(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Адміністративний менеджмент у сфері захисту інформації»

Другого (магістерського) рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

СМЯ НАУ 09.01.08 – 03 – 2021

Освітньо-професійна програма
Затверджена Вченою радою
протокол № 5 від 29.06.2021р.

Вводиться в дію наказом ректора
Ректор

М.Луцький

наказ № 320/од від 01.06.2021р

КИЇВ

Стандарт вищої освіти України: другий (магістерський) рівень, галузь знань 12 – Інформаційні технології, спеціальність 125 – Кібербезпека. Затверджено і введено в дію наказом Міністерства освіти і науки України від 18.03.2021 р. № 332

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

_____ (Нестеренко К.С.)

ПОГОДЖЕНО

Кафедрою безпеки інформаційних технологій

протокол засідання № 4а

від "5" 05 2021 р.

Завідувач кафедри

_____ (Корченко О.Г.)

ПОГОДЖЕНО

Студентською радою Факультету кібербезпеки, комп'ютерної та програмної інженерії

протокол № 21/5-н-ФКІКПІ

від "11" травня 2021 р.

Голова Студентської ради

Факультету кібербезпеки, комп'ютерної та програмної інженерії

_____ (Прощаваєв В.)

ПЕРЕДМОВА

Розроблено робочою групою освітньо-професійної програми (спеціальності 125 Кібербезпека, рік вступу – 2021-й та наступні до нової редакції освітньої програми) у складі:

ГАРАНТ ОСВІТНЬОЇ ПРОГРАМИ:

ІВАНЧЕНКО Є.В., к.т.н., проф., професор кафедри безпеки інформаційних технологій _____

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

КОРЧЕНКО О.Г., д.т.н., проф., завідувач кафедри безпеки інформаційних технологій _____ (підпис)

БРИЛЬ В.М., к.т.н., проф., професор кафедри безпеки інформаційних технологій _____ (підпис)

ХОХЛАЧОВА Ю.Є., к.т.н., доц., доцент кафедри безпеки інформаційних технологій _____ (підпис)

КАРАУШ К.О., студентка кафедри безпеки інформаційних технологій, групи КІ-171М _____ (підпис)

ЗОВНІШНІЙ СТЕЙКХОЛДЕР
ЛАХНО В.А., д.т.н., проф., завідувач кафедри комп'ютерних систем і мереж Національного університету біоресурсів і природокористування України _____ (підпис)

Рецензії-відгуки зовнішніх стейкхолдерів (додаються).

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	Магістр Магістр з кібербезпеки
1.3.	Офіційна назва освітньо-професійної програми та спеціалізації (за наявності)	Адміністративний менеджмент у сфері захисту інформації
1.4.	Тип диплому та обсяг освітньо-професійної програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 рік 4 місяці
1.5.	Акредитаційна інституція	Акредитовано, Акредитаційна комісія Міністерства освіти і науки України, сертифікат про акредитацію УД 11008106 від 27 грудня 2018 р.
1.6.	Період акредитації	1 липня 2023 р.
1.7.	Цикл/рівень	Другий (магістерський) рівень 7 рівень Національної рамки кваліфікацій України (НРК України), другий цикл Європейського простору вищої освіти (FQ-EHEA), 7 рівень Європейської рамки кваліфікацій для навчання впродовж життя (EQF-LLL).
1.8.	Передумови	Наявність ступеня бакалавра
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 освітньо-професійної програми полягає в підготовці висококваліфікованих та конкурентоспроможних фахівців на глобальному ринку праці, які володіють достатніми ґрунтовними компетентностями для ефективного виконання завдань інноваційного характеру у сфері захисту інформації; розробці, використанні та впровадженні сучасних технологій забезпечення інформаційної та кібербезпеки, а опанування специфічних знань особливостей професійної діяльності в авіаційному секторі, дозволяє вирішувати практичні завдання підвищення рівня безпекових процесів в авіаційній галузі. ОПП «Адміністративний менеджмент у сфері захисту інформації» 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'єкт діяльності:* – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; – інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; – процеси управління інформаційною безпекою та/або кібербезпекою об'єктів, що підлягають захисту; – технології, методи, моделі та засоби інформаційної

		безпеки та/або кібербезпеки. *Цілі навчання:* Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері управління інформаційною та/або кібербезпекою. *Теоретичний зміст предметної області. Знання:* теоретичних засад наукоємних технологій; міжнародних стандартів і практик щодо здійснення професійної діяльності; принципів створення та супроводу складних систем; моделювання та оптимізації безпекових процесів; теорії, моделей та принципів управління кібербезпекою, методів побудови та аналізу криптосистем, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки. *Методи, методики та технології:* Методи, моделі, методики та технології створення, аналізу та управління системами інформаційної безпеки, а також методи та моделі розробки та 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), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
3.2.	Орієнтація освітньо-професійної програми	Освітньо-професійна програма має прикладну орієнтацію. Акцентована на здобуття студентами знань, умінь, навичок та інших компетентностей для успішного здійснення професійної діяльності, а також на розвиток здатності розв'язувати складні задачі і проблеми в галузі інформаційних технологій та адміністративного управління в сфері захисту інформації, у рамках яких можлива подальша професійна кар'єра і подальше навчання.
3.3.	Основний фокус освітньо-професійної програми та спеціалізації	Загальна вища освіта в галузі «Інформаційні технології» з поглибленою спеціалізованою підготовкою в сфері інформаційної та кібербезпеки, в тому числі моделювання, оптимізації та адмініструванні безпекових процесів в сфері захисту інформації. Ключові слова: кібербезпека, інформаційна безпека, криптографічний захист інформації, захист персональних даних, захист інформації, захист від несанкціонованого доступу, електронний цифровий підпис.
3.4.	Особливості освітньо-професійної програми	Програма передбачає вивчення: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і

		практик щодо здійснення професійної діяльності; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління захистом інформації; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів технічного та крипто-графічного захисту інформації; – автоматизованих систем проєктування засобів захисту інформації. 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. Проведений аналіз показав необхідність продовжувати формування та реалізацію моделі підготовки фахівців з акцентом на технічний напрям ІТ підприємств, та урахуванням потреб сучасної транспортної, а саме, авіаційної галузі України. 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 підготовлені до роботи за національним класифікатором України : - фахівець із організації інформаційної безпеки; - фахівець із організації захисту інформації з обмеженим доступом; - фахівець з режиму секретності ; - фахівець з розроблення комп'ютерних програм; - фахівець з інформаційних технологій; - інспектор з організації захисту секретної інформації.
4.2.	Подальше навчання	Право продовжити навчання на третьому (освітньо-науковому) 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, виробнича та переддипломна практика на підприємствах, підготовка кваліфікаційної роботи.
5.2.	Оцінювання	Усні та письмові екзамени, лабораторні звіти, курсові роботи, презентації, поточний контроль, Єдиний державний кваліфікаційний іспит, захист кваліфікаційної роботи.
Розділ 6. Програмні компетентності		
6.1.	Інтегральна Компетентність (ІК)	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
6.2.	Загальні компетентності (ЗК)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Здатність проводити дослідження на відповідному рівні. ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.

		ЗК4. Здатність оцінювати та забезпечувати якість виконуваних робіт. ЗК5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
6.3.	Фахові компетентності (ФК)	ФК1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. ФК2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. ФК3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. ФК4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. ФК5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ФК6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ФК7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. ФК8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ФК9. Здатність аналізувати, розробляти і супро-

		воджувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. ФК10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки. ФК11. Здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати та захищати прийняті рішення. ФК12. Здатність організовувати роботу колективів виконавців, приймати управлінські рішення в умовах спектра думок, визначати порядок виконання робіт, вибирати оптимальні рішення при створенні систем захисту інформації. ФК13. Здатність готувати та здійснювати публічні виступи з презентацією отриманих результатів, готувати науково-технічні публікації (звіти, статті тощо) за результатами виконаних досліджень.
Розділ 7. Програмні результати навчання		
7.1.	Програмні результати навчання	ПРН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес/операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН2. - інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах; - критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. ПРН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. ПРН5. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

		ПРН6. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. ПРН7. - аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки; - виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації ПРН8. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. ПРН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. ПРН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. ПРН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ПРН12. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. ПРН13. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. ПРН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому. ПРН15. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. ПРН16. Приймати обґрунтовані рішення з

		організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. ПРН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання. ПРН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. ПРН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. ПРН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. ПРН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. ПРН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
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 ЄС.
9.3.	Навчання іноземних здобувачів вищої освіти	Створено умови для навчання іноземних здобувачів вищої освіти.

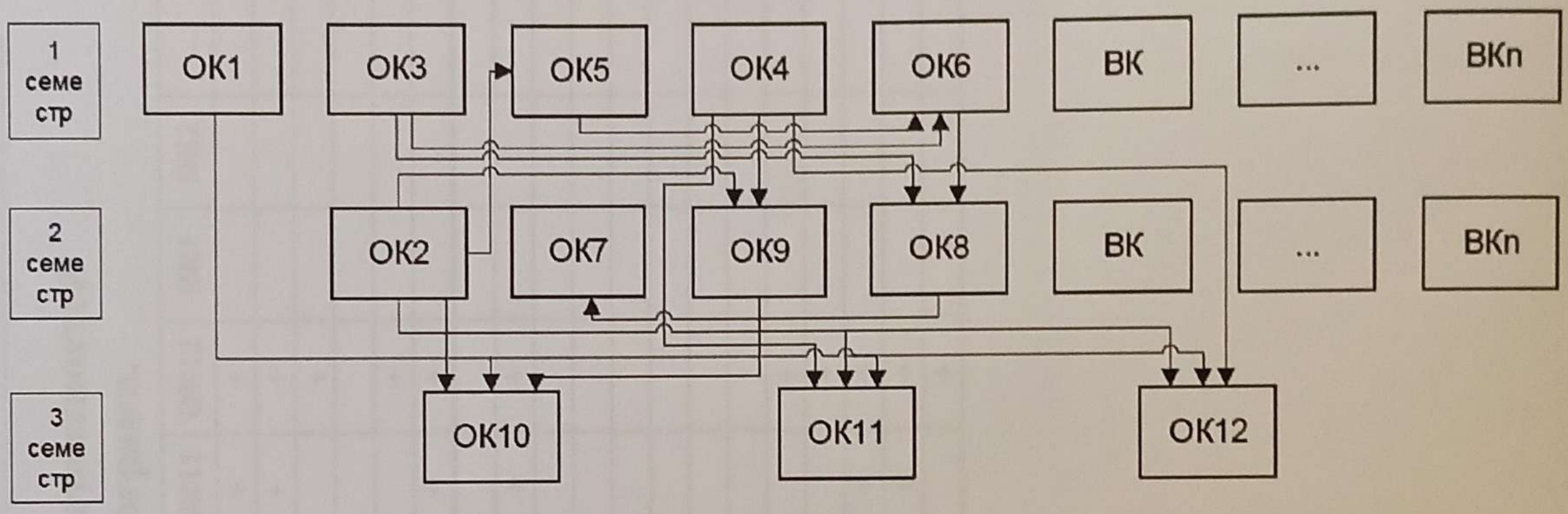
2. Перелік компонент освітньо-професійної програми та їх логічна послідовність

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.	Ділова іноземна мова	3,5	Екзамен	1
ОК 2.	Наукові комунікації у фаховій діяльності	3,5	Диференційований залік	2
ОК 3.	Методи побудови та аналізу криптосистем	3,5	Екзамен	1
ОК 4.	Методологія прикладних досліджень у сфері кібербезпеки (в т.ч. курсовий проєкт)	4,0	Диференційований залік	1
ОК 5.	Моделювання та оптимізація безпекових процесів авіаційної галузі	3,5	Екзамен	1
ОК 6.	Організаційні моделі кібербезпеки	3,5	Диференційований залік	1
ОК 7.	Аудит інформаційної безпеки	6,0	Екзамен	2
ОК 8.	Інтелектуалізовані системи інформаційної безпеки (в т.ч. курсова робота)	7,0	Екзамен	2
ОК 9.	Науково-дослідна практика в області адміністративного менеджменту у сфері захисту інформації	4,5	Диференційований залік	2
ОК 10	Переддипломна практика	10,5	Диференційований залік	3
ОК 11	Єдиний державний кваліфікаційний іспит	1,5	Екзамен	3
ОК 12	Кваліфікаційна робота	15,0	Захист	3
Загальний обсяг обов'язкових компонент:		66 кредитів		
Вибіркові компоненти*				
ВК 1.	Дисципліна 1	4,0	Диференційований залік	
ВК 2.	Дисципліна 2	4,0	Диференційований залік	
…	…			
ВК n.	Дисципліна n	4,0	Диференційований залік	
Загальний обсяг вибіркових компонент*		24 кредити		
Загальний обсяг освітньо-професійної програми		90 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 Єдиного державного кваліфікаційного іспиту та захисту кваліфікаційної роботи та завершується видачею документу встановленого зразка про присудження йому освітньої кваліфікації: Магістр з кібербезеки.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має передбачати розв'язання складної задачі у сфері кібербезпеки, 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 ЕК. Для виступу здобувачеві вищої освіти надається до 15 хвилин. 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	ОК12	ВК1	ВК2	…	ВКп
ІК	+	+	+	+	+	+	+	+	+	+	+	+				
ЗК1		+	+	+		+	+	+	+	+	+	+				
ЗК2	+	+	+		+	+	+	+	+	+		+				
ЗК3		+		+		+		+								
ЗК4		+		+	+	+	+	+				+				
ЗК5	+	+								+	+	+				
ФК1				+				+								
ФК2	+	+		+	+	+	+				+	+				
ФК3			+	+	+	+	+		+	+						
ФК4						+	+	+	+							
ФК5					+	+		+								
ФК6			+			+		+		+						
ФК7				+	+	+	+		+							
ФК8			+					+								
ФК9				+		+	+		+	+		+				
ФК10		+		+					+	+		+				
ФК11	+	+		+					+	+	+	+				
ФК12		+		+					+	+	+	+				
ФК13		+					+		+	+		+				

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

	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ВК1	ВК2	…	ВКп
ПРН1	+								+	+	+	+				
ПРН2		+		+		+			+	+	+	+				
ПРН3		+	+	+		+										
ПРН4			+			+	+	+	+	+		+				
ПРН5	+	+		+	+	+	+					+				
ПРН6			+		+	+		+								
ПРН7				+	+		+									
ПРН8				+		+	+					+				
ПРН9			+	+	+			+								
ПРН10					+	+	+									
ПРН11		+		+	+	+			+	+	+	+				
ПРН12				+		+	+									
ПРН13			+	+	+	+	+					+				
ПРН14						+		+	+	+	+	+				
ПРН15		+		+	+	+			+	+	+	+				
ПРН16				+		+	+									
ПРН17		+		+		+			+	+	+	+				
ПРН18		+		+					+	+		+				
ПРН19			+	+		+	+					+				
ПРН20		+		+								+				
ПРН21						+		+								
ПРН22									+	+	+	+				
ПРН23			+	+				+								

РЕЦЕНЗІЯ-ВІДГУК
на освітньо-професійну програму
«Адміністративний менеджмент у сфері захисту інформації»
Спеціальності 125 «Кібербезпека»
другого (магістерського) рівня вищої освіти

Рецензована освітньо-професійна програма «Адміністративний менеджмент у сфері захисту інформації» розроблена колективом кафедри безпеки інформаційних технологій факультету кібербезпеки, комп'ютерної та програмної інженерії.

Освітньо-професійна програма «Адміністративний менеджмент у сфері захисту інформації» за спеціальністю 125 «Кібербезпека» розроблена з урахуванням вимог потенційних роботодавців, які підтвердили потребу у фахівцях цієї спеціальності.

В основі освітньо-професійної програми визначені програмні компетентності виходячи із завдань спеціальності. Вони розподілені на загальні та фахові компетентності. Зміст усіх компетентностей орієнтовано на знання та уміння з використання новітніх методів та підходів забезпезпечення кібербезпеки. Усі компетентності носять практичний характер і можуть бути використані у професійній діяльності майбутніх фахівців.

Освітньо-професійна програма містить систему освітніх компонентів, які вбудовані в логічній послідовності вивчення, що забезпечує формування ряд відповідних фахових компетентностей та дозволить підготувати фахівців другого (магістерського) рівня вищої освіти.

Мета освітньо-професійної програми полягає в підготовці висококваліфікованих, конкурентоспроможних фахівців за другим (магістерським) рівнем у галузі 125 «Кібербезпека» та забезпечення фундаментальної підготовки у вигляді поглиблених теоретичних і практичних знань, умінь та навичок, достатніх для ефективного виконання задач дослідницького та/або інноваційного характеру у сфері захисту інформації.

Зазначений в освітньо-професійній програмі об'єкт діяльності цілком відповідає сучасним потребам ІТ-галузі та забезпечення інформаційної та\або кібербезпеки.

Особливої уваги заслуговує орієнтація освітньо-професійної програми, зокрема, підготовка висококваліфікованих і креативних спеціалістів, які володіють навичками науково-дослідницького й інноваційного характеру та спроможні проводити наукові дослідження, вирішувати певні проблеми та завдання у сфері забезпечення інформаційної та\або кібербезпеки.

Освітньо-професійна програма «Адміністративний менеджмент у сфері захисту інформації» спеціальності 125 «Кібербезпека» повністю відповідає кваліфікаційній характеристиці випускників з повною вищою освітою за освітньо-кваліфікаційним рівнем «Магістр» і сприяє забезпеченню відповідності результатів навчання запитам потенційних роботодавців.

Завідувач кафедри
комп'ютерних систем і мереж
Національного університету
біоресурсів і природокористування
України, д.т.н., проф. В.А. Лахно

Підпис завідувача
пров. фахівець ВК

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ВІДДІЛ КАДРІВ
М. КИЇВ