяців (заочна форма навчання)
1.5.	Акредитаційна інституція	Акредитовано, Акредитаційна комісія Міністерства освіти і науки України, сертифікат про акредитацію НД 1193809 від 31 жовтня 2017 року
1.6.	Період акредитації	1 липня 2027 р.
1.7.	Цикл/рівень	6 рівень Національної рамки кваліфікацій України (НРК України), перший цикл Європейського простору вищої освіти (FQ-EHEA), 6 рівень Європейської рамки кваліфікацій для навчання впродовж життя (EQF-LLL)
1.8.	Передумови	Повна загальна середня освіта
1.9.	Форма навчання	Очна (денна), заочна
1.10	Мова(и) викладання	Українська
1.11	Інтернет-адреса постійного розміщення опису освітньо-професійної програми	http://www.nau.edu.ua http://fccpi.nau.edu.ua/ http://www.bit.nau.edu.ua
Розділ 2. Ціль освітньо-професійної програми		
2.1.	Ціль освітньої програми полягає в підготовці висококваліфікованих та конкурентоспроможних фахівців з ґрунтованими компетентностями у розробці та впровадженні сучасних систем управління інформаційною безпекою. ОПП «Управління інформаційною безпекою» відповідає місії та цілям НАУ, щодо внеску НАУ у розвиток суспільства через генерацію нових знань і надання високоякісних освітніх послуг при підготовці фахівців з кібербезпеки в авіаційно-космічній галузі.	
Розділ 3. Характеристика освітньо-професійної програми		
3.1	Предметна область (Об'єкт діяльності, теоретичний зміст)	Об'єкти діяльності: комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; технології забезпечення складових безпеки інформації: інформаційна безпека, кібербезпека, безпека інформації; процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. Теоретичний зміст: Знання: – законодавчої, нормативно-правової бази України та вимог відповідних, в тому числі, міжнародних стандартів і практик щодо здійснення професійної діяльності; теорії та моделей 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; автоматизованих систем проєктування.
3.2.	Орієнтація освітньо-професійної програми	Освітньо-професійна програма прикладної орієнтації, що базується на загально-відомих наукових і практичних результатах в галузі інформаційної безпеки, у рамках яких можлива подальша професійна кар'єра і подальше навчання.
3.3.	Основний фокус освітньо-професійної програми та спеціалізації (за наявності)	Загальна вища освіта першого (бакалаврського) рівня спеціальності 125 Кібербезпека Ключові слова: кібербезпека, інформаційна безпека, управління інформаційною безпекою, криптографічні та технічні методи захисту інформації, захист персональних даних, захист інформації, захист від несанкціонованого доступу, кібербезпека проводових та безпроводових мереж, система менеджменту інформаційної безпеки.
3.4.	Особливості освітньо-професійної програми	Програма передбачає вивчення основ: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів впровадження і супроводу систем управління інформаційною безпекою; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною безпекою; – методів та засобів виявлення, управління та ідентифікації ризиків та інцидентів інформаційної безпеки; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів і засобів технічного та крипто-графічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих засобів проєктування систем управління інформаційною безпекою. Постійний та систематичний моніторинг ринку освітніх послуг, аналіз вакансій і потенційних можливостей ринку праці, експертне опитування керівників і провідних спеціалістів підприємств різних форм власності стали основою з підготовки фахівців освітньо-професійної програми «Управління інформаційною безпекою». Проведений аналіз показав необхідність продовжувати підготовку фахівців здатних використовувати і впроваджувати технології управління інформаційною та/або кібербезпекою, які володіють знаннями механізмів забезпечення

		безпеки та ефективними засобами обмежень ризиків в інформаційних системах. Це забезпечує можливість отримання якісної професійної освіти в галузі ІТ та робить вказану ОПП унікальною.
Розділ 4. Придатність випускників до працевлаштування та подальшого навчання		
4.1.	Придатність до працевлаштування	Випускники отримують можливість працювати фахівцями з організації інформаційної безпеки в складі відповідних департаментів, підприємств та банків, розробниками та тестувальниками застосунків, що потребують виконання особливих вимог щодо інформаційної та кібернетичної безпеки; співробітниками служб захисту інформації; адміністраторами інформаційної та кібернетичної безпеки, проектувальниками систем захисту в кіберпросторі.
4.2.	Подальше навчання	Право продовжити навчання на другому (магістерському) рівні вищої освіти. Право набувати додаткові кваліфікації в системі післядипломної освіти.
Розділ 5. Викладання та оцінювання		
5.1.	Викладання та навчання (методи, методики, технології, інструменти та обладнання)	Лекції, лабораторні роботи, семінари, практичні заняття, проєктна робота в командах, самостійна робота на основі підручників та конспектів, консультації з викладачами, навчальний комп'ютерний практикум, фахова та технологічна практика, підготовка кваліфікаційної роботи.
5.2.	Оцінювання	Усні та письмові екзамени, лабораторні звіти, курсові роботи, презентації, поточний контроль, захист кваліфікаційної роботи.
Розділ 6. Програмні компетентності		
6.1.	Інтегральна Компетентність (ІК)	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов
6.2.	Загальні компетентності (ЗК)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області та розуміння професії. ЗК3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК5. Здатність до пошуку, оброблення та аналізу інформації. ЗК6. 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. ЗК7. 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.
6.3.	Фахові компетентності (ФК)	ФК1. 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. ФК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. ФК3. Здатність до використання програмних та програмноапаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. ФК4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. ФК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. ФК6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження. ФК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) ФК8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. ФК9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. ФК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. ФК11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. ФК12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки. ФК13. Здатність застосовувати методи теорії інформації та кодування, обробки та захисту інформації при наявності завад в каналах передачі даних.

		ФК14. Здатність застосовувати теоретичні знання та практичні навички із побудови, керування, модернізації, моніторингу та аналізу продуктивності сучасних інформаційно-комунікаційних систем. ФК15. Здатність застосовувати теоретичні знання та практичні навички з організації та функціонування сучасних операційних систем, уміння зі створення та використання ефективного програмного забезпечення для керування обчислювальними ресурсами в багато користувальницьких операційних системах. ФК16. Здатність застосовувати методи та засоби організаційного характеру для побудови системи управління інформаційною безпекою. ФК17. Здатність застосовувати методи та засоби стеганографічного захисту інформації.
Розділ 7. Програмні результати навчання		
7.1.	Програмні результати навчання	ПРН1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. ПРН2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. ПРН3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. ПРН4. 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. ПРН5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. ПРН6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. ПРН7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. ПРН8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. ПРН9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. ПРН10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем. ПРН11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. ПРН12. Розробляти моделі загроз та порушника. ПРН13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на

		стандартизованих технологіях та протоколах передачі даних. ПРН14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень. ПРН15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. ПРН16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів. ПРН17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент. ПРН18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. ПРН19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах. ПРН20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах. ПРН21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. ПРН22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки. ПРН23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. ПРН24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових). ПРН25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.

		ПРН26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем. ПРН27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах. ПРН28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки. ПРН29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів. ПРН30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем. ПРН31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем. ПРН32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки. ПРН33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків. ПРН34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації. ПРН35. 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. ПРН36. Виявляти небезпечні сигнали технічних засобів. ПРН37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН39. Проводити атестацію (спираючись на облік та

		обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. ПРН40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. ПРН42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. ПРН43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. ПРН44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами. ПРН45. Застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів. ПРН46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. ПРН47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. ПРН48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах. ПРН49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах. ПРН50. Забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних). ПРН51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах. ПРН52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. ПРН53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз. ПРН54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність

		його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ПРН55. Оволодіння навичками працювати самостійно при виконанні курсових робіт, курсових проєктів, дипломних робіт. ПРН56. Здатність продемонструвати знання та розуміння професійної діяльності на основі впровадженої системи управління інформаційною безпекою.
Розділ 8. Ресурсне забезпечення реалізації програми		
8.1.	Кадрове забезпечення	Всі науково-педагогічні працівники, що забезпечують освітньо-професійну програму за кваліфікацією відповідають профілю і напряму дисциплін, що викладаються, мають необхідний стаж педагогічної роботи та досвід практичної роботи. У процесі організації навчального процесу залучаються професіонали з досвідом дослідницької, управлінської, інноваційної, творчої та фахової роботи, іноземні лектори.
8.2.	Матеріально-технічне забезпечення	Навчальні приміщення, комп'ютерні робочі місця, мультимедійні класи дозволяють повністю забезпечити освітній процес протягом усього циклу підготовки за освітньою програмою.
8.3	Інформаційне та навчально-методичне забезпечення	Офіційний веб-сайт www.nau.edu.ua містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила прийому, контакти. Матеріали навчально-методичного забезпечення освітньої програми викладені в репозитарії НАУ за посиланням: http://er.nau.edu.ua/handle/NAU/14303 Всі ресурси науково-технічної бібліотеки доступні через сайт університету: http://www.lib.nau.edu.ua Читальний зал забезпечений бездротовим доступом до мережі Інтернет. Електронний репозитарій наукової бібліотеки НАУ: http://er.nau.edu.ua
Розділ 9. Академічна мобільність		
9.1.	Національна кредитна мобільність	У рамках двосторонніх договорів між Національним авіаційним університетом та вітчизняними закладами вищої освіти.
9.2.	Міжнародна кредитна мобільність	У рамках Еразмус+К1 договір про співробітництво між Національним авіаційним університетом та навчальними закладами ЕС.
9.3.	Навчання іноземних здобувачів вищої освіти	Створено умови для навчання іноземних здобувачів вищої освіти.

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

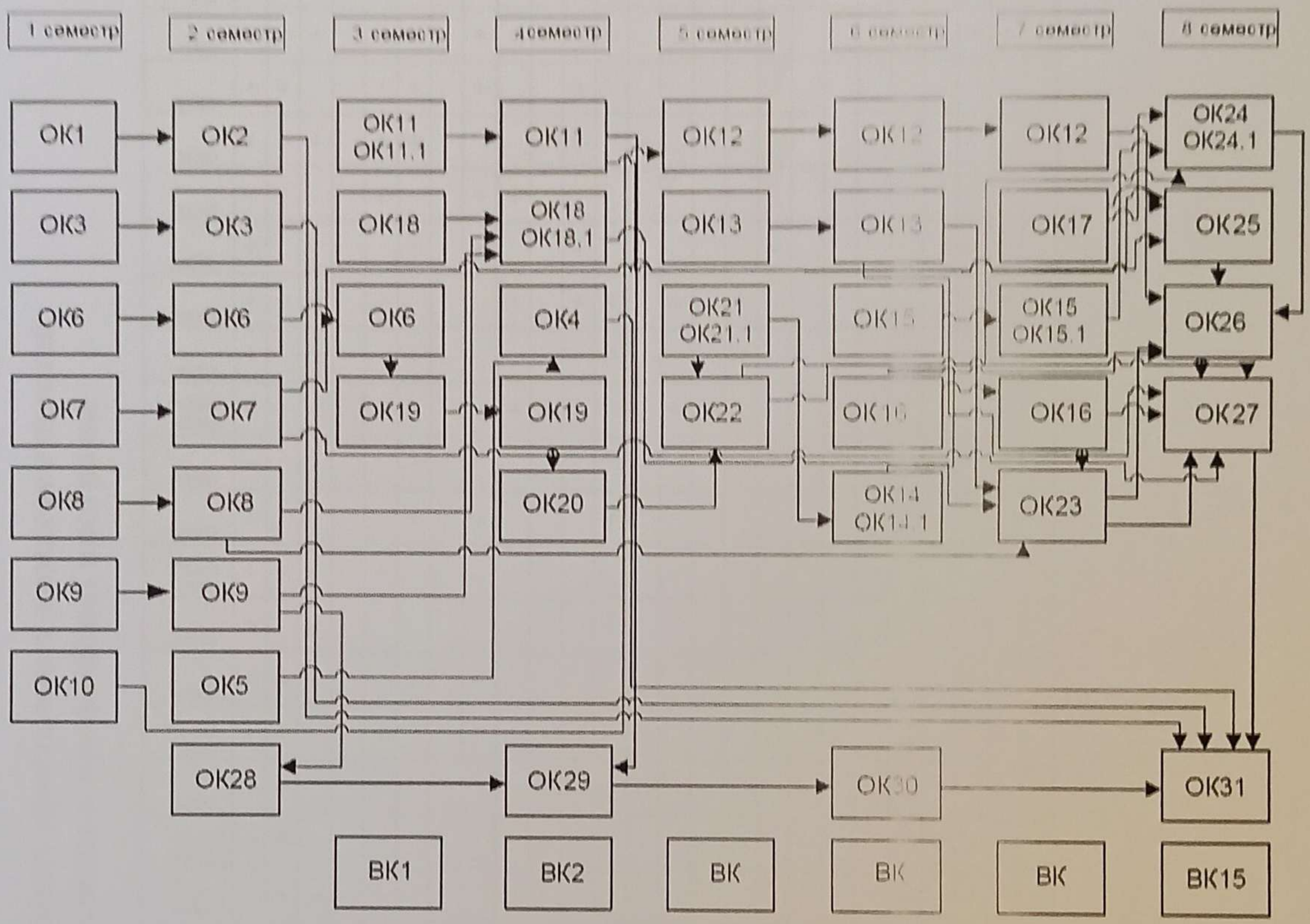
2.1. Перелік компонент

Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проєкти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю	Семестр
1	2	3	4	5
Обов'язкові компоненти				
ОК 1.	Історія української державності та культури	3.0	Екзамен	1
ОК 2.	Ділова українська мова	3.0	Екзамен	2
ОК 3.	Фахова іноземна мова	4.5	Диференційований залік Екзамен	1 2
ОК 4.	Філософія	3.5	Екзамен	4
ОК 5.	Фізичне виховання та самовдосконалення	3.0	Диференційований залік	2
ОК 6.	Вища математика	14.0	Екзамен Диференційований залік Екзамен	1 2 3
ОК 7.	Фізика	10.5	Диференційований залік Екзамен	1 2
ОК 8.	Інформаційні технології	11.5	Екзамен Диференційований залік	1 2
ОК 9.	Основи автоматизованої обробки інформації	6.5	Диференційований залік Диференційований залік	1 2
ОК 10	Основи кібербезпеки	4.5	Диференційований залік	1
ОК 11	Апаратне забезпечення інформаційних систем	5.0	Диференційований залік Екзамен	3 4
ОК 11.1	Курсова робота з дисципліни «Апаратне забезпечення інформаційних систем»	1.0	Захист	3
ОК 12	Авіаційна безпека та кібербезпека авіаційних інформаційних систем	10.5	Екзамен Диференційований залік Диференційований залік	5 6 7
ОК 13	Захищені комп`ютерні системи та мережі	8.0	Диференційований залік Екзамен	5 6
ОК 14	Управління інформаційною безпекою	3.0	Екзамен	6
ОК 14.1	Курсова робота з дисципліни «Управління інформаційною безпекою»	1.0	Захист	6
ОК 15	Прикладна криптологія	7.5	Екзамен Екзамен	6 7
ОК 15.1	Курсова робота з дисципліни «Прикладна криптологія»	1.0	Захист	7

ОК 16	Операційні системи та технології їх захисту	7.0	Диференційований залік Екзамен	6 7
ОК 17	Системи технічного захисту інформації	3.5	Екзамен	7
ОК 18	Технології програмування	9.5	Екзамен Екзамен	3 4
ОК 18.1	Курсова робота з дисципліни «Технології програмування»	1.0	Захист	4
ОК 19	Дискретна математика	9.5	Екзамен Диференційований залік	3 4
ОК 20	Технології забезпечення безперервності бізнес-процесів	4.0	Диференційований залік	4
ОК 21	Оцінювання та управління ризиками інформаційної безпеки	4.5	Екзамен	5
ОК 21.1	Курсова робота з дисципліни «Оцінювання та управління ризиками інформаційної безпеки»	1.0	Захист	5
ОК 22	Технології виявлення уразливостей інформаційних систем	4.5	Екзамен	5
ОК 23	Основи інтернет-технології	3.5	Диференційований залік	7
ОК 24	Комплексні системи захисту інформації	2.5	Екзамен	8
ОК 24.1	Курсовий проєкт з дисципліни «Комплексні системи захисту інформації»	1.5	Захист	8
ОК 25	Тестування безпеки інформаційних систем	4.0	Екзамен	8
ОК 26	Інцидент-менеджмент у кіберпросторі	3.5	Екзамен	8
ОК 27	Інформаційне забезпечення управлінської діяльності	3.0	Диференційований залік	8
ОК 28	Фахова ознайомлювальна практика	3.0	Диференційований залік	2
ОК 29	Навчальний комп`ютерний практикум	3.0	Диференційований залік	4
ОК 30	Технологічна практика	3.0	Диференційований залік	6
ОК 31	Кваліфікаційна робота	7.5	Захист	8
Загальний обсяг обов'язкових компонент:		180 кредитів		
Вибіркові компоненти				
ВК 1.	Дисципліна 1	4.0	Диференційований залік	
ВК 2.	Дисципліна 2	4.0	Диференційований залік	
...	...			
ВК 15.	Дисципліна 15	4.0	Диференційований залік	
Загальний обсяг вибіркових компонент*		60 кредитів		
Загальний обсяг освітньо-професійної програми		240 кредитів		

**Реалізація права здобувачів вищої освіти на вільний вибір навчальних дисциплін та створення індивідуальної освітньої траєкторії регламентується Законом України «Про вищу освіту» та внутрішніми нормативними актами НАУ. Вибіркові компоненти обираються здобувачами вищої освіти із каталогів рекомендованих та альтернативних вибіркових дисциплін.*

2.2. Структурно-логічна схема освітньо-професійної програми



3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація випускників освітньо-професійної програми проводиться у формі захисту кваліфікаційної роботи та завершується видачею документу встановленого зразка про присудження йому освітнього ступеня бакалавра із присвоєнням освітньої кваліфікації: Бакалавр з кібербезеки.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має передбачати розв'язання складної задачі у сфері управління інформаційно безпекою, що потребує проведення досліджень та/або здійснення інновацій. Кваліфікаційна робота не повинна містити академічний плагіат, фабрикацію та фальсифікацію. Кваліфікаційна робота обов'язково включає елементи наукової новизни та відповідає вимогам академічної доброчесності.
Вимоги до публічного захисту (демонстрації)	Захист кваліфікаційних робіт проводиться шляхом публічного захисту на відкритому засіданні ДЕК. Обов'язковою умовою є наявність презентації.

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11 ОК11.1	ОК12	ОК13	ОК14 ОК14.1	ОК15 ОК15.1	ОК16	ОК17	ОК18 ОК18.1	ОК19	ОК20	ОК21 ОК21.1	ОК22	ОК23	ОК24 ОК24.1	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ВК1	ВК2	…	ВК15
ІК	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				
ЗК1						+	+	+			+		+	+	+	+	+	+	+		+			+		+		+	+	+	+				
ЗК2				+						+		+		+	+	+				+				+		+			+		+				
ЗК3	+	+	+																																
ЗК4								+		+	+	+	+	+	+	+	+	+			+			+		+		+	+	+	+				
ЗК5	+			+		+			+				+						+			+	+		+		+		+	+	+				
ЗК6	+	+			+																														
ЗК7	+	+	+	+	+		+	+			+	+										+					+	+		+	+				
ФК1		+	+							+				+							+			+		+		+			+				
ФК2								+								+							+	+					+		+				
ФК3								+	+		+					+		+						+		+	+		+	+	+				
ФК4										+				+						+		+			+	+					+				
ФК5														+				+						+					+						
ФК6							+					+		+							+			+		+									
ФК7														+										+											
ФК8						+													+						+	+									
ФК9														+													+								
ФК10															+		+																		
ФК11														+																					
ФК12	+			+						+		+									+	+				+					+				
ФК13															+		+																		
ФК14													+			+															+				
ФК15								+			+		+		+	+														+					
ФК16														+							+			+		+									
ФК17															+																				

5. Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньо-професійної програми

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11 ОК11.1	ОК12	ОК13	ОК14 ОК14.1	ОК15 ОК15.1	ОК16	ОК17	ОК18 ОК18.1	ОК19	ОК20	ОК21 ОК21.1	ОК22	ОК23	ОК24 ОК24.1	ОК25	ОК26	ОК27	ОК28	ОК29	ОК30	ОК31	ВК1	ВК2	…	ВК15
ПРН1		+	+											+							+				+						+				
ПРН2						+	+			+				+							+				+						+				
ПРН3									+														+				+				+				
ПРН4														+						+	+	+		+	+										
ПРН5								+								+		+		+		+	+												
ПРН6								+		+					+			+					+												
ПРН7										+		+		+										+		+									
ПРН8										+				+										+											
ПРН9														+							+	+		+		+									
ПРН10													+			+								+											
ПРН11								+					+			+							+												
ПРН12										+				+										+		+									
ПРН13													+			+							+		+										
ПРН14											+				+			+													+				
ПРН15											+		+		+			+																	
ПРН16										+														+											
ПРН17											+		+			+																			
ПРН18								+			+							+						+											
ПРН19												+		+							+	+			+										
ПРН20															+							+				+									
ПРН21														+							+				+										
ПРН22													+			+							+	+			+								
ПРН23														+	+		+															+			
ПРН24													+	+	+								+												
ПРН25														+							+					+	+								
ПРН26													+	+										+											
ПРН27								+														+													
ПРН28						+															+				+	+									
ПРН29										+											+	+		+											
ПРН30													+									+	+												
ПРН31								+		+		+											+												
ПРН32																				+						+								
ПРН33																				+	+					+								
ПРН34														+										+											

ПРН35														+									+														
ПРН36																	+						+														
ПРН37										+							+						+														
ПРН38										+							+																				
ПРН39										+							+								+												
ПРН40																	+								+												
ПРН41														+						+							+										
ПРН42														+						+						+	+										
ПРН43										+				+													+										
ПРН44										+				+						+	+																
ПРН45										+				+							+																
ПРН46														+							+																
ПРН47														+	+				+																		
ПРН48															+					+								+									
ПРН49																						+	+	+													
ПРН50											+		+		+			+																			
ПРН51													+											+	+												
ПРН52														+										+				+									
ПРН53								+							+	+		+											+								
ПРН54	+	+		+	+																			+					+	+	+	+				
ПРН55											+			+	+			+			+			+					+	+	+	+				
ПРН56														+							+			+	+											

РЕЦЕНЗІЯ-ВІДГУК
на освітньо-професійну програму
“Управління інформаційною безпекою”
Спеціальності 125 “Кібербезпека”
першого (бакалаврського) рівня вищої освіти

Рецензована освітньо-професійна програма “Управління інформаційною безпекою” розроблена колективом кафедри безпеки інформаційних технологій факультету кібербезпеки, комп’ютерної та програмної інженерії Національного авіаційного університету.

Цілі освітньої програми полягають в підготовці висококваліфікованих та конкурентоспроможних фахівців з ґрунтованими компетентностями у розробці та впровадженні сучасних систем управління інформаційною безпекою, здатних використовувати у своїй професійній діяльності знання: законодавчої, нормативно-правової бази України та вимог відповідних, в тому числі 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; автоматизованих систем проєктування.

Освітньо-професійна програма “Управління інформаційною безпекою” базується на загальновідомих наукових і практичних результатах в галузі інформаційної безпеки, у рамках яких можлива подальша професійна кар’єра і подальше навчання.

В освітньо-професійній програмі визначені програмні компетентності. Вони розділені на загальні та фахові та найбільш відповідні для даної програми. Фахові компетентності мати практичний характер і можуть бути використані у професійній діяльності.

Навчальний план підготовки бакалаврів освітньо-професійної програми “Управління інформаційною безпекою” за спеціальністю 125 “Кібербезпека” повністю відповідає завданням освітньо-професійної програми.

Загалом, послідовність вивчення дисциплін, навчальний план та графік навчального процесу, перелік та обсяг нормативних та вибіркових дисциплін, структурно-логічна схема відповідають критеріям підготовки здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю 125 “Кібербезпека”, дозволяють отримати загальні та фахові компетентності Стандарту вищої освіти за спеціальністю 125 “Кібербезпека”, та покликані сприяти забезпеченню відповідності програмних результатів навчання запитам потенційних роботодавців (стейкхолдерів).

Завідувач кафедри кібербезпеки та
інформаційних технологій Харківського
національного економічного університету
ім. С. Кузнеця д.т.н., проф. Сергій ЄВСЕЄВ

ХНЕУ ім.С.Кузнеця
ЗАСВІДЧУЮ
ВЧЕНИЙ СЕКРЕТАР