

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»



ОСВІТНЬО – ПРОФЕСІЙНА ПРОГРАМА

«Безпека інформаційних і комунікаційних систем»

Другого (магістерського) рівня вищої освіти

за спеціальністю F5 «Кібербезпека та захист інформації»

галузі знань F «Інформаційні технології»

СМЯ KAI ОП М ID69358– 01 – 2025

Освітньо-професійна програма
затверджена Вченою радою KAI
протокол № 5 від 26.03. 2025 р.
Вводиться в дію наказом в.о. президента KAI
від 30.03. 2025 р. № 209/ог



В.о. президента

Ксенія СЕМЕНОВА

КИЇВ

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації»	Шифр документа	СМЯ КАІ ОП М ID69358 – 01 – 2025
		Стор. 2 з 22	

Враховано Стандарт вищої освіти України: другий (магістерський) рівень; галузь знань 12 «Інформаційні технології», спеціальність 125 «Кібербезпека та захист інформації» (в редакції постанови Кабінету міністрів України від 16.12.2022 №1392 «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти».

Стандарт вищої освіти України затверджено і введено в дію наказом Міністерства освіти і науки України від 18.03.2021 р. № 332.

ЛИСТ ПОГОДЖЕННЯ освітньо-професійної програми

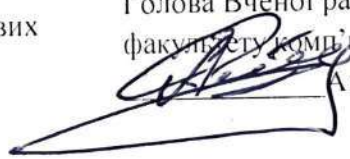
ПОГОДЖЕНО

Науково-методичною радою КАІ
протокол № 3
від « 25 » 03 2025 р.

Голова НМР КАІ, проректор з з наукових досліджень та трансферу технологій
 Сергій ГНАТЮК

ПОГОДЖЕНО

Вченою радою факультету комп'ютерних наук та технологій
протокол № 3
від « 12 » 03 2025 р.

Голова Вченої ради факультету комп'ютерних наук та технологій
 Андрій ФЕСЕНКО

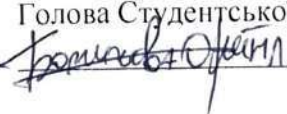
ПОГОДЖЕНО

Кафедрою кібербезпеки
протокол засідання № 5
від « 11 » 03 2025 р.

Завідувач кафедри  Анна ІЛЬЄНКО

ПОГОДЖЕНО

Студентською радою факультету комп'ютерних наук та технологій
протокол № 25/1-п-ФКНТ
від « 10 » 03 2025 р.

Голова Студентської ради факультету
 Орина БОЛИЧОВА

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»	Шифр документа	СМЯ КАІ ОП М ID69358-01-2025
		Стор. 3 з 22	

ПЕРЕДМОВА

Розроблено робочою групою освітньо-професійної програми (спеціальності F5 «Кібербезпека та захист інформації») у складі:

у складі:

ГАРАНТ ОСВІТНЬОЇ ПРОГРАМИ:

ІЛЬСНКО Анна - к.т.н., доц., завідувач кафедри кібербезпеки
Вадимівна


підпис гаранта

ЧЛЕНИ РОБОЧОЇ ГРУПИ:

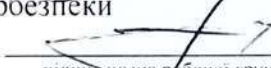
ВИСОЦЬКА Олена - к.т.н., доцент кафедри кібербезпеки
Олександрівна


підпис члена робочої групи

ПЕТРЕНКО Андрій - к.т.н., доц., доцент кафедри кібербезпеки
Борисович


підпис члена робочої групи

ГАЛАТА Лілія Павлівна - доктор філософії, доцент кафедри кібербезпеки


підпис члена робочої групи

МАЛЯРЕНКО Софія - здобувачка вищої освіти за освітньою програмою,
Дмитрівна група М-125-24-1-БІ


підпис здобувача вищої освіти

ЗОВНІШНІ СТЕЙКГОЛДЕРИ:

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


підпис

ПЕДЧЕНКО Євгеній Максимович, начальник відділу систем інформаційної безпеки ТОВ «СІТОН ДІДЖИТАЛ»


підпис

ОЛЕКСІЮК Лілія Віталіївна, голова Всеукраїнської асоціації «Інформаційна безпека та інформаційні технології»


підпис

Рецензії, відгуки зовнішніх стейкхолдерів (додаються).

Рівень документа – 3б

Плановий термін між ревізіями – 1 рік

Контрольний примірник

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»	Шифр документа	СМЯ КАІ ОП М ID69358– 01 – 2025
		Стор. 4 з 22	

1. Профіль освітньо-професійної програми

Розділ 1. Загальна інформація		
1.1.	Повна назва закладу вищої освіти та структурного підрозділу	Державний університет «Київський авіаційний інститут» Факультет комп'ютерних наук та технологій Кафедра кібербезпеки;
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. Очна (денна), заочна форми здобуття освіти. Розрахункові строки виконання освітньої програми: – 1 рік 6 місяців (денна форма здобуття освіти); – 1 рік 6 місяців (заочна форма здобуття освіти)
1.5.	Акредитаційна інституція	Національне агентство із забезпечення якості вищої освіти
1.6.	Період акредитації	Сертифікат про акредитацію освітньої програми 9925, дійсний до 22.10.2025
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 F5 (125) Кібербезпека та захист інформації 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.	Мова(и) викладання	Українська
1.10.	Інтернет-адреса постійного розміщення опису освітньої програми	http://kai.edu.ua http://www.kszi.nau.edu.ua

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»	Шифр документа	СМЯ KAI ОП М ID69358– 01 – 2025
		Стор. 5 з 22	

Розділ 2. Ціль освітньо-професійної програми		
2.1.		Ціль освітньо-професійної програми полягає у підготовці висококваліфікованих, конкурентоспроможних фахівців на глобальному ринку праці, здатних розв'язувати задачі дослідницького та інноваційного характеру у сфері кібербезпеки та захисту інформації. Програма забезпечує здобувачів фундаментальною підготовкою, що включає поглиблені теоретичні та практичні знання, уміння та навички, необхідні для ефективного виконання професійних завдань у сфері захисту інформації, зокрема з урахуванням специфіки авіаційної галузі. Здобувачі оволодівають сучасними методами, технологіями та засобами забезпечення безпеки інформаційних і комунікаційних систем, включаючи їх проєктування, впровадження та експлуатацію. Програма сприяє розвитку інноваційного мислення, генерації нових знань та технологічних рішень, що відповідають потребам сучасного ІТ-ринку та авіаційної галузі України, забезпечуючи позитивний внесок у розвиток суспільства на національному та міжнародному рівнях.
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,

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»	Шифр документа	СМЯ КАІ ОП М ID69358– 01 – 2025
		Стор. 6 з 22	

		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 знань 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	Вища освіта в галузі «Інформаційні технології» з поглибленою спеціалізованою підготовкою в сфері інформаційної та кібербезпеки, включаючи моделювання, розробку, впровадження і експлуатацію програмних та програмно-апаратних комплексів і засобів захисту. Освітня програма охоплює технології безпеки інформаційно-комунікаційних систем, захист мережевої інфраструктури, підходи щодо моніторингу та аудиту кібербезпеки та розробку систем захисту кіберпростору для об'єктів критичної інфраструктури, зокрема авіаційної галузі та народного господарства, відповідно до міжнародних стандартів та вимог. Ключові слова: кібербезпека, інформаційна безпека, криптографічний захист інформації, захист персональних даних, захист інформації, захист від

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»	Шифр документа	СМЯ КАІ ОП М ID69358– 01 – 2025
		Стор. 7 з 22	

		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 (освітньо-науковому) рівні вищої освіти. Право набувати додаткові кваліфікації в системі післядипломної освіти

Розділ 5. Викладання та оцінювання

5.1.	Викладання та навчання (методи, методики, технології, інструменти та обладнання)	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 (проєктів), кваліфікаційної роботи. Методи, методики та технології. Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі,
------	--	---

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»	Шифр документа	СМЯ KAI ОП М ID69358– 01 – 2025
		Стор. 8 з 22	

		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	Відповідно до Положення про організацію освітнього процесу в KAI, рейтингової системи оцінювання набутих студентом знань та вмінь, визначеної для кожної навчальної дисципліни її робочою програмою, інших нормативних документів.
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 та захисту інформації
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

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»	Шифр документа	СМЯ КАІ ОП М ID69358– 01 – 2025
		Стор. 9 з 22	

		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
--	--	---

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»	Шифр документа	СМЯ КАІ ОП М ID69358– 01 – 2025
		Стор. 10 з 22	

		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. ФК13. Здатність до розробки, впровадження та підтримки сучасних технологій захисту мережевих інфраструктур, включаючи механізми виявлення атак та мінімізації ризиків безпеки інформаційних систем. ФК14. Здатність досліджувати, розробляти та впроваджувати технології створення та застосування систем захисту кіберпростору, з урахуванням новітніх методів захисту даних. ФК15. Здатність розробляти, впроваджувати та оцінювати ефективність стратегій кіберстійкості інформаційно-комунікаційних систем у контексті концепції сталого розвитку, використовуючи методи мінімізації кіберризиків, сучасні технології захисту та механізми забезпечення безпечного кіберпростору для розвитку цифрового суспільства (Цілі сталого розвитку 9, 11, 16).
--	--	--

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. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
------	-------------------------------------	---

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»	Шифр документа	СМЯ КАІ ОП М ID69358– 01 – 2025
		Стор. 11 з 22	

		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
--	--	--

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»	Шифр документа	СМЯ КАІ ОП М ID69358– 01 – 2025
		Стор. 12 з 22	

		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 напрямку 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 натурального, 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
--	--	---

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»	Шифр документа	СМЯ КАІ ОП М ID69358– 01 – 2025
		Стор. 13 з 22	

		іншої доступної інформації. <i>Додаткові програмні результати навчання, які пов'язані з особливостями освітньої програми:</i> 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. ПРН 25. Проектувати та впроваджувати безпечне мережеве середовище для ефективного обміну даними та безперервного функціонування бізнес-процесів і сервісів, використовуючи спеціалізоване мережеве обладнання, відповідно до сучасних стандартів інформаційної безпеки. ПРН 26. Розробляти, впроваджувати та адмініструвати системи захисту мережевих інфраструктур, забезпечуючи їхню стійкість до сучасних кіберзагроз. ПРН 27. Розробляти та впроваджувати комплексні рішення для забезпечення безпеки кіберпростору, використовуючи новітні технології та засоби захисту інформаційних ресурсів. ПРН28. Аналізувати кіберризики, розробляти та впроваджувати стратегії кіберстійкості інформаційно-комунікаційних систем, застосовуючи сучасні технології захисту та методи забезпечення безперервності функціонування критичних інформаційних ресурсів відповідно до принципів сталого розвитку (Цілі сталого розвитку 9, 11, 16), міжнародних стандартів та регуляторних вимог.
--	--	---

Розділ 8. Ресурсне забезпечення реалізації програми

8.1.	Кадрове забезпечення	Всі науково-педагогічні працівники, що забезпечують освітньо-професійну програму за кваліфікацією відповідають профілю і напрямку 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.kai.edu.ua містить інформацію про освітні програми, навчальну, наукову і виховну діяльність, структурні підрозділи, правила

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»	Шифр документа	СМЯ КАІ ОП М ID69358– 01 – 2025
		Стор. 14 з 22	

		прийому, контакти. Матеріали навчально-методичного забезпечення освітньої програми викладені в репозитарії КАІ за посиланням: https://er.nau.edu.ua/handle/NAU/9161 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 КАІ: http://er.nau.edu.ua
Розділ 9. Академічна мобільність		
9.1.	Національна кредитна мобільність	У рамках двосторонніх договорів між Державним університетом «Київський авіаційний інститут» та вітчизняними закладами вищої освіти.
9.2.	Міжнародна кредитна мобільність	У рамках Еразмус+K1 договір про співробітництво між Державним університетом «Київський авіаційний інститут» та навчальними закладами ЄС
9.3.	Навчання іноземних здобувачів вищої освіти	Створено умови для навчання іноземних здобувачів вищої освіти.

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»	Шифр документа	СМЯ KAI ОП М ID69358– 01 – 2025
		Стор. 15 з 22	

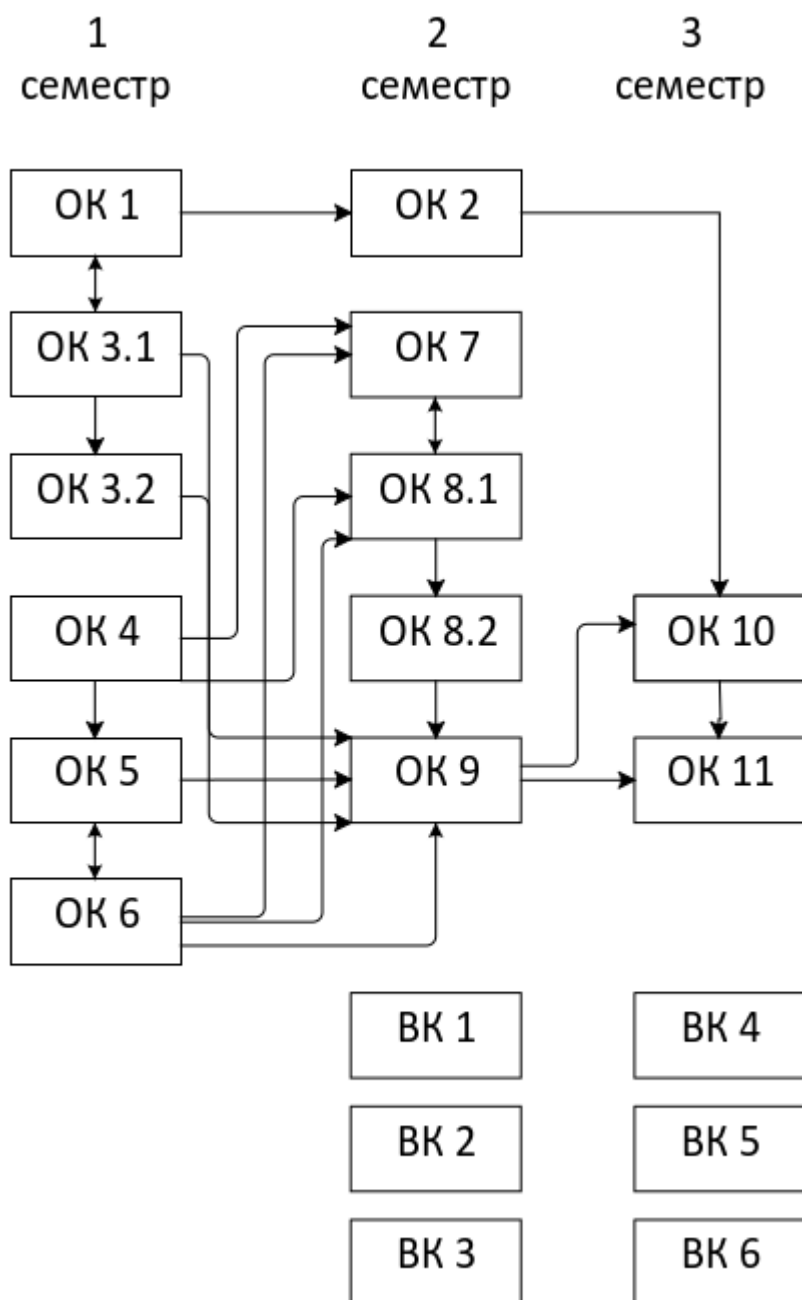
2. Перелік компонентів освітньо-професійної програми та їх логічна послідовність

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				
OK1	Ділова іноземна мова	3,5	Екзамен	1
OK2	Наукові комунікації у фаховій діяльності	3,5	Диференційований залік	2
OK3.1	Методологія прикладних досліджень у сфері кібербезпеки	6,5	Диференційований залік	1
OK3.2	Курсовий проект з дисципліни Методологія прикладних досліджень у сфері кібербезпеки	1,5	Захист	1
OK4	Методи побудови та аналізу криптосистем	6	Екзамен	1
OK5	Моделювання та оптимізація безпекових процесів авіаційної галузі	6	Екзамен	1
OK6	Моніторинг та аудит кібербезпеки	6,5	Диференційований залік	1
OK7	Технології захисту мережевих інфраструктур	5,0	Екзамен	2
OK8.1	Технології створення та застосування систем захисту кіберпростору	2,5	Екзамен	2
OK8.2	Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	1,0	Захист	2
OK9	Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	6,0	Диференційований залік	2
OK10	Переддипломна практика	9,0	Диференційований залік	3
OK11	Кваліфікаційна робота	9,0	Захист	3
Загальний обсяг обов'язкових компонентів:		66 кредитів ЄКТС		
Вибіркові компоненти *				
BK 1	Дисципліна 1	4,0	Диференційований залік	2
BK 2	Дисципліна 2	4,0	Диференційований залік	2
BK 3	Дисципліна 3	4,0	Диференційований залік	2
BK 4	Дисципліна 4	4,0	Диференційований залік	3
BK 5	Дисципліна 5	4,0	Диференційований залік	3
BK 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 KAI.

2.2. Структурно-логічна схема освітньо-професійної програми



	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»	Шифр документа	СМЯ КАІ ОП М ID69358– 01 – 2025
		Стор. 17 з 22	

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 та захисту інформації 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.

компонентам освітньо-професійної програми

[illegible]

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

[illegible]

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»	Шифр документа	СМЯ КАІ ОП М ID69358– 01 – 2025
		Стор. 20 з 22	

6. Система внутрішнього забезпечення якості вищої освіти-КАІ

Якість освітньо-професійної програми визначається внутрішньою системою забезпечення якості вищої освіти та освітньої діяльності КАІ, яка функціонує згідно з Положенням про систему забезпечення якості вищої освіти та освітньої діяльності 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>

7. International Civil Aviation Organization. (2022). Annex 17 to the Convention on International Civil Aviation: Security—Safeguarding international civil aviation against acts of unlawful interference (12 ed.). ICAO.

	Система менеджменту якості ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»	Шифр документа	СМЯ КАІ ОП М ID69358– 01 – 2025
		Стор. 22 з 22	

(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	Анульованого			

(Ф 03.02 – 32)

УЗГОДЖЕННЯ ЗМІН

	Підпис	Ініціали, прізвище	Посада	Дата
Розробник				
Узгоджено				
Узгоджено				
Узгоджено				

Рецензія на освітньо-професійну програму

«Безпека інформаційних і комунікаційних систем» спеціальності F5 «Кібербезпека та захист інформації» другого (магістерського) рівня вищої освіти

Освітньо-професійна програма «Безпека інформаційних і комунікаційних систем», що реалізується на кафедрі кібербезпеки Державного університету «Київський авіаційний інститут» визначає ключові аспекти організації навчального процесу, включаючи мету, очікувані результати, зміст, умови впровадження освітнього процесу та критерії оцінювання якості підготовки випускників.

Освітня програма побудована логічно й структуровано, містить інтегральну, загальні та фахові компетентності, що відповідають сучасним вимогам до фахівців у галузі кібербезпеки. У програмі детально проаналізовано очікувані програмні результати навчання, що дозволяє досягти високого рівня підготовки здобувачів.

Забезпечення навчального процесу здійснюється науково-педагогічними працівниками кафедри, які володіють необхідними кваліфікаціями для викладання дисциплін, що входять до складу програми.

Навчальний план магістерської підготовки відповідає завданням програми та забезпечує логічну послідовність вивчення дисциплін, обґрунтованість їхнього змісту й обсягу. Важливим компонентом програми є детально розроблені матриці відповідності компетентностей та результатів навчання освітнім компонентам.

Програма включає всі необхідні структурні й змістовні елементи, що відповідають сучасним запитам ІТ-галузі та практичним вимогам професійної діяльності фахівців у сфері кібербезпеки. Вона враховує специфіку захисту інформації на об'єктах критичної інфраструктури, зокрема в авіаційній галузі, та забезпечує формування у випускників знань, умінь і навичок, необхідних для ефективної професійної діяльності. Представлений в освітньо-професійній програмі перелік освітніх компонент (ОК) повністю охоплює специфіку підготовки майбутніх фахівців у сфері кібербезпеки, але задля висвітлення авіаційної спрямованості освітньої програми доцільно посилити ОК5 «Моделювання та оптимізація безпекових процесів авіаційної галузі» за рахунок збільшення обсягу кредитів ЄКТС (з 3,5 кредитів до 6 кредитів) та додати додаткові фахові компетентності і програмні результати навчання, які пов'язані з особливостями освітньої програми. Також доцільно включити до переліку нормативних документів, на яких базується освітньо-професійна програма Додатку 17 «Міжнародні стандарти та рекомендована практика. Авіаційна безпека. Захист міжнародної цивільної авіації від актів незаконного втручання» (12 видання, липень 2022 року).



На основі проведеного аналізу можна зробити висновок, що представлена освітньо-професійна програма «Безпека інформаційних і комунікаційних систем» підготовки магістрів за спеціальністю F5 «Кібербезпека та захист інформації» галузі F «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 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 ПУПІНІН

ЗАТВЕРДЖУЮДиректор товариства з обмеженою
відповідальністю «СІТОН ДІДЖИТАЛ»

(підпис)

"10" 02

М.П.

**РЕЦЕНЗІЯ****на освітньо-професійну програму
«Безпека інформаційних і комунікаційних систем»
спеціальності F5 «Кібербезпека та захист інформації»
другого (магістерського) рівня вищої освіти**

Мета освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» полягає у підготовці фахівців у сфері інформаційних технологій, які здатні покривати теоретичні та практичні аспекти в галузі захисту інформації, а також застосовувати і впроваджувати сучасні технології інформаційної та кібербезпеки. Особливістю даної програми є її унікальність при використанні підходів та специфіки авіаційної галузі.

Розробники освітньо-професійної програми забезпечили здобувачів збалансованим набором освітніх компонентів. Структура та обсяг дисциплін відповідають логічній послідовності підготовки магістрів і враховують актуальні тенденції в галузі кібербезпеки. Компетентності програми орієнтовані на здобуття знань і навичок із використання новітніх методів і підходів у забезпеченні інформаційної безпеки. Практична спрямованість фахових компетентностей робить їх цінними для подальшої професійної діяльності випускників за спеціальністю F5 «Кібербезпека та захист інформації».

Цілі програми, її зміст та орієнтація на практичне застосування забезпечують її актуальність як для здобувачів освіти, так і для роботодавців у сфері інформаційної та кібербезпеки. Представлений в освітньо-професійній програмі перелік освітніх компонентів (ОК) безпосередньо стосується підготовки майбутніх фахівців у сфері кібербезпеки. Для забезпечення програмних результатів навчання (ПРН), що пов'язані з особливістю освітньої програми доцільно посилити ОК6 «Моніторинг та аудит кібербезпеки» за рахунок збільшення обсягу кредитів ЄКТС (з 3,5 кредитів до 6,5 кредитів), що дозволить розвинути з здобувачів вищої освіти навички та вміння щодо моніторингу та аналізу кібербезпеки та забезпечити ПРН 9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки та ПРН 14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, операційних процесів у сфері інформаційної безпеки та кібербезпеки в цілому.

Також рекомендуємо ввести вибіркову дисципліну «Технології розслідування інцидентів кібербезпеки», що дозволить додатково забезпечити 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.

Таким чином, освітньо-професійна програма «Безпека інформаційних і комунікаційних систем» відповідає сучасним стандартам підготовки магістрів за спеціальністю F5 «Кібербезпека та захист інформації». Вона рекомендується для використання у навчальному процесі з метою якісної підготовки здобувачів другого (магістерського) рівня вищої освіти.



Всеукраїнська асоціація
«Інформаційна безпека та інформаційні технології»
Україна, 03124, м. Київ, вул. Миколи Василенка, буд. 23-А, кв.54
+380 67 5001015, www.vaibit.org.ua, info@vaibit.org.ua

Вих. 10 від 13.02.2025 р.

РЕЦЕНЗІЯ
на освітньо-професійну програму
«Безпека інформаційних і комунікаційних систем»
спеціальності F5 «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 F5 «Кібербезпека та захист інформації» розроблена співробітниками Факультету комп'ютерних наук та технологій Державного університету «Київський авіаційний інститут».

Структура освітньо-професійної програми логічна та послідовна. Структурування програми узгоджено зі сформульованими цілями та завданнями навчального процесу. 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 F5 «Кібербезпека та захист інформації». Освітньо-професійна програма включає фундаментальні та спеціалізовані дисципліни, що охоплюють методи криптографічного захисту, управління безпекою, аналіз загроз, аудит і моніторинг кібербезпеки та інші. Кваліфікаційний профіль випускника програми повністю відповідає потребам сучасного ринку праці. Перевагою освітньо-професійної програми є її прикладна спрямованість та галузева унікальність, а саме орієнтація на авіаційну сферу надає додаткові переваги випускникам.

В цілому, представлена на розгляд та рецензію ОПП, враховує новітні тенденції та проблеми розвитку освітнянської галузі й сприятиме підготовці висококваліфікованих фахівців та інтеграції України в європейський загальноосвітній та науковий простір.

На нашу думку, освітньо-професійна програма «Безпека інформаційних і комунікаційних систем» підготовки здобувачів вищої освіти другого (магістерського) рівня спеціальності F5 «Кібербезпека та захист інформації» повністю відповідає встановленим вимогам, забезпечує здобувачам фундаментальну професійну підготовку, а також може бути рекомендована до впровадження в освітній процес університету.

Голова Асоціації



Лілія Олексюк

Рецензія

на освітньо-професійну програму
«Безпека інформаційних і комунікаційних систем»
спеціальності F5 «Кібербезпека та захист інформації»
другого (магістерського) рівня вищої освіти

Освітньо-професійну програму «Безпека інформаційних і комунікаційних систем» розроблено колективом кафедри кібербезпеки Факультету комп'ютерних наук та технологій Державного університету «Київський авіаційний інститут».

Програма базується на чітко визначених програмних компетентностях, що відповідають завданням спеціальності. Вони поділені на загальні та фахові компетентності, орієнтовані на опанування сучасних методів і підходів у забезпеченні кібербезпеки. Усі компетентності мають практичну спрямованість та можуть бути застосовані в професійній діяльності випускників.

Структура програми передбачає логічно побудовану систему освітніх компонентів, яка сприяє поступовому формуванню необхідних фахових компетентностей. Такий підхід дозволяє забезпечити підготовку висококваліфікованих спеціалістів другого (магістерського) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації».

Мета освітньо-професійної програми полягає у підготовці конкурентоспроможних фахівців, здатних ефективно виконувати завдання інноваційного характеру в галузі кібербезпеки. Програма забезпечує студентів глибокими теоретичними знаннями, практичними навичками та вміннями, необхідними для проектування, експлуатації та впровадження сучасних технологій, методів і засобів захисту інформаційних і комунікаційних систем. Окреслений у програмі об'єкт професійної діяльності повністю відповідає актуальним потребам ІТ-галузі, зокрема у сфері забезпечення кібербезпеки об'єктів критичної інфраструктури, включаючи авіаційну галузь.

Вагомою перевагою даної освітньої програми є те, що окрім обов'язкових (нормативних) компонентів, вона містить блок дисциплін вільного вибору, що дає змогу здобувачам освіти реалізувати своє право на формування індивідуальної освітньої траєкторії підготовки з урахуванням потреб ринку. Цикл практичної підготовки здобувачів вищої освіти, що включає науководослідну практику у сфері безпеки інформаційних і комунікаційних систем, а також переддипломну практику у достатньому обсязі забезпечує набуття випускниками компетентностей, необхідних для вирішення практичних завдань у сфері кібербезпеки та захисту інформації.

Освітньо-професійна програма «Безпека інформаційних і комунікаційних систем» спеціальності F5 «Кібербезпека та захист інформації» відповідає кваліфікаційним вимогам випускників магістерського рівня. Вона сприяє

забезпеченню відповідності результатів навчання сучасним запитам роботодавців.

**Начальник Управління протидії
кіберзлочинам в місті Києві
Департаменту кіберполіції
Національної поліції України
полковник поліції**



В'ячеслав КУЛУШ