ПРОЄКТ

(Ф 03.02 – 107)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний авіаційний університет

ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Безпека інформаційних і комунікаційних систем»

Другого (магістерського) рівня вищої освіти

за спеціальністю __125 «Кібербезпека та захист інформації»_____

галузі знань ____12 Інформаційні технології_____

СМЯ НАУ ОПП 18.02 – 04 – 2024

Освітньо-професійна програма
Затверджена Вченою радою Університету
Протокол №_____ від _____2024 р.

Вводиться в дію наказом ректора
Т.в.о. ректора
_____
Наказ №_____ від _____2024 р.

КИЇВ

Враховано Стандарт вищої освіти України: другого (магістерського) рівня, галузі 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 р. № 332.

ЛИСТ ПОГОДЖЕННЯ
освітньо-професійної програми

ПОГОДЖЕНО
Науково-методичною радою
Національного авіаційного університету
протокол №_____
від «_____»_____2024 р.
Голова Науково-методичної ради,
проректор з навчальної роботи
_____ Полухін А.В.

ПОГОДЖЕНО
Вченою радою Факультету кібербезпеки
та програмної інженерії
протокол №_____
від «_____»_____2024 р.
Голова вченої ради факультету
_____ Пономаренко О.В.

ПОГОДЖЕНО
Кафедрою комп‘ютеризованих систем
захисту інформації
протокол засідання №_____
від «_____»_____2024р.
Завідувач кафедри
_____ Степанов М.М.

ПОГОДЖЕНО
Студентською радою Факультету
кібербезпеки та програмної інженерії
протокол №_____
від «_____»_____2024 р.
Голова студентської ради
_____ Васьковська А.О.

ПЕРЕДМОВА

Розроблено робочою групою освітньо-професійної програми (спеціальності 125 «Кібербезпека та захист інформації»)

у складі:

ГАРАНТ ОСВІТНЬОЇ ПРОГРАМИ:

СТЕПАНОВ Михайло Миколайович	- д.т.н., с.н.с., завідувач кафедри комп'ютеризованих систем захисту інформації

_____
підпис гаранта

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

ІЛЬЄНКО Анна Вадимівна	- к.т.н., доц., доцент кафедри комп'ютеризованих систем захисту інформації

_____
підпис члена робочої групи

ВИСОЦЬКА Олена Олександрівна	- к.т.н., доц., доцент кафедри комп'ютеризованих систем захисту інформації

_____
підпис члена робочої групи

ПЕТРЕНКО Андрій Борисович	- к.т.н., доц., доцент кафедри комп'ютеризованих систем захисту інформації

_____
підпис члена робочої групи

ГАЛИЧ Євгенія Олександрівна	- здобувачка вищої освіти

_____
підпис здобувача вищої освіти

ЗОВНІШНІ СТЕЙКХОЛДЕРИ:

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, Навчально-науковий інститут неперервної освіти, Факультет кібербезпеки та програмної інженерії, кафедра комп'ютеризованих систем захисту інформації
1.2.	Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Освітній ступінь Магістр Магістр з кібербезпеки
1.3.	Офіційна назва освітньо-професійної програми	Безпека інформаційних і комунікаційних систем
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	Національне агентство із забезпечення якості вищої освіти
1.6.	Період акредитації	Термін дії сертифікату до 01.07.2023 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	Для здобуття освітнього рівня магістра можуть вступати особи, що здобули освітній рівень бакалавра. Програма фахових вступних випробувань для осіб, що здобули попередній рівень вищої освіти за іншими спеціальностями повинна передбачати перевірку набуття особою компетентностей та результатів навчання, що визначені стандартом вищої освіти зі спеціальності 125 Кібербезпека для першого (бакалаврського) рівня вищої освіти.
1.9.	Форма навчання	Очна (денна), заочна
1.10	Мова(и) викладання	Українська
1.11	Інтернет-адреса постійного розміщення опису освітньої програми	http://www.nau.edu.ua http://www.kszi.nau.edu.ua
Розділ 2. Ціль освітньо-професійної програми		
2.1.	Ціль освітньої-професійної програми «Безпека інформаційних і комунікаційних систем» полягає в підготовці висококваліфікованих, конкурентоспроможних фахівців за другим (магістерським) рівнем за спеціальністю 125 «Кібербезпека та захист інформації» та забезпечення студентів фундаментальною підготовкою у вигляді поглиблених теоретичних і практичних знань, умінь та навичок, достатніх для ефективного виконання завдань інноваційного характеру та відповідного рівня професійної діяльності в галузі захисту інформації; оволодіння студентами знаннями,	

	вміннями та навичками з проєктування, експлуатації та впровадження сучасних технологій, методів та засобів забезпечення безпеки інформаційних і комунікаційних систем. ОПП «Безпека інформаційних і комунікаційних систем» відповідає місії НАУ, у якій наголошується щодо внеску НАУ у розвиток суспільства на національному та міжнародному рівнях через генерацію нових знань та інноваційних ідей і надання високоякісних освітніх та науково-дослідних послуг громадянам України та іноземцям під час підготовки фахівців з кібербезпеки з урахуванням специфіки авіаційної галузі. У ОПП немає аналогів серед ЗВО України щодо врахування галузевого контексту функціонування авіаційного сектору.У ОПП немає аналогів серед ЗВО України щодо врахування галузевого контексту функціонування авіаційного сектору.	
Розділ 3. Характеристика освітньо-професійної програми		
3.1	Предметна область (об’єкт діяльності, теоретичний зміст)	**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. **Цілі навчання:** Підготовка фахівців, здатних розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. **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. Базується на загальновідомих положеннях, результатах сучасних наукових досліджень та нових знаннях у сфері кібербезпеки, необхідних для майбутньої професійної діяльності магістрів, здатних вирішувати певні проблеми і задачі за умови оволодіння системою компетентностей.
3.3.	Основний фокус освітньо-професійної програми	Спеціальна освіта та професійна підготовка в галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека та захист інформації Ключові слова: кібербезпека, криптосистема, технології забезпечення безпеки інформації
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; методів та засобів організації і впровадження комплексу заходів щодо забезпечення кібербезпеки; структурних моделей організації систем безпеки інформаційних мереж та програмно-апаратних комплексів захисту інформації; методів та засобів технічного та криптографічного захисту інформації тощо. Відмінність програми – реалізація моделі підготовки фахівців в сфері безпеки інформаційних і комунікаційних систем з урахуванням потреб ІТ ринку, а також авіаційної галузі України.
Розділ 4. Придатність випускників до працевлаштування та подальшого навчання		
4.1.	Придатність до працевлаштування	Випускники підготовлені до роботи у сфері кібербезпеки в складі відповідних служб захисту інформації організацій, підприємств та банків; у сфері розробки, впровадження і експлуатації програмних та програмно-апаратних комплексів та засобів захисту інформації; в галузі кібербезпеки в складі правоохоронних органів; у сфері забезпечення кібербезпеки в кіберпросторі (зокрема, на об'єктах критичної інфраструктури, в службах та підрозділах авіаційної безпеки)
4.2.	Подальше навчання	Право продовжити навчання на третьому (освітньонауковому) 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)	Ґрунтуються на принципах студентоцентризму та індивідуально-особистісного підходу; реалізуються через навчання на основі досліджень, посилення практичної орієнтованості та творчої спрямованості у формі комбінації лекцій, практичних занять, самостійної навчальної і дослідницької роботи, розв'язування прикладних задач, виконання проєктів, навчальних та виробничих практик, курсових робіт (проектів), кваліфікаційної роботи. **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	Накопичувальна бально-рейтингова система, що передбачає оцінювання студентів за усіма видами аудиторної та позааудиторної освітньої діяльності у вигляді поточного, семестрового контролю та атестації.
Розділ 6. Програмні компетентності		
6.1.	Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
6.2.	Загальні компетентності (ЗК)	**ЗК 1.** Здатність застосовувати знання у практичних ситуаціях. **ЗК 2.** Здатність проводити дослідження на відповідному рівні. **ЗК 3.** Здатність до абстрактного мислення, аналізу та

		синтезу. **ЗК 4.** Здатність оцінювати та забезпечувати якість виконуваних робіт. **ЗК 5.** Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності). **ЗК 6.** Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
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 супроводжувати 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. **ФК 11.** Здатність проєктувати, розробляти, впроваджувати і супроводжувати програмні та програмно-апаратні комплекси і системи засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних системах на об'єктах критичної інфраструктури держави, включаючи авіаційну галузь. **ФК 12.** Здатність до проєктування, впровадження, супроводження інформаційних мереж і ресурсів, з метою забезпечення захисту інформації та безперервного функціонування з використанням сучасних технологій інформаційної безпеки та/або кібербезпеки на об'єктах критичної інфраструктури держави, включаючи авіаційну галузь.
Розділ 7. Програмні результати навчання		
7.1.	Програмні результати навчання (ПРН)	**ПРН 1.** 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. **ПРН 2**. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або

		мультидисциплінарних контекстах. **ПРН 3**. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. **ПРН 4**. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. **ПРН 5**. 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. **ПРН 6**. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. **ПРН 7**. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. **ПРН 8**. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури. **ПРН 9**. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. **ПРН 10**. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. **ПРН 11**. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. **ПРН 12**. 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. **ПРН 13**. 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. **ПРН 14**. 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. **ПРН 15**. 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. **ПРН 16**. 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. **ПРН 17**. 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. **ПРН 18**. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. **ПРН 19**. 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. **ПРН 20**. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. **ПРН 21**. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. **ПРН 22**. 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. **ПРН 23**. 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. **ПРН 24.** Вирішувати задачі проектування та супроводу захищених інформаційних мереж та комплексів з використанням сучасних методів та технологій забезпечення інформаційної безпеки та/або кібербезпеки для забезпечення необхідного рівня захищеності на об'єктах критичної інфраструктури держави, включаючи авіаційну галузь.
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. Під час 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/9162 Усі 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	У рамках двосторонніх договорів між Національним

	мобільність	авіаційним університетом та вітчизняними закладами вищої освіти.
9.2.	Міжнародна кредитна мобільність	У рамках Еразмус+К1 договір про співробітництво між НАУ 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

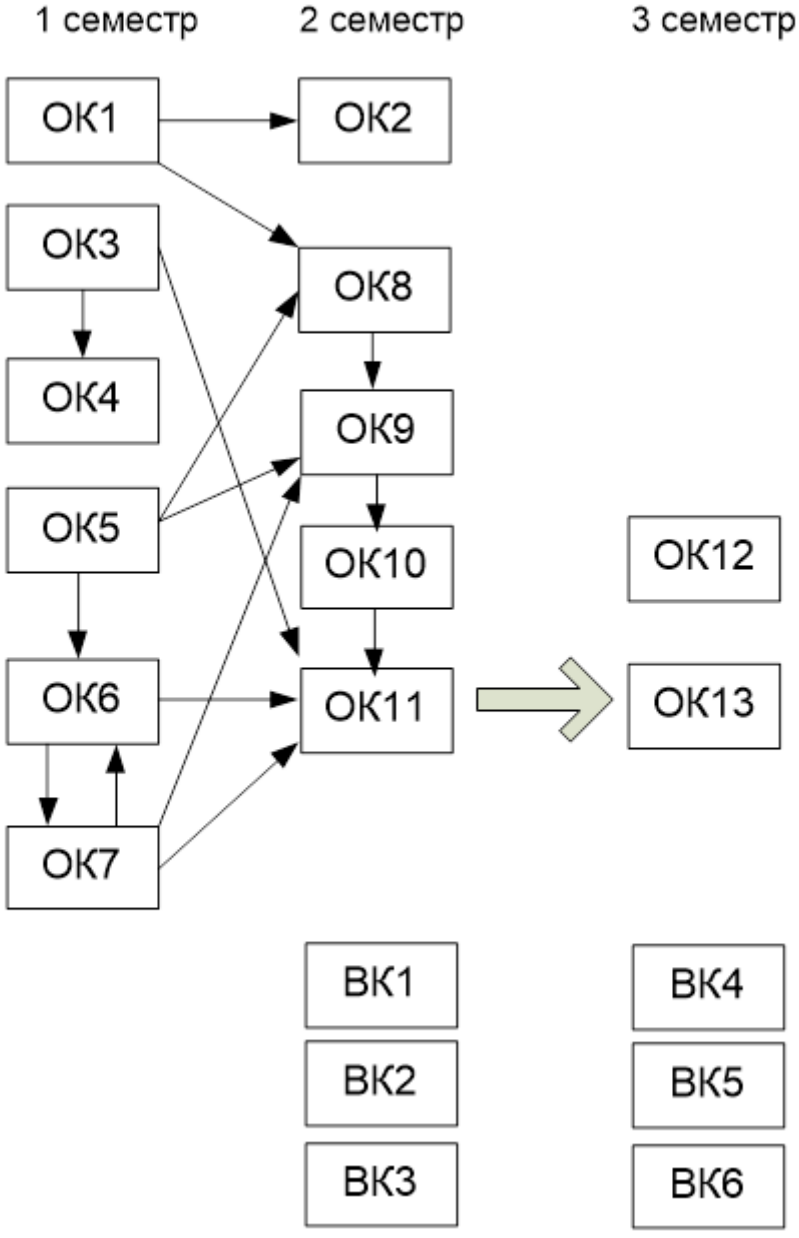
2.1. Перелік освітніх компонентів ОПП

Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кіль-кість кредитів	Форма підсумкового контролю	Семестр (відповідно до форми навчання)	
				денна	заочна
Обов'язкові компоненти ОПП					
ОК1.	Ділова іноземна мова	3,5	Екзамен	1	1
ОК2.	Наукові комунікації у фаховій діяльності	3,5	Диференційований залік	2	2
ОК3.	Методологія прикладних досліджень у сфері кібербезпеки	6,5	Диференційований залік	1	1
ОК4.	Курсовий проєкт з дисципліни Методологія прикладних досліджень у сфері кібербезпеки	1,5	Захист	1	1
ОК5.	Методи побудови та аналізу криптосистем	6	Екзамен	1	1
ОК6.	Моделювання та оптимізація безпекових процесів авіаційної галузі	6	Екзамен	1	1
ОК7.	Моніторинг та аудит кібербезпеки	6,5	Диференційований залік	1	1
ОК8.	Захист комунікаційних мереж засобами Cisco	3,0	Екзамен	2	2
ОК9.	Технології створення та застосування систем захисту кіберпростору	4,5	Екзамен	2	2
ОК10	Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	1,0	Захист	2	2
ОК11.	Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	6,0	Диференційований залік	2	2
ОК12.	Переддипломна практика	9,0	Диференційований залік	3	3
ОК13.	Кваліфікаційна робота	9,0	Захист	3	3
Загальний обсяг обов'язкових компонент:		**66 кредитів ЄКТС**			
Вибіркові компоненти *					
ВК 1.		4,0	Диференційований залік	2	2
ВК 2.		4,0	Диференційований залік	2	2
ВК 3.		4,0	Диференційований залік	2	2
ВК 4.		4,0	Диференційований залік	3	3
ВК 5.		4,0	Диференційований залік	3	3
ВК 6.		4,0	Диференційований залік	3	3
Загальний обсяг вибіркових компонент		**24 кредитів 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 здійснюється у формі публічного захисту кваліфікаційної роботи.
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 не повинна містити академічного плагіату, фабрикації, фальсифікації. Кваліфікаційна робота має бути розміщена на офіційному сайті (або у репозитарії) закладу вищої освіти або його підрозділу. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

Компоненти	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13	ВК 1	…	ВК 6
ІК	+	+	+	+	+	+	+	+	+	+	+	+	+			
ЗК1	+	+		+	+	+	+	+	+	+	+	+	+			
ЗК2		+		+	+	+	+	+	+	+	+	+	+			
ЗК3		+	+	+	+	+	+	+	+	+	+	+	+			
ЗК4		+	+	+		+	+	+	+	+	+	+	+			
ЗК5	+	+		+		+	+	+	+	+	+	+	+			
ЗК6	+	+		+	+	+	+	+	+	+	+	+	+			
ФК1			+			+		+	+	+	+	+	+			
ФК2			+				+		+	+	+	+	+			
ФК3			+		+	+		+	+	+	+	+	+			
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	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13	ВК 1	…	ВК 6
ПРН1	+	+		+		+	+	+	+	+	+	+	+			
ПРН2	+	+	+	+		+	+	+	+	+	+	+	+			
ПРН3			+	+	+						+	+	+			
ПРН4					+	+		+	+	+	+	+	+			
ПРН5			+			+	+	+	+	+	+	+	+			
ПРН6					+	+	+	+	+	+	+	+	+			
ПРН7			+				+				+	+	+			
ПРН8			+			+	+	+	+	+	+	+	+			
ПРН9			+		+		+				+	+	+			
ПРН10							+				+	+	+			
ПРН11			+					+	+	+	+	+	+			
ПРН12							+				+	+	+			
ПРН13					+						+	+	+			
ПРН14							+				+	+	+			
ПРН15		+	+			+	+	+	+	+	+	+	+			
ПРН16			+			+			+	+	+	+	+			
ПРН17	+	+		+		+	+	+	+	+	+	+	+			
ПРН18			+				+	+	+	+	+	+	+			
ПРН19			+		+	+			+	+	+	+	+			
ПРН20			+	+		+	+				+	+	+			
ПРН21						+	+	+	+	+	+	+	+			
ПРН22						+			+	+	+	+	+			
ПРН23			+		+	+	+	+	+	+	+	+	+			
ПРН24							+	+	+	+	+	+	+			

(Ф 03.02 – 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки

(Ф 03.02 – 02)

АРКУШ ОЗНАЙОМЛЕННЯ З ДОКУМЕНТОМ

№ пор.	Прізвище ім'я по-батькові	Підпис ознайомленої особи	Дата ознайом-лення	Примітки

(Ф 03.02 – 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЇ

№ пор.	Прізвище ім'я по-батькові	Дата ревізії	Підпис	Висновок щодо адекватності

(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			

(Ф 03.02 – 32)

УЗГОДЖЕННЯ ЗМІН

	Підпис	Ініціали, прізвище	Посада	Дата
Розробник				
Узгоджено				
Узгоджено				
Узгоджено				