(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Системи технічного захисту інформації, автоматизація її обробки»

Другого (магістерського) рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

СМЯ НАУ ОПП 09.01.10 –03– 2021

Освітньо-професійна програма
затверджена Вченою радою Університету
Протокол № 4 від 11.04. 2021 р.

Вводиться в дію наказом ректора
Ректор
_____ М. Луцький
Наказ № 246/о від 19.04. 2021 р.

Із змінами,
внесеними на підставі результатів
перегляду освітньої програми,
відповідно до наказу ректора
від 07.06.2022 № 143/од

НАЧАЛЬНИК НМВ НАУ

Для вступників на навчання, починаючи з 2023 року вступу, освітньо-професійна програма переведена на спеціальність 125 Кібербезпека та захист інформації (рішення Вченої ради від 15.02.2023 р., протокол № 2, введене в дію наказом ректора від 23.02.2023 р. № 069/од; підстава: зміни до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, внесені постановою Кабінету Міністрів України від 16.12.2022 р. № 1392).

НАЧАЛЬНИК НМВ НАУ

Стандарт вищої освіти України: другий (магістерський) рівень
галузь знань 12 «Інформаційні технології»
спеціальність 125 «Кібербезпека»
Стандарт вищої освіти затверджено і введено в дію наказом Міністерства освіти і науки України від «18» березня 2021 р. № 332

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

ПОГОДЖЕНО
Науково-методичною радою
Національного авіаційного університету
протокол № 3
від «20» 04 2021 р.
Голова Науково-методичної ради
проректор з навчальної роботи
_____________ А. Полухін

ПОГОДЖЕНО
Вченою радою Факультету кібербезпеки, комп'ютерної та програмної інженерії
протокол № 5
від «15» квітня 2021 р.
Голова Вченої ради факультету
_____________ К. Нестеренко

ПОГОДЖЕНО
Кафедрою засобів захисту інформації
протокол засідання № 8
від «14» квітня 2021 р.
Завідувач кафедри
_____________ В. Козловський

ПОГОДЖЕНО
Студентською радою Факультету кібербезпеки, комп'ютерної та програмної інженерії
протокол № 1/4.04.2021
від «14» квітня 2021 р.
Голова студентської ради
_____________ В. Прощаваєв

ПЕРЕДМОВА

РОЗРОБЛЕНО РОБОЧОЮ ГРУПОЮ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ (спеціальності 125 «Кібербезпека») у складі:

ГАРАНТ ОСВІТНЬОЇ ПРОГРАМИ:

ЛАЗАРЕНКО С.В. – д.т.н., доцент, професор кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії

(підпис)

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

КОЗЛОВСЬКИЙ В.В. – д.т.н., професор, завідувач кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії

(підпис)

ТЕМНІКОВ В.О. – д.т.н., доцент, професор кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії

(підпис)

ШВЕЦЬ В.А. – к.т.н., доцент, доцент кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії

(підпис)

МАРТИНЮК Г.В. – (к.т.н., доцент, доцент кафедри засобів захисту інформації Факультету кібербезпеки, комп'ютерної та програмної інженерії)

(підпис)

Бурекін Максим Павлович

(П.І.Б. здобувача вищої освіти)

(підпис здобувача вищої освіти)

ЗОВНІШНІ СТЕЙКХОЛДЕРИ

Савченко В.А. – д.т.н., професор, директор Навчально-наукового інституту захисту інформації Державного університету телекомунікацій

(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 засобів захисту інформації
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)	Системи технічного захисту інформації, автоматизація її обробки
1.4.	Тип диплому та обсяг освітньо-професійної програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 рік 4 місяці(денна форма навчання)/ 1 рік 4 місяці (заочна форма навчання).
1.5.	Акредитаційна інституція	Міністерство освіти і науки України, рішення Акредитаційної комісії від 12.11.2018 сертифікат серія УД № 11005811
1.6.	Період акредитації	До 01.07.2023 р., чергова
1.7.	Цикл/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	Вища освіта зі ступенем бакалавр
1.9.	Форма навчання	Інституційна з елементами дистанційної: очна, заочна, мережева.
1.10.	Мова(и) викладання	Українська
1.11.	Інтернет-адреса постійного розміщення опису освітньо-професійної програми	http://www.nau.edu.ua http://www.kzzi.nau.edu.ua
Розділ 2. Ціль освітньо-професійної програми		
2.1.	Ціллю ОПП «Системи технічного захисту інформації, автоматизація її обробки» є підготовка фахівців, які володіють сучасними загально-науковими й спеціальними знаннями та технологіями інформаційної та/або кібербезпеки, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. Опанування специфічних знань особливостей професійної діяльності в авіаційному секторі, застосування яких дозволяє вирішувати практичні завдання підвищення рівня безпеки в авіації. ОПП «Системи технічного захисту інформації, автоматизація її обробки» відповідає місії НАУ, у якій наголошується, щодо внеску НАУ у розвиток суспільства на національному та міжнародному рівнях через генерацію нових знань та інноваційних ідей на основі інтеграції та інтернаціоналізації освіти, досліджень і практики, так і надання високоякісних освітніх та науково-дослідних послуг громадянам України та іноземцям 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*: системи та комплекси технічного захисту інформації на об'єктах інформаційної діяльності; системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків). *Теоретичний зміст предметної області*: теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки.
3.2.	Орієнтація освітньо-професійної програми	Програма має прикладну орієнтацію. Освітньо-професійна програма базується на загальновідомих наукових результатах в галузі інформаційних технології, інформаційної безпеки та/або кібербезпеки 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 та професійна підготовка в галузі 12 – «Інформаційні технології» за спеціальністю 125 – «Кібербезпека». Ключові слова: технічний захист інформації, автоматизовані системи захисту інформації, обробка інформації з обмеженим доступом
3.4.	Особливості освітньо-професійної програми	Об'єкти вивчення: – 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; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; – інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних

		(інформаційних потоків); – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою; – технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. На відміну від інших освітніх програм увага приділяється автоматизованим системам та комплексам технічного захисту інформації.
Розділ 4. Придатність випускників до працевлаштування та подальшого навчання		
4.1.	Придатність до працевлаштування	Випускники отримують можливість працевлаштування до підприємств (організацій, установ) різних форм власності в галузі «Інформаційних технологій» за спеціальністю «Кібербезпека» на відповідні посади та обіймати посади в інших секторах економіки, при наявності сертифікатів про опанування відповідних програм підготовки.
4.2.	Подальше навчання	Продовження навчання за третім (освітньо-науковим) рівнем вищої освіти для отримання ступеня «Доктор філософії», отримання другої вищої освіти.
Розділ 5. Викладання та оцінювання		
5.1.	Викладання та навчання (методи, методики, технології, інструменти та обладнання)	*Методи, методики та технології*: Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. *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.
5.2.	Оцінювання	Усні, письмові, творчі, тестові та комбіновані екзамени, диференційовані заліки, лабораторні звіти, звіти із практичних робіт та практик, реферати, захист курсових проектів, презентації, поточний контроль та захист кваліфікаційної роботи.
Розділ 6. Програмні компетентності		
6.1.	Інтегральна компетентність (ІК)	ІК1. 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. КЗ4. 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.

6.3.	Фахові компетентності (ФК)	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 супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі

6.3.	Фахові компетентності (ФК)	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 проводити ліцензування, атестацію та сертифікацію об'єктів інформаційної діяльності. ФК12. Здатність розробляти проектну документацію, програми та методики випробувань та організовувати тестування і налагодження комплексів засобів захисту та охорони об'єктів інформаційної діяльності.
Розділ 7. Програмні результати навчання		
7.1.	Програмні результати навчання (ПРН)	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. 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. 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. ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту,

7.1.	Програмні результати навчання (ПРН)	технології створення та використання спеціалізованого програмного забезпечення. ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. 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 та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. ПРН13. 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. 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.

7.1.	Програмні результати навчання (ПРН)	ПРН15. 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. 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. ПРН19. 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

7.1.	Програмні результати навчання (ПРН)	знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації. ПРН24. Визначати відомості, які відносяться до інформації з обмеженим доступом, організовувати допуск та доступ персоналу до інформації з обмеженим доступом згідно чинного законодавства та встановленої політики інформаційної та/або кібербезпеки. ПРН25. Організовувати внутрішньо-об'єктовий та пропускний режими на підприємстві. ПРН26. Здійснювати оцінювання захищеності інформації, що циркулює на об'єкті інформаційної діяльності. ПРН27. Використовувати методи та засоби пошуку закладних пристроїв.
Розділ 8. Ресурсне забезпечення реалізації програми		
8.1.	Кадрове забезпечення	Кадрове забезпечення відповідає ліцензійним вимогам. 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. В процесі організації навчального процесу залучаються професіонали з досвідом дослідницької, управлінської, інноваційної, творчої та фахової роботи, іноземні лектори.
8.2.	Матеріально-технічне забезпечення	Матеріально-технічна база випускової кафедри засобів захисту інформації дозволяє забезпечити підготовку фахівців на першому (бакалаврському) рівні вищої освіти за ОПП: – забезпеченість комп'ютерними робочими місцями та прикладними комп'ютерними програмами достатнє для виконання навчальних планів; – усі комп'ютери кафедри під'єднані до локальної мережі університету з можливістю виходу в глобальну мережу Інтернет; – для ведення документації та забезпечення навчально-методичними матеріалами освітнього процесу кафедра в достатній кількості забезпечена оргтехнікою (принтерами, МФУ, сканерами); – навчальні лабораторії оснащені технічними засобами та спеціалізованим програмним забезпеченням, необхідними приладами та обладнанням (охоронними

8.2.	Матеріально-технічне забезпечення	системами відеоспостереження, засобами та комплексами виявлення закладних пристроїв, засобами просторового та мережевого захисту інформації). Усі приміщення відповідають будівельним та санітарним нормам, гуртожитками забезпечені усі потребуючі, наявна соціальна інфраструктура включає спортивний комплекс, пункти харчування, центр творчості, медпункт і базу відпочинку. З метою якісної підготовки студентів використовуються охоронні системи відеоспостереження, засоби та комплекси виявлення закладних пристроїв, засоби просторового та мережевого захисту інформації.
8.3	Інформаційне та навчально-методичне забезпечення	Забезпечення навчальною та навчально-методичною літературою, доступ до фахових періодичних видань професійного спрямування, упровадження електронного каталогу та можливість роботи з електронними підручниками здійснюється за рахунок фондів Науково-технічної бібліотеки НАУ. Всі студенти забезпечені підручниками та навчальними посібниками з компонентів ОПП. Відповідне інформаційне та навчально-методичне забезпечення розташоване на освітніх платформах Google Classroom, Moodle (Modular Object-Oriented Dynamic Learning Environment). 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	Національна кредитна мобільність здобувачів вищої освіти, наукових і науково-педагогічних працівників, у т.ч. навчання, стажування, проведення наукових досліджень, викладання та підвищення кваліфікації організовується на підставі партнерських угод про співпрацю між Національним авіаційним університетом та закладами вищої освіти в Україні: – Національним технічним університетом

		України «Київським політехнічним інститутом імені Ігоря Сікорського»; – Харківським національним університетом радіоелектроніки.
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 компонентів

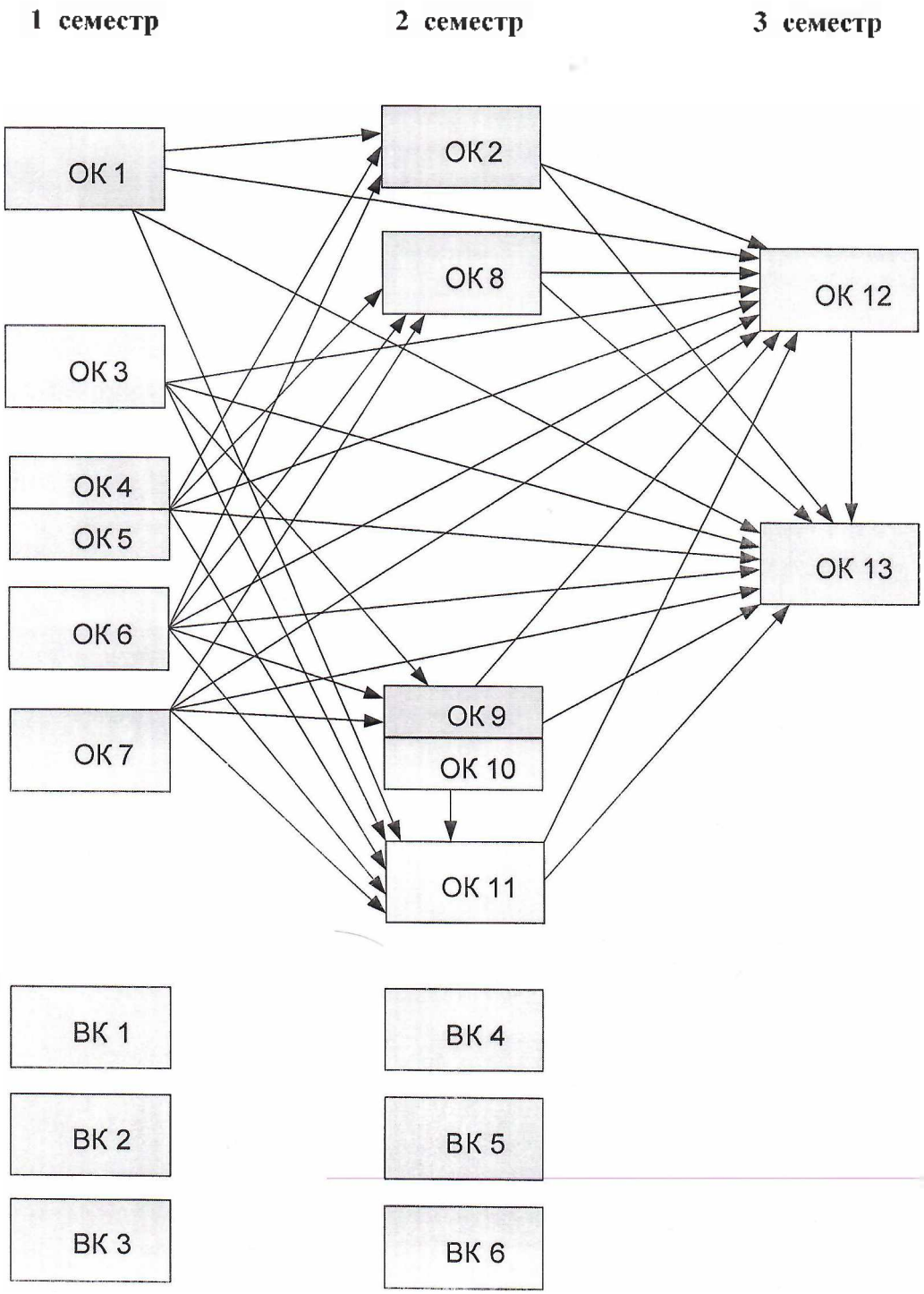
Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю	Семестр (відповідно до форми навчання)	
				денна	заочна
1	2	3	4	5	6
Обов'язкові компоненти					
ОК1.	Ділова іноземна мова	3.5	Екзамен	1	1
ОК2.	Наукові комунікації у фаховій діяльності	3.5	Диференційований залік	2	1, 2
ОК3.	Методи побудови та аналізу криптосистем	3.5	Екзамен	1	1
ОК4.	Методологія прикладних досліджень у сфері кбербезпеки	2.5	Диференційований залік	1	1
ОК5.	Курсовий проект з Методології прикладних досліджень у сфері кбербезпеки	1.5	Захист	1	1
ОК6.	Моделювання та оптимізація безпекових процесів авіаційної галузі	3.5	Екзамен	1	1
ОК7.	Безпека в кібернетичному просторі	3.5	Диференційований залік	1	1
ОК8.	Спеціальні вимірювання	6.0	Екзамен	2	1, 2
ОК9.	Автоматизація обробки інформації з обмеженим доступом	6.0	Диференційований залік	2	1, 2

1	2	3	4	5	6
ОК10.	Курсова робота з Автоматизації обробки інформації з обмеженим доступом	1.0	Захист	2	2
ОК11.	Науково-дослідна практика у сфері систем технічного захисту інформації, автоматизації її обробки	4.5	Диферен-ційований залік	2	2
ОК12.	Переддипломна практика	10.5	Диферен-ційований залік	3	3
ОК13.	Кваліфікаційна робота	16.5	Захист	3	3
Загальний обсяг обов'язкових компонентів:		66 кредитів ЄКТС			
Вибіркові компоненти*					
ВК1.	Дисципліна 1	4.0	Диферен-ційований залік	1	1
ВК2.	Дисципліна 2	4.0	Диферен-ційований залік	1	1
ВК3.	Дисципліна 3	4.0	Диферен-ційований залік	1	1
ВК4.	Дисципліна 4	4.0	Диферен-ційований залік	2	1, 2
ВК5.	Дисципліна 5	4.0	Диферен-ційований залік	2	1, 2
ВК6.	Дисципліна 6	4.0	Диферен-ційований залік	2	1, 2
Загальний обсяг вибіркових компонентів*		24 кредити ЄКТС			
Загальний обсяг освітньо-професійної програми		90 кредитів ЄКТС			

* *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 (денна форма навчання)



3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здобувачів ОС «Магістр» здійснюється у формі публічного захисту кваліфікаційної магістерської роботи і завершується видачою документу встановленого зразку про присудження їм освітнього ступеня «Магістр» із присвоєнням освітньої кваліфікації: «Магістр з кібербезпеки», за спеціальністю 125 «Кібербезпека».
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій. Кваліфікаційна робота магістра не повинна містити академічного плагіату, у тому числі некоректних текстових запозичень, фабрикації та фальсифікації. Кваліфікаційна робота має бути розміщена на сайті Університету або його структурного підрозділу, або у репозитарії.
Вимоги до публічного захисту (демонстрації)	Публічний захист кваліфікаційної магістерської роботи відбувається на засіданні екзаменаційної комісії. Порядок захисту передбачає представлення здобувача й поданих документів; виступ здобувача; відповіді здобувача на запитання членів екзаменаційної комісії та присутніх. Виступ здобувача має супроводжуватись презентацією.

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

Компоненти / Компетентності	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ВК1	ВК2	ВК3	ВК4	ВК5	ВК6
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
ІК1	+	+	+	+	+	+	+	+	+	+	+	+	+						
ЗК1	+	+	+	+	+	+	+	+	+	+	+	+	+						
ЗК2	+	+	+	+	+	+	+	+			+	+	+						
ЗК3		+	+	+	+	+	+				+	+	+						
ЗК4		+	+	+	+	+	+	+	+	+	+	+	+						
ЗК5	+	+		+	+	+	+	+	+	+	+	+	+						
ФК1	+	+		+	+	+	+				+	+	+						
ФК2	+		+	+	+	+	+	+	+	+	+	+	+						
ФК3			+	+	+	+	+	+			+	+	+						

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
ФК4	+					+	+		+	+	+	+	+						
ФК5		+		+	+	+	+	+			+	+	+						
ФК6						+	+		+	+	+	+	+						
ФК7				+	+	+	+	+			+	+	+						
ФК8			+	+	+			+			+	+	+						
ФК9						+	+				+	+	+						
ФК10	+	+	+	+	+	+	+	+	+	+	+	+	+						
ФК11							+		+	+	+	+	+						
ФК12		+		+	+		+	+			+	+	+						

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

Компоненти / Програмні результати навчання	ОК1	ОК2	ОК3	ОК4	ОК5	ОК6	ОК7	ОК8	ОК9	ОК10	ОК11	ОК12	ОК13	ВК1	ВК2	ВК3	ВК4	ВК5	ВК6
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
ПРН1	+	+		+	+						+	+	+						
ПРН2			+			+	+	+			+	+	+						
ПРН3		+	+	+	+			+			+	+	+						
ПРН4	+	+		+	+	+	+		+	+	+	+	+						
ПРН5	+	+				+	+				+	+	+						
ПРН6			+			+	+	+	+	+	+	+	+						
ПРН7	+	+				+	+	+	+	+	+	+	+						
ПРН8			+	+	+		+		+	+	+	+	+						
ПРН9						+	+		+	+	+	+	+						
ПРН10						+	+	+	+	+	+	+	+						
ПРН11						+	+		+	+	+	+	+						
ПРН12	+	+		+	+	+	+				+	+	+						
ПРН13			+	+	+						+	+	+						
ПРН14	+					+	+		+	+	+	+	+						
ПРН15		+		+	+	+	+	+	+	+	+	+	+						
ПРН16		+				+	+				+	+	+						
ПРН17	+	+	+	+	+	+	+	+	+	+	+	+	+						
ПРН18		+	+				+				+	+	+						
ПРН19	+	+		+	+	+	+	+			+	+	+						
ПРН20	+	+	+	+	+	+	+	+			+	+	+						
ПРН21				+	+	+	+	+			+	+	+						
ПРН22		+		+	+			+			+	+	+						
ПРН23	+		+			+	+	+	+	+	+	+	+						

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
ПРН24						+	+		+	+	+	+	+						
ПРН25						+	+		+	+	+	+	+						
ПРН26			+	+	+		+	+	+	+	+	+	+						
ПРН27				+	+	+	+	+			+	+	+						

6. Система внутрішнього забезпечення якості вищої освіти НАУ

Якість освітньо-професійної програми визначається внутрішньою системою забезпечення якості вищої освіти та освітньої діяльності НАУ, яка функціонує згідно з Положенням про систему забезпечення якості вищої освіти та освітньої діяльності, затвердженого рішенням вченої ради Університету від 28.11.2018 (протокол № 8) та відповідає вимогам Закону України «Про вищу освіту» від 01.07.2014 № 1556-VII (Розділ V Забезпечення якості вищої освіти, ст.16).

7. Перелік нормативних документів, на яких базується освітньо-профссійна програма

1. «Про освіту»: Закон України від 05.09.2017 № 2145-VIII [Електронний ресурс]. – режим доступу: http://zakon.rada.gov.ua/laws/show/2145-19

2. «Про вищу освіту»: Закон України від 01.07.2014 № 1556-VII [Електронний ресурс]. – режим доступу: http://zakon4.rada.gov.ua/laws/show/1556-18

3. Постанова Кабінету Міністрів України від 25.06.2020 р. № 519 «Про внесення змін у додаток до постанови Кабінету Міністрів України від 23 листопада 2011 р. № 1341».

4. Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти: Постанова Кабінету Міністрів України від 29.04.2015 р. № 266 [Електронний ресурс]. – режим доступу: http://zakon2.rada.gov.ua/laws/show/266-2015-%D0%BF

5. Класифікація видів економічної діяльності : ДК 009:2010. – На заміну ДК 009:2005; Чинний від 2012-01-01. – (Національний класифікатор України).

6. Класифікатор професій ДК 003:2010. – На заміну ДК 003:2005; Чинний від 2010-11-01. -(Національний класифікатор України).

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

8. Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.2016 № 96/2016.

9. Положення про освітні програми Національного авіаційного університету, погоджено Радою з якості НАУ (протокол від 28.04.2020 № 2) та уведено в дію наказом ректора від 07.05.2020 № 148/од.

(Ф 03.02 – 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки
1	ОЗОІ	08.02.22	Ковань О.М		

(Ф 03.02 – 02)

АРКУШ ОЗНАЙОМЛЕННЯ З ДОКУМЕНТОМ

№ пор.	Прізвище ім'я по-батькові	Підпис ознайомленої особи	Дата ознайом-лення	Примітки
1	Лазаренко Сергій Володимирович		08.02.2022	
2.	Лазаренко С.В.		08.06.2022	
3.	Лазаренко С.В		25.02.2023	
4	Ковалевський В.В.		27.02.2023	
5.	Шевць В.Я.		28.02.23	
6.	Шеробок Т.Л.		27.02.23	
7	Туровський О.Л		25.02.23	
8.	Мелешко Т.В		28.02.23	
9.	Чирва О.Л.		28.02.23	
10.	Сорокун А.Д.		28.02.23	

(Ф 03.02 – 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЇ

№ пор.	Прізвище ім'я по-батькові	Дата ревізії	Підпис	Висновок щодо адекватності
1	Лазаренко С.В	22.08.2022		Є актуальною, прот.
				№0 від 22.08.2022 (засідання [illegible]-прот. №5
				від 25.04.2022)
2	Лазаренко С.В.	28.08.2023		Є актуальною, прот.
				№7 від 28.08.2023 (засідання [illegible]-прот. №1
				від 31.01.2023)
3.	Лазаренко С.В	12.02.2024		[illegible] ОПП, прот.
				№4 від 12.02.2024

(Ф 03.02 – 03)

АРКУШ ОБЛІКУ ЗМІН

№ зміни	№ листа (сторінки)				Підпис особи, яка внесла зміну	Дата внесення зміни	Дата введення зміни
	Зміненого	Заміненого	Нового	Анульо-ваного			
1.	—	14-19	—	—		07.06.2022	01.07.2022
	Зміни внесено на підставі результатів перегляду ОПП						
	відповідно до наказу ректора від 07.06.2022 №147/од						

НАЧАЛЬНИК НМВ НАУ

(Ф 03.02 – 32)

УЗГОДЖЕННЯ ЗМІН

	Підпис	Ініціали, прізвище	Посада	Дата
Розробник				
Узгоджено				
Узгоджено				
Узгоджено				
Узгоджено				