(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 № 4 від 17.04. 2024 р.

Голова комісії з реорганізації НАУ,
в.о. ректора

Ксенія СЕМЕНОВА

Наказ № 164/ос від 23.04. 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 № 3
від «16» 04 2024 р.
Голова Науково-методичної ради,
проректор з навчальної роботи
_____ Анатолій ПОЛУХІН

ПОГОДЖЕНО
Вченою радою Факультету кібербезпеки
та програмної інженерії
протокол № 1
від «22» 03 2024 р.
Голова вченої ради факультету
_____ Олександр ПОНОМАРЕНКО

ПОГОДЖЕНО
Кафедрою комп'ютеризованих систем
захисту інформації
протокол засідання № 13
від «19» 03 2024р.
Завідувач кафедри
_____ Михайло СТЕПАНОВ

ПОГОДЖЕНО
Студентською радою Факультету
кібербезпеки та програмної інженерії
протокол № 24/3-п-РКПП
від «20» березня 2024 р.
Голова студентської ради
_____ Анна ВАСЬКОВСЬКА

ПРИМІТКА. Відповідно до п. 1.47 наказу голови комісії з реорганізації НАУ, в.о. ректора від 28.03.2024 № 120/од «Про введення в дію рішень Вченої ради університету від 20 березня 2024 року (протокол № 3)» реалізація освітнього процесу за цією редакцією освітньої програми в 2024-2025 навчальному році відтермінована у зв'язку з реорганізацією Національного авіаційного університету.

ПЕРЕДМОВА

Розроблено робочою групою освітньо-професійної програми (спеціальності 125 «Кібербезпека та захист інформації», рік вступу 2024-й та наступний до нової редакції освітньої програми)

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

ТРІЩУН Артем Володимирович - здобувач вищої освіти, який навчається на освітній програмі «Безпека інформаційних і комунікаційних систем»

підпис здобувача вищої освіти

ЗОВНІШНІ СТЕЙКХОЛДЕРИ:

СКЛАДАНИЙ Павло Миколайович, к.т.н., доц., завідувач кафедри інформаційної та кібернетичної безпеки ім. проф. Володимира Бурячка Київського столичного університету ім. Бориса Грінченка

підпис

КМЕТИК Назарій Володимирович, начальник відділу інформаційних технологій з безпеки ТОВ «Алгорітм-Х»

підпис

ПУПИНІН Олександр Сергійович, начальник відділу розвитку та підтримки систем захисту від кіберзагроз і технічного захисту інформації Державного підприємства обслуговування повітряного руху України

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, Навчально-науковий інститут неперервної освіти, Факультет кібербезпеки та програмної інженерії, кафедра комп'ютеризованих систем захисту інформації; Навчально-науковий інститут неперервної освіти (заочна форма навчання)
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 (денна форма навчання) / 1 рік 4 місяці (заочна форма навчання)
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. Заклад вищої освіти має право визнати та перезарахувати кредити ЄКТС, отримані за попередньою освітньою програмою підготовки магістра (спеціаліста) за іншою спеціальністю. Максимальний обсяг кредитів ЄКТС, що може бути перезарахований, становить 25% від загального обсягу освітньої програми.
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 освітньо-професійної програми полягає в підготовці висококваліфікованих, конкурентоспроможних фахівців на глобальному ринку праці, здатних розв'язувати задачі дослідницького та інноваційного характеру у сфері кібербезпеки та захисту інформації, забезпечення здобувачів вищої освіти фундаментальною підготовкою у вигляді поглиблених теоретичних і практичних знань, умінь та навичок, достатніх для ефективного виконання завдань відповідного рівня професійної діяльності в сфері захисту інформації та з урахуванням специфіки авіаційної галузі; оволодіння студентами знаннями, вміннями та навичками з проєктування, експлуатації та впровадження сучасних технологій, методів та засобів забезпечення безпеки інформаційних і комунікаційних систем задля позитивного внеску у розвитку суспільства на національному та міжнародному рівнях через генерацію нових знань та інноваційних ідей з урахуванням потреб ІТ ринку, а також авіаційної галузі України.	
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. **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.
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	Загальна вища освіта в галузі «Інформаційні технології» з поглибленою спеціалізованою підготовкою в сфері інформаційної та кібербезпеки, в тому числі моделювання, розробка, впровадження і експлуатація програмних та програмно-апаратних комплексів та засобів захисту інформації на об'єктах критичної інфраструктури, авіаційної галузі та народного господарства. Ключові слова: кібербезпека, інформаційна безпека, криптографічний захист інформації, захист

		персональних даних, захист інформації, захист від несанкціонованого доступу, електронний цифровий підпис, 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. У ОПП немає аналогів серед ЗВО України щодо врахування галузевого контексту функціонування авіаційного сектору.
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.

5.2.	Оцінювання	Відповідно до Положення про організацію освітнього процесу в Національному авіаційному університеті, Положення про організацію та проведення поточного і семестрового контролю, рейтингової системи оцінювання набутих студентом знань та вмінь, визначеної для кожної навчальної дисципліни її робочою програмою.
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)	**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).
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. ***Додаткові компетентності, пов'язані з особливостями освітньої програми:*** **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. ***Додатковий програмний результат навчання, пов'язаний з особливостями освітньої програми:*** **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 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 НАУ та навчальними закладами ЄС
9.3.	Навчання іноземних здобувачів вищої освіти	Створено умови для навчання іноземних здобувачів вищої освіти.

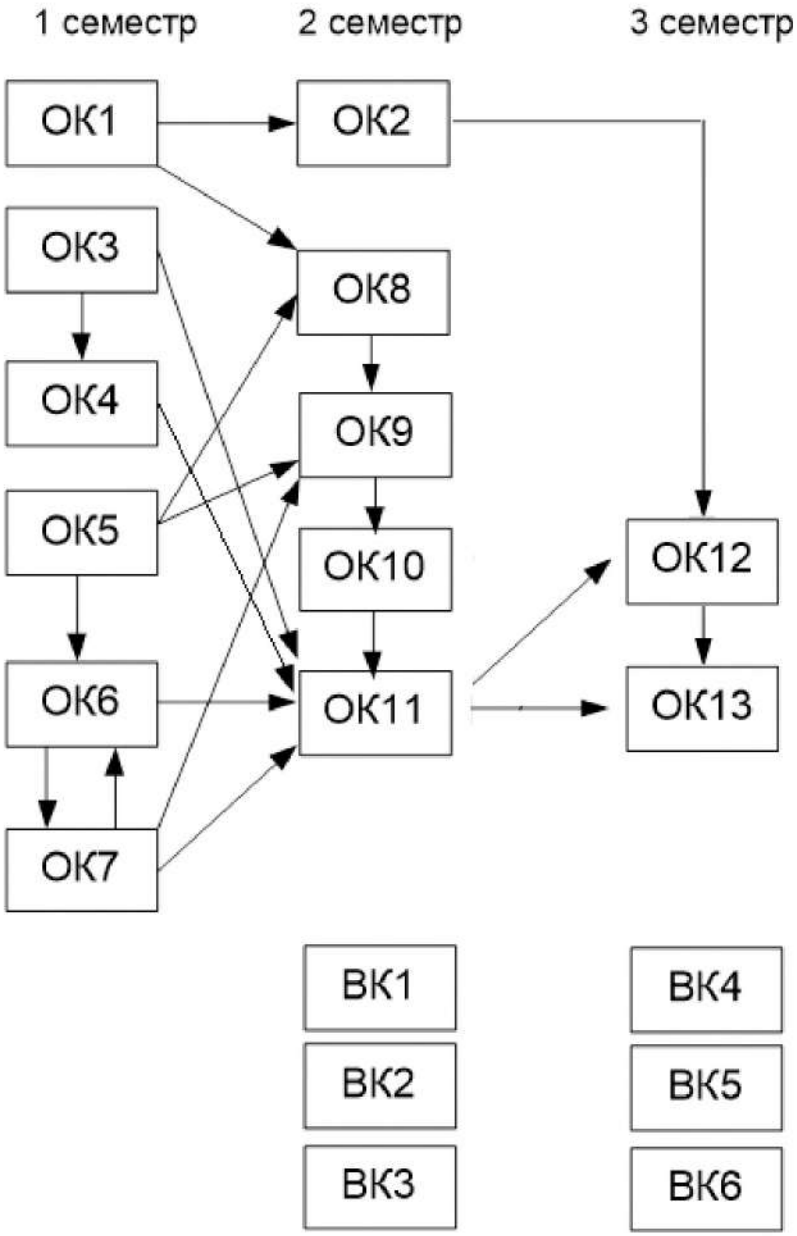
2. Перелік компонентів освітньо-професійної програми та їх логічна послідовність

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
Обов'язкові компоненти ОПП				
ОК1.	Ділова іноземна мова	3,5	Екзамен	1
ОК2.	Наукові комунікації у фаховій діяльності	3,5	Диференційований залік	2
ОК3.	Методологія прикладних досліджень у сфері кібербезпеки	6,5	Диференційований залік	1
ОК4.	Курсовий проєкт з дисципліни Методологія прикладних досліджень у сфері кібербезпеки	1,5	Захист	1
ОК5.	Методи побудови та аналізу криптосистем	6	Екзамен	1
ОК6.	Моделювання та оптимізація безпекових процесів авіаційної галузі	6	Екзамен	1
ОК7.	Моніторинг та аудит кібербезпеки	6,5	Диференційований залік	1
ОК8.	Захист комунікаційних мереж засобами Cisco	3,0	Екзамен	2
ОК9.	Технології створення та застосування систем захисту кіберпростору	4,5	Екзамен	2
ОК10	Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	1,0	Захист	2
ОК11.	Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	6,0	Диференційований залік	2
ОК12.	Переддипломна практика	9,0	Диференційований залік	3
ОК13.	Кваліфікаційна робота	9,0	Захист	3
Загальний обсяг обов'язкових компонентів:		**66 кредитів ЄКТС**		
Вибіркові компоненти *				
ВК 1.	Дисципліна 1	4,0	Диференційований залік	2
ВК 2.	Дисципліна 2	4,0	Диференційований залік	2
ВК 3.	Дисципліна 3	4,0	Диференційований залік	2
ВК 4.	Дисципліна 4	4,0	Диференційований залік	3
ВК 5.	Дисципліна 5	4,0	Диференційований залік	3
ВК 6.	Дисципліна 6	4,0	Диференційований залік	3
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



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	+	+		+		+	+	+	+	+	+	+	+			
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							+	+	+	+	+	+	+			

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, затвердженим рішенням Вченої ради університету від 28.11.2018 (протокол № 8), та відповідає вимогам Закону України «Про вищу освіту» від 01.07.2014 № 1556-VII (із змінами; розділ V «Забезпечення якості вищої освіти», стаття 16).

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

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

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

3. Постанова Кабінету Міністрів України від 23.11.2011 № 1341 «Про затвердження Національної рамки кваліфікацій» (із змінами) [Електронний ресурс]. – режим доступу: https://zakon.rada.gov.ua/laws/show/1341-2011-п

4. Стандарт вищої освіти зі спеціальності 125 Кібербезпека 12 Інформаційні технології для другого (магістерського) рівня вищої освіти, затверджений наказом Міністерства освіти і науки України від 18.03.2021 № 332

5. Постанова Кабінету Міністрів України від 29.04.2015 № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» (із змінами) [Електронний ресурс]. – режим доступу: https://zakon.rada.gov.ua/laws/show/266-2015-п

6. Національний класифікатор України. Класифікація видів економічної діяльності: ДК 009:2010, затверджений наказом Держспоживстандарту України від 11.10.2010 № 457 (із змінами) [Електронний ресурс]. – режим доступу: https://zakon.rada.gov.ua/rada/show/vb457609-10

(Ф 03.02 – 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки
1	0302	01.05.2024	Коваль О.М.	[signature]	

(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				

ТОВ «Алгорітм-Х»
ЄДРПОУ 41098587
вул. Вікентія Хвойки, 18/14
м. Київ, Україна, 04080
тел.: (067) 431-02-02, (044) 221-74-82
e-mail: info@algorytmx.com.ua

20 ЛЮТ 2024 №2002/2

РЕЦЕНЗІЯ-ВІДГУК
на освітньо-професійну програму
«Безпека інформаційних і комунікаційних систем»
Спеціальності 125 «Кібербезпека та захист інформації»
другого (магістерського) рівня вищої освіти

Ціль освітньої-професійної програми «Безпека інформаційних і комунікаційних систем» полягає в підготовці конкурентних на ринку праці фахівців в галузі інформаційних технологій, здатних розв'язувати складні спеціалізовані завдання або практичні проблеми захисту інформації, використовувати і впроваджувати технології інформаційної та/або кібербезпеки.

Освітньо-професійна програма «Безпека інформаційних і комунікаційних систем» відповідає місії Національного авіаційного університету (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 освітньо-професійної програми немає аналогів серед ЗВО України щодо врахування галузевого контексту функціонування авіаційного сектору.

Розробники програми пропонують здобувачам вищої освіти збалансований набір освітніх компонент. Перелік та обсяг нормативних дисциплін відповідає структурно-логічній схемі підготовки здобувачів вищої освіти ступеня освіти магістр. Зміст усіх компетентностей орієнтовано на знання та уміння з використання новітніх методів та підходів у галузі забезпечення інформаційної безпеки та/або кібербезпеки. Фахові компетентності носять практичний характер і можуть бути використані у подальшій професійній діяльності зі спеціальності 125 «Кібербезпека та захист інформації».

Заявлена ціль освітньої програми «Безпека інформаційних і комунікаційних систем» дозволяє вважати її сучасною і цікавою для здобувачів вищої освіти та роботодавців в сфері кібербезпеки.

Зважаючи на зазначене, вважаю, що представлена освітньо-професійна програма «Безпека інформаційних і комунікаційних систем» підготовки магістрів за спеціальністю 125 «Кібербезпека та захист інформації» галузі 12 «Інформаційні технології» є відмінно структурованою та збалансованою, що здійснює підготовку висококваліфікованих та конкурентоспроможних фахівців у сфері безпеки інформаційних і комунікаційних систем з урахуванням потреб ІТ ринку, а також авіаційної галузі України.

Начальник відділу
інформаційних технологій з безпеки
ТОВ «Алгорітм-Х» Назарій КМЕТИК

УКРАЇНА * М. КИЇВ * ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ АЛГОРІТМ-Х Ідент. код 41098587

ВІДГУК-РЕЦЕНЗІЯ
на освітньо-професійну програму «Безпека інформаційних і комунікаційних систем» Спеціальності 125 «Кібербезпека та захист інформації» другого (магістерського) рівня вищої освіти

Освітньо-професійна програма, що реалізується в Національному авіаційному університеті на кафедрі комп'ютеризованих систем захисту інформації за спеціальністю 125 «Кібербезпека та захист інформації» являє собою систему документів, розроблену закладом вищої освіти з врахуванням Стандарту вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для другого (магістерського) рівня вищої освіти.

Освітньо-професійна програма регламентує цілі, очікувані результати, зміст, умови та технології реалізації освітнього процесу, оцінку якості підготовки випускника за даною спеціальністю . Освітньо-професійна програма складена логічно. У ній визначені програмні компетентності, а саме інтегральна компетентність, загальні та фахові компетентності. Проаналізовані програмні результати навчання.

Кадрове забезпечення освітньо-професійної програми забезпечується науково-педагогічними працівниками кафедри комп'ютеризованих систем захисту інформації, що відповідають профілю дисциплін, які викладаються.

Навчальний план підготовки магістрів повністю відповідає завданням освітньо-професійної програми «Безпека інформаційних і комунікаційних систем». Структурно-логічній схемі освітньо-професійної програми відповідає послідовність вивчення, перелік та обсяг обов'язкових компонентів освітньо-професійної програми. Проаналізовано матрицю відповідності програмних компетентностей компонентам освітньо-професійної програми та матрицю забезпечення програмних результатів навчання відповідними компонентами освітньо-професійної програми. Дана освітньо-професійна програма містить у собі усі необхідні структурні та змістові складові, відображає сучасні вимоги до фахівців в галузі кібербезпеки і відповідає вимогам практичного використання набутих ними знань і навичок.

Запропонована кафедрою комп'ютеризованих систем захисту інформації освітньо-професійна програма «Безпека інформаційних і комунікаційних систем» дозволяє забезпечити високоякісну підготовку магістрів за спеціальністю 125 «Кібербезпека та захист інформації» в сфері захисту інформації з урахуванням специфіки авіаційної галузі.

З урахуванням вищесказаного вважаю, що рецензовану освітньо-професійну програму «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти можна рекомендувати до використання для підготовки здобувачів за спеціальністю 125 «Кібербезпека та захист інформації».

Начальник відділу розвитку та підтримки
систем захисту від кіберзагроз і
технічного захисту інформації
управління з цифрової трансформації,
інформаційних технологій та кіберзахисту
Державного підприємства обслуговування
повітряного руху України

Олександр ПУПИНІН

11.03.2024

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА

ФАКУЛЬТЕТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
ТА МАТЕМАТИКИ
вул. Левка Лук'яненка, 13-Б, м. Київ, Україна, 04207
Тел.: +380 44 428-34-14
fitm.kubg.edu.ua, fitm@kubg.edu.ua

BORYS GRINCHENKO
KYIV METROPOLITAN UNIVERSITY

FACULTY
OF INFORMATION TECHNOLOGIES
AND MATHEMATICS
13-B Levka Lukianenka St, Kyiv, Ukraine, 04207
Tel.: +380 44 428-34-14
fitm.kubg.edu.ua, fitm@kubg.edu.ua

20.02.2024 № 8

РЕЦЕНЗІЯ-ВІДГУК
на освітньо-професійну програму «Безпека інформаційних і комунікаційних систем» Спеціальності 125 «Кібербезпека та захист інформації» другого (магістерського) рівня вищої освіти

На сьогоднішній день у контексті глобальних викликів інформаційного розвитку людства і розбудови національної системи забезпечення інформаційної безпеки та її інтеграції у європейський простір якісна підготовка здобувачів вищої освіти в сфері забезпечення кібербезпеки є дуже важливим завданням. Така потреба сучасного ринку праці викликана необхідністю мати висококваліфікованих, конкурентоспроможних фахівців, які здатні вирішувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення кібербезпеки та захисту інформації. Рецензована освітньо-професійна програма «Безпека інформаційних і комунікаційних систем» спеціальності 125 «Кібербезпека» розроблена співробітниками Факультету кібербезпеки та програмної інженерії Національного авіаційного університету, після консультації із науковцями, потенційними роботодавцями, які підтвердили необхідність підготовки фахівців цієї спеціальності.

Структура освітньо-професійної програми логічна та послідовна. Структурування програми узгоджено зі сформульованими цілями та завданнями навчального процесу. При формуванні цілей, фахових компетенцій і програмних результатів навчання враховано потреби стейкхолдерів. Зміст усіх компетентностей орієнтовано на знання та уміння з використання новітніх методів та підходів в сфері забезпечення кібербезпеки та захисту інформації, а фахові компетентності носять практичний характер. Перелік та обсяг нормативних та вибіркових дисциплін відповідають структурно-логічній

схемі підготовки здобувачів вищої освіти другого (магістерського) рівня вищої освіти освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» спеціальності 125 «Кібербезпека та захист інформації». Кваліфікаційний профіль випускника програми повністю відповідає потребам сучасного ринку праці.

Підсумовуючи викладена, вважаю, що освітньо-професійна програма «Безпека інформаційних і комунікаційних систем» підготовки здобувачів вищої освіти другого (магістерського) рівня спеціальності 125 «Кібербезпека та захист інформації» повністю відповідає встановленим вимогам, забезпечить здобувачам фундаментальну професійну підготовку, а також може бути рекомендована до впровадження в освітній процес університету.

Рецензент:
Завідувач кафедри
інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка
Київського столичного
університету імені Бориса Грінченка,
кандидат технічних наук, доцент Павло СКЛАДАННИЙ

Підпис Павла СКЛАДАННОГО засвідчую
Декан Факультету інформаційних технологій та математики
кандидат фізико-математичних наук,
старший науковий співробітник Оксана ЛИТВИН