

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	Національний університет «Київський авіаційний інститут»
Освітня програма	69365 Системи та технології кібербезпеки
Рівень вищої освіти	Магістр
Спеціальність	F5 Кібербезпека та захист інформації

Відомості про самооцінювання є частиною акредитаційної справи, поданої до Національного агентства із забезпечення якості вищої освіти для акредитації зазначеної вище освітньої програми. Відповідальність за підготовку і зміст відомостей несе заклад вищої освіти, який подає програму на акредитацію.

Детальніше про мету і порядок проведення акредитації можна дізнатися на вебсайті Національного агентства – <https://naqa.gov.ua/>

Використані скорочення:

ID	ідентифікатор
ВСП	відокремлений структурний підрозділ
ЄДЕБО	Єдина державна електронна база з питань освіти
ЄКТС	Європейська кредитна трансферно-накопичувальна система
ЗВО	заклад вищої освіти
ОП	освітня програма

Загальні відомості

1. Інформація про ЗВО (ВСП ЗВО)

Реєстраційний номер ЗВО у ЄДЕБО	7208
Повна назва ЗВО	Національний університет «Київський авіаційний інститут»
Ідентифікаційний код ЗВО	45853942
ПІБ керівника ЗВО	Семенова Ксенія Ігорівна
Посилання на офіційний веб-сайт ЗВО	http://www.nau.edu.ua

2. Посилання на інформацію про ЗВО (ВСП ЗВО) у Реєстрі суб'єктів освітньої діяльності ЄДЕБО

<https://registry.edbo.gov.ua/university/7208>

3. Загальна інформація про ОП, яка подається на акредитацію

ID освітньої програми в ЄДЕБО	69365
Назва ОП	Системи та технології кібербезпеки
Галузь знань	F Інформаційні технології
Спеціальність	F5 Кібербезпека та захист інформації
Спеціалізація (за наявності)	<i>відсутня</i>
Рівень вищої освіти	Магістр
Тип освітньої програми	Освітньо-професійна
Вступ на освітню програму здійснюється на основі ступеня (рівня)	Бакалавр, Магістр (ОКР «спеціаліст»)
Структурний підрозділ (кафедра або інший підрозділ), відповідальний за реалізацію ОП	Кафедра технічного захисту інформації Факультету комп'ютерних наук та технологій
Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП	Кафедра кібербезпеки, Кафедра іноземних мов професійного спрямування, Кафедра української мови, історії та інформаційної діяльності
Місце (адреса) провадження освітньої діяльності за ОП	проспект Гузара Любомира, 1, м. Київ, Україна, 03058
Освітня програма передбачає присвоєння професійної кваліфікації	<i>не передбачає</i>
Професійна кваліфікація, яка присвоюється за ОП (за наявності)	<i>відсутня</i>
Мова (мови) викладання	Українська
ID гаранта ОП у ЄДЕБО	494737
ПІБ гаранта ОП	Кудренко Станіслава Олексіївна
Посада гаранта ОП	Доцент
Корпоративна електронна адреса гаранта ОП	stanislava.kudrenko@npp.kai.edu.ua
Контактний телефон гаранта ОП	+38(063)-766-81-51
Додатковий телефон гаранта ОП	+38(044)-406-70-56

Форми здобуття освіти на ОП	Термін навчання
очна денна	1 р. 6 міс.

4. Загальні відомості про ОП, історію її розроблення та впровадження

Підготовка фахівців у сфері інформаційної безпеки в університеті має багаторічну історію, а сучасний етап розвитку ОПП «Системи та технології кібербезпеки» другого (магістерського) рівня вищої освіти розпочався з її редакції 2023 року.

Редакція ОПП 2023 року за спеціальністю 125 «Кібербезпека та захист інформації» була затверджена Вченою радою Національного авіаційного університету 19.04.2023 (протокол № 4) та введена в дію наказом ректора від 01.05.2023 № 180/од. Обсяг програми становив 90 кредитів ЕКТС, а її особливістю була орієнтація на підготовку фахівців у сфері інформаційної та кібербезпеки з урахуванням специфіки авіаційної галузі.

У 2024–2025 роках ОПП було переглянуто у зв'язку зі змінами у переліку галузей знань і спеціальностей, переходом до спеціальності F5 «Кібербезпека та захист інформації» та необхідністю актуалізації змісту підготовки. Під час перегляду уточнено мету, фокус і особливості програми, оновлено фахові компетентності, програмні результати навчання та зміст освітніх компонентів. Посилено складові, пов'язані з оцінюванням кіберризиків, аудитом інформаційної безпеки, розробленням політик безпеки, використанням сучасних систем кіберзахисту та забезпеченням кіберстійкості. Особливості програми конкретизовано додатковими фаховими компетентностями ФК11–ФК14 та програмними результатами навчання ПРН24–ПРН26.

Оновлена редакція ОПП розроблялася із залученням заінтересованих сторін та була оприлюднена для громадського обговорення. Її погоджено кафедрою технічного захисту інформації 14.04.2025, Вченою радою Факультету комп'ютерних наук та технологій 16.04.2025, Науково-методичною радою КАІ 22.04.2025 та Студентською радою факультету. ОПП затверджена Вченою радою КАІ 23.04.2025 (протокол № 6) та введена в дію наказом від 29.04.2025 № 283/од. Чинна редакція має обсяг 90 кредитів ЕКТС, з яких 66 кредитів становлять обов'язкові та 24 кредити – вибіркові освітні компоненти.

5. Інформація про контингент здобувачів вищої освіти на ОП станом на 1 жовтня поточного навчального року у розрізі форм здобуття освіти та ліцензійний обсяг за ОП

Рік навчання	Навчальний рік, у якому відбувся набір здобувачів відповідного року навчання	Обсяг набору на ОП у відповідному навчальному році	Контингент студентів на відповідному році навчання станом на 1 жовтня поточного навчального року	У тому числі іноземців
			ОД	ОД
1 курс	2026 - 2027	40	29	1
2 курс	2025 - 2026	69	31	0

Умовні позначення: ОД – очна денна; ОВ – очна вечірня; З – заочна; Дс – дистанційна; М – мережева; Дл – дуальна.

6. Інформація про інші ОП ЗВО за відповідною спеціальністю

Рівень вищої освіти	Інформація про освітні програми
початковий рівень (короткий цикл)	програми відсутні
перший (бакалаврський) рівень	програми відсутні
другий (магістерський) рівень	69358 Безпека інформаційних і комунікаційних систем 69363 Системи технічного захисту інформації, автоматизація її обробки 69365 Системи та технології кібербезпеки
третій (освітньо-науковий/освітньо-творчий) рівень	програми відсутні

7. Інформація про площі приміщень ЗВО станом на момент подання відомостей про самооцінювання, кв. м.

	Загальна площа	Навчальна площа
Усі приміщення ЗВО	280233	162338
Власні приміщення ЗВО (на праві власності, господарського відання або оперативного управління)	280233	162338
Приміщення, які використовуються на іншому праві, аніж	0	0

право власності, господарського відання або оперативного управління (оренда, безоплатне користування тощо)		
Приміщення, здані в оренду	9283	0

Примітка. Для ЗВО із ВСП інформація зазначається:

- ☐ щодо ОП, яка реалізується у базовому ЗВО – без урахування приміщень ВСП;
- ☐ щодо ОП, яка реалізується у ВСП – лише щодо приміщень даного ВСП.

8. Документи щодо ОП

Документ	Назва файла	Хеш файла
Освітня програма	<i>2025 F5 ОПП М Системи та технології кібербезпеки.pdf</i>	SxRdTnwgNVBgtymViWgz02NBHkSFjQySofJjZLqlMFs=
Навчальний план за ОП	<i>НМ-4-F5-3-2025.pdf</i>	XQXr9/p+Lxmp23hBstcPrLlQfy9qZoSvxNcajYsjF7I=
Навчальний план за ОП	<i>НП «Системи та технології кібербезпеки» (денна, F5, магістратура, 2026).pdf</i>	osaKbLxf88rO3Mn4zvGtsRoyjCt6d5WpN9exrx/cu8=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямом (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	<i>Рецензія ТОВ УНІКОММ_СТК.pdf</i>	qpoa8+xGHTeOyZkNoeoJg3Sg+ihnNVlnUreF4RCMwcM=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямом (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	<i>Рецензія ІПМЕ.pdf</i>	I5AQXJqL/yvpBij2Hx8pRqzBc2TDDV9PqKc4gV+HFQg=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямом (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	<i>Рецензія_Seeton_Digital.pdf</i>	zADycTZOHbIAEQCENospef4jwnBu4J+Vmc4jEXSrFCc=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямом (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	<i>Рецензія Інститут прикладних систем управління 2026.PDF</i>	zTy+FgqOoprIv5v9OZfbjT8pm1WwHjKFlqezJ9Otj5M=

1. Проєктування освітньої програми

Чи освітня програма дає можливість досягти результатів навчання, визначених стандартом вищої освіти за відповідною спеціальністю та рівнем вищої освіти? Якщо стандарт вищої освіти за відповідною спеціальністю та рівнем вищої освіти відсутній, поясніть, яким чином визначені ОП програмні результати навчання відповідають вимогам Національної рамки кваліфікацій для відповідного кваліфікаційного рівня?

Наказом МОН України від 18.03.2021 № 332 затверджено Стандарт вищої освіти зі спеціальності 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти, вимоги якого враховано під час розроблення ОП «Системи та технології кібербезпеки». Відповідно до чинного переліку спеціальностей ОП реалізується за спеціальністю F5 «Кібербезпека та захист інформації» галузі знань F «Інформаційні технології».

Зміст ОП дає можливість досягти результатів навчання, визначених Стандартом. ПРН1–ПРН23 ОП відповідають результатам навчання, передбаченим Стандартом, а ПРН24–ПРН26 конкретизують особливості та фокус ОП. ПРН24 передбачає аналіз та оцінювання ефективності й рівня захищеності інформаційних ресурсів, у тому числі в авіаційній галузі. ПРН25 спрямований на вирішення завдань забезпечення та супроводу комплексних систем

захисту інформації і протидії несанкціонованому доступу. ПРН26 передбачає розроблення та впровадження стратегій кіберстійкості, спрямованих на захист критичної цифрової інфраструктури, мінімізацію кіберризиків та розвиток механізмів реагування на кіберзагрози.

Сукупність ПРН1–ПРН26 забезпечується обов'язковими освітніми компонентами, що відображено у матриці забезпечення програмних результатів навчання ОП. Зміст ОП відповідає дескрипторам 7 рівня Національної рамки кваліфікацій та забезпечує формування спеціалізованих знань, методологічних умінь, здатності до критичного й оригінального мислення, проведення досліджень та розв'язання складних задач дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Форма та вимоги до атестації здобувачів другого (магістерського) рівня вищої освіти відповідають Стандарту та передбачають виконання і публічний захист кваліфікаційної роботи.

Чи зміст освітньої програми враховує вимоги відповідних професійних стандартів (за наявності)?

Присвоєння професійної кваліфікації в межах ОП «Системи та технології кібербезпеки» не передбачено.

Водночас при розробленні та перегляді ОП враховано положення професійних стандартів у сфері кібербезпеки та захисту інформації, зокрема: «Аудитор інформаційних технологій (з кібербезпеки)», «Фахівець з підтримки інфраструктури кіберзахисту», «Фахівець з реагування на інциденти кібербезпеки», «Фахівець з кібердосліджень та розробок систем безпеки», затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 23.01.2024 № 38.

Положення зазначених професійних стандартів враховуються у професійній спрямованості ОП, змісті професійно орієнтованих освітніх компонентів, практичній підготовці, курсових роботах і проєктах та тематиці кваліфікаційних робіт. Це сприяє формуванню у здобувачів компетентностей, необхідних для аналізу й оцінювання захищеності інформаційних систем, управління інформаційною безпекою, аудиту, реагування на кіберінциденти, забезпечення функціонування систем кіберзахисту та кіберстійкості критичної інфраструктури.

Чи мета освітньої програми та програмні результати навчання визначаються з урахуванням потреб заінтересованих сторін (стейкхолдерів)?

- здобувачі вищої освіти та випускники програми

Інтереси та пропозиції здобувачів другого (магістерського) рівня вищої освіти та випускників враховуються під час формування і перегляду цілей ОП, компетентностей, ПРН та змісту освітніх компонентів. Перегляд ОП «Системи та технології кібербезпеки» здійснюється кафедрою ТЗІ із залученням заінтересованих сторін. У 2025 році оновлення ОП проводилося відповідно до наказу в.о. президента КАІ від 14.01.2025 № 19/од. Подальше обговорення ОП відбулося на розширеному засіданні кафедри ТЗІ (протокол № 2 від 23.02.2026) (<https://go.kai.edu.ua/3BHALc>), під час якого враховано пропозиції студентки Афанасевої О.М. щодо актуальності редакції ОП та доцільності включення результатів наукової діяльності й публікацій НПП кафедри до навчально-методичного забезпечення обов'язкових ОК. Публічне обговорення та перегляд проєктів ОП здійснюються на сайті кафедри ТЗІ (<https://surl.li/guqrev/>) та КАІ (<https://go.kai.edu.ua/gqGNwM>). Опитування здобувачів проводяться систематично, їх результати обговорюються на засіданнях кафедри та висвітлюються на сайті КАІ (<https://go.kai.edu.ua/R5eDsu>). Студенти залучаються до роботи Вченої ради ФКНТ та беруть активну участь в обговоренні ОП під час її розгляду і затвердження, що підтверджується протоколами кафедри 20.03.2024 № 6, 14.04.2025 № 7 та 23.02.2026 № 2 (<https://go.kai.edu.ua/3BHALc>).

- роботодавці

Під час перегляду ОП «Системи та технології кібербезпеки» на розширеному засіданні кафедри ТЗІ (протокол № 2 від 23.02.2026) (<https://go.kai.edu.ua/WCDemZ>) враховано позиції та пропозиції роботодавців. Начальник відділу інформаційної безпеки ДП «Інформаційні судові системи» Паламарчук Ю.І. відзначив актуальність поточної редакції ОП та її відповідність чинному законодавству у сфері освіти і потребам ринку праці. Генеральний директор ТОВ «УНІКОММ» Ставнюк В.В. також підтвердив актуальність ОП. Окремо роботодавцями рекомендовано посилити матеріально-технічне забезпечення кафедри для підвищення професійної орієнтації майбутніх фахівців та їх конкурентоспроможності; пропозицію враховано.

Інтереси роботодавців враховуються також під час формування змісту освітніх компонентів, фахових компетентностей і ПРН, зокрема щодо здатності працювати в команді й автономно та застосовувати набуті знання у професійній діяльності. Рецензії та інформація про взаємодію зі стейкхолдерами розміщуються на сайті кафедри ТЗІ (<https://go.kai.edu.ua/5br6a3>).x дверей, Днів професій та інших профорієнтаційних і кар'єрних заходів КАІ (<http://iro.kai.edu.ua>).

- академічна спільнота

Інтереси академічної спільноти враховуються під час обговорення та рецензування ОП, участі НПП і здобувачів у наукових конференціях, семінарах, спільних дослідженнях, програмах підвищення кваліфікації та стажування. До перегляду ОП залучаються представники інших ЗВО і наукових установ. Зокрема, професор Державного університету інформаційно-комунікаційних технологій Савченко В.А. під час обговорення ОП відзначив її актуальність та унікальність, зумовлену авіаційною складовою (протокол кафедри № 2 від 23.02.2026) (<https://surl.li/guqrev>). Рецензію на ОП надав д.т.н. Гільгурт С.Я., представник Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Здобувачі залучаються до наукової комунікації та апробації результатів досліджень через участь у науково-практичній студентській конференції «Технічний захист інформації», яку проводить кафедра ТЗІ ФКНТ КАІ (https://www.kzzi.kai.edu.ua/stud_conference/). До оргкомітету залучаються НПП кафедри та представники академічної спільноти. Здобувачі також мають можливість подавати результати досліджень до наукового журналу КАІ «Наукоємні технології» категорії «Б», головним редактором якого є завідувач

- інші стейкхолдери

Взаємодія з іншими заінтересованими сторонами охоплює потенційних вступників та їх батьків, випускників, представників професійного середовища, організацій-партнерів і баз практичної підготовки. Комунікація здійснюється під час Днів відкритих дверей, Днів професій, профорієнтаційних і кар'єрних заходів, фахових конференцій та зустрічей (<http://iro.kai.edu.ua>; <https://www.kzzi.kai.edu.ua>).

23–24 травня 2025 року кафедра ТЗІ ФКНТ долучилася до Фестивалю кар'єри на ВДНГ у Києві, що забезпечило безпосередню комунікацію з молоддю, потенційними вступниками, представниками роботодавців і професійного середовища. Такі заходи використовуються для з'ясування очікувань щодо підготовки фахівців, актуальних професійних компетентностей і потреб ринку праці.

Пропозиції заінтересованих сторін враховуються під час перегляду ОП, змісту освітніх компонентів та робочих програм. Проекти ОП оприлюднюються для громадського обговорення на сайтах KAI (<https://surl.li/vsfamo>) та кафедри ТЗІ (<https://surl.li/rzfabe>).

Чи мета освітньої програми відповідає місії та стратегії закладу вищої освіти?

Мета ОП відповідає місії KAI та Стратегії розвитку KAI на період 2025–2030 років (<https://surl.li/btmbrp>), якою визначено пріоритети розвитку освіти, науки, інновацій, цифрової трансформації та міжнародної співпраці.

Орієнтація ОП на кібербезпеку, критичну інфраструктуру та авіаційну галузь узгоджується з профілем університету, сучасними потребами ринку праці, інтересами роботодавців та академічної спільноти.

Мета ОП «Системи та технології кібербезпеки» полягає у підготовці висококваліфікованих і конкурентоспроможних фахівців у сфері кібербезпеки та захисту інформації, здатних розробляти, впроваджувати та управляти сучасними системами захисту інформації, оцінювати кіберризики, реалізовувати політики інформаційної безпеки та застосовувати новітні технології кіберзахисту, зокрема у критичних інформаційних інфраструктурах та авіаційній галузі.

Зміст і спрямованість ОП відображено на сайті кафедри ТЗІ та у матеріалах щодо спеціальності F5 «Кібербезпека та захист інформації» (<https://www.kzzi.kai.edu.ua>; <https://pk.kai.edu.ua/specialties/kiberbezpeka-ta-zahyst-informacziyi/>).

Чи мета освітньої програми та програмні результати навчання визначаються з урахуванням тенденцій розвитку науки і спеціальності?

Мета та програмні результати навчання ОП «Системи та технології кібербезпеки» відповідають сучасним тенденціям розвитку кібербезпеки та орієнтовані на розв'язання дослідницьких та інноваційних задач. Під час розроблення і перегляду ОП враховуються актуальні напрями: моделювання та прогнозування безпекових процесів, криптографічний захист, управління інформаційною безпекою, аудит і моніторинг, реагування на кіберінциденти, кіберстійкість критичної інфраструктури та інтелектуалізовані системи кіберзахисту. Аналізуються ринок праці (<https://www.work.ua>, <https://robota.ua>, <https://ua.joblum.com>), науково-технологічні тенденції та досвід провідних ЗВО.

Зазначені напрями відображено в ОК «Методи побудови та аналізу криптосистем», «Методологія прикладних досліджень у сфері кібербезпеки», «Моделювання та оптимізація безпекових процесів авіаційної галузі», «Організаційні моделі кібербезпеки», «Аудит інформаційної безпеки», «Інтелектуалізовані системи інформаційної безпеки», а також у тематиці курсових і кваліфікаційних робіт. Сучасні тенденції відображено у ПРН3, 4, 6, 7, 8, 10, 12, 14, 16, 19, 21, 22, 23 (<https://www.kzzi.kai.edu.ua/robotch-ta-navtchalyn-programi/>). ПРН24–ПРН26 конкретизують специфіку ОП щодо оцінювання захищеності, функціонування комплексних систем захисту та кіберстійкості критичної цифрової інфраструктури.

Чи мета освітньої програми та програмні результати навчання визначаються з урахуванням тенденцій розвитку ринку праці, галузевого та регіонального контексту?

При формуванні цілей і ПРН ОП враховано актуальні потреби ринку праці, галузевий та регіональний контекст через взаємодію кафедри з роботодавцями та професійним середовищем, зокрема ДП «Інформаційні судові системи» (<https://ics.gov.ua/ics/>), ТОВ «УНІКОММ» (<https://unicomm.com.ua/>) та КП «Міжнародний аеропорт "Київ" (Жуляни)» (<https://www.airport.kiev.ua/>). Під час перегляду ОП представники роботодавців підтвердили її актуальність і відповідність потребам ринку праці.

Галузевий контекст конкретизовано в ОК5 «Моделювання та оптимізація безпекових процесів авіаційної галузі», ОК6 «Організаційні моделі кібербезпеки», ОК7 «Аудит інформаційної безпеки», ОК8.1 «Інтелектуалізовані системи інформаційної безпеки», а також у ПРН24–ПРН26, що передбачають оцінювання захищеності, супровід систем захисту та забезпечення кіберстійкості, у тому числі в авіаційній сфері.

Актуальність підготовки посилюється Законом України від 27.03.2025 № 4336-IX «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» (<https://zakon.rada.gov.ua/laws/show/4336-20>). Міжнародний контекст враховано через досвід проєкту USAID «Кібербезпека критично важливої інфраструктури України» (<https://fcst.kai.edu.ua/usaidd/>).

Чи мета освітньої програми та програмні результати навчання визначаються з урахуванням досвіду аналогічних вітчизняних освітніх програм?

При формуванні та перегляді ОП «Системи та технології кібербезпеки» враховано досвід аналогічних вітчизняних магістерських ОП. Проаналізовано програми Київського національного університету імені Тараса Шевченка (https://kbzi.knu.ua/magistr_specialty_f5/), НТУ України «КПІ ім. Ігоря Сікорського» (https://osvita.kpi.ua/125_OPPM_STZI), Національного університету «Львівська політехніка» (<https://lpnu.ua/sites/default/files/2021/program/15950/opp2024proekt.pdf>), Державного університету інформаційно-комунікаційних технологій (<https://www.duikt.edu.ua/ua/1826-osvitno-profesiyni-programi-kafedra-upravlinnya-informatsiynoyu-ta-kibernetichnoyu-bezpekoju>) та Київського столичного університету імені Бориса Грінченка (<https://fitm.kubg.edu.ua/struktura1/kafedry/kafedra-informatsiinoi-ta-kibernetichnoi-bezpeky-im-profesora-volodymyra-buriachka/navchalno-metodychna-robota.html>). Результати аналізу відображено у протоколах кафедри від 01.07.2024 № 12 та 25.08.2025 № 11 (<https://www.kzzi.kai.edu.ua/protokoli-pro-analz-nshih-op/>). За результатами порівняння сформовано комплекс обов'язкових і вибіркових ОК для професійної, практичної та дослідницької підготовки. Враховано також досвід НПП кафедри у проєкті USAID «Кібербезпека критично важливої інфраструктури України» (https://pdf.usaid.gov/pdf_docs/PA00XX1T.pdf) та курсів Train the Trainer: Supporting Ukraine's Cyber Resilience. Цей досвід використовується для актуалізації змісту ОП щодо кіберстійкості, кіберризиків і захисту критичної інфраструктури.

Чи мета освітньої програми та програмні результати навчання визначаються з урахуванням досвіду аналогічних іноземних освітніх програм?

Мета ОП та програмні результати навчання формувалися з урахуванням кращих практик і досвіду освітніх програм закордонних університетів у сфері кібербезпеки, зокрема California State University, San Bernardino — Master of Science in Cybersecurity and Analytics (<https://www.csusb.edu/cege/explore/programs/master-science-cybersecurity-and-analytics-overview>), Kansas State University — Master of Science in Computer Science із напрямом Cybersecurity (<https://engg.k-state.edu/academics/graduate/cs/>), Ягеллонського університету (м. Краків) (<https://eurostudy.info/uk/info/yagellonskij-universitet>).

Урахування досвіду зазначених ЗВО сприяло орієнтації ОП на актуальні світові тенденції у сфері кібербезпеки, поєднання технічних та управлінських компетентностей, розвиток практичної підготовки та soft skills, формування здатності оцінювати кіберризик, управляти інформаційною безпекою та забезпечувати захист критичної інфраструктури.

При формуванні змісту ОП враховуються міжнародні стандарти серії ISO/IEC 27000, рекомендації NIST та підходи NICE (National Initiative for Cybersecurity Education).

Розробники ОП також орієнтувалися на досвід закордонних закладів вищої освіти, у яких викладачі кафедри проходили підвищення кваліфікації, зокрема професори Козловський В.В. та Лазаренко С.В. в Akademia Techniczna Humanistyczna w Bielsku-Białej (м. Бельсько-Бяла, Польща). Урахування міжнародного досвіду сприяє забезпеченню якості освітнього процесу, професійній мобільності здобувачів та інтеграції ОП у міжнародний освітній і професійний простір.

2. Структура та зміст освітньої програми

Яким є обсяг ОП (у кредитах ЄКТС)?

90

Яким є обсяг освітніх компонентів (у кредитах ЄКТС), спрямованих на формування компетентностей, визначених стандартом вищої освіти за відповідною спеціальністю та рівнем вищої освіти (за наявності)?

66

Який обсяг (у кредитах ЄКТС) відводиться на дисципліни за вибором здобувачів вищої освіти?

24

Продемонструйте, що зміст ОП відповідає предметній області заявленої для неї спеціальності (спеціальностям, якщо освітня програма є міждисциплінарною)?

Зміст ОП «Системи та технології кібербезпеки» відповідає предметній області спеціальності F5 «Кібербезпека та захист інформації» та вимогам стандарту вищої освіти другого (магістерського) рівня. Об'єктами вивчення є інформаційні, інформаційно-комунікаційні, інформаційно-телекомунікаційні й автоматизовані системи; інформаційні ресурси; програмне та програмно-апаратне забезпечення кіберзахисту; системи управління інформаційною безпекою; технології, методи й моделі кібербезпеки. Нормативний контекст визначається, зокрема, Законом України «Про основні засади забезпечення кібербезпеки України» (<https://zakon.rada.gov.ua/laws/show/2163-19>) та Законом України «Про критичну інфраструктуру» (<https://zakon.rada.gov.ua/laws/show/1882-20>).

Ціллю навчання є підготовка фахівців, здатних розв'язувати задачі дослідницького та інноваційного характеру у сфері кібербезпеки. Теоретичний зміст охоплює системний аналіз, моделювання й оптимізацію, математичні методи, криптографічний і технічний захист інформації, управління ризиками та сучасні технології кіберзахисту. Актуальні підходи до кіберзахисту та критичної інфраструктури представлені також у матеріалах Держспецзв'язку

(<https://cip.gov.ua>).

Галузева спрямованість ОП враховує специфіку авіаційної галузі. Вона узгоджується з Aviation Cybersecurity Strategy ICAO, яка визначає кіберстійкість цивільної авіації, управління, політики безпеки, обмін інформацією, реагування на інциденти та підготовку кадрів як ключові напрями (<https://www.icao.int/aviation-cybersecurity/strategy>). Підходи до управління кіберризиками в авіації конкретизовано також у ICAO Global Cyber Risk Considerations (<https://www.icao.int/aviation-cybersecurity/Doc10213>).

Професійну спрямованість забезпечують ОК3 «Методи побудови та аналізу криптосистем», ОК4.1 «Методологія прикладних досліджень у сфері кібербезпеки», ОК5 «Моделювання та оптимізація безпекових процесів авіаційної галузі», ОК6 «Організаційні моделі кібербезпеки», ОК7 «Аудит інформаційної безпеки», ОК8.1 «Інтелектуалізовані системи інформаційної безпеки», ОК9, ОК10 та ОК11. Робочі програми ОК оприлюднюються на сайті кафедри ТЗІ (<https://www.kzzi.kai.edu.ua/robotch-ta-navtchalyn-programi/>).

Яким чином здобувачам вищої освіти забезпечена можливість формування індивідуальної освітньої траєкторії?

Формування індивідуальної освітньої траєкторії здобувачів вищої освіти в КАІ забезпечується відповідно до Положення про організацію освітнього процесу (<https://surl.li/onvugc>), Тимчасового порядку вибору навчальних дисциплін здобувачами вищої освіти на першому (бакалаврському) та другому (магістерському) рівнях вищої освіти в КАІ в системі «Digital University» (<https://surl.li/ignbul>) та Опису процедури вибору дисциплін (<https://surl.li/fuyqaf>). Процедури вибору навчальних дисциплін представлені за посиланням: (<https://surl.li/haezzzr>). Основним документом щодо формування індивідуальної освітньої траєкторії є індивідуальний навчальний план здобувача.

Загальний обсяг ОП становить 90 кредитів ЄКТС, з яких 24 кредити ЄКТС відведено на вибіркові компоненти, що становить 26,7% загального обсягу ОП та відповідає вимозі щодо забезпечення здобувачеві можливості вибору навчальних дисциплін в обсязі не менше 25%.

Під час формування індивідуальної освітньої траєкторії здобувач також має можливість обирати тематику досліджень, курсових і кваліфікаційних робіт, брати участь у програмах академічної мобільності, навчатися одночасно за кількома освітніми програмами, а також зараховувати результати навчання, отримані у неформальній та/або інформальній освіті.

Яким чином здобувачі вищої освіти можуть реалізувати своє право на вибір навчальних дисциплін?

Вибір навчальних дисциплін здійснюється відповідно до встановленої в КАІ процедури, що передбачає строки організації вибору та алгоритм електронного запису через систему «Digital University» (<https://cabinet.nau.edu.ua/login>).

Здобувачі завчасно інформуються про початок процедури вибору через офіційні канали комунікації, зокрема корпоративну електронну пошту, особистий кабінет у системі «Digital University», сайт та інформаційні ресурси університету. Процедура формування індивідуальної освітньої траєкторії, інформація про вибіркові дисципліни та силабуси висвітлюються на сайті кафедри ТЗІ (<https://go.kai.edu.ua/ЕсКВ9h>) та КАІ (<https://go.kai.edu.ua/bkBdsc>). У встановлені строки здобувач входить до особистого кабінету, ознайомлюється з каталогом вибіркових дисциплін та їх силабусами, визначає пріоритетність і підтверджує свій вибір.

ОП «Системи та технології кібербезпеки» передбачає шість вибіркових компонентів ВК1–ВК6 обсягом 4 кредити ЄКТС кожний, загалом 24 кредити ЄКТС, що становить 26,7% загального обсягу ОП.

Каталог вибіркових освітніх компонентів КАІ включає загальноуніверситетські та факультетські дисципліни. Здобувач має можливість ознайомитися зі змістом дисциплін до здійснення вибору та сформулювати власну індивідуальну освітню траєкторію відповідно до професійних інтересів і освітніх потреб.

Опишіть, яким чином ОП та навчальний план передбачають практичну підготовку здобувачів вищої освіти, яка дозволяє здобути компетентності, необхідні для подальшої професійної діяльності

Практична підготовка здобувачів за ОП «Системи та технології кібербезпеки» здійснюється відповідно до Положення про організацію освітнього процесу в КАІ (<https://surl.li/onvugc>) та Положення про організацію та проведення практик здобувачів вищої освіти КАІ (<https://surl.li/rfwuoz>).

Практична підготовка реалізується як у межах професійно орієнтованих ОК через виконання практичних і лабораторних робіт, курсового проекту та курсової роботи, так і під час проходження практик. Навчальним планом передбачено ОК9 «Науково-дослідна практика в області систем та технологій кібербезпеки» обсягом 6 кредитів ЄКТС та ОК10 «Переддипломна практика» обсягом 9 кредитів ЄКТС.

Науково-дослідна практика спрямована на формування дослідницьких компетентностей, застосування методів аналізу, моделювання та оцінювання процесів у сфері кібербезпеки. Переддипломна практика забезпечує інтеграцію набутих знань і практичних навичок та підготовку матеріалів для кваліфікаційної роботи.

Базами практик можуть бути підприємства, організації, установи та структурні підрозділи КАІ. Практики проводяться на підставі відповідних договорів, інформація про взаємодію з базами практик висвітлюється на сайті кафедри ТЗІ (<http://www.kzzi.kai.edu.ua/prohodzhennya-praktiki/a>).

Продемонструйте, що ОП дозволяє забезпечити набуття здобувачами вищої освіти соціальних навичок (soft skills) упродовж періоду навчання

ОП «Системи та технології кібербезпеки» забезпечує формування соціальних навичок, необхідних для професійної діяльності сучасного фахівця у сфері кібербезпеки та захисту інформації. Відповідно до ОП здобувачі мають бути

здатними спілкуватися з представниками інших професійних груп, зрозуміло доносити власні висновки, організовувати роботу колективів, приймати управлінські рішення та працювати в умовах різних поглядів і підходів. Формуванню soft skills сприяють ОК1 «Ділова іноземна мова», ОК2 «Наукові комунікації у фаховій діяльності», професійно орієнтовані та дослідницькі ОК, виконання курсового проєкту і курсової роботи, практик та кваліфікаційної роботи. Під час навчання здобувачі готують доповіді й презентації, беруть участь у дискусіях, виконують індивідуальні й командні завдання, презентують результати власної роботи та взаємодіють із представниками професійного середовища.

Розвитку соціально-комунікативних навичок сприяють також дисципліни вільного вибору (<https://go.kai.edu.ua/4ereDF>), участь у студентських наукових конференціях кафедри ТЗІ (https://www.kzzi.kai.edu.ua/stud_conference/), діяльність студентського самоврядування та факультетські ініціативи ФКНТ (<https://fcst.kai.edu.ua/>). Студентське самоврядування в КАІ діє на принципах відкритості, добровільності, виборності та рівності участі студентів.

Продемонструйте, що зміст освітньої програми має чітку структуру; освітні компоненти, включені до освітньої програми, становлять логічну взаємопов'язану систему та в сукупності дають можливість досягти заявленої мети та програмних результатів навчання. Продемонструйте, що зміст освітньої програми забезпечує формування загальнокультурних та громадянських компетентностей, досягнення програмних результатів навчання, що передбачають готовність здобувача самостійно здійснювати аналіз та визначати закономірності суспільних процесів

ОП «Системи та технології кібербезпеки» має чітку структуру та логічну послідовність освітніх компонентів, які в сукупності забезпечують досягнення мети ОП та ПРН1–ПРН26. Загальний обсяг ОП становить 90 кредитів ЄКТС, із них 66 кредитів припадає на обов'язкові компоненти та 24 кредити — на вибіркові. Структура, перелік ОК і матриці відповідності наведені в ОП, оприлюдненій на сайті кафедри ТЗІ (<https://www.kzzi.kai.edu.ua/osvtnyo-profesyn-programi/>).

У першому семестрі формуються фундаментальні, професійні й дослідницькі компетентності через ОК1, ОК3, ОК4.1, ОК4.2, ОК5, ОК6; у другому — поглиблюються через ОК2, ОК7, ОК8.1, ОК8.2, ОК9 та ВК1–ВК3; у третьому — інтегруються через ОК10, ОК11 та ВК4–ВК6. Взаємозв'язок компонентів відображено у структурно-логічній схемі, матриці відповідності компетентностей та матриці забезпечення ПРН.

Організація освітнього процесу регламентується чинним Положенням КАІ (<https://surl.li/onvugc>), а реалізація індивідуальної освітньої траєкторії та вибіркової складової — відповідними процедурами вибору дисциплін (<https://surl.li/ignbul>; <https://surl.li/fyuyqaf>).

Формування загальнокультурних і громадянських компетентностей забезпечується через розвиток критичного мислення, професійної комунікації, дослідницьких навичок, відповідального прийняття рішень, дотримання академічної доброчесності та усвідомлення соціальної ролі кібербезпеки. Додаткові можливості для цього забезпечують студентське самоврядування та університетське середовище (<https://nau.edu.ua/ua/menu/studentu/ofis-studenta.html>).

Який підхід використовує ЗВО для співвіднесення обсягу окремих освітніх компонентів ОП (у кредитах ЄКТС) із фактичним навантаженням здобувачів вищої освіти (включно із самостійною роботою)?

У КАІ співвіднесення обсягу освітніх компонентів у кредитах ЄКТС із фактичним навчальним навантаженням здобувачів здійснюється відповідно до Положення про організацію освітнього процесу в КАІ (<https://surl.li/onvugc>) та навчальних планів ОП.

Один кредит ЄКТС відповідає 30 годинам загального навчального навантаження здобувача, що охоплює аудиторну та самостійну роботу, практичну підготовку, виконання індивідуальних завдань та інші види навчальної діяльності. Під час визначення обсягу ОК враховуються його зміст і складність, очікувані результати навчання, кількість аудиторних годин, види навчальних занять та необхідний обсяг самостійної роботи. В ОП «Системи та технології кібербезпеки» передбачено лекційні, практичні та лабораторні заняття, самостійну й науково-дослідну роботу, курсовий проєкт, курсову роботу та практики.

Відповідність запланованого навантаження фактичному оцінюється також за результатами опитувань здобувачів на загальноуніверситетському (<https://surl.li/ctckzz>) та кафедральному рівнях (<https://go.kai.edu.ua/Kda8qq>).

Результати опитувань можуть враховуватися під час удосконалення організації освітнього процесу та збалансування навчального навантаження.

Яким чином структура освітньої програми, освітні компоненти забезпечують практикоорієнтованість освітньої програми? Якщо за ОП здійснюється підготовка здобувачів вищої освіти за дуальною формою освіти, опишіть модель та форми її реалізації

Практикоорієнтованість ОП «Системи та технології кібербезпеки» забезпечується інтеграцією теоретичних знань і практичної підготовки протягом усього періоду навчання. Практична складова реалізується через практичні та лабораторні заняття, виконання курсового проєкту і курсової роботи, розв'язування прикладних задач, дослідницькі та проєктні завдання, ОК9 «Науково-дослідна практика в області систем та технологій кібербезпеки», ОК10 «Переддипломна практика» та ОК11 «Кваліфікаційна робота». Робочі програми освітніх компонентів оприлюднено на сайті кафедри ТЗІ (<https://www.kzzi.kai.edu.ua/robotch-ta-navtchalyn-programi/>).

Зміст ОП забезпечує набуття практичних навичок з аналізу та оцінювання захищеності інформаційних систем, криптографічного захисту інформації, моделювання безпекових процесів, управління інформаційною безпекою, аудиту, застосування інтелектуалізованих систем інформаційної безпеки та розроблення стратегій кіберстійкості. Організація практичної підготовки здійснюється відповідно до Положення про організацію освітнього процесу КАІ (<https://surl.li/onvugc>).

Для практичної підготовки використовуються Навчальний центр «ІТ Академія», навчально-дослідна лабораторія протидії кіберзагрозам в авіаційній галузі (<https://cyberlab.nau.edu.ua/>), кіберполігон Cyber Range UA (<http://surl.li/sybbki>) та лабораторія AxxonSoft (<https://surl.li/ancyop>). У КАІ діє Положення про дуальну форму здобуття вищої освіти (<https://surl.li/dyllph>). Підготовка здобувачів за ОП за дуальною формою не здійснюється.

Яким чином ОП забезпечує набуття здобувачами навичок і компетентностей направлених на досягнення глобальних цілей сталого розвитку до 2030 року, проголошених резолюцією Генеральної Асамблеї Організації Об'єднаних Націй від 25 вересня 2015 року № 70/1, визначених Указом Президента України від 30 вересня 2019 року № 722

ОП «Системи та технології кібербезпеки» забезпечує набуття здобувачами знань, навичок і компетентностей, спрямованих на досягнення глобальних Цілей сталого розвитку до 2030 року, проголошених резолюцією Генеральної Асамблеї ООН №70/1 «Перетворення нашого світу: Порядок денний у сфері сталого розвитку до 2030 року» (<https://sdgs.un.org/2030agenda>) та визначених для України Указом Президента України від 30.09.2019 №722/2019 (<https://www.president.gov.ua/documents/7222019-29825>).

Безпосередньо особливості ОП щодо сталого розвитку відображено у ФК14 та ПРН26. ФК14 передбачає здатність розробляти та впроваджувати стратегії кіберстійкості в межах концепції сталого розвитку, спрямовані на зменшення кіберризиків, захист критичної інфраструктури, створення безпечного цифрового простору та підтримку інновацій, що відповідає Цілі 9 «Промисловість, інновації та інфраструктура» і Цілі 16 «Мир, справедливість та сильні інституції» (<https://sdgs.un.org/goals>).

ПРН26 передбачає розроблення і впровадження стратегій кіберстійкості, захист критичної цифрової інфраструктури, підвищення стійкості інформаційних систем до атак, мінімізацію кіберризиків та розвиток механізмів реагування на кіберзагрози. Його досягнення сприяє реалізації Цілей 9, 11 «Сталий розвиток міст і громад» та 16. Таким чином, ОП формує компетентності, необхідні для розвитку безпечного й стійкого цифрового середовища, інновацій, захисту критичної інфраструктури та кіберстійкості держави і суспільства.

3. Доступ до освітньої програми та визнання результатів навчання

Наведіть посилання на вебсторінку, яка містить інформацію про правила прийому на навчання та вимоги до вступників ОП

Інформація про правила прийому на навчання та вимоги до вступників ОП розміщена на вебсторінці Приймальної комісії <https://pk.kai.edu.ua/official-docs/>

Поясніть, як правила прийому на навчання та вимоги до вступників ураховують особливості ОП?

Вступ на ОП «Системи та технології кібербезпеки» спеціальності F5 «Кібербезпека та захист інформації» здійснюється відповідно до Закону України «Про вищу освіту» (<https://zakon.rada.gov.ua/laws/show/1556-18>), Порядку прийому на навчання для здобуття вищої освіти у 2026 році та Правил прийому до КАІ і додатків до них, оприлюднених на сайті приймальної комісії (<https://pk.kai.edu.ua/official-docs/>).

Вступ на ОП здійснюється на основі диплома бакалавра, спеціаліста або магістра за результатами ЄВІ та ЄДКІ або ЄФВВ з інформаційних технологій — для вступників, які завершили навчання за іншою спеціальністю або у роки, що передують року вступу, у випадках, визначених чинними Правилами прийому. Для вступників на основі диплома спеціаліста або магістра передбачена можливість вступу за результатами випробувань у закладі освіти: співбесіди з іноземної мови замість ЄВІ та співбесіди з ЄФВВ з інформаційних технологій.

Особливості предметної області ОП враховуються на державному рівні під час формування програми профільного ЄФВВ з інформаційних технологій та програми ЄДКІ «Кібербезпека та захист інформації». Це забезпечує перевірку базових знань і компетентностей вступників у сфері інформаційних технологій, інформаційної та кібербезпеки.

Програми вступних випробувань і співбесід, що проводяться в КАІ, розміщені на сайті приймальної комісії (<https://pk.kai.edu.ua/exam-programs/?level=master>).

Яким документом ЗВО регулюється питання визнання результатів навчання та кваліфікацій, отриманих на інших освітніх програмах? Яким чином забезпечується доступність цієї процедури для учасників освітнього процесу?

Визнання результатів навчання та кваліфікацій, отриманих на інших освітніх програмах, регулюється Положенням про визнання результатів навчання в Національному університеті «Київський авіаційний інститут» НУ КАІ П 03.01(07)–01–2026 (<https://go.kai.edu.ua/Ht6tQ3>). Положення визначає процедури визнання результатів формальної, неформальної та/або інформальної освіти, а також результатів академічної мобільності.

Доступність і прозорість процедури забезпечуються оприлюдненням Положення та визначених у ньому критеріїв і процедур, дотриманням принципів рівності, неупередженості та недискримінації. Для здобувачів з особливими освітніми потребами передбачено створення умов розумного пристосування. До роботи Комісії залучається представник студентського самоврядування, який здійснює моніторинг дотримання академічних прав здобувачів. У разі незгоди з рішенням Комісії здобувач має право протягом трьох робочих днів подати апеляцію та брати участь у її розгляді Апеляційною комісією.

Наведіть конкретні приклади та прийняті рішення щодо визнання результатів навчання та

кваліфікацій, отриманих на інших освітніх програмах (зокрема під час академічної мобільності)

Рішення щодо визнання результатів навчання та кваліфікацій, отриманих на інших освітніх програмах (зокрема під час академічної мобільності), ухвалюється колегіально спеціальною Комісією (<https://go.kai.edu.ua/MPqYFX>) протягом 5 робочих днів із дня реєстрації заяви за умови простої більшості голосів та присутності не менше 2/3 її складу. На підставі аналізу академічних довідок, офіційних сертифікатів чи документів з ЗВО-партнера Комісія виносить позитивний або негативний висновок про повне, часткове або асиметричне визнання обов'язкових дисциплін залежно від збігу програмних результатів. При цьому вивчені під час внутрішньої чи міжнародної академічної мобільності вибіркові курси за заявою здобувача зараховуються повністю як компоненти вільного вибору під їхніми оригінальними назвами. Якщо встановлена загальна академічна різниця не перевищує ліміт у 20 кредитів ЄКТС, ухвалюється рішення про зарахування здобувача на поточний семестр. Перевищення цього ліміту є підставою для відмови в зарахуванні на поточний семестр через неможливість успішного виконання програми, після чого особі офіційно пропонують поновлення чи переведення з пониженням курсу (семестру). Фінальний висновок обов'язково фіксується у Протоколі засідання, підписується Головою та секретарем і стає підставою для оформлення відомості перезарахованих дисциплін.

На сьогодні випадків визнання результатів навчання, отриманих на інших освітніх програмах або під час академічної мобільності, на ОПП «Системи та технології кібербезпеки» не було.

Яким документом ЗВО регулюється питання визнання результатів навчання, отриманих в неформальній та/або інформальній освіті? Яким чином забезпечується доступність цієї процедури для учасників освітнього процесу?

Питання визнання результатів навчання, здобутих у неформальній та/або інформальній освіті, регулюється розділом 6 Положення про визнання результатів навчання в Національному університеті «Київський авіаційний інститут» (<https://go.kai.edu.ua/tMU9dE>) (<https://go.kai.edu.ua/tMU9dE>). Процедура ініціюється за заявою здобувача та поданням документів, що підтверджують набуті результати навчання. Комісія аналізує їх відповідність робочій програмі відповідного ОК, за потреби проводить співбесіду та приймає рішення про повне визнання результатів як семестрового контролю, часткове визнання як поточного контролю, невизнання або призначення додаткового контрольного заходу. Для спеціальностей галузі знань F допускається визнання результатів неформальної та/або інформальної освіти в обсязі до 35% освітньої програми. Не підлягають такому визнанню результати з підсумкової атестації, а також практики за відсутності відповідного договору. До складу Комісії з правом дорадчого голосу залучається представник студентського самоврядування, який здійснює громадський контроль за дотриманням академічних прав здобувача та принципу неупередженості. Інформація про можливість визнання таких результатів доводиться до здобувачів через інформаційні ресурси КАІ та під час організаційної роботи зі студентами.

Наведіть конкретні приклади та прийняті рішення щодо визнання результатів навчання отриманих у неформальній та/або інформальній освіті

На сьогодні випадків визнання результатів навчання, отриманих шляхом неформальної та/або інформальної освіти, на ОПП «Системи та технології кібербезпеки» не було.

4. Навчання і викладання за освітньою програмою

Продемонструйте, що освітній процес на освітній програмі відповідає вимогам законодавства (наведіть посилання на відповідні документи). Яким чином методи, засоби та технології навчання і викладання на ОП сприяють досягненню мети та програмних результатів навчання?

Освітній процес за ОП «Системи та технології кібербезпеки» здійснюється відповідно до Закону України «Про освіту» (<https://zakon.rada.gov.ua/laws/show/2145-19>), Закону України «Про вищу освіту» (<https://zakon.rada.gov.ua/laws/show/1556-18>), Стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня, затвердженого наказом МОН України від 18.03.2021 №332 (<https://mon.gov.ua/npa/pro-zatverdzhennya-standartu-vishoyi-osviti-za-specialnistyu-125-kiberbezpeka-dlya-drugogo-magisterskogo-rivnya-vishoyi-osviti>), та Положення про організацію освітнього процесу КАІ (<https://surl.li/ovugc>). Навчання реалізується через лекції, практичні й лабораторні заняття, самостійну та дослідницьку роботу, курсові проекти і роботи, практики та кваліфікаційну роботу. Застосовуються проблемне й проектне навчання, математичне та комп'ютерне моделювання, аналіз і прогнозування, експериментальні методи, дискусії, презентації, індивідуальні й командні завдання. Відповідність методів навчання ПРН конкретизується у робочих програмах ОК (<https://www.kzzi.kai.edu.ua/robotch-ta-navtchalyn-programi/>). Досягненню дослідницьких ПРН сприяє участь здобувачів у наукових заходах, зокрема «ABIA», «Політ» та студентській науково-практичній конференції «Технічний захист інформації» (https://www.kzzi.kai.edu.ua/stud_conference/).

Продемонструйте, яким чином методи, засоби та технології навчання і викладання відповідають вимогам студентоцентрованого підходу. Яким є рівень задоволеності здобувачів вищої освіти методами навчання і викладання відповідно до результатів опитувань?

Студентоцентризований підхід на ОП реалізується відповідно до Положення про організацію освітнього процесу КАІ

(<https://surl.li/onvugc>) через урахування освітніх потреб здобувачів, формування індивідуальної освітньої траєкторії, вибір навчальних дисциплін і систематичний зворотний зв'язок. Організаційну та консультативну підтримку забезпечують кафедра і деканат ФКНТ (<https://fcst.kai.edu.ua/contact/>).

У робочих програмах ОК конкретизовано проблемний, пояснювально-ілюстративний, дослідницький та практикоорієнтований методи, самостійне розв'язування задач, лабораторні й проєктні завдання, презентацію та захист результатів (<https://www.kzzi.kai.edu.ua/robotch-ta-navtchalyn-programi/>). Індивідуальна траєкторія формується через вибір дисциплін у Digital University (<https://surl.li/ignbul>; <https://surl.li/fyyqaf>).

За результатами опитування 2026 р. (25 респондентів) 96% здобувачів оцінили практичну підготовку на достатньому або високому рівні, 96% — якість професорсько-викладацького складу, 96% — зміст та актуальність навчальних програм, 84% — застосування інноваційних та інтерактивних методів навчання (<http://www.kzzi.kai.edu.ua/opituvannya-studentv/>). Результати обговорюються на засіданнях кафедри (<https://go.kai.edu.ua/e4TmXX>) та враховуються під час удосконалення освітнього процесу.

Продемонструйте, яким чином забезпечується відповідність методів, засобів та технологій навчання і викладання на ОП принципам академічної свободи

Академічна свобода на ОП забезпечується відповідно до Закону України «Про освіту» (<https://zakon.rada.gov.ua/laws/show/2145-19>) та Положення про організацію освітнього процесу КАІ (<https://surl.li/onvugc>). Методи, засоби та технології навчання ґрунтуються на принципах свободи слова і творчості, поширення знань та орієнтації на здобувача як активного суб'єкта освітнього процесу.

Академічна свобода здобувачів реалізується через право формувати індивідуальну освітню траєкторію, обирати дисципліни в Digital University (<https://surl.li/ignbul>; <https://surl.li/fyyqaf>), теми курсових і кваліфікаційних робіт та напрями власних досліджень, брати участь в академічній мобільності в Україні й за кордоном (<http://surl.li/kwbwo>), визнавати результати неформальної освіти та брати участь у студентському самоврядуванні (<http://surl.li/agydd>).

НПП мають право на свободу викладання, вільний вибір форм, методів, засобів і технологій навчання відповідно до цілей ОК та ПРН, творчий підхід до подання навчального матеріалу, оновлення змісту дисциплін з урахуванням розвитку науки, технологій, професійних практик і результатів власних досліджень без необґрунтованого втручання в науково-педагогічну діяльність.

Академічна мобільність учасників освітнього процесу підтримується також міжнародними програмами КАІ, зокрема Erasmus+ (<https://imco.kai.edu.ua/>). Це забезпечує здобувачам свободу формування власної освітньої траєкторії, а викладачам — можливість самостійно обирати найбільш доцільні методи для досягнення заявлених ПРН.

Опишіть, яким чином і у які строки учасникам освітнього процесу надається інформація щодо цілей, змісту та очікуваних результатів навчання, порядку та критеріїв оцінювання у межах окремих освітніх компонентів

Інформація про цілі, зміст, очікувані результати навчання, форми контролю та порядок оцінювання за кожним ОК надається здобувачам до початку його вивчення та уточнюється викладачем на першому занятті. Вона міститься у робочих програмах ОК, оприлюднених на сайті кафедри ТЗІ (<https://www.kzzi.kai.edu.ua/robotch-ta-navtchalyn-programi/>), де визначено мету і завдання дисципліни, ПРН, тематичний план, методи навчання, види навчальної роботи та рейтингову систему оцінювання. Наприклад, в ОК7 окремо визначено перелік питань до екзамену, який розробляється відповідно до робочої програми, затверджується кафедрою та доводиться до відома студентів. Поточні завдання, навчально-методичні матеріали, строки їх виконання та додаткова інформація доступні здобувачам у Google Classroom. Контрольні заходи проводяться відповідно до графіка освітнього процесу та робочих програм ОК. Організація освітнього процесу регламентується чинним Положенням КАІ (<https://surl.li/onvugc>). Інформація про вибіркові компоненти надається до початку процедури вибору; порядок вибору дисциплін у Digital University визначено документами КАІ (<https://surl.li/ignbul>; <https://surl.li/fyyqaf>).

Опишіть, яким чином відбувається поєднання навчання і досліджень під час реалізації ОП

Поєднання навчання і досліджень під час реалізації ОП забезпечується через виконання дослідницьких завдань у межах лабораторних, практичних і самостійних робіт, курсового проєкту, курсової роботи, ОК9 «Науково-дослідна практика в області систем та технологій кібербезпеки» та ОК11 «Кваліфікаційна робота».

При кафедрі ТЗІ функціонує студентський науковий гурток «Технології кібербезпеки та захисту інформації» (<https://www.kzzi.kai.edu.ua/naukoviy-gurtok-kafedri-tz/>), діяльність якого спрямована на розвиток дослідницьких компетентностей, роботу з практичними кейсами, аналіз кіберзагроз, підготовку наукових публікацій, тез доповідей і презентацій, участь у конференціях, хакатонах та конкурсах.

Здобувачі беруть участь у студентській науково-практичній конференції «Технічний захист інформації» (https://www.kzzi.kai.edu.ua/stud_conference/), міжнародній конференції «Політ», «ABIA», інших наукових і професійних заходах. У 2024–2025 роках здобувачі спеціальності брали участь у командних змаганнях із кібербезпеки: University CTF 2024 HACKTHEBOX (<https://surl.li/npdmbn>), CTF Snyk 2025 (<https://surl.li/jxivnw>), Cyber Apocalypse CTF 2025 HACKTHEBOX (<https://surl.li/tynlkd>).

Участь у таких заходах дає змогу застосовувати теоретичні знання під час розв'язання реальних і модельних задач, формує навички постановки дослідницьких завдань, аналізу результатів, командної роботи та презентації власних напрацювань.

Продемонструйте, із посиланням на конкретні приклади, яким чином викладачі оновлюють зміст освітніх компонентів на основі наукових досягнень і сучасних практик у відповідній галузі

У КАІ діє Рада з якості КАІ (<https://nau.edu.ua/ua/menu/quality/rada-z-yakosti/>), одним із завдань якої є моніторинг та періодичний перегляд освітніх програм. Відповідно до принципу академічної свободи НПП систематично

оновлюють зміст ОК з урахуванням сучасних наукових публікацій, змін нормативно-правової бази, міжнародних стандартів і професійних практик у сфері кібербезпеки.

Конкретним прикладом є оновлення у 2026 р. робочих програм ОК6 «Організаційні моделі кібербезпеки», ОК7 «Аудит інформаційної безпеки», ОК9 «Науково-дослідна практика в області систем та технологій кібербезпеки» та ОК10 «Переддипломна практика», розглянуте на засіданні кафедри ТЗІ 24.04.2026, протокол №4. Робочі програми ОК оприлюднено на сайті кафедри (<https://www.kzzi.kai.edu.ua/robotch-ta-navtchalyn-programi/>).

В ОК6 оновлено структуру дисципліни та сформовано тематичний план із 10 взаємопов'язаних тем, що охоплюють системи управління кібербезпекою, стратегії та політики безпеки, ISO/IEC і NIST, управління кіберризиками, безперервність бізнес/операційних процесів, реагування на кіберінциденти, аудит і моніторинг, захист критичної інфраструктури та кіберстійкості. Оновлено джерельну базу, зокрема включено NIST Cybersecurity Framework 2.0 (<https://www.nist.gov/cyberframework>), ISO/IEC 27001:2022 (<https://www.iso.org/standard/27001>), ISO/IEC 27002:2022 та ISO/IEC 27005:2022.

В ОК7 актуалізовано теми щодо програми аудиту, внутрішнього аудиту СУІБ, управління ризиками, опрацювання результатів аудиту та підготовки аудиторів. До професійних ресурсів включено CERT-UA (<https://cert.gov.ua/>), Держспецзв'язку (<https://cip.gov.ua/>), NIST (<https://www.nist.gov/>), ENISA (<https://www.enisa.europa.eu/>), ISACA (<https://www.isaca.org/>), OWASP (<https://owasp.org/>) та SANS (<https://www.sans.org/>).

Оновлення ОК9 та ОК10 спрямовано на посилення дослідницької і практичної підготовки, зокрема аналіз кіберризиків, захист інформації, супровід СУІБ, реагування на кіберінциденти та підготовку матеріалів для ОК11 «Кваліфікаційна робота». Тематика кваліфікаційних робіт магістрів другого року навчання формується та щороку актуалізується відповідно до сучасних напрямів кібербезпеки й змісту ОП.

Опишіть, яким чином навчання, викладання та наукові дослідження пов'язані з інтернаціоналізацією діяльності за освітньою програмою та закладу вищої освіти

Інтернаціоналізація навчання, викладання та наукової діяльності в межах ОП «Системи та технології кібербезпеки» реалізується через використання міжнародних стандартів і професійних практик у змісті освітніх компонентів, академічну мобільність, закордонні стажування НПП та міжнародну публікаційну активність.

У навчальному процесі використовуються ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, NIST Cybersecurity Framework (<https://www.nist.gov/cyberframework>), матеріали ISACA (<https://www.isaca.org/>), ENISA (<https://www.enisa.europa.eu/>) та OWASP (<https://owasp.org/>), що відображено, зокрема, у змісті ОК6 «Організаційні моделі кібербезпеки» та ОК7 «Аудит інформаційної безпеки».

Професори Козловський В.В. та Лазаренко С.В. проходили стажування в Технічно-гуманітарній академії у Бельсько-Бялій (Польща). Кудренко С.О. пройшла тренінговий курс з питань охорони прав інтелектуальної власності та комерціалізації результатів досліджень у контексті РП ЄС «Горизонт Європа». Інформація про підвищення кваліфікації НПП представлена на сайті кафедри (<http://www.kzzi.kai.edu.ua/pdvishtennya-kvalifikats-vikladatchv/>).

Міжнародна складова підтримується можливостями академічної мобільності та Erasmus+ у KAI (<https://imco.kai.edu.ua/>). Наукова діяльність НПП підтверджується публікаціями у виданнях, що індексуються у Scopus. Отриманий міжнародний досвід використовується під час оновлення змісту ОК і навчально-методичного забезпечення ОП.

5. Контрольні заходи, оцінювання здобувачів вищої освіти та академічна доброчесність

Яким чином форми контрольних заходів та критерії оцінювання здобувачів вищої освіти дають можливість встановити досягнення здобувачем вищої освіти результатів навчання для окремого освітнього компонента та/або освітньої програми в цілому?

Форми контрольних заходів та критерії оцінювання здобувачів визначаються відповідно до Положення про організацію освітнього процесу KAI (<https://surl.li/onvugc>), ОП та робочих програм освітніх компонентів (<https://go.kai.edu.ua/CHLVCH>). Для кожного ОК вони встановлюються з урахуванням його змісту, видів навчальної діяльності та ПРН, досягнення яких він забезпечує.

В ОП застосовуються поточний, модульний і семестровий контроль, а також підсумкова атестація. Поточний контроль здійснюється у формі усного та письмового опитування, тестування, виконання і захисту практичних та лабораторних робіт, індивідуальних завдань. Це дає змогу оцінити як засвоєння теоретичного матеріалу, так і здатність здобувача застосовувати знання та вміння під час виконання практичних завдань.

Критерії оцінювання та розподіл балів за видами навчальної роботи визначаються у робочих програмах ОК і доводяться до відома здобувачів на початку вивчення дисципліни. Накопичення балів за передбачені види діяльності дає змогу встановити рівень досягнення результатів навчання за конкретним ОК.

Модульний контроль оцінює засвоєння логічно завершених частин дисципліни, а семестровий контроль у формі екзамену, диференційованого заліку, захисту курсового проекту чи курсової роботи забезпечує комплексне оцінювання результатів навчання за ОК. Досягнення результатів навчання за ОП у цілому підтверджується виконанням і публічним захистом кваліфікаційної роботи.

Яким чином забезпечуються чіткість та зрозумілість форм контрольних заходів та критеріїв оцінювання навчальних досягнень здобувачів вищої освіти?

Чіткість і зрозумілість форм контрольних заходів та критеріїв оцінювання забезпечуються Положенням про організацію освітнього процесу в KAI (<https://surl.li/onvugc>), навчальним планом ОП та робочими програмами освітніх компонентів. У кожній РП визначено види навчальної діяльності, форми поточного, модульного та семестрового контролю, кількість балів за окремі види робіт, умови допуску до підсумкового контролю та шкалу

оцінювання.

На початку вивчення ОК викладач ознайомлює здобувачів із формами контрольних заходів, вимогами до виконання завдань, критеріями оцінювання та порядком формування підсумкової оцінки. У разі потреби вимоги до окремих видів робіт додатково уточнюються під час консультацій. Робочі програми ОК розміщуються у відкритому доступі на сайті кафедри, що дає можливість здобувачам завчасно ознайомитися із системою оцінювання (<https://www.kzzi.kai.edu.ua/robotch-ta-navtchalyn-programi/>).

Окремо порядок проведення підсумкової атестації та оцінювання її результатів регламентується Положенням про атестацію здобувачів вищої освіти, затвердженим наказом №193/од від 10.05.2023 (<https://go.kai.edu.ua/8hwVnu>).

Яким чином і у які строки інформація про форми контрольних заходів та критерії оцінювання доводиться до здобувачів вищої освіти?

Інформація про форми контрольних заходів, порядок оцінювання та розподіл балів доводиться до здобувачів на початку вивчення відповідного ОК. Процедури оцінювання регламентуються Положенням про організацію освітнього процесу КАІ (<https://surl.li/onvugc>) та конкретизуються у робочих програмах освітніх компонентів. У робочих програмах зазначаються форми поточного, модульного і семестрового контролю, види навчальної діяльності, максимальна кількість балів за їх виконання, умови допуску до підсумкового контролю та шкала оцінювання. На першому занятті викладач ознайомлює здобувачів із порядком виконання завдань, системою нарахування балів та умовами формування підсумкової оцінки.

Робочі програми ОК розміщені у відкритому доступі на сайті кафедри (<https://go.kai.edu.ua/CHLVCH>). Графік освітнього процесу та розклад занять і контрольних заходів оприлюднюються на інформаційних ресурсах ФКНТ (<https://fcst.kai.edu.ua/>) та кафедри ТЗІ (<https://www.kzzi.kai.edu.ua>). Навчальні матеріали та інформація щодо виконання завдань також доступні здобувачам через Google Classroom.

Яким чином форми атестації здобувачів вищої освіти відповідають вимогам стандарту вищої освіти (за наявності)? Пр продемонструйте, що результати навчання підтверджуються результатами єдиного державного кваліфікаційного іспиту за спеціальностями, за якими він запроваджений

Атестація здобувачів другого (магістерського) рівня за ОП «Системи та технології кібербезпеки» здійснюється відповідно до Стандарту вищої освіти зі спеціальності 125 «Кібербезпека та захист інформації» шляхом публічного захисту кваліфікаційної роботи, що передбачено чинною ОП (<https://www.kzzi.kai.edu.ua/osvtnyo-profesyn-programi/>). Процедура підготовки та проведення атестації регламентується Положенням про атестацію здобувачів вищої освіти (<http://surl.li/iascde>) та Положенням про кваліфікаційні роботи (проекти) здобувачів вищої освіти (<http://surl.li/kyzlf>).

Кваліфікаційна робота має бути спрямована на розв'язання складної задачі у сфері інформаційної безпеки та/або кібербезпеки та передбачати проведення дослідження і/або інноваційну діяльність. Захист відбувається публічно перед екзаменаційною комісією. Кваліфікаційні роботи здобувачів оприлюднюються в інституційному репозитарії КАІ (<https://er.kai.edu.ua/>).

Яким документом ЗВО регулюється процедура проведення контрольних заходів? Яким чином забезпечується його доступність для учасників освітнього процесу?

Процедура проведення контрольних заходів регулюється Положенням про організацію освітнього процесу в КАІ (<https://surl.li/onvug>), Положенням про атестацію здобувачів вищої освіти (<http://surl.li/iascde>) та іншими нормативними документами КАІ, про організацію та проведення практик здобувачів вищої освіти КАІ (<https://go.kai.edu.ua/rt2PBP>).

Усі чинні положення доступні для учасників освітнього процесу на сайті КАІ (<http://surl.li/eisxl>).

Графіки навчального процесу, розклади контрольних заходів та інша організаційна інформація розміщуються на сайтах факультету (<https://fcst.kai.edu.ua/>) та кафедри (<https://www.kzzi.kai.edu.ua>).

Яким чином процедури проведення контрольних заходів забезпечують об'єктивність екзаменаторів? Якими є процедури запобігання та врегулювання конфлікту інтересів? Наведіть приклади застосування відповідних процедур на ОП

Порядок організації та проведення контрольних заходів визначається Положенням про організацію освітнього процесу (<https://surl.li/onvug>) та Положенням про атестацію здобувачів вищої освіти (<http://surl.li/iascde>).

Семестровий контроль з дисципліни проводить лектор із залученням викладачів, які проводили практичні або лабораторні заняття. Перед екзаменами проводяться консультації згідно із затвердженим графіком.

Контрольні заходи здійснюються з дотриманням принципів академічної доброчесності (<https://surl.li/fpfutl>).

У КАІ діють Декларації про дотримання академічної доброчесності НПП та здобувача вищої освіти (<https://surl.li/fpfutl>).

Запобігання та врегулювання конфлікту інтересів здійснюється відповідно до Закону України «Про запобігання корупції». Здобувачі можуть звертатися до куратора, декана, президента, органів студентського самоврядування (<http://surl.li/neojgv>), відділу з питань запобігання та виявлення корупції (<https://nau.edu.ua/ua/menu/studentu/zapobigannya-koruptsii.html>) або скористатися Скринькою довіри (<https://bit.ly/454Jaog>).

На ОП конфліктів інтересів та скарг здобувачів на упередженість або необ'єктивність екзаменаторів не було.

Яким чином процедури ЗВО урегульовують порядок повторного проходження контрольних заходів? Наведіть приклади застосування відповідних правил на ОП

Повторне проходження контрольних заходів регулюється Положенням про організацію освітнього процесу КАІ (<https://surl.li/onvugc>). У разі виникнення академічної заборгованості здобувач має право ліквідувати її у строки, визначені університетом; відповідні графіки доводяться до здобувачів через кафедру, деканат та інформаційні ресурси КАІ. Практика оприлюднення таких графіків застосовується в університеті (<https://flsc.kai.edu.ua/2026/08/21/графік-ліквідації-академічних-забор/>).

Повторне складання контрольного заходу здійснюється у встановленому Положенням порядку. У разі повторного отримання незадовільної оцінки перескладання проводиться перед комісією, склад якої визначається деканом факультету за поданням кафедри. До складу комісії можуть входити представники деканату, завідувач кафедри та НПП відповідного профілю. Оцінка, виставлена комісією, є остаточною. Повторне складання позитивної оцінки з метою її підвищення не допускається.

Інформація щодо організації освітнього процесу та нормативних документів КАІ також доступна на офіційних університетських ресурсах (<https://tkrs.kai.edu.ua/zdobuvacham/>; <https://fcst.kai.edu.ua/>).

Яким чином процедури ЗВО урегульовують порядок оскарження процедури та результатів проведення контрольних заходів? Наведіть приклади застосування відповідних правил на ОП

Порядок оскарження процедури та результатів проведення контрольних заходів регулюється Положенням про організацію освітнього процесу в НУ «КАІ» (<https://surl.li/onvugc>). Здобувач, який не погоджується з виставленою позитивною оцінкою, має право подати письмову апеляцію до деканату факультету не пізніше наступного робочого дня після оголошення результатів оцінювання.

Для розгляду апеляції декан створює апеляційну комісію, до складу якої входять завідувач кафедри та НПП кафедри. Апеляція розглядається у присутності здобувача протягом двох робочих днів. За результатами розгляду оцінка може бути залишена без змін або підвищена, але не може бути знижена.

Рішення апеляційної комісії оформлюється протоколом, оголошується здобувачу після завершення розгляду, фіксується на його письмовій роботі та засвідчується підписами осіб, які брали участь у розгляді апеляції. На ОП «Системи та технології кібербезпеки» випадків оскарження процедури або результатів проведення контрольних заходів не зафіксовано.

Які документи ЗВО містять політику, стандарти і процедури дотримання академічної доброчесності?

Політика, стандарти та процедури дотримання академічної доброчесності в КАІ визначені системою взаємопов'язаних внутрішніх нормативних документів (<https://nau.edu.ua/ua/menu/quality/akademichna-dobrochestnist/>). Базовим документом є Політика академічної доброчесності КАІ (<https://surl.li/moafzr>), яка визначає основні принципи академічної доброчесності, права та обов'язки учасників освітнього і наукового процесу, а також механізми запобігання, виявлення та реагування на порушення.

Процедурний рівень забезпечується Порядком перевірки наукових, кваліфікаційних та освітніх (навчальних) робіт на наявність ознак порушень академічної доброчесності, який визначає єдину процедуру автоматизованої перевірки, експертного оцінювання її результатів та подальших дій, а також Порядком розгляду повідомлень про порушення академічної доброчесності, що регламентує подання і розгляд повідомлень, встановлення факту порушення та прийняття відповідних рішень. Дотримання встановлених принципів підтримується також ознайомленням учасників освітнього процесу з вимогами академічної доброчесності та підписанням Декларації про дотримання академічної доброчесності.

Які технологічні рішення використовуються на ОП як інструменти протидії порушенням академічної доброчесності? Вкажіть посилання на репозиторій ЗВО, що містить кваліфікаційні роботи здобувачів вищої освіти ОП

Як інструмент запобігання порушенням академічної доброчесності в КАІ використовується система StrikePlagiarism, яка забезпечує автоматизований аналіз академічних і наукових текстів, виявлення текстових збігів та ознак можливого використання генеративного штучного інтелекту. Перевірка є складовою внутрішньої системи забезпечення якості та застосовується, зокрема, до кваліфікаційних робіт перед їх захистом.

Результати автоматизованої перевірки мають допоміжний характер і самі по собі не є підставою для встановлення факту порушення академічної доброчесності. У разі виявлення відповідних ознак проводиться експертне оцінювання з урахуванням характеру та обсягу текстових збігів, коректності цитування, специфіки галузі знань і задекларованого використання інструментів штучного інтелекту.

Зберігання та відкритий доступ до академічних і наукових матеріалів, зокрема кваліфікаційних робіт здобувачів вищої освіти, забезпечує Електронний репозитарій КАІ (<https://er.kai.edu.ua/home>).

Яким чином ЗВО популяризує академічну доброчесність серед здобувачів вищої освіти ОП?

КАІ популяризує академічну доброчесність через її інтеграцію в освітній процес і культуру якості, ознайомлення здобувачів із відповідними вимогами, проведення освітніх і просвітницьких заходів та формування навичок відповідального використання ШІ. У 2025–2026 рр. проведено, зокрема, «КАІ Студії #5: Академічна доброчесність і штучний інтелект» (<https://www.youtube.com/watch?v=YogKLhR9dh4>), майстер-клас «Штучний інтелект і академічна доброчесність: як студентам користуватися AI чесно та відповідально» (<https://nau.edu.ua/ua/news/2025/10/24152.html>), семінар «Хижацькі видання: розпізнати та уникнути - місія нездійсненна?» (<https://nau.edu.ua/ua/news/2025/11/24181.html>). 19.03.2026 за участі представників НАЗК та проекту «Прозорі університети» проведено лекцію «Доброчесність у закладах вищої освіти: цінності та принципи»

(<https://nau.edu.ua/ua/news/2026/4/24326.html>). 18.06.2026 Центром якості досліджень та академічної доброчесності організовано методичний семінар «Перевірка академічних робіт: від звіту до висновку» (<https://nau.edu.ua/ua/news/2026/6/24377.html>) за участі представниці StrikePlagiarism, присвячений єдиним підходам до аналізу звітів подібності, ШІ-детекції та практичних кейсів. З 2026/2027 н.р. запроваджено загальноуніверситетську вибіркову дисципліну «Антикорупція та доброчесність».

Яким чином ЗВО реагує на порушення академічної доброчесності? Наведіть приклади відповідних ситуацій щодо здобувачів вищої освіти відповідної ОП

У КАІ діє регламентована процедура реагування на можливі порушення академічної доброчесності (<https://h1.nu/1DX3y>). Виявлення ознак порушення, зокрема за результатами автоматизованої перевірки академічного тексту, не є автоматичним встановленням факту порушення чи підставою для застосування санкцій. У разі виявлення таких ознак здійснюється експертне оцінювання, а матеріали за наявності відповідних підстав передаються для розгляду в установленому порядку. Повідомлення про можливі порушення розглядаються відповідно до Порядку розгляду повідомлень про порушення академічної доброчесності із забезпеченням об'єктивності, неупередженості, конфіденційності, недопущення конфлікту інтересів, а також права особи бути поінформованою про розгляд, надавати пояснення та докази. У разі встановлення порушення застосовуються визначені законодавством і внутрішніми актами КАІ заходи академічної відповідальності; забезпечується право на оскарження.

Фактів порушення академічної доброчесності в межах реалізації ОП не встановлено.

6. Людські ресурси

Продемонструйте, що викладачі, залучені до реалізації освітньої програми, з огляду на їх кваліфікацію та/або професійний досвід спроможні забезпечити освітні компоненти, які вони реалізують у межах освітньої програми, з урахуванням вимог щодо викладачів, визначених законодавством

Реалізацію ОПП «Системи та технології кібербезпеки» забезпечують 9 НПП, серед яких 5 докторів та 4 кандидати наук. Академічна та/або професійна кваліфікація викладачів відповідає змісту закріплених ОК і підтверджується освітою, науковими ступенями, публікаціями, підвищенням кваліфікації, науковою та професійною діяльністю. ОК1 «Ділова іноземна мова» викладає Теремінко Л.Г., к.пед.н., доцент. Її освіта за спеціальністю «Мова і література» та дослідження з методики викладання іноземної мови професійного спрямування, зокрема для ІТ-спеціальностей, відповідають змісту ОК.

ОК2 «Наукові комунікації у фаховій діяльності» викладає Приходько О.Ю., к.пед.н., доцент, співавтор навчальних посібників «Наукові комунікації у фаховій діяльності», «Академічна доброчесність та професійна етика» та практикумів із наукової комунікації.

ОК3 «Методи побудови та аналізу криптосистем» викладає Ільченко А.В., к.т.н., доцент, завідувач кафедри кібербезпеки, освіта, науковий ступінь та науково-методичні праці якої пов'язані із захистом інформації та криптографією.

ОК4.1 «Методологія прикладних досліджень у сфері кібербезпеки» та ОК4.2 (курсний проєкт) забезпечує Ахромович В.М., д.т.н., професор, який має значний досвід наукової діяльності, підготовки й атестації наукових кадрів та дослідження у сфері кібербезпеки. ОК5 «Моделювання та оптимізація безпекових процесів авіаційної галузі» викладає Міщенко А.В., д.т.н., професор. Його дослідження стосуються інформаційної безпеки авіатранспортного комплексу та кіберзахисту критичної інфраструктури; у 2010–2024 рр. працював технічним директором КП «Міжнародний аеропорт "Київ" (Жуляни)».

ОК6 «Організаційні моделі кібербезпеки» забезпечують Кудренко С.О., к.т.н., доцент, та Лазаренко С.В., д.т.н., професор, який проводить лабораторні заняття. Практичний досвід Лазаренка С.В. включає роботу у сфері спеціального зв'язку ДП «Українські спеціальні системи» та ТОВ «УНІКОММ». ОК7 «Аудит інформаційної безпеки» викладає Кудренко С.О.; її наукові та навчально-методичні напрацювання охоплюють кібербезпеку, захист інформації, оцінювання й тестування стану безпеки інформаційних систем.

ОК8.1 «Інтелектуалізовані системи інформаційної безпеки» та ОК8.2 (курсва робота) забезпечує Темніков В.О., д.т.н. зі спеціальності «Інформаційні технології», доцент. Його дослідження пов'язані з інтелектуальними інформаційними технологіями, нечіткою логікою, експертним оцінюванням і системами підтримки прийняття рішень; має публікації у Scopus та досвід керівництва НДР.

ОК9 «Науково-дослідна практика в області систем та технологій кібербезпеки» та ОК10 «Переддипломна практика» забезпечують Лазаренко С.В. і Козловський В.В., д.т.н., професори, досвід яких забезпечує належне науково-методичне керівництво практичною та дослідницькою підготовкою. До керівництва ОК11 «Кваліфікаційна робота» залучаються НПП відповідно до їх наукової спеціалізації, професійного досвіду та тематики робіт здобувачів.

Продемонструйте, що процедури конкурсного відбору викладачів є прозорими, недискримінаційними, дають можливість забезпечити потрібний рівень їхнього професіоналізму для успішної реалізації освітньої програми та послідовно застосовуються

Конкурсний відбір НПП здійснюється відповідно до Порядку проведення конкурсного відбору при заміщенні вакантних посад НПП (<https://go.kai.edu.ua/W7VEy2>), яким визначено вимоги до кваліфікації та досвіду кандидатів. Специфікою конкурсного відбору в КАІ є проведення конкурсною комісією співбесід з кожним кандидатом. До

конкурсу та співбесід допускаються кандидати, які виконали встановлені умови участі в конкурсі. Унікальною практикою КАІ є залучення до складу конкурсної комісії зовнішніх експертів-практиків, досвід яких відповідає профілю кафедри. Метою їх залучення є встановлення рівня актуальності фахової компетентності кандидатів. Прозорість процедури забезпечується проведенням відкритого конкурсу, оголошення про який публікується на офіційному сайті КАІ та порталі вакансій robota.ua. Відсутність обмежень за статтю, віком, релігійними чи політичними переконаннями забезпечує недискримінаційний характер процедури та рівний доступ кандидатів до участі в конкурсному відборі.

Опишіть, із посиланням на конкретні приклади, яким чином заклад вищої освіти залучає роботодавців, їх організації, професіоналів-практиків та експертів галузі до реалізації освітнього процесу

Кафедра технічного захисту інформації системно залучає роботодавців, професіоналів-практиків та експертів галузі до реалізації ОПП «Системи та технології кібербезпеки». Основними формами співпраці є участь у розробленні та перегляді ОПП, її рецензування, проведення практико-орієнтованих занять, підвищення кваліфікації НПП та організація практичної підготовки здобувачів. До співпраці залучаються ДП «Українські спеціальні системи», ТОВ «Світ IT-рішень», ТОВ «Національні конфіденційні мережі», ТОВ «АВТОР», ТОВ «УТБ», ДП «ІСС», ТОВ «УНІКОММ» (<https://www.kzzi.kai.edu.ua/>).

Прикладами залучення професіоналів-практиків є проведення представниками ТОВ «НКМ» заняття «Побудова захищених інформаційно-комунікаційних систем спеціального призначення» (протокол №3 від 15.10.2024); фахівцями ТОВ «Світ IT-рішень» — «Спеціальна перевірка технічних засобів та ОІД» (протокол №13 від 30.09.2025); представниками ТОВ «УТБ» — «Сучасні засоби та системи запобігання несанкціонованому доступу в АС» (протокол №14 від 20.10.2025) <https://drive.google.com/drive/folders/1nVY1UcEbfoNJfYrQnEvyYpk958XeNRVX>. Практична підготовка здобувачів здійснюється, зокрема, на базі ТОВ «Національні конфіденційні мережі» відповідно до договору про співпрацю від 28.02.2019 №583 (<http://www.kzzi.kai.edu.ua/prohodzhennya-praktiki/>).

Яким чином ЗВО сприяє професійному розвитку викладачів ОП? Наведіть конкретні приклади такого сприяння

Розвиток професійної компетентності НПП є одним із напрямів кадрової політики КАІ. Університет створює умови для підвищення кваліфікації та стажувань, участі у програмах академічної мобільності, освітніх і наукових проєктах, тренінгах та професійних заходах. Процедури підвищення кваліфікації регламентуються відповідним Положенням (<https://surl.li/zqrrxd>).

Конкретними прикладами професійного розвитку НПП ОПП є: Кудренко С.О. — підвищення кваліфікації за програмою «Технології програмування C/Embedded» сертифікатної програми «Інженерія вбудованих систем та Інтернет речей» у КПІ ім. Ігоря Сікорського спільно з GlobalLogic; Козловський В.В. — стажування в University of Bielsko-Biala (Польща), підвищення кваліфікації в ICAO European Regional Aviation Security Training Centre та ТОВ «IT-ABIA» з авіаційної кібербезпеки; Лазаренко С.В. — стажування в ТОВ «Світ інформаційно-телекомунікаційних рішень»; Темніков В.О. — стажування в ТОВ «Національні конфіденційні мережі» та підготовка тренерів з проведення кіберсимуляцій на базі Cyber Range UA; Міщенко А.В. — участь у програмі USAID (<https://fcst.kai.edu.ua/usaidd/>.) з менторства технічних директорів з кібербезпеки критичної інфраструктури, підвищення кваліфікації в ТОВ «IT-ABIA» та підготовка тренерів Cyber Range UA. НПП також брали участь у Train the Trainer: Supporting Ukraine's Cyber Resilience (<http://www.kzzi.kai.edu.ua/pdvishtennya-kvalifikats-vikladatchv/>).

Наведіть конкретні приклади заохочення розвитку викладацької майстерності

У КАІ функціонує система матеріального та нематеріального стимулювання професійного розвитку НПП, що передбачає преміювання, матеріальну допомогу, винагороди, нагородження грамотами і подяками та представлення до відомчих і державних відзнак. Система заохочення регламентується Статутом (<https://nau.edu.ua/ua/menu/un%D1%96versitet/pro-universitet/statut-universitetu.html>), Колективним договором (<https://nau.edu.ua/site/variables/news/2024/12/Kolektyvnyi%20dohovir%202024-2025.pdf>), Положенням про преміювання працівників КАІ (<http://drive.google.com/file/d/1AtiOsFtmMVTsuNsEJtY64WBxMM5l9Gom/view?usp=sharing>) та Положенням про винагороду від президента КАІ (<https://nau.edu.ua/site/variables/news/2025/2/Polozhennia%20vynahoroda.pdf>).

Нематеріальне стимулювання здійснюється шляхом відзначення НПП на рівні факультету та університету, а також представлення до відзнак МОН України та інших органів державної влади.

Конкретними прикладами заохочення НПП, залучених до реалізації ОПП, є відзначення Козловського В.В. відзнакою Київського міського голови та Лазаренка С.В. — відомчою відзнакою.

7. Освітнє середовище та матеріальні ресурси

Продемонструйте, яким чином навчально-методичне забезпечення, фінансові та матеріально-технічні ресурси (програмне забезпечення, обладнання, бібліотека, інша інфраструктура тощо) ОП забезпечують досягнення визначених ОП мети та програмних результатів навчання

Матеріально-технічні ресурси КАІ забезпечують освітній процес за ОП у т.ч. в умовах дистанційного та змішаного навчання. Інфраструктура об'єднує 12 навчальних корпусів зі спеціалізованими лабораторіями, 12 гуртожитків, Авіаційний медичний центр, профілакторій, ЦКМ, ІОЦ, Навчально-спортивний оздоровчий центр, Науково-

технічну бібліотеку (<https://surl.li/ibdnws>). Бібліотечний фонд за спеціальністю відповідає чинним ЛУ і щорічно поповнюється (<https://lib.kai.edu.ua>); здобувачам і викладачам надано доступ до міжнародних наукометричних баз Web of Science, Scopus, JSTOR. Навчальні приміщення та лабораторії кафедр укомплектовані необхідним обладнанням, мають доступу до Інтернет, є мультимедійні проектори. Програмне забезпечення KAI включає Google Workspace for Education (корпоративну пошту з доменом університету для всіх учасників освітнього процесу, Google Drive з необмеженим хмарним сховищем, Google Classroom, Google Meet, Google Docs, Sheets, Slides), Microsoft Office 365 Education, Zoom Education та Digital University. Функціонують лабораторії та центри: НЦ «ІТ Академія», НДЛ «Протидії кіберзагрозам в АГ» (<https://cyberlab.nau.edu.ua/>), кіберполігон Cyber Range UA (<https://surl.li/emdkif>; <http://surl.li/vevapn>), лабораторії AxxonSoft (<https://surl.li/tisexh>). Здобувачі мають вільний доступ до РП (<http://www.kzzi.kai.edu.ua/robotch-ta-navtchalyn-programi/>), репозитарію (<https://er.kai.edu.ua/home>), матеріалів у Google Classroom. Фінансове забезпечення спрямовується на підтримку та оновлення зазначених ресурсів.

Продемонструйте, яким чином заклад вищої освіти забезпечує доступ викладачів і здобувачів вищої освіти до відповідної інфраструктури та інформаційних ресурсів, потрібних для навчання, викладацької та/або наукової діяльності в межах освітньої програми, відповідно до законодавства

KAI забезпечує безоплатний доступ викладачів і здобувачів ВО до відповідної інфраструктури, інформаційних ресурсів та мережі Інтернет. У KAI працюють центри: Авіаційний медичний, Інформаційно-обчислювальний, Навчально-спортивний оздоровчий, KAI DEEP TECH, Центр мовної сертифікації та англомовної освіти, Центр підтримки технологій та інновацій (TISC), Навчально-консультативний центр підвищення кваліфікації, сертифікації та перепідготовки кадрів (<https://surl.li/cqgmhb>). Управління міжнародного співробітництва та освіти забезпечує реалізацію заходів, передбачених Стратегією інтернаціоналізації співробітництва в галузі освіти (<https://imco.nau.edu.ua/>). НТБ KAI надає доступ до різних платформ і матеріалів (<https://lib.nau.edu.ua/sources/>; <https://jrnل.nau.edu.ua/>). Для здобувачів ВО доступні IBM Academy (<https://surl.li/pfaaqh>) та грантові програми (<https://surl.li/jzyubq>). Простір для неформальної освіти представлений NAU-hub (<https://surl.li/jmtlyw>), DHub (<https://surl.li/ktujhc>), LAB418 (<https://surl.li/ryekaa>), Clever Space (<https://surl.li/fqrxix>). У межах ОП здобувачі можуть користуватися ресурсами Навчально-наукової лабораторії інтелектуальних систем (<http://surl.li/qkcheb>), Кіберполігону CyberRangeUA (<https://surl.li/cdoqep>), AxxonSoft LAB (<https://surl.li/frhfqk>; <https://surl.li/atqyxz>), KAI-Ajax LAB (<https://surl.li/jzrycv>). KAI має власне студмістечко (<https://studcity.nau.edu.ua/>); усі гуртожитки територіально розташовані компактно в кампусі університету.

Опишіть, яким чином освітнє середовище надає можливість задовольнити потреби та інтереси здобувачів вищої освіти, які навчаються за освітньою програмою, та є безпечним для їх життя, фізичного та ментального здоров'я

Освітнє середовище KAI створює умови для реалізації освітніх, професійних і наукових інтересів здобувачів ОП. Вони мають безоплатний доступ до навчальної інфраструктури, Інтернету, фондів Науково-технічної бібліотеки та фахових інформаційних ресурсів (<https://lib.nau.edu.ua/sources/>; <https://jrnل.nau.edu.ua/>). У межах ОП здобувачі користуються ресурсами профільних лабораторій і спеціалізованих середовищ, зокрема лабораторій ФКНТ (<https://ccs.nau.edu.ua/pro-kafedry/labs-cabinets>), кіберполігону CyberRangeUA (<https://nau.edu.ua/ua/news/2025/6/24024.html>), AxxonSoft LAB (<https://nau.edu.ua/ua/news/2025/8/24082.html>) та Науково-дослідної лабораторії протидії кіберзагрозам в авіаційній галузі (<https://www.cyberlab.nau.edu.ua/>). Індивідуальні освітні потреби реалізуються через вибіркові ОК, академічну мобільність, неформальну освіту, участь у наукових гуртках, конференціях, дослідницьких і грантових ініціативах; діє NAU-hub (<http://aviator.nau.edu.ua/nau-hub/52-nau-hub-tse-prostir-neformalnoi-osvity-v-nau>). У KAI затверджено інструкцію щодо дій у надзвичайних ситуаціях (наказ №222/од від 26.07.2022) та алгоритм дій за сигналом «Повітряна тривога» (<https://lnk.ua/eslcP154b>), врегульовано розподіл укриттів. Управління житлового сервісу (<https://lnk.ua/8FAO5WyiZ>) організовує пункти підтримки під час відключень електроенергії.

Опишіть, яким чином заклад вищої освіти забезпечує освітню, організаційну, інформаційну, консультативну та соціальну підтримку, підтримку фізичного та ментального здоров'я здобувачів вищої освіти, які навчаються за освітньою програмою.

Соціальна підтримка здобувачів реалізується відповідно до законодавства України та локальних актів KAI через механізми стипендіального й соціального забезпечення, підтримку окремих категорій здобувачів та взаємодію з відповідними структурними підрозділами Університету. Важливу роль у цьому відіграє Офіс студента (<https://nau.edu.ua/ua/menu/studentu/ofis-studenta.html>), який функціонує як єдине вікно для звернень студентів і випускників: оформлення довідок, консультування щодо організації навчання, індивідуального графіка, перескладання, користування електронними сервісами KAI та інших питань навчання і студентського життя. Підтримка ментального здоров'я забезпечується, зокрема, через Кабінет психологічної підтримки KAI (<https://go.kai.edu.ua/aFTX8H>). Здобувачі можуть отримати психологічну допомогу та скористатися інформаційними матеріалами щодо психологічного здоров'я, поведінки у кризових ситуаціях і підтримання психологічної стійкості. Підтримка фізичного здоров'я та безпеки охоплює інформаційно-просвітницькі заходи щодо дій у надзвичайних ситуаціях, правил безпечної поведінки та надання домедичної допомоги. Відповідні вимоги та рекомендації визначені нормативними матеріалами KAI (<https://go.kai.edu.ua/Levq4v>), а практичні матеріали з домедичної допомоги доступні на спеціалізованому ресурсі (<https://go.kai.edu.ua/ERb33S>). Ефективність і доступність механізмів підтримки оцінюються шляхом отримання зворотного зв'язку від здобувачів. У KAI проводяться опитування щодо якості освітнього процесу, умов навчання, взаємодії з викладачами та освітнього середовища; їх результати використовуються для визначення проблем і подальшого вдосконалення відповідних сервісів та організації навчання (<https://go.kai.edu.ua/ekpG9T>).

Яким чином ЗВО створює достатні умови для реалізації права на освіту особами з особливими освітніми потребами? Наведіть посилання на конкретні приклади створення таких умов на ОП (якщо такі були)

У КАІ створено комплексну систему забезпечення права на освіту осіб з особливими освітніми потребами. Її засади визначає Політика рівності, інклюзії та доступності (<https://surl.li/wzjbfxf>), що закріплює принципи рівних можливостей, недискримінації та інтеграції інклюзії в освітню, наукову, адміністративну й комунікаційну діяльність Університету. Діє Порядок супроводу осіб з ОП, який визначає механізми підтримки та адаптації освітнього процесу. Для виявлення індивідуальних потреб здобувачів, слухачів курсів і вступників запроваджено гугл-форму «Визначення потреб у супроводі осіб з особливими освітніми потребами в КАІ» (<https://surl.li/foejrjp>). Окремо Порядком організації екзаменів та атестацій для осіб з ОП врегульовано створення належних умов під час контрольних заходів без зниження академічних вимог. Під час навчання застосовуються гнучкі методи, адаптовані матеріали, дистанційні засоби комунікації та індивідуальні організаційні рішення. Для формування інклюзивної культури проведено науково-практичний семінар «Стратегія інклюзії: формування безбар'єрного середовища як професійна та соціальна компетенція». Для захисту прав учасників освітнього процесу створено Комісії розгляду скарг з питань рівності, інклюзії та доступності. Зворотний зв'язок отримується через опитування, електронні звернення та безпосередню комунікацію. Координацію роботи здійснюють Управління організації вступної кампанії та освітньої інклюзії та омбудсмен з питань інклюзії.

Продемонструйте наявність унормованих антикорупційних політик, процедур реагування на випадки цькування, дискримінації, сексуального домагання, інших конфліктних ситуацій, які є доступними для всіх учасників освітнього процесу та яких послідовно дотримуються під час реалізації освітньої програми

Освітня діяльність у КАІ ґрунтується на принципах рівності прав і можливостей, недискримінації, взаємної поваги, відкритості та прозорості. Процедури запобігання та реагування на випадки цькування, мобінгу, кібербулінгу, сексуальних домагань та інших проявів неналежної поведінки визначені Положенням про запобігання та протидію булінгу, мобінгу, кібербулінгу, харасменту в КАІ (<https://bit.ly/3B86qV5>). Для розгляду звернень щодо порушення етичних норм, дискримінації, психологічного тиску та інших конфліктних ситуацій функціонує Комісія з питань етики та врегулювання скарг КАІ (<https://go.kai.edu.ua/QXthQV>).

Запобігання та виявлення корупції здійснюється відповідно до антикорупційної політики та процедур КАІ.

Інформація щодо запобігання корупції, нормативні документи, контакти відповідального підрозділу та канали повідомлення про можливі порушення доступні на офіційному сайті КАІ (<https://nau.edu.ua/ua/menu/studentu/zapobigannya-koruptsii.html>).

Здобувачі також можуть звертатися до гаранта ОП, завідувача кафедри, деканату та органів студентського самоврядування. За час реалізації ОП випадків конфліктних ситуацій, пов'язаних із булінгом, дискримінацією, сексуальними домаганнями або корупцією, не зафіксовано.

8. Внутрішнє забезпечення якості освітньої програми

Яким документом ЗВО регулюються процедури розроблення, затвердження, моніторингу та періодичного перегляду ОП? Наведіть посилання на цей документ, оприлюднений у відкритому доступі на своєму вебсайті

Процедури розроблення, затвердження та періодичного перегляду ОП в КАІ регулюються такими документами:

- Положення про організацію освітнього процесу (розділ 12 та 13) (<https://surl.li/xbpwwgw>)
- Положення про Раду з якості освітньої діяльності та вищої освіти КАІ (<https://surl.li/zyobxi>)

Прозорість діяльності Ради з якості забезпечується оприлюдненням планів та звітів проведеної роботи, результатів моніторингу якості освіти (<http://surl.li/sbfzrl>).

Накази про щорічний перегляд ОПП публікуються відкритому доступі на вебсайті КАІ у вкладках Забезпечення якості — Проекти освітніх програм (<https://salo.li/2593e33>).

Яким чином та з якою періодичністю відбувається перегляд ОП? Які зміни були внесені до ОП за результатами останнього перегляду, чим вони були обґрунтовані?

Відповідно до розділів 12, 13 Положення про організацію освітнього процесу в КАІ (<https://surl.li/onvugc>) здійснюються постійний моніторинг та періодичний перегляд ОП із залученням робочої групи, здобувачів, роботодавців і представників академічної спільноти. Інформація про ОП та результати її обговорення оприлюднюється на сайті кафедри (<https://www.kzzi.kai.edu.ua/osvtnyo-profesyn-programi>).

У 2024 році під час громадського обговорення нової редакції ОП Лахно В.А. запропонував урахувати професійні стандарти у сфері кібербезпеки, Корченко О.Г. — включити до нормативної бази Annex 17 ICAO, Хохлачова Ю.Є. — скоригувати структурно-логічну схему відповідно до переліку ОК. Пропозиції враховано (протокол від 01.04.2024 №3а (<https://go.kai.edu.ua/k7kSux>)). Розроблену редакцію ОП у 2024–2025 н.р. не реалізовано у зв'язку з реорганізацією НАУ.

У 2025 році розроблено нову редакцію ОП, введену в дію наказом в.о. президента КАІ від 29.04.2025 №283/од. За результатами обговорення враховано пропозиції гаранта ОП Зибіна С.В. щодо приведення програми у відповідність до постанови КМУ від 30.08.2024 №1021: шифр спеціальності змінено з 125 на F5, галузі знань — з 12 на F, строк

навчання 1 рік 4 місяці — на розрахунковий строк виконання ОП 1 рік 6 місяців для денної та заочної форм, уточнено опис ОП. За пропозиціями Іванченка І.С. скориговано мету, програмні результати навчання та структурно-логічну схему; Приходько Т.Ю. — предметну область і розподіл аудиторних годин; Козловського В.В. — доповнено фахові компетентності; зовнішнього стейкхолдера Євгенія Педченка — посилено практичну складову підготовки; здобувача Жарюка А.О. — оновлено навчально-методичне забезпечення обов'язкових ОК; Лахна В.А. — враховано вимоги професійних стандартів. Результати обговорення оформлено додатком до протоколу від 14.04.2025 №7. У 2026 році відповідно до наказу президента КАІ від 16.02.2026 №173/ст проведено черговий щорічний перегляд ОП. До обговорення залучено здобувачку Афанасєву О.М., роботодавців Паламарчука Ю.І. (ДП «Інформаційні судові системи»), Ставнюка В.В. (ТОВ «УНІКОММ»), представника академічної спільноти Савченка В.А. та робочу групу ОП. Під час перегляду враховано досвід реалізації програми, тенденції розвитку спеціальності й ринку праці, результати наукових досліджень і стан матеріально-технічного забезпечення. Здобувачами запропоновано ширше використовувати результати наукової діяльності та публікації НПП у навчально-методичному забезпеченні обов'язкових ОК, зовнішніми стейкхолдерами — продовжити поліпшення матеріально-технічного забезпечення кафедри. Пропозиції враховано; чинну редакцію ОП визнано актуальною та такою, що відповідає законодавству, нормативним документам КАІ, тенденціям розвитку спеціальності та ринку праці (протокол від 23.02.2026 №2; <https://www.kzzi.kai.edu.ua/prokti-opp/>).

Продемонструйте, із посиланням на конкретні приклади, як здобувачі вищої освіти залучені до процесу періодичного перегляду ОП та інших процедур забезпечення її якості, а їх пропозиції беруться до уваги під час перегляду ОП

Студенти є повноцінними учасниками процедур забезпечення якості та періодичного перегляду ОП. Їх залучення здійснюється через участь у робочих групах, обговорення проєктів ОП на засіданнях кафедри, опитування та безпосередню комунікацію з гарантом і НПП. У 2025 році здобувач Жарюк А.О., група М-125-24-1-СК, звернув увагу на необхідність посилення зв'язку навчального процесу з актуальними науковими результатами кафедри. За його пропозицією до навчально-методичного забезпечення обов'язкових ОК рекомендовано включати результати наукової діяльності та публікації НПП; у матеріалах обговорення зафіксовано їх упровадження до ОК5, ОК6, ОК7, ОК8.1 (протоколи від 10.02.2025 №2 та від 14.04.2025 №7(<https://go.kai.edu.ua/k7kSux>)). У 2026 році здобувачка Афанасєва О.М., група М-125-24-1-СК висловила пропозицію щодо доцільності включення результатів наукової діяльності та змісту наукових публікацій НПП кафедри до навчально-методичного забезпечення обов'язкових ОК. Пропозицію враховано під час щорічного перегляду ОП (протокол від 23.02.2026 №2(<https://go.kai.edu.ua/k7kSux>))). Результати й пропозиції здобувачів розглянуто на розширеному засіданні кафедри 23.02.2026 (протокол №2) та враховано під час щорічного перегляду ОП. Додатковим механізмом зворотного зв'язку є опитування здобувачів, результати та матеріали яких розміщуються на сайті кафедри (<http://www.kzzi.kai.edu.ua/steykholderi/>). Здобувачі також можуть подавати пропозиції під час відкритого обговорення проєктів ОП, зустрічей із гарантом, НПП та через корпоративні засоби комунікації.

Яким чином студентське самоврядування бере участь у процедурах внутрішнього забезпечення якості ОП?

Участь студентського самоврядування у процедурах внутрішнього забезпечення якості ОП регламентується Положенням про організацію освітнього процесу в КАІ (<https://surl.li/xbpwwg>) та Положенням про студентське самоврядування КАІ (<https://surl.li/bjswqo>). Представники Студентської ради КАІ входять до складу Вченої ради, Ради з якості, комісії з якості факультету та інших колегіальних органів, що дає їм можливість брати участь в обговоренні питань організації освітнього процесу та забезпечення його якості. Регулярно проводяться зустрічі студентів з адміністрацією КАІ; зокрема у лютому 2026 р. обговорювалися питання організації освітнього процесу (https://t.me/studrada_kai/3629). За ініціативи Студентської ради можуть проводитися цільові опитування здобувачів: у лютому 2026 р. проведено опитування щодо проблем організації навчання, за результатами якого напрацьовано відповідні рішення (https://t.me/studrada_kai/3635). Формалізованим механізмом участі студентського самоврядування є погодження навчальних планів головами студентських рад, що забезпечує ознайомлення представників здобувачів зі структурою підготовки, послідовністю ОК, розподілом кредитів ЄКТС та обсягом практичної підготовки. Студенти також можуть брати участь у публічному обговоренні проєктів ОП та опитуваннях, розміщених на сайтах КАІ і кафедри (<https://surl.li/wzhtxh>; <https://www.kzzi.kai.edu.ua/opituvannya-studentv/>).

Продемонструйте, із посиланням на конкретні приклади, як роботодавці безпосередньо або через свої об'єднання залучені до періодичного перегляду ОП та інших процедур забезпечення її якості

Роботодавці системно залучаються до перегляду ОП та процедур внутрішнього забезпечення її якості через участь у робочих групах і розширених засіданнях кафедри, надання пропозицій до змісту ОП, опитування стейкхолдерів, організацію практик, стажування НПП та професійне консультування. Під час перегляду ОП у 2025 році зовнішній стейкхолдер Євгеній Педченко запропонував посилити практичну складову підготовки шляхом збільшення обсягу науково-дослідної практики та оптимізації кредитів переддипломної практики і підготовки кваліфікаційної роботи; пропозицію враховано (протоколи від 10.02.2025 №2 та 14.04.2025 №7 — <https://go.kai.edu.ua/k7kSux>). У 2026 році Паламарчук Ю.І., начальник відділу інформаційної безпеки ДП «Інформаційні судові системи», підтвердив актуальність ОП і її відповідність вимогам ринку праці, а Ставнюк В.В., генеральний директор ТОВ «УНІКОММ», — актуальність чинної редакції; також рекомендовано поліпшувати матеріально-технічне забезпечення кафедри (протокол від 23.02.2026 №2). Результати опитувань роботодавців і стейкхолдерів використовуються під час перегляду ОП (<http://www.kzzi.kai.edu.ua/steykholderi/>). Важливим каналом взаємодії є практична підготовка здобувачів на підприємствах і в організаціях-партнерах (<https://www.kzzi.kai.edu.ua/prohodzhennya-praktiki>).

Опишіть практику збирання, аналізу та врахування інформації щодо кар'єрного шляху та траєкторій працевлаштування випускників ОП (зазначте в разі проходження акредитації вперше)

Збирання та врахування інформації щодо кар'єрних траєкторій випускників ОП здійснюється на рівні кафедри та факультету через анкетування, комунікацію з випускниками, керівниками кваліфікаційних робіт і кураторами груп, а також через професійні та соціальні мережі. Кафедра підтримує зв'язок із випускниками, поширює інформацію про вакансії, організовує зустрічі з роботодавцями та залучає здобувачів до кар'єрних заходів (<https://www.kzzi.kai.edu.ua/nash-vipuskniki>). Показовим прикладом професійної траєкторії є Жарюк Артур Олексійович, який під час навчання брав участь у перегляді ОП, а надалі продовжив професійну діяльність у КАІ як адміністратор платформи «Digital University», беручи участь у забезпеченні цифрової інфраструктури університету та акредитаційних процедурах. Інформація про професійний розвиток випускників використовується як один із каналів зворотного зв'язку під час оцінювання актуальності змісту ОП та її відповідності потребам ринку праці. Додатково КАІ проводить кар'єрні заходи, зустрічі з роботодавцями та ярмарки вакансій, що сприяє працевлаштуванню здобувачів і підтриманню подальшого зв'язку з випускниками.

Продемонструйте, що система забезпечення якості закладу вищої освіти забезпечує вчасне реагування на результати моніторингу освітньої програми та/або освітньої діяльності з реалізації освітньої програми, зокрема здійсненого через опитування заінтересованих сторін

Процедури внутрішнього забезпечення якості ОП регламентовані розділом 12 Положення про організацію освітнього процесу в НУ «КАІ» (<https://surl.li/xbpwgw>). Система має багаторівневу структуру: на рівні університету діють Рада з якості освітньої діяльності та вищої освіти і відділ моніторингу якості вищої освіти, на рівні факультету — комісія із забезпечення якості вищої освіти, на рівні ОП — робоча група, яка здійснює розроблення, моніторинг і періодичний перегляд програми. Процедuru перегляду ОП у 2025–2026 рр. ініційовано наказами президента КАІ (<https://surl.li/hdlyjh>; <https://surl.li/runkdf>). Відділ моніторингу якості проводить загальноуніверситетський й цільові опитування (<https://surl.li/tqbxva>; <https://surl.li/ctbeui>), на кафедральному рівні додатково здійснюються опитування стейкхолдерів (<https://www.kzzi.kai.edu.ua/steikholderi/>).

Механізм удосконалення ОП має простежуваніший характер: пропозиція або зауваження розглядається робочою групою та кафедрою, за потреби виноситься на факультетський рівень і реалізується шляхом внесення змін до ОП або робочих програм ОК. У 2025 р. враховано пропозиції гаранта Зибіна С.В. щодо приведення програми у відповідність до постанови КМУ від 30.08.2024 №1021, Іванченка І.С. — щодо коригування мети, ПРН і структурно-логічної схеми, Приходько Т.Ю. — предметної області та розподілу аудиторних годин, Козловського В.В. — доповнення фахових компетентностей, зовнішнього стейкхолдера Євгенія Педченка — посилення практичної складової, здобувача Жарюка А.О. — оновлення навчально-методичного забезпечення обов'язкових ОК. Результати оформлено протоколами від 10.02.2025 №2 та від 14.04.2025 №7.

У 2026 р. під час чергового перегляду ОП враховано позиції здобувачів, роботодавців та академічної спільноти. Здобувачами порушено питання подальшого включення результатів наукової діяльності НПП до навчально-методичного забезпечення обов'язкових ОК; роботодавцями рекомендовано вдосконалювати матеріально-технічне забезпечення кафедри. Пропозиції розглянуто на розширеному засіданні кафедри 23.02.2026 (протокол №2 <https://go.kai.edu.ua/zsq9QV>) та враховано під час перегляду ОП.

Результати зовнішнього оцінювання також трансформуються у конкретні зміни. У рецензії Інституту прикладних систем управління НАН України від 15.04.2026 рекомендовано актуалізувати зміст ОК2, ОК5, ОК6, ОК7 та ОК8. Зокрема, для ОК6 рекомендовано розширити тематику ризик-апетиту, реєстру кіберризиків, SOC, CSIRT/CERT, KPI/KRI та оцінювання зрілості системи кібербезпеки; відповідні положення включено до оновленої робочої програми ОК6. Рецензії та відгуки зовнішніх стейкхолдерів оприлюднюються на сайті кафедри (<https://www.kzzi.kai.edu.ua/steikholderi/>), що забезпечує простежуваність зв'язку «зовнішня оцінка → рішення → зміна в ОП/ОК».

Продемонструйте, що результати зовнішнього забезпечення якості вищої освіти беруться до уваги під час удосконалення ОП. Яким чином зауваження та рекомендації з останньої акредитації та акредитацій інших ОП були ураховані під час удосконалення цієї ОП?

На інституційному рівні у 2025 році запроваджено постакредитаційний моніторинг, що передбачає опрацювання зауважень та рекомендацій, наданих ЕГ та ГЕР під час проходження акредитації освітніх програм.

Результати опрацювання узагальнюються у зведеній таблиці, яка за кожною позицією фіксує: виявлений недолік або рекомендацію; критерій оцінювання, до якого вона належить; кваліфікацію рекомендації як такої, що має загальноуніверситетський характер; відповідальну особу; строк виконання; підхід до врахування в короткостроковій та довгостроковій перспективі. Окремо передбачено можливість зафіксувати обґрунтування щодо недоцільності врахування конкретної рекомендації, що робить позицію університету прозорою та аргументованою.

Рекомендації інституційного характеру опрацьовуються на рівні вищого керівництва КАІ із залученням проректорів та керівників структурних підрозділів, що забезпечує чіткий розподіл повноважень і відповідальності. За підсумками формується орієнтовний план заходів, спрямованих на усунення виявлених недоліків та реалізацію наданих рекомендацій, із дотриманням встановлених строків. Завдяки цьому результати зовнішнього забезпечення якості за однією ОП стають ресурсом для вдосконалення всіх програм університету.

Акредитація ОП «Системи та технології кібербезпеки» є первинною, тому зауважень і рекомендацій за результатами попередніх акредитаційних експертиз саме цієї програми немає.

Водночас аналіз рекомендацій, наданих ЕГ та ГЕР під час акредитації інших ОП КАІ, було використано для вдосконалення ОП «Системи та технології кібербезпеки». Зокрема: 1) посилено вимоги до відповідності кваліфікації та професійного досвіду НПП освітнім компонентам, які вони забезпечують; 2) посилено систематичний перегляд і актуалізацію змісту ОК та робочих програм з урахуванням сучасних професійних вимог, стандартів і розвитку галузі; 3) розширено залучення здобувачів, роботодавців та інших стейкхолдерів до перегляду й удосконалення ОП. (Водночас аналіз рекомендацій, наданих ЕГ та ГЕР під час акредитації інших ОП КАІ, було використано для

вдосконалення ОП «Системи та технології кібербезпеки». Зокрема: 1) посилено вимоги до відповідності кваліфікації та професійного досвіду НПП освітнім компонентам, які вони забезпечують; 2) посилено систематичний перегляд і актуалізацію змісту ОК та робочих програм з урахуванням сучасних професійних вимог, стандартів і розвитку галузі; 3) розширено залучення здобувачів, роботодавців та інших стейкхолдерів до перегляду й удосконалення ОП. (<http://www.kzzi.kai.edu.ua/osvtnyo-profesyn-programi/>)

Опишіть, яким чином учасники академічної спільноти залучені до процедур внутрішнього забезпечення якості ОП

Внутрішнє забезпечення якості ОП здійснюється на рівнях університету, факультету, кафедри, викладачів і здобувачів відповідно до розділу 12 Положення про організацію освітнього процесу НУ «КАІ» (<https://surl.li/xbpwwg>). На інституційному рівні НПП беруть участь у роботі Вченої ради КАІ (<https://vchenarada.nau.edu.ua/>), Ради з якості (<https://go.kai.edu.ua/97v8tk>) та інших колегіальних органів. На рівні факультету й кафедри питання якості ОП розглядаються на засіданнях Вченої ради факультету, комісії із забезпечення якості та кафедри.

У 2026 р. до розширеного обговорення ОП були залучені представники академічної спільноти та роботодавці. Академічна спільнота також бере участь у зовнішньому рецензуванні ОП: рецензії надавали представники установ НАН України та інших організацій, а їх рекомендації враховувалися під час актуалізації змісту окремих ОК. Рецензії та результати обговорень оприлюднюються на сайті кафедри (<https://www.kzzi.kai.edu.ua/steykholderi/>). НПП ОП співпрацюють із науковцями інших ЗВО та наукових установ у межах спільних публікацій, конференцій і наукових заходів, зокрема за участю Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України та Інституту прикладних систем управління НАН України. Результати такої взаємодії використовуються для оновлення змісту ОК і навчально-методичного забезпечення.

Продемонструйте, що в академічній спільноті закладу вищої освіти формується культура якості освіти

КАІ – університет нового покоління, осередок інженерної, авіаційної та оборонної освіти, де культура якості є важливою характеристикою академічної спільноти. Вона базується на цінностях доброчесності, лідерства та сміливості, компетентності, орієнтації на інтереси України, just culture, рівності, інклюзії та digital як норми. Політика забезпечення якості є складовою стратегічного менеджменту відповідно до Стратегії розвитку КАІ на 2025–2030 рр. (<https://go.kai.edu.ua/MbewzX>).

Університет є учасником експериментального проєкту з розвитку автономії закладів вищої освіти та функціонує в умовах оновленої моделі корпоративного врядування. Наглядова рада здійснює стратегічний нагляд за розвитком університету, контролює реалізацію ключових управлінських рішень та ефективність використання ресурсів (<https://go.kai.edu.ua/9zVnSa>).

У системі управління застосовуються OKR, KPI, проєктний та процесний підходи. Факультети, інститути й центри реалізують свої повноваження в межах загальної стратегії університету. Управління розвитком і якістю освіти функціонує як безперервний цикл «планування – реалізація – моніторинг – періодичний перегляд», що забезпечує системне залучення академічної спільноти, здобувачів і стейкхолдерів до вдосконалення ОП. Координацію процедур внутрішнього забезпечення якості здійснює Рада з якості КАІ (<https://go.kai.edu.ua/tpRXBs>).

9. Прозорість і публічність

Якими документами ЗВО регулюються права та обов'язки усіх учасників освітнього процесу? Яким чином забезпечується їх доступність для учасників освітнього процесу?

Права та обов'язки учасників освітнього процесу в КАІ регулюються системою установчих і внутрішніх нормативних документів університету. Основними є Статут КАІ (<https://nau.edu.ua/ua/menu/un%D1%96versitet/pro-universitet/statut-universitetu.html>) та Стратегія розвитку КАІ на 2025–2030 рр., які визначають засади діяльності університету, права та відповідальність учасників академічної спільноти. Організацію освітнього процесу, права й обов'язки здобувачів та НПП, порядок навчання, оцінювання, практичної підготовки, атестації та інші академічні процедури регламентує Положення про організацію освітнього процесу в КАІ (<https://surl.li/onvugc>). Порядок визнання результатів навчання визначено Положенням про визнання результатів навчання (<https://go.kai.edu.ua/hvrZnh>).

Питання академічної доброчесності регулюються чинною Політикою академічної доброчесності КАІ та іншими документами системи академічної доброчесності, розміщеними на спеціальній сторінці університету (<https://nau.edu.ua/ua/menu/quality/akademichna-dobrochestnist/>). Принципи рівності, інклюзії та доступності визначені відповідною Політикою КАІ (<https://go.kai.edu.ua/GcDC9B>), а порядок захисту прав учасників освітнього процесу та розгляду скарг – чинними внутрішніми нормативними документами університету. Усі зазначені документи оприлюднюються на офіційному вебсайті КАІ та перебувають у відкритому доступі, що забезпечує можливість ознайомлення з ними всіх учасників освітнього процесу.

Наведіть посилання на вебсторінку, яка містить інформацію про оприлюднення ЗВО відповідного проєкту освітньої програми для отримання зауважень та пропозицій заінтересованих сторін (стейкхолдерів).

Інформація про оприлюднення КАІ відповідного проєкту ОП для отримання зауважень та пропозицій

заінтересованих сторін (стейкхолдерів) розміщена на вебсторінці KAI з проєктами нормативних документів (<https://surl.li/zjdtou>), у розділі громадського обговорення (<https://surl.li/bqzmym>), а також на сайті кафедри технічного захисту інформації (<https://www.kzzi.kai.edu.ua/osvtnyo-profesyn-programi/>).

Наведіть посилання на оприлюднену у відкритому доступі на своєму вебсайті інформацію про освітню програму (освітню програму у повному обсязі, навчальні плани, робочі програми навчальних дисциплін, можливості формування індивідуальної освітньої траєкторії здобувачів вищої освіти) в обсязі, достатньому для інформування відповідних заінтересованих сторін та суспільства

На офіційному вебсайті KAI (<https://go.kai.edu.ua/X3Tzt9>) та сайті кафедри технічного захисту інформації (<https://www.kzzi.kai.edu.ua/osvtnyo-profesyn-programi/>) у відкритому доступі оприлюднено інформацію щодо ОП «Системи та технології кібербезпеки», зокрема освітньо-професійну програму у повному обсязі. Навчальні плани розміщено у відповідному розділі сайту кафедри (<https://www.kzzi.kai.edu.ua/navtchalyniy-protses/>). Робочі програми навчальних дисциплін та інші навчально-методичні матеріали оприлюднено у відповідному розділі сайту кафедри (<https://www.kzzi.kai.edu.ua/robotch-ta-navtchalyn-programi/>). Інформація щодо можливостей формування індивідуальної освітньої траєкторії здобувачів представлена на офіційному сайті KAI (<https://go.kai.edu.ua/bkBdsc>). Інформація про НПП, залучених до реалізації ОП, представлена на окремих сторінках викладачів (<https://surl.li/rrghdc>). Затверджені освітні програми KAI оприлюднено на офіційному вебсайті університету (<https://nau.edu.ua/ua/menu/quality/ects/zagalna-informatsiya/informatsiya-po-osvitnih-programah.html>).

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП?

ОП «Системи та технології кібербезпеки» реалізується в KAI — галузевому університеті з потужною інженерною та авіаційною складовою, що створює умови для міждисциплінарної підготовки та досліджень у сфері кібербезпеки. Особливістю ОП є поєднання сучасних технологій кіберзахисту з проблематикою авіаційної галузі, критичної інфраструктури та складних інформаційних систем. Зміст програми враховує професійні стандарти у сфері кібербезпеки та положення Annex 17 ICAO, що посилює її галузеву спрямованість.

Сильними сторонами ОП є:

- комплексний підхід до підготовки магістрів, що охоплює криптографічний захист, методологію прикладних досліджень, моделювання та оптимізацію безпекових процесів, організаційні моделі кібербезпеки, аудит інформаційної безпеки та інтелектуалізовані системи інформаційної безпеки;
- спрямованість на формування здатності інтегрувати фундаментальні та спеціальні знання для розв'язання складних задач інформаційної та кібербезпеки, зокрема у мультидисциплінарному та галузевому контексті;
- виражена авіаційна складова ОП, що реалізується через ОК «Моделювання та оптимізація безпекових процесів авіаційної галузі» та врахування міжнародних вимог до авіаційної безпеки;
- наукова спрямованість підготовки: здобувачі залучаються до досліджень, конференцій, публікацій і виконання кваліфікаційних робіт з актуальної тематики кібербезпеки;
- потужний кадровий потенціал кафедри, який поєднує наукову кваліфікацію НПП, практичний досвід у сфері кібербезпеки й авіаційної галузі, публікаційну активність у виданнях Scopus та Web of Science;
- систематичний перегляд і оновлення ОП із залученням здобувачів, роботодавців та академічної спільноти; пропозиції стейкхолдерів враховуються при коригуванні змісту ОК, компетентностей, ПРН і практичної підготовки;
- можливість формування індивідуальної освітньої траєкторії, участі в академічній мобільності та вибору освітніх компонентів;
- налагоджена взаємодія з роботодавцями, науковими установами та організаціями-партнерами, що реалізується через рецензування ОП, практики, професійні заходи, стажування та спільні наукові активності.

Слабкою стороною ОП можливо вважати обмежену академічну мобільність здобувачів вищої освіти у міжнародних науково-практичних заходах, грантових програмах та недостатнє залучення іноземних фахівців до участі у освітньому процесі та науковій діяльності за ОП у зв'язку з дією правового режиму воєнного стану.

Якими є перспективи розвитку ОП упродовж найближчих 3 років? Які конкретні заходи ЗВО планує здійснити задля реалізації цих перспектив?

Перспективи розвитку ОП «Системи та технології кібербезпеки» упродовж найближчих трьох років пов'язані з подальшим оновленням її змісту відповідно до сучасних тенденцій у сфері кібербезпеки, посиленням практичної та дослідницької складових, розвитком міжнародної співпраці, розширенням взаємодії зі стейкхолдерами та вдосконаленням матеріально-технічного забезпечення.

Передбачається систематична актуалізація змісту ОК з урахуванням розвитку технологій управління кіберризиками, SOC та CSIRT/CERT, реагування на кіберінциденти, аудиту інформаційної безпеки, threat intelligence, MITRE ATT&CK, CVE, штучного інтелекту й інтелектуальних методів аналізу кіберзагроз. Окрему увагу планується приділяти розвитку авіаційної складової ОП, проблематиці кіберстійкості, захисту критичної інфраструктури, хмарних, розподілених і кіберфізичних систем. До навчально-методичного забезпечення ОК і надалі включатимуться результати актуальних наукових досліджень НПП кафедри.

Планується посилювати практичну підготовку шляхом розширення співпраці з підприємствами та установами-партнерами, баз практик, залучення фахівців-практиків до гостьових лекцій, професійного консультування, рецензування ОП і кваліфікаційних робіт. Передбачається подальше вдосконалення матеріально-технічної бази кафедри для проведення практичних і дослідницьких робіт з моделювання кіберінцидентів, аудиту та оцінювання

захищеності інформаційних систем.

Важливим напрямом є розвиток міжнародної складової: розширення академічної мобільності здобувачів і НПП, участі у міжнародних грантових та наукових проєктах, конференціях і спільних дослідженнях, залучення іноземних фахівців до освітнього процесу. Щорічний моніторинг ОП із залученням здобувачів, роботодавців, випускників та академічної спільноти забезпечуватиме коригування запланованих заходів відповідно до змін нормативної бази, технологій і потреб ринку праці.

Запевнення

Запевняємо, що уся інформація, наведена у відомостях та доданих до них матеріалах, є достовірною.

Гарантуємо, що ЗВО за запитом експертної групи надасть будь-які документи та додаткову інформацію, яка стосується освітньої програми та/або освітньої діяльності за цією освітньою програмою.

Надаємо згоду на опрацювання та оприлюднення цих відомостей про самооцінювання та усіх доданих до них матеріалів у повному обсязі у відкритому доступі.

Додатки:

Таблиця 1. Інформація про обов'язкові освітні компоненти ОП

Таблиця 2. Зведена інформація про викладачів ОП

Таблиця 3. Матриця відповідності програмних результатів навчання, освітніх компонентів, методів навчання та оцінювання

Шляхом підписання цього документа запевняю, що я належним чином уповноважений на здійснення такої дії від імені закладу вищої освіти та за потреби надам документ, який посвідчує ці повноваження.

Документ підписаний кваліфікованим електронним підписом/кваліфікованою електронною печаткою.

Інформація про КЕП

ПІБ:

Дата: 28.09.2026 р.

Таблиця 1. Інформація про освітні компоненти ОП

Назва освітнього компонента	Вид освітнього компонента	Силабус або інші навчально-методичні матеріали		Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього*
		Назва файла	Хеш файла	
Ділова іноземна мова	навчальна дисципліна	<i>OK1_РП_Ділова іноземна мова.pdf</i>	PKSrX8aeddBwvMTEWhJET1OhQeatD+DsEI7nYB3shbo=	Обладнання: Навчальна аудиторія з використанням мультимедійного комплексу (ноутбук, проектор, екран настінний). Програмне забезпечення: Корпоративна платформа дистанційного навчання під ліцензією Google GSuite for Education (Google Classroom, Google Meet, Google форми / документи / презентації) з використанням матеріалів електронного навчального курсу.
Наукові комунікації у фаховій діяльності	навчальна дисципліна	<i>OK2_РП_Наукові комунікації у фаховій діяльності-2026.pdf</i>	dNNJFTisw8LcyfkKWC/wCR2ZAGcu8hUFFQlcl+igwno=	Обладнання: Навчальна аудиторія з використанням мультимедійного комплексу (ноутбук, проектор, екран настінний). Програмне забезпечення: корпоративна платформа дистанційного навчання під ліцензією Google GSuite for Education (Google Classroom, Google Meet, Google форми / документи / презентації) з використанням матеріалів електронного навчального курсу.
Методи побудови та аналізу криптосистем	навчальна дисципліна	<i>OK3_РП_Методи побудови та аналізу криптосистем-2026.pdf</i>	tWOE7ju6i6ORlO8ULZ528g5rVaDkCbdc7X3yLuEnXBM=	Обладнання: 1. Навчальна аудиторія, для проведення навчання здобувачів вищої освіти з використанням мультимедійних інформаційних систем та технологій. 2. IP-шифратор «CryptoIP-448» 3. Програмний комплекс криптографічного захисту інформації «Криптосервер 2.0». Програмне забезпечення: Корпоративна платформа дистанційного навчання під ліцензією Google GSuite for Education (Google Classroom, Google Meet, Google форми / документи / презентації) з використанням матеріалів електронного навчального курсу.
Методологія прикладних досліджень у сфері кібербезпеки	навчальна дисципліна	<i>OK4_РП_Методологія прикладних досліджень у сфері кібербезпеки-2026.pdf</i>	sHfIPUBwisCZOISxED25W/JPnZatgd/eInxi99bV5A=	Обладнання: Навчальна аудиторія з використанням мультимедійного комплексу (ноутбук, проектор, екран настінний). Програмне забезпечення: Корпоративна платформа дистанційного навчання під ліцензією Google GSuite for Education (Google Classroom, Google Meet, Google форми / документи / презентації) з

				використанням матеріалів електронного навчального курсу.
Методологія прикладних досліджень у сфері кібербезпеки	курсова робота (проект)	Методичні рекомендації до КР_Методологія прикладних досліджень у сфері кібербезпеки.pdf	wXowGF/MxsSCqtNoQbFmMI7ma+lPa5oLmNytoGODiVM=	Обладнання: Навчальна аудиторія з використанням мультимедійного комплексу (ноутбук, проектор, екран настінний). Програмне забезпечення: Корпоративна платформа дистанційного навчання під ліцензією Google GSuite for Education (Google Classroom, Google Meet, Google форми / документи / презентації) з використанням матеріалів електронного навчального курсу.
Моделювання та оптимізація безпечних процесів авіаційної галузі	навчальна дисципліна	OK5_РП_Моделювання та оптимізація безпечних процесів авіаційної галузі-2026.pdf	AoCulbWEDIEzmGbVappSPqGK1e3ooSqSoGxrzAbDphA=	1. Навчальна аудиторія, для проведення навчання здобувачів вищої освіти з використанням мультимедійних інформаційних систем та технологій. 2. Скануючий приймач «AR-5000» 3. Скануючий приймач «AR-8600» 4. Пошуковий комплекс «Digi Scan Labs» 5. Пошуковий комплекс ST-031 «Піранья» 6. Нелінійний радіолокатор «NR-μ» 7. Генератор «SRC-300A» (багатофункціональний засіб блокування мобільних пристроїв) 8. АТС «PEEINTN» 9. IP-шифратор «CryptoIP-448» 10. Навчальний стенд дослідження охоронних систем 11. ППК ОП «Дунай» 16/32 12. Ретрополятор «Дунай Р-1000» 13. ПК «Satel» 14. ППК «ВБД 6-12» 15. Навчальний комплект охоронної системи INTEGRA 64 WSR 16. Навчальний стенд дослідження систем відеоспостереження 17. Програмактор комплексу відеонагляду 18. Пульт керування системою відеонагляду Panasonic CN161 19. Камера Panasonic WV-CW960 20. Комутатор 3COM 21. Комутатор SRW208P 22. Комутатор VM-42 23. Зчитувач даних SAGEM MA 520 24. Пристрій цифрового запису відеоданих WY HD220 25. Аналого-цифровий перетворювач B480 26. DSP камера відеонагляду з кронштейном 27. Камера NVL-5500 28. Камера NVC-180BH 29. Камера Panasonic WV-CF294 30. Камера Samsung SNC-B2315P 31. Камера WyY N-202 32. Монітор виведення даних LD2000/6 Програмне забезпечення: Корпоративна платформа дистанційного навчання під ліцензією Google GSuite for Education (Google Classroom, Google Meet, Google форми / документи / презентації) з використанням матеріалів електронного навчального курсу.

Організаційні моделі кібербезпеки	навчальна дисципліна	<i>OK6_Організаційні_моделі_кібербезпеки.pdf</i>	bANKgIauLwnZh38f6HdpXx/8jNEWSTnwynZGw3Sb1E=	Обладнання: Навчальна аудиторія, для проведення навчання здобувачів вищої освіти з використанням мультимедійних інформаційних систем та технологій. Програмне забезпечення: Корпоративна платформа дистанційного навчання під ліцензією Google GSuite for Education (Google Classroom, Google Meet, Google Форми / Документи / Презентації); diagrams.net (draw.io) для побудови організаційних схем; Google Sheets для аналізу та оцінювання кіберризиків; матеріали електронного навчального курсу
Аудит інформаційної безпеки	навчальна дисципліна	<i>OK7_Аудит_інформаційної_безпеки.pdf</i>	ybpqRCcaXLQ4KoB3wP5o7cGV177siIlyFLQmEfoKd4w=	Обладнання: Навчальна аудиторія з використанням мультимедійного комплексу (ноутбук, проектор, екран настінний); детектор радіочастоти RD-14; індикатор поля з функцією вимірювання частоти RD-16М; пошуковий комплекс ST-031 «Піранья»; нелінійний радіолокатор NR-μ; навчальний стенд дослідження систем відеоспостереження. Програмне забезпечення: Корпоративна платформа дистанційного навчання під ліцензією Google GSuite for Education (Google Classroom, Google Meet, Google Форми / Документи / Презентації) з використанням матеріалів електронного навчального курсу.
Інтелектуалізовані системи інформаційної безпеки	навчальна дисципліна	<i>OK8_Інтелектуалізовані_системи_інформаційної_безпеки.pdf</i>	UboCnd4mFd2YBwlDhKtovh8gMaLglRzA+XGc6omys04=	Обладнання: Навчальна аудиторія з використанням мультимедійного комплексу (ноутбук, проектор, екран настінний); навчальний стенд дослідження охоронних систем; ППК ОП «Дунай» 16/32. Програмне забезпечення: Корпоративна платформа дистанційного навчання під ліцензією Google GSuite for Education (Google Classroom, Google Meet, Google Форми / Документи / Презентації); Python; Jupyter Notebook; NumPy; Pandas; scikit-learn; TensorFlow.
Інтелектуалізовані системи інформаційної безпеки	курсowa робота (проект)	<i>Методичні_рекомендації_ICIB_KP.pdf</i>	mnJHn6K71W67QCdcE8rDAbyrNy54s7B1NlaACcs/baA=	Обладнання: Навчальна аудиторія з використанням мультимедійного комплексу (ноутбук, проектор, екран настінний). Програмне забезпечення: Корпоративна платформа дистанційного навчання під ліцензією Google GSuite for Education (Google Classroom, Google Meet, Google Форми / Документи / Презентації); Python; Jupyter Notebook; NumPy; Pandas; PyTorch; Kaggle.
Науково-дослідна практика в області систем та технологій кібербезпеки	практика	<i>OK9_РП_Науково_дослідна_практика_СТК.pdf</i>	zKUlepdQdkIAuIeM4Xt19Mm+mgwbxJT XgZ6HyhvMvTA=	Обладнання: Науково-дослідна практика у сфері систем та технологій кібербезпеки проводиться на базах практики

				згідно з договорами між університетом і підприємствами та організаціями. Для захисту результатів науково-дослідної практики та представлення результатів наукових досліджень застосовується навчальна аудиторія з мультимедійним комплексом (ноутбук, проектор, екран настінний). Програмне забезпечення: Корпоративна платформа дистанційного навчання під ліцензією Google GSuite for Education (Google Classroom, Google Meet, Google Форми / Документи / Презентації) з використанням матеріалів електронного навчального курсу.
Переддипломна практика	практика	OK1o_РП_Переддипломна_практика_СТК.pdf	xH+uTJX7UaOy7AYWDR+hqII6sBCQp46QofcEgJn1Vkl=	Обладнання: Переддипломна практика проводиться на базах практики згідно з договорами між університетом і підприємствами та організаціями. Для захисту результатів переддипломної практики та представлення результатів наукових досліджень застосовується навчальна аудиторія: мультимедійний комплекс (ноутбук, проектор, екран настінний). Програмне забезпечення: Корпоративна платформа дистанційного навчання під ліцензією Google GSuite for Education (Google Classroom, Google Meet, Google форми / документи / презентації) з використанням матеріалів електронного навчального курсу.
Кваліфікаційна робота	підсумкова атестація	Положення про кваліфікаційні роботи.pdf	gdnPqQxyW5Dr5jdNT/fbwURm83i8kmm pg/hMLrTBv1g=	Обладнання: Навчальна аудиторія з використання мультимедійного комплексу (ноутбук, проектор, екран настінний). Програмне забезпечення: Корпоративна платформа дистанційного навчання під ліцензією Google GSuite for Education (Google Classroom, Google Meet, Google форми / документи / презентації).

* наводяться відомості, як мінімум, щодо наявності відповідного матеріально-технічного забезпечення, його достатності для реалізації ОП; для обладнання/устаткування – також кількість, рік введення в експлуатацію, рік останнього ремонту; для програмного забезпечення – також кількість ліцензій та версія програмного забезпечення

Таблиця 2. Зведена інформація про відповідність НПП освітнім компонентам

ІД викладача	ПІБ	Посада	Структурний підрозділ	Кваліфікація викладача	Стаж	Навчальні дисципліни, що їх викладає викладач на ОП	Обґрунтування відповідності освітньому компоненту (кваліфікація, професійний досвід, наукові публікації)
494533	Льєнко	Завідувач	Факультет	Диплом	16	Методи	Освіта: Національний

	Анна Вадимівна	кафедри, Основне місце роботи	комп'ютерних наук та технологій	магістра, Національний авіаційний університет, рік закінчення: 2009, спеціальність: Захист інформації в комп'ютерних системах та мережах, Диплом кандидата наук ДК 002600, виданий 17.02.2012, Атестат доцента 12/ДЦ 042200, виданий 28.04.2015	побудови та аналізу криптосистем	авіаційний університет, 2009 р., спеціальність – «Захист інформації в комп'ютерних системах та мережах», кваліфікація – «науковий співробітник (безпека підприємств, установ та організацій)» Науковий ступінь: Кандидат технічних наук, 05.13.21 – Системи захисту інформації, тема дисертації «Методи підвищення ефективності захищених інформаційно- комунікаційних систем на основі ідентифікації кодових конструкцій». Вчене звання: Доцент кафедри комп'ютеризованих систем захисту інформації. Підвищення кваліфікації: 1. Cybersecurity Summer Instructor Training Program under the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity course Web security. Термін 11.07.2022р.- 31.08.2022р. Сертифікат (180 годин/6 кредитів ЄКТС). 2. Softserve. Тема «Підвищення кваліфікації: Вдосконалення викладання у вищій освіті: інституційний та індивідуальний виміри». Термін 22.12.2022р. Сертифікат (2 години/0,067 кредита ЄКТС). 3. Sigma Software University. Тема «Практичні кейси проектного навчання, створення e-learning курсу». Термін 28.01.2023р. Сертифікат (30 годин/1 кредит ЄКТС). 4. Проект Еразмус+ №: 101085825 - ERASMUS-JMO-2022- MODULE. Тема «Європейський досвід для підвищення стійкості критично важливих об'єктів в Україні». Термін 25.04.2023р. Сертифікат (1,5 години/0,05 кредита ЄКТС). 5. Літня школа 2023 у
--	---------------------------	--	--	--	---	---

							рамках проєкту Еразмус+ модуль Жан Моне, тема - «Європейський досвід для підвищення стійкості критично важливих об'єктів в Україні». Термін 17.07.2023р. – 04.08.2023 р. Сертифікат (120 годин/4 кредита ЄКТС). 6. EPAM та IT Ukraine Association. Тема: «Teachers Internship: Deep Dive into AWS (Amazon Web Services)». Термін липень 2023р. Сертифікат (60 годин/2 кредита ЄКТС). 7. Sigma Software University і IT Ukraine Association. Тема «Teachers Smart Up: Summer Edition 2023». Термін 17.07.2023р. - 21.07.2023 р. Сертифікат (1 кредит ЄКТС). 8. Sigma Software University. Тема «Як розробити ефективний курс електронного навчання». Термін 02.04.2023р. Сертифікат (2 години/0,067 кредита ЄКТС). 9. GlobalLogic Education. Тема «ІТ-інструменти для викладачів». Термін липень-серпень 2023 р. Сертифікат (18 годин/0,6 кредита ЄКТС). 10. SoftServe. Тема «Tech Summer Bootcamp for Teachers -2023». Термін липень-серпень 2023 р. Сертифікат (9,9 годин/0,33 кредита ЄКТС) 11. EPAM та IT Ukraine Association. Тема: «Teachers Internship (Winter 2024) / Інструменти штучного інтелекту для викладачів і дослідників» Термін січень-лютий 2024. Сертифікат (90 годин/3 кредита ЄКТС). 12. Sigma Software University. Sigma Software University: Teachers Smart Up: Winter Edition 3.0 2024 / Тренди в ІТ. Термін: 22-26 січня 2024 Сертифікат (30 годин/1 кредит ЄКТС)
--	--	--	--	--	--	--	--

							Види і результати професійної діяльності, згідно п. 38 Ліцензійних умов провадження освітньої діяльності: 1, 3, 4, 7, 8, 9, 12, 14 п. 1 1. Anna Ilyenko Program Module of Cryptographic Protection Critically Important Information of Civil Aviation Channels / Sergii Ilyenko, Anna Ilyenko // Lecture Notes on Data Engineering and Communications Technologies. – Vol.134.– 2022. – pp. 235–247.(Scopus) 2. Ільєнко А., Ільєнко С.,Кваша Д., Мазур Я. Практичні підходи щодо виявлення вразливостей в інформаційно-телекомунікаційних мережах // Кібербезпека: освіта, наука, техніка. – 2023. – Т.3 № 19. – С. 46-56. (фахове видання категорії В). 3. Anna Ilyenko, Sergii Ilyenko, Olena Prokopenko, Hennadii Hulak, and Iryna Melnyk. Practical Aspects of Using Fully Homomorphic Encryption Systems to Protect Cloud Computing. Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II 2023), Kyiv, Ukraine, October 26, 2023, vol. 3550, pp. 226-233. Available at: https://ceur-ws.org/Vol-3550/short5.pdf. (Scopus). 4. Ільєнко А.В. Перспективи інтеграції штучного інтелекту в системи кібербезпеки / С.Ільєнко, О.Яковенко, Є.Галич, В.Павленко// Кібербезпека: освіта, наука, техніка. – 2024. – Т.1 № 25. – С. 318-329. (фахове видання категорії В). 5. Ільєнко А.В. Сучасні кіберзагрози критичної інфраструктури України та світу / А.В.Ільєнко, В.А.Телющенко, О.В.Дубчак // Кібербезпека: освіта,
--	--	--	--	--	--	--	---

							наука, техніка. – 2025. – Т.3 № 27. – С.150-164. (У фаховому виданні категорії В). п.3 1.Маніпулювання: технології, засоби впливу та шляхи захисту: навчальний посібник / Петрик В. М., Присяжнюк М. М., Черненко О. Є., Карпович О. М., Закаблуковська О. О. та ін.; за заг. ред. В. М. Петрика, М. М. Присяжнюка. – К., Видавничий центр “Кафедра”, 2026. – 336 с. 2.Петрик В.М., Кононович В.Г., Аль-Файюмі Халед та ін. Кібергігієна: аналіз в контексті кіберпсихології та соціальної інженерії: навч. посіб. [за заг. ред. В. М. Петрика, С. В. Стайкуци. – К.; Видавничий центр “Кафедра”, 2026. - 360 с. п. 4 1. Ільєнко А.В. Прикладна криптологія // Лабораторний практикум для студентів. – К.: НАУ, 2022. – 60 с. 2. Робоча програма та НМК «Методи побудови та аналізу криптосистем» ОС Магістр. 2025. – 14 с. 3. Робоча програма та НМК «Моніторинг та аудит кібербезпеки» ОС Магістр. 2025. – 12 с. п.7 1. Секретар спеціалізованої вченої ради Д 26.062.01 KAI https://mon.gov.ua/npra/pro-zatverdzhenniarishen-atestatsiinoikolehii-ministerstva 2. Участь в атестації наукових кадрів як члена не менше трьох разових спеціалізованих вчених рад 2.1. Рецензент: Петляк Наталія Сергіївна — доктор філософії за спеціальністю 125 «Кібербезпека». Тема дисертації: «Моделі та методи виявлення аномального трафіку в інформаційно-комунікаційних системах». Захист — 14.08.2025, Державний
--	--	--	--	--	--	--	---

							університет «Київський авіаційний інститут», диплом Н25 №002772 від 29.08.2025. 2.2. Рецензент: Скуратівський Анатолій Анатолійович — доктор філософії за спеціальністю 122 «Комп'ютерні науки». Тема дисертації: «Методи та інструментальні засоби управління вимогами кібербезпеки при впровадженні програмного забезпечення в бізнесі». Захист — 15.06.2026, Національний університет «Київський авіаційний інститут», диплом Н26 №001770 від 30.06.2026. 2.3. Рецензент: Терейковський Олег Ігорович — доктор філософії за спеціальністю 125 «Кібербезпека». Тема дисертації: «Нейромережеві методи та моделі біометричної автентифікації в інформаційних системах об'єктів критичної інфраструктури». Захист — 07.07.2026, Національний університет «Київський авіаційний інститут», диплом Н26 №002740 від 28.07.2026. п. 8 1. НДР № 5-2024/18.02 «Система забезпечення кібербезпеки та стійкості об'єктів критичної інфраструктури». Термін виконання - 01.03.2024 р. – 30.06.2026 р. (відповідальний виконавець) п.9 1. Експерт Національного агентства із забезпечення якості вищої освіти, член галузевої експертної ради. Протокол № 17 (89) від 18.11.2025 за спеціальність 125 "Кібербезпека та захист інформації" https://surl.li/nddnhy
--	--	--	--	--	--	--	--

							п. 12 1. Ільєнко А.В. Актуальні вразливості проведення автентифікації за допомогою JSON WEB TOKEN / М.С. Остапенко, І.А. Кравчук // Eurasian scientific discussions: the 9th International scientific and practical conference, 25-27 september 2022 г.: abstracts. – Barcelona (Spain), 2022. – P. 78-83. матеріали Міжнародної конференції) 2. Ільєнко А.В. Сучасні криптографічні методи захисту інформації / А. Є. Кармазіна, І.А. Кравчук // Science and innovation of modern world: the 1st International scientific and practical conference, 28-30 september 2022 г.: abstracts. – London (United Kingdom), 2022. – P. 106-110. матеріали Міжнародної конференції) 3. Анна Ільєнко, Тищенко Олександр, Ірина Кравчук Перспективи використання гомоморфного шифрування для хмарних обчислень // Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS): V міжнародна науково-практична конференція, 27-28 жовтня 2022 р.: тези доповіді. – К., 2022. – С.21-22. матеріали Міжнародної конференції) 4. Ільєнко А., Якимчук Є. А., Кравчук І. А. Програмний модуль автентифікації користувачів з використанням непрозорих токенів // Modern problems of science, education and society: VIII Міжнародна науково-практична конференція, 9-11 жовтня 2023 р.: тези доповіді. – К., 2023. – С.358-360. 5. Ільєнко А., Галич Є.О., Павленко В.Г.Сучасний стан забезпечення кібербезпеки та стійкості об'єктів критичної
--	--	--	--	--	--	--	---

							інфраструктури України // Живучість та резильєнтність – 2023: міжнародна науково-практична конференція 19 жовтня 2023 р.: тези доповіді. – К., 2023. – С.45-48. 6. Ільєнко А.В. Підхід щодо перевірки цифрових сертифікатів з використанням технології blockchain / А.В. Ільєнко, С.С. Ільєнко, О.Л. Яковенко // CSNT-2024: XV міжнародна науково-практична конференція, 25-26 квітня 2024: тези доп. - К., 2024 .- С.74-75. 7. Ільєнко А.В. Застосування засобів штучного інтелекту у кібербезпеці / А.В. Ільєнко, Є. Галич, В. Павленко // Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS): VI міжнародна науково-практична конференція, 26 квітня 2024: тези доп. - К., 2024 .- С.21-22. 8. Ільєнко А.В. Крипто-стеганографічний модуль для захисту інформаційних ресурсів / А.В. Ільєнко, М.В. Руденко // Science in the modern world: innovations and challenges: I Міжнародна науково-практична конференція, 27-29.09.2024 р.; тези доповіді. – Торонто (Канада), 2024. – Р. 144-150. 9. Ільєнко А.В. Технології шифрування ресурсів / Смаль А. О., А.В. Ільєнко // European congress of scientific achievements: X Міжнародна науково-практична конференція, 7-9.10.2024 р.; тези доповіді. – Барселона (Іспанія), 2024. – Р. 132-136. п. 14 Керівництво постійно діючим студентським науковим гуртком «Криптографічні методи захисту інформації» (https://kszi.kai.edu.ua/naukova-robotag/naukovi-gurtki)
--	--	--	--	--	--	--	--

494468	Ахрамович Володимир Миколайович	Професор, Основне місце роботи	Факультет комп'ютерних наук та технологій	Диплом спеціаліста, Київський орденна Леніна політехнічний інститут, рік закінчення: 1980, спеціальність: Технологія машинобудування, металорізальні верстати та інструменти, Диплом доктора наук ДД 011778, виданий 29.06.2021, Диплом кандидата наук КД 049266, виданий 18.12.1991, Атестат доцента ДЦАР 000530, виданий 28.11.1995, Атестат професора АП 004630, виданий 23.12.2022, Атестат старшого наукового співробітника (старшого дослідника) СН 000401, виданий 07.06.1993	32	Методологія прикладних досліджень у сфері кібербезпеки	Освіта: Київський політехнічний інститут, 1980 р. спеціальність – «Технологія машинобудування, металорізальні верстати та інструменти», кваліфікація – Інженер – механік. Науковий ступінь: Доктор технічних наук, 05.13.21 – Системи захисту інформації, тема дисертації - «Методологічні основи забезпечення захисту інформації в соціальних мережах». Вчене звання: Професор кафедри кібербезпеки. Підвищення кваліфікації: 1. International Historical Biographical Institute (Dubai-New York-Rome-Jerusalem-Beljing). Тема - Studying Experience and Professional Achivements for Forming a Successful Personality and Transforming of the World. Термін - 18.02.2022 - 23.04.2022. Сертифікат № 6524 від 23.04.2022 (180 годин/6 кредитів ЄКТС). Види і результати професійної діяльності, згідно п. 38 Ліцензійних умов провадження освітньої діяльності: 1, 3, 7, 8, 12, 19 п. 1 1. Akhramovych V , Shuklin G , Pepa Y , Lehominova S , Muzhanova T , Dzyuba T , Yakymenko Y. Methodology for Calculating the Index of Protection of a Social Media from its Centrality. International Journal of Emerging Technology and Advanced Engineering. Volume 13, Issue 04, April 2023.- pp. 17-26. DOI: 10.46338/ijetaeo423_03. (Scopus, квартал Q2). 2. R. Khrashchevskiy, V. Klobukov, V. Kozlovskiy, V. Akhramovych, S.
--------	---------------------------------	--------------------------------	---	---	----	--	---

							Lazarenko. Method of calculating information protection from mutual influence of users in social networks // International Journal of Computer Network and Information Security (IJCNIS), Volume № 15, Number 5 (2023), pp. 27–40. DOI: https://doi.org/10.5815/ijcnis.2023.05.03. (Scopus, квартал Q1). 3. Akhramovych V., Pepa Y., Zahynei A., Akhramovych Vadym, Dzyuba T., Danylov I. Method for Calculating the Information Security Indicator in Social Media with Consideration of the Path Duration Between Clients // Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, 2024. – 14(1). – PP. 71–77. (Scopus). 4. Volodymyr Akhramovych, Yuriy Pepa, Anton Zahynei, Vadym Akhramovych, Taras Dzyuba, Ihor Danylov. Method for calculating the information security indicator in social media with consideration of the path duration between clients. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska" – IAPGOS. Volume № 14, Number 1 (2024), pp. 71–77. DOI: http://doi.org/10.35784/iapgos.5720.2024.03.31. (Scopus) 5. Akhramovych Volodymyr, Lehominova Svitlana, Stefurak Oleh, Akhramovych Vadym, Chuprun Sergii, "Methodology for Searching for the Dependence Between Data Defensiveness and Volume of Social Network Evolution", International Journal of Computer Network and Information Security(IJCNIS), Vol.16, No.6, pp.1-19, 2024. DOI:10.5815/ijcnis.2024.06.01 (Scopus, квартал Q1). 6. Володимир Ахрамович, Вадим Ахрамович. Аналіз безпеки інформації в корпоративних та локальних мережах в умовах нечітких множин Ukrainian
--	--	--	--	--	--	--	---

Scientific Journal of Information Security, 2025, vol. 31, issue 1, pp. 15-22.
 7. Ахрамович В.М., Ахрамович В.В. Пошук вторгнень у мережах в умовах невизначеності. Захист інформації, К. КАІ. Том 27, № 2, липень-грудень 2025. с.-94-105.
 8. Akhromovych V., Akhromovych V., Chuprun S. CONDITIONS OF UNCERTAINTY OF INFORMATION SYSTEMS RISKS AND QUANTITATIVE ASSESSMENT OF BANK. Colloquium-journal №9 (274), 2026 . Część 1 . (Warszawa, Polska). Pp.-99-104.

п. 3
 Serhii Yevseiev, Yuliia Khokhlachova, Serhii Ostapov, Oleksandr Laptiev, Olha Korol, Stanislav Milevskyi, Oleksandr Milov, Serhii Pohasii, Yevgen Melenti, Hrebenuk Vitalii, Alla Havrylova, Serhii Herasymov, Roman Korolev, Oleg Barabash, Valentyn Sobchuk, Roman Kyrychok, German Shuklin, Volodymyr Akhramovych, Vitalii Savchenko, Sergii Golovashych, Oleksandr Lezik, Ivan Opirskyy, Oleksandr Voitko, Kseniia Yerhidgei, Serhii Mykus, Yurii Pribyliev, Oleksandr Prokopenko, Andrii Vlasov, Nataliia Dzheniuk, Maksym Tolkachov. Models of socio-cyber-physical systems security. Monograph. – Kharkiv: PC technology center, 2023. – 168 p. (1,5 авт. аркуша; с. 76-103)
https://www.researchgate.net/publication/372568735_Models_of_socio-cyber-physical_systems_security_Monograph
 Scopus.

п. 7
 1. Член разової спеціалізованої ради при захисті дисертації на здобуття наукового ступеня доктор філософії Марченка Віталія Вікторовича, тема - «Метод виявлення шкідливих процесів в інформаційній

							системі підприємства на основі ідентифікації та діагностування станів логічних об'єктів»». 2023 р. 2. Голова експертної комісії спеціалізованої ради Д 26.861.06 при захисті дисертації на здобуття наукового ступеня доктора технічних наук Іванченко Євгенії Вікторівни «Методи та моделі оцінювання стану кіберзахисту критичної інфраструктури держави», ДСК. 2024 р. 3. Голова разової спеціалізованої вченої ради при захисті Педченко Євгена Максимовича на здобуття наукового ступеня «Доктор філософії». Тема дисертації: Методи та моделі оцінювання стану кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури. Шифр наукової спеціальності: 125. Дата захисту: 23.06.2025 4. Член разової спеціалізованої ради при захисті дисертації на здобуття наукового ступеня доктор філософії Скуратівського Анатолія Анатолійовича. Тема дисертації: Методи та інструментальні засоби управління вимогами кібербезпеки при впровадженні програмного забезпечення в бізнесі. Шифр наукової спеціальності: 122, дата захисту: 15.06.2026 5. Член спеціалізованої вченої ради Д 26.062.01 KAI з 2025 року. п. 8 Член редакційної колегії наукового видання "Безпека інформації" (KAI) з 01.01.2026 (https://jrnل.kai.edu.ua/index.php/Infosecurity/editorialboard) п. 12 1. Akhramovych V., Akhramovych V., Ilyenko A., Halata L.,
--	--	--	--	--	--	--	--

							Yakovenko O., Halych Y. The methodology for researching the cybersecurity of social platforms in relation to the number of communities // CSDP'2025: Cyber Security and Data Protection (Lviv, Ukraine, July 31, 2025). – Vol. 4042. – 2025. – P. 153–166. – Режим доступу: https://ceur-ws.org/Vol-4042/paper12.pdf (Scopus). 2. Akhramovich V. M., Areshkov M. M. Parallelization of the hashing process in authentication systems.// Innovations of modern science and education. Proceedings of the 3rd International scientific and practical conference. Perfect Publishing, Vancouver, Canada. 2025. Pp. 272-282. URL: https://sci-conf.com.ua/iii-mizhnarodna-naukovo-praktichna-konferentsiya-innovations-of-modern-science-and-education-28-30-11-2025-vankuver-kanada-arhiv/ 3. Ахрамович В.М., Санченко В.І. Розвиток агентних систем штучного інтелекту та пов'язані загрози інформаційній безпеці. The 8th International scientific and practical conference “Academic research by scientists in the field of modern technologies” (October 21-24, 2025) Milan, Italy. International Science Group. 2025. 264 p.-pp. 44-50. 4. Ахрамович В. М., Єльчанінов Д. О. Організація відновлення даних у субд MS SQL server // Global trends in science and education: XI Міжнародна науково-практична конференція 17-19 листопада Київ. 2025 р.: -с.234-241. 5. Левченя Г.В., Ахрамович В.М. Система підвищення ефективності захисту інформації в корпоративних мережах. Proceedings of the 2nd International scientific and practical conference. MDPC Publishing, Berlin,
--	--	--	--	--	--	--	--

							Germany. 2025. Pp. 164-168. URL: https://sciconf.com.ua/ii-mizhnarodna-naukovo-praktichna-konferentsiya-science-and-educationsynergy-of-innovation-28-30-09-2025-berlin-nimechchina-arhiv. 6. Ахрамович В.М., Чупрун С.Г. Захист інформації в хмарній системі. The 14th International scientific and practical conference “Features and trends of interdisciplinary scientific research” (April 7-10, 2026) Sofia, Bulgaria. International Science Group. 2026. Pp. 42-46. DOI – 10.46299/ISG.2026.1.14 7. Володимир Ахрамович, Володимир Санченко. Захист агентних систем ші від prompt-ін’єкцій методом покрокового аналітичного міркування (cot guard). IX Міжнародна науково-практична конференція. Проблеми кібербезпеки інформаційно-комунікаційних систем» (PCSICS). Київ. 24 квітня 2026 року. С. 184-186. 8. Володимир Ахрамович, Володимир Санченко. Виявлення prompt-ін’єкцій у великих мовних моделях методами семантичного аналізу //The 3rd international scientific and practical conference «INFORMATION SYSTEMS AND TECHNOLOGY: RESULTS AND PROSPECTS» (IST 2026). Pp. 337-340. п. 19 Участь в громадській організації «Східно-європейське наукове товариство» (з 18.06.2021)
494547	Міщенко Андрій Віталійович	Професор, Основне місце роботи	Факультет комп'ютерних наук та технологій	Диплом спеціаліста, Київське вище військово-авіаційне інженерне училище, рік закінчення: 1989,	16	Моделювання та оптимізація безпечових процесів авіаційної галузі	Освіта: 1. Київське вище військово-авіаційне-інженерне училище, 1989 р., спеціальність – «Авіаційне обладнання літальних апаратів», кваліфікація –

				спеціальність: Авіаційне обладнання, Диплом магістра, Національний технічний університет України "Київський політехнічний інститут", рік закінчення: 2009, спеціальність: Управління інноваційною діяльністю, Диплом магістра, Національна академія оборони України, рік закінчення: 2004, спеціальність: Організація технічного забезпечення Військово-Повітряних Сил, Диплом доктора наук ДД 005534, виданий 12.05.2016, Диплом кандидата наук ДК 004679, виданий 13.10.1999, Аттестат доцента 02ДЦ 014434, виданий 16.06.2005, Аттестат професора АП 000463, виданий 05.07.2018		Інженер електрик, диплом спеціаліста ПВ № 539092 від 24.06.1989 р. 2. Національна академія оборони України, 2009 р., спеціальність – «Організація технічного забезпечення ВПС», кваліфікація – «магістр військового управління», диплом магістра МО № 13606927 від 18.06.2004 р. 3. Національний технічний університет України «Київський політехнічний інститут», 2009., спеціальність – «Управління інноваційної діяльністю», кваліфікація – «магістр з управління інноваційною діяльністю», диплом магістра КВ № 3563604 від 28.02.2009 р. Науковий ступінь: Доктор технічних наук, 21.05.01 – «Інформаційна безпека держави», тема дисертації – «Методологічні та організаційно-технічні основи забезпечення інформаційної безпеки авіатранспортного комплексу України». Вчене звання: Професор кафедри засобів захисту інформації. Підвищення кваліфікації: 1. Програма USAID з менторства технічних директорів, тема - кібербезпека критичної інфраструктури в Україні, Certificate of Completion від 11.01.2022 р. 2. ТОВ «ІТ-АВІА». Курс підвищення кваліфікації на тему - «Підготовка авіаційного персоналу з основ авіаційної кібербезпеки та технічного менеджменту кіберзахисту». Сертифікат від 24.05.2024 р. (6 кредитів ЄКТС/180 годин). 3. ФКНТ КАІ. Терамін 19.11.2025- 18.12.2025 р., тема - "Підготовка тренерів з організації
--	--	--	--	---	--	---

							та проведення кіберсимуляцій на базі Cyber Range UA”/ Сертифікат №НО 45853942/003416-25 (4 кредити ЄКТС/120 годин). Види і результати професійної діяльності, згідно п. 38 Ліцензійних умов провадження освітньої діяльності: 1, 2, 3, 7, 12, 14, 19, 20. п. 1 1. Штомпель М. А., Нестеренко К. С., Міщенко А. В. Оцінювання ефективності біоінспірованого методу декодування кодів з малою щільністю перевірок на парність. Системи озброєння і військова техніка. 2022. № 1 (69). С. 115-19. https://doi.org/10.30748/soivt.2022.69.13 (Категорія В). 2. Андрій Міщенко Перспективна структура мультиагентної системи управління транспортною мережею зв'язку на основі технології CARRIER ETHERNET / Олександр Туровський, Андрій Міщенко, Віталій Клобуков, Олег Кітура, Костянтин Полонський// Наукоємні технології. – 2022 – Том 54 № 2 (2022) С.112-117 (Категорія В). 3. Mishchenko, A., Dalkıran, A., Novakovska, I., Skrypnyk, L. and Ishchenko, N. (2023), "Environmentally sustainable airport development: Ukrainian case of decarbonization", Aircraft Engineering and Aerospace Technology, Vol. 95 No. 3, pp. 488-500. https://doi.org/10.1108/AEAT-06-2022-0154. https://doi.org/10.1108/AEAT-06-2022-0154 (Google Scholar). 4. Міщенко А.В., Іщенко Н.Ф., Ліщиновська Н.О., Скрипник Л.Р. Безпека держави в енергонебезпечності об'єктів критичної інфраструктури. Наука і техніка
--	--	--	--	--	--	--	--

							сьогодні. 2023. №.2(16) С. 401-416. doi: 10.52058/2786-6025-2 023-2(16)-401-415 (in Ukrainian). https://doi.org/10.52058/2786-6025-2023-2(16)-401-415 (Google Scholar). 5. Increasing the energy dependence of state facilities of critical infrastructure based on the use of geoinformation/ A. Mishchenko¹, L. Skrypnyk², N. Ishchenko², I. Novakovska³, A. Koshel// International Conference of Young Professionals “GeoTerrace-2023” 2-4 October 2023, Lviv, Ukraine. p.1-5. (DOI: https://doi.org/10.3997/2214-4609.2023510092). 6. Міщенко А.В., План управління безпекою інформаційних активів об’єктів авіатранспортного комплексу України/ Лазаренко С.В., Міщенко А.В., Шульга В.П., Моркляник Б.В., Ліщиновська Н.О.// Захист інформації. – К. : НАУ. – 2023. № 4, том № 25. – С. 213 – 221 (Категорія В). 7. Use of L2TP and IPsec protocols to protect information of aviation critical infrastructure in wartime / Andrii Mishchenko, Yuriy Amirov, Vladyslav Lavrynenko //Global Scientific and Academic Research Journal of Multidisciplinary Studies [ISSN: 2583-4088], 2025, p.31-33. п. 2 Патент на корисну модель №155204 від 31.01.2024 п. 3 1. Міщенко Андрій Управління та забезпечення кібербезпеки на авіапідприємстві /Міщенко Андрій, Аміров Юрій, Ліщиновська Наталія, Grzegorz Tuszynski // SCIENTIFIC MULTIDISCIPLINARY MONOGRAPH – ISBN – 979-8-89589-184-3, 2024. – 404 с. (2 авторських аркушів) 2. Оптимізація розміщення функцій
--	--	--	--	--	--	--	---

							виявлення вторгнень у багаторівневій архітектурі EDGE-FOG-CLOUD для IoT-мереж / Пастущак Д.В., Міщенко А.В.// Колективна монографія за матеріалами □ Міжнародної науково-практичної конференції «Прикладні системи управління та робототехніка» (Київ, 12-13 листопада 2025 р.) / За заг. ред. С.О. Довгого. – Київ, ІПСУ НАН України, 2025. – 252 (с.134-136). п. 7 1. Член спеціалізованої вченої ради Д 26.062.19 Національного авіаційного університету (до 2022 року). 2. Член спеціалізованої вченої ради Д 26.062.01 Національного університету «Київський авіаційний інститут» п. 12 1. Міщенко А.В. Оцінка наслідків соціотехнічних атак на об'єкти критичної інфраструктури / Дівізінюк М.М., Міщенко А.В., Лазаренко С.В., Клобуков В.В. // VIII міжнародна науково-практична конференція «Актуальні питання забезпечення кібербезпеки та захисту інформації», 2-5 лютого 2022. - К.: Європейський університет. збірн. тез. - С. 84 - 95. 2. Міщенко А.В. Методологічні аспекти планування щодо забезпечення безпеки інформаційних активів об'єктів критичної інфраструктури / Міщенко А. В., Ліщиновська Н. О., Аміров Ю. Р. // Міжнародна науково-практична конференція «Виклики і загрози для критичної інфраструктури», 29-30 червня 2023. - Detroit, Michigan, USA. збірник тез. - С. 302 - 306. 3. Increasing the energy
--	--	--	--	--	--	--	---

							dependence of state facilities of critical infrastructure based on the use of geoinformation/ A. Mishchenko, L. Skrypnyk, N. Ishchenko, I. Novakovska, A. Koshel// International Conference of Young Professionals “GeoTerrace-2023” 2-4 October 2023, Lviv, Ukraine. p.1-5. (DOI: https://doi.org/10.3997/2214-4609.2023510092). 4. OPTIMIZING IDS FUNCTION PLACEMENT IN MULTI-LAYER EDGE-FOG-CLOUD IOT ARCHITECTURE: A MILP-BASED APPROACH / Daniel Pastushchak, Andrii Mishchenko // Digital Transformation: Strengthening the Cybersecurity Capacities in the Modern World 4-5 November 2025, Krakow p.72 (https://duikt.edu.ua/ua/2935-mizhnarodna-naukovo-praktichna-konferenciya-cifrova-transformaciya-posilennya-kiberbezpekovih-spromozhnostey-u-suchasnomu-sviti) 5. І.С. Кузнецов, А.В. Міщенко, А.В. Льюнко. (2025). Теоретичний підхід до створення захищеного розподіленого хмарного середовища на основі технології blockchain. Тези доповідей «Резильєнтність динамічних систем»: збірник праць Всеукраїнської науково-практичної інтернет-конференції здобувачів вищої освіти і молодих вчених, 6 листопада 2025 року. Київ: Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, 2025. С. 41-43. 6. Кузнецов І.С. , Міщенко А.В., Льюнко А.В. (2025). Теоретичні засади формування резильєнтного розподіленого хмарного середовища за допомогою BLOCKCHAIN-технологій. Тези доповідей «Прикладні
--	--	--	--	--	--	--	---

							системи управління та робототехніка»: збірник праць Всеукраїнської науково-практичної інтернет-конференції здобувачів вищої освіти і молодих вчених, 12-13 листопада 2025 року. Київ Інститут Прикладних систем Управління НАН України, 2025. С. 151-153. п. 14 Керівник постійно діючого студентського наукового гуртка «Технології кібербезпеки та захисту інформації» (https://www.kzzi.kai.edu.ua) п. 19 Участь в громадській організації «Громадська організація IT DEUS (Команда розвитку України)» (з 2022 р.). п. 20 1. 1989 - 2006 р.р. - військова служба на посадах офіцерського та старшого офіцерського складу. 2. 2010 - 2024 р.р. - технічний директор КП Міжнародний аеропорт «Київ» (Жуляни).
494737	Кудренко Станіслава Олексіївна	Доцент, Основне місце роботи	Факультет комп'ютерних наук та технологій	Диплом магістра, Національний авіаційний університет, рік закінчення: 2006, спеціальність: 090702 Радіoeлектронні пристрої, системи та комплекси, Диплом кандидата наук ДК 065192, виданий 26.01.2011, Атестат доцента АД 013058, виданий 20.06.2023	19	Організаційні моделі кібербезпеки	Освіта: Національний авіаційний університет, рік закінчення: 2006, спеціальність: 090702 Радіoeлектронні пристрої, системи та комплекси Науковий ступінь: кандидат технічних наук зі спеціальності 05.13.12- Системи автоматизації проектувальних робіт Тема дисертації: «Автоматизація проектування оптимальних аерокосмічних комплексів» Вчене звання: доцент кафедри комп'ютерних систем та мереж Підвищення кваліфікації: З 25 жовтня по 25 грудня 2023 року пройдено стажування (обсяг професійної підготовки – 180 годин) шляхом участі у авторському тренінгу «Технології

							програмування C/Embedded» сертифікованої програми «Інженерія вбудованих систем та Інтернет речей», який проводиться спільно з компанією Global Logic на кафедрі обчислювальної техніки факультету інформатики та обчислювальної техніки Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Звіт про стажування (протокол засідання кафедри КСМ № 1 від 10.01.2024). Види і результати професійної діяльності, згідно п. 38 Ліцензійних умов провадження освітньої діяльності: 1, 4, 7, 8, 9, 12, 13, 19. п. 1 Сураєв В., Кудренко С. Пріоритетність управління у IT-сервісах для авіаційного персоналу. Проблеми інформатизації та управління. 2024. Т. 78. С. 120–123. (фахове видання категорії «Б»). Shklyar O., Balanyuk Y., Kudrenko S. Load Balancing and Cloud Node Resilience Enhancement Algorithm Based on Predicted Integral Index. Problems of Informatization and Control. 2025. Vol. 3(83). P. 148–153. DOI: 10.18372/2073-4751.83.20512. Кудренко С.О., Німич О.В., Макєєв І.Г. Метод прогнозування компрометації вузлів у середовищі edge та fog для об'єктів критичної інфраструктури. Захист інформації. 2025. Т. 27. С. 87–93. DOI: 10.18372/2410-7840.27.21183. Stolyar A., Makieiev I., Kudrenko S. ReliefF-Based Feature Selection for Traffic Anomaly Detection. Problems of Informatization and Management. 2024. Vol. 80. P. 64–70. (фахове видання категорії «Б»).
--	--	--	--	--	--	--	---

							Stolyar A., Kudrenko S. Security Mechanisms for AODV and E-AODV Protocols Against Black Hole and Gray Tunnel Attacks. Problems of Informatization and Management. 2025. Vol. 81. P. 119–125. DOI: 10.18372/2073-4751.81.20137. (фахове видання категорії «Б»). Kudrenko S., Kozlovskiy V., Alkema V. Neural Network Approach to Ensuring the Resilience of Industrial IoT Systems under Conditions of Peripheral Node Integrity Violation. Кібербезпека: освіта, наука, техніка. 2026. № 33. DOI: 10.28925/2663-4023.2026.33.1147. Kudrenko S., Nimych O., Makieiev I. Method for Detecting Anomalous Local Updates and Isolating Malicious Participants in Federated Learning Systems. Наукоємні технології. 2026. Vol. 70, No. 2. P. 182–190. DOI: 10.18372/2310-5461.70.21194 п.4 Кудренко С. О., Пекуровський Г. В. Оцінювання та тестування стану безпеки інформаційних систем : робоча програма навчальної дисципліни / Національний університет «Київський авіаційний інститут», каф. технічного захисту інформації. Затв. на засіданні кафедри, протокол № 2 від 23.02.2026. Київ, 2026. 14 с. Theory of Digital Automata: Guide to Laboratory Works. Лабораторний практикум для студентів спеціальності 123 «Комп'ютерна інженерія». – К.: НАУ, 2024. – 56 с. / Maliarchuk V. O., Kudrenko S. O.Stoliar A. L. Теорія цифрових автоматів: Лабораторний практикум для студентів спеціальності 123 «Комп'ютерна інженерія». – К.: KAI,
--	--	--	--	--	--	--	--

						2025. – 56 с. / Малярчук В. О., Кудренко С. О., Столяр А. Л.
						п.7 2023 - 2025 Вчений секретар спеціалізованої вченої ради з присудження ступеню доктора наук Д 26.062.07 Державного університету «Київський авіаційний інститут»
						п.8 Відповідальний секретар фахового наукового видання «Проблеми інформатизації та управління» кат.Б (https://jrnل.kai.edu.ua/index.php/PIU)
						п.9 Член експертної групи з акредитації освітніх програм 08.10.2024
						п. 12 1. Kozlovskyi V., Kudrenko S., Makieiev I. Adaptive Data Processing Model at Edge and Fog Levels of Industrial IoT Systems under Device Compromise Conditions // V Міжнародна науково- практична конференція «Новітні технологічні тенденції інтелектуальної індустрії та Інтернету речей». – 2026. – С. 63. 2. Kozlovskyi V., Kudrenko S., Makieiev I. Adaptive Data Processing Model at Edge and Fog Levels of Industrial IoT Systems under Device Compromise Conditions // V Міжнародна науково- практична конференція «Новітні технологічні тенденції інтелектуальної індустрії та Інтернету речей». – 2026. – С. 63. 3. Козловський В.В., Кудренко С.О. Застосування машинного навчання для передбачення відмов та загроз у системах автоматизації підприємств // Прикладні системи управління та робототехніка: матеріали І Міжнародної науково- практичної

							конференції, 12–13 листопада 2025 р., Київ, Україна. – К., 2025. С 173-175 4. С.О.Кудренко, А.Л.Столяр Захист інформації в системі дистанційного спілкування // Комп'ютерні системи та мережні технології (CSNT-2024): матеріали XV Міжнар. наук.-техн. конф. (м. Київ, 25–26 квітня 2024 р.). – К., 2024. – С. 97–101. 5. Алькема В.В., Кудренко С.О. Гузій М.М. ДУ «Київський авіаційний інститут» формальна контейнерна модель цифрового двійника на основі мультисортних алгебр. Сучасні тенденції розвитку системного програмування: тези доповідей науково-практичної конференції, м. Київ. – 20-21 листопада 2025 р., Державний університет «Київський авіаційний інститут», – К.: ДУ КАІ, 2025. – С. 104-105. п.13. проведення навчальних занять із спеціальних дисциплін англійською мовою 2024-2025 навчальний рік: Дисципліни Computer Electronics (68 аудиторних годин) , Nanoelectronics (51 аудиторних годин) Modelling of Computer Systems (67 аудиторних годин) 2022-2023 навчальний рік: Information Security of Computer Systems and Networks (53 аудиторних годин) - п.19. ГО "ІНСТИТУТ МЕНЕДЖМЕНТУ ТА СТРАТЕГІЙ" Дата входження до складу: 07.10.2024 (документ - довідка від голови)
494737	Кудренко Станіслава Олексіївна	Доцент, Основне місце роботи	Факультет комп'ютерних наук та технологій	Диплом магістра, Національний авіаційний університет, рік закінчення: 2006, спеціальність:	19	Аудит інформаційної безпеки	Освіта: Національний авіаційний університет, рік закінчення: 2006, спеціальність: 090702 Радіоелектронні пристрої, системи та комплекси

				090702 Радіоелектрон ні пристрої, системи та комплекси, Диплом кандидата наук ДК 065192, виданий 26.01.2011, Атестат доцента АД 013058, виданий 20.06.2023		Науковий ступінь: кандидат технічних наук зі спеціальності 05.13.12- Системи автоматизації проектувальних робіт Тема дисертації: «Автоматизація проектування оптимальних аерокосмічних комплексів» Вчене звання: доцент кафедри комп'ютерних систем та мереж Підвищення кваліфікації: З 25 жовтня по 25 грудня 2023 року пройдено стажування (обсяг професійної підготовки – 180 годин) шляхом участі у авторському тренінгу «Технології програмування C/Embedded» сертифікованої програми «Інженерія вбудованих систем та Інтернет речей», який проводиться спільно з компанією Global Logic на кафедрі обчислювальної техніки факультету інформатики та обчислювальної техніки Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Звіт про стажування (протокол засідання кафедри КСМ № 1 від 10.01.2024). Види і результати професійної діяльності, згідно п. 38 Ліцензійних умов провадження освітньої діяльності: 1, 4, 7, 8, 9, 12, 13, 19. п. 1. Stolyar A., Makieiev I., Kudrenko S. ReliefF- Based Feature Selection for Traffic Anomaly Detection. Problems of Informatization and Management. 2024. Vol. 80. P. 64–70. DOI: 10.18372/2073- 4751.80.19779. (фахове видання категорії «Б»). 2. Stolyar A., Kudrenko S. Security Mechanisms for AODV and E-AODV Protocols Against Black Hole and Gray Tunnel Attacks. Problems of
--	--	--	--	---	--	---

								Informationization and Management. 2025. Vol. 81. P. 119–125. DOI: 10.18372/2073-4751.81.20137. (фахове видання категорії «Б»). 3. Кудренко С.О., Німич О.В., Макєєв І.Г. Метод прогнозування компрометації вузлів у середовищі edge та fog для об'єктів критичної інфраструктури. Захист інформації. 2025. Т. 27, № 2. С. 87–93. DOI: 10.18372/2410-7840.27.21183. (фахове видання категорії «Б»). 4. Kudrenko S., Kozlovskiy V., Alkema V. Neural Network Approach to Ensuring the Resilience of Industrial IoT Systems under Conditions of Peripheral Node Integrity Violation. Кібербезпека: освіта, наука, техніка. 2026. № 33. С. 112–120. DOI: 10.28925/2663-4023.2026.33.1147. (фахове видання категорії «Б»). 5. Кудренко С.О., Німич О.В., Макєєв І.Г., Алькема В.В. A Robust Client Update Aggregation Algorithm for Counteracting Model Poisoning Attacks in Federated Learning. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2026. № 63. С. 59–68. DOI: 10.36910/6775-2524-0560-2026-63-06. (фахове видання категорії «Б»). 6. Kudrenko S., Nimych O., Makieiev I. Method for Detecting Anomalous Local Updates and Isolating Malicious Participants in Federated Learning Systems. Наукоємні технології. 2026. Т. 70, № 2. С. 182–190. DOI: 10.18372/2310-5461.70.21194. (фахове видання категорії «Б»). 7. Kudrenko S. Proactive GNSS Interference Mitigation Against Jamming and Spoofing Using Compact Neural Models. Наукоємні технології. 2026. Т. 69, № 1. С. 69–73. DOI: 10.18372/2310-
--	--	--	--	--	--	--	--	---

							5461.69.20948. (фахове видання категорії «Б»). Кудренко С. О., Пекуровський Г. В. Оцінювання та тестування стану безпеки інформаційних систем : робоча програма навчальної дисципліни / Національний університет «Київський авіаційний інститут», каф. технічного захисту інформації. Затв. на засіданні кафедри, протокол № 2 від 23.02.2026. Київ, 2026. 14 с. п.4 Theory of Digital Automata: Guide to Laboratory Works. Лабораторний практикум для студентів спеціальності 123 «Комп'ютерна інженерія». – К.: НАУ, 2024. – 56 с. / Maliarchuk V. O., Kudrenko S. O.Stoliar A. L. Теорія цифрових автоматів: Лабораторний практикум для студентів спеціальності 123 «Комп'ютерна інженерія». – К.: KAI, 2025. – 56 с. / Малярчук В. О.,Кудренко С. О., Столяр А. Л. п.7 2023 - 2025 Вчений секретар спеціалізованої вченої ради з присудження ступеню доктора наук Д 26.062.07 Державного університету «Київський авіаційний інститут» п.8 Відповідальний секретар фахового наукового видання «Проблеми інформатизації та управління» кат.Б (https://jrnل.kai.edu.ua/index.php/PIU) п.9 Член експертної групи з акредитації освітніх програм 08.10.2024 п. 12 1. Kozlovskiy V., Kudrenko S., Makieiev I. Adaptive Data
--	--	--	--	--	--	--	--

							Processing Model at Edge and Fog Levels of Industrial IoT Systems under Device Compromise Conditions // V Міжнародна науково-практична конференція «Новітні технологічні тенденції інтелектуальної індустрії та Інтернету речей». – 2026. – С. 63. 2. Kozlovskiy V., Kudrenko S., Makieiev I. Adaptive Data Processing Model at Edge and Fog Levels of Industrial IoT Systems under Device Compromise Conditions // V Міжнародна науково-практична конференція «Новітні технологічні тенденції інтелектуальної індустрії та Інтернету речей». – 2026. – С. 63. 3. Козловський В.В., Кудренко С.О. Застосування машинного навчання для передбачення відмов та загроз у системах автоматизації підприємств // Прикладні системи управління та робототехніка: матеріали I Міжнародної науково-практичної конференції, 12–13 листопада 2025 р., Київ, Україна. – К., 2025. С 173-175 4. С.О.Кудренко, А.Л.Столяр Захист інформації в системі дистанційного спілкування // Комп'ютерні системи та мережні технології (CSNT-2024): матеріали XV Міжнар. наук.-техн. конф. (м. Київ, 25–26 квітня 2024 р.). – К., 2024. – С. 97–101. 5. Алькема В.В., Кудренко С.О. Гузій М.М. ДУ «Київський авіаційний інститут» формальна контейнерна модель цифрового двійника на основі мультисортних алгебр. Сучасні тенденції розвитку системного програмування: тези доповідей науково-практичної конференції, м. Київ. – 20-21 листопада 2025 р., Державний
--	--	--	--	--	--	--	---

							університет «Київський авіаційний інститут», – К.: ДУ КАІ, 2025. – С. 104-105. п.13. проведення навчальних занять із спеціальних дисциплін англійською мовою 2024-2025 навчальний рік: Дисципліни Computer Electronics (68 аудиторних годин) , Nanoelectronics (51 аудиторних годин) Modelling of Computer Systems (67 аудиторних годин) 2022-2023 навчальний рік: Information Security of Computer Systems and Networks (53 аудиторних годин) - п.19. ГРОМАДСЬКА ОРГАНІЗАЦІЯ "ІНСТИТУТ МЕНЕДЖМЕНТУ ТА СТРАТЕГІЙ" Дата входження до складу: 07.10.2024 (документ - довідка від голови)
494703	Темніков Володимир Олександров ич	Професор, Основне місце роботи	Факультет комп'ютерних наук та технологій	Диплом спеціаліста, Київський ордена Леніна політехнічний інститут, рік закінчення: 1974, спеціальність: Звукотехніка, Диплом доктора наук ДД 009862, виданий 14.05.2020, Диплом кандидата наук КН 007726, виданий 22.03.1995, Атестат доцента 02ДЦ 001258, виданий 28.04.2004, Атестат старшого наукового співробітника (старшого дослідника) СН 002381, виданий 04.06.1996	26	Інтелектуалізо вані системи інформаційної безпеки	109316 ТЕМНІКОВ Володимир Олександрович Професор кафедри технічного захисту інформації (1 ставка), основне місце роботи Кафедра технічного захисту інформації Факультету комп'ютерних наук та технологій Диплом кандидата технічних наук КН №007726 від 22.03.1995р. Диплом доктора технічних наук ДД № 009862 від 14.05.2020 р. Атестат доцента кафедри засобів захисту інформації 02ДЦ, № 001258 від 28.04.2004 р. 50 років ОК10. «Переддипломна практика», ОК11 «Кваліфікаційна робота». Освіта: Київський політехнічний інститут, 1974 р., спеціальність – «Звукотехніка», кваліфікація –

							«Інженер-електрик», диплом спеціаліста ІІ № 075650 від 01.03.1974 р. Науковий ступінь: Доктор технічних наук, 05.13.06 – «Інформаційні технології», тема дисертації – «Моделі і методи контролю та управління функціональністю авіадиспетчерів». Вчене звання: Доцент кафедри засобів захисту інформації. Підвищення кваліфікації: 1. Науково-дослідний Інститут Люблінського науково-технологічного парку та IESF Міжнародна фундація науковців та освітян. Термін 28.11.2024 - 07.12.2024 р., тема – «Міжнародний досвід використання штучного інтелекту в освітньому процесі (частина І) / Сертифікат №ES/21871 від 07.12.2024 р. (1.5 кредити ЄКТС/45 годин). 2. Науково-дослідний Інститут Люблінського науково-технологічного парку та IESF Міжнародна фундація науковців та освітян. Термін 13 – 24.03.2025 р., тема – «Міжнародний досвід використання штучного інтелекту в освітньому процесі (частина ІІ) / Сертифікат №ES/23283 від 24.03.2025р. (1.5 кредити ЄКТС/45 годин). 3. Інститут зі справ публічної адміністрації (м. Люблін, Республіка Польща). Термін 05 - 14.06.2025 р., тема – «Інноваційні цифрові інструменти для дистанційного навчання: при підготовці здобувачів освіти в країнах Європейського Союзу / Сертифікат № ES/24040 від 14.06.2025 р. (1.5 кредити ЄКТС/45 годин). 4. Інститут зі справ публічної адміністрації (м. Люблін, Республіка
--	--	--	--	--	--	--	---

							Польща). Термін 17 - 26.06.2025 р., тема – «Неформальна освіта у підготовці доктора філософії (PHD) в країнах Європейського Союзу та Україні» / Сертифікат №ES/24131 від 26.06.2025 р. (1.5 кредити ЄКТС/45 годин). 5. КАІ. Термін 19.11.2025 - 18.12.2025 р., тема – «Підготовка тренерів з організації та проведення кіберсимуляцій на базі Cyber Range UA» / Сертифікат №НО 45853942/003418-25 (4 кредити ЄКТС/120 годин). 6. ТОВ «УНІКОММ». Термін з 09.03.2026 р. по 29.05.2026 р., тема - «Управління інформаційною безпекою та ризиками в організаціях телекомунікаційної сфери». Звіт про стажування (6 кредитів ЄКТС/180 годин). Види і результати професійної діяльності, згідно п. 38 Ліцензійних умов провадження освітньої діяльності: 1, 8, 9, 12, 19. п. 1 1. Tavrov, D., Temnikov, V., Temnikova, O., Temnikov, A. (2023). Perceptual Computing Based Framework for Assessing Organizational Performance According to Industry 5.0 Paradigm. In: Hu, Z., Zhang, Q., He, M. (eds) Advances in Artificial Systems for Logistics Engineering III. ICAILE 2023. Lecture Notes on Data Engineering and Communications Technologies, vol 180. Springer, Cham. https://doi.org/10.1007/978-3-031-36115-9_14 (Scopus) 2. Темніков В.О., Тавров Д.Ю., Темнікова О.Л., Темніков А.В. Підхід до оцінювання ефективності роботи підприємств на основі перцептивних обчислень // Grail of Science. – 2023. – №26. – С.253-257 (World of Papers), CrossRef, OUCI, Google
--	--	--	--	--	--	--	--

							Scholar, ResearchGate, ORCID, OpenAIRE) 3. Al-Ani F., Abdulkareem S., Mohammed M., Temnikov V. The Photovoltaic Active Dual Tracking Approach is Transforming Renewable Energy // Proceeding of The 35th Conference of Fruct Association (FRUCT'35) (Tampere, Finland, April 24-26, 2024). – P.51-62 (Scopus) 4. Yayha, M.A., Samoea, R.F., Abedah, M., Fahmi, A.M., Temnikov, V. Innovation and Technology Management in Modern Enterprises // Journal of Ecohumanism, 2024. – V3. – No.5. – P. 895–908 (Scopus) 5. Hurova I., Shapovalov H., Ishchuk A., Morklyanyk B., Balanyuk Yu., Temnikov V., Hnatovska H., Kalyta O. Cyberculture and Sustainable Development: Communicative, Ethical and Technological Transformations // European Journal of Sustainable Development. – 2025. – Vol.14. – №4. – PP.553-566 // ISSN: 2239-5938 (Scopus) 6. Abduljabbar H., Abdullah W., Bazool S., Muhsin A., Alfalahi S., Temnikov V. AI-Driven Environmental Impact Assessments: Ethical and Legal Considerations // Environment and Social Psychology. – 2025. – Vol.10. – №12. – ESP-3994 // ISSN: 2424-8975 (Scopus) п. 8 Науковий керівник НДР «Інформаційна та авіаційна безпека об'єктів критичної інфраструктури», 2019-2022 рр., шифр «35/14.01.04»; номер держреєстрації № 0119U102297. п. 9 Член фахової науково-методично-редакційної секції № 4 «Інформаційні технології» Науково-методично-редакційної ради КАІ (2022-2026 рр.)
--	--	--	--	--	--	--	--

п. 12

1. Темніков А. В., Темніков В. О. Моделі оцінювання функціонального стану авіадиспетчерів із застосуванням теорії нечітких множин // X Всесвітній конгрес “Авіація в XXI столітті” – “Безпека в авіації та космічні технології” (28–30 вересня 2022 р., Київ). – Київ: НАУ, 2022. – С. 2.5.35–2.5.39.

2. Темніков В., Темніков А. Інформаційна технологія проведення добору працівників // INFORMATION TECHNOLOGIES AND COMPUTER MODELLING: Proceedings of the International Scientific Conference (6–8 липня 2023 р., Івано-Франківськ). – Івано-Франківськ, 2023. – С. 57–58.

3. Темніков В.О., Темніков А.В., Темнікова О.Л. Інформаційна технологія професійного добору працівників на основі оцінювання їх функціонального стану // XVI Міжнародна науково-технічна конференція «ABIA-2023». Матеріали конференції. – К.: НАУ, 2023. – С. 13.52-13.54

4. Темніков В.О., Темніков А.В., Темнікова О.Л. Моделювання інформаційних систем підтримки прийняття управлінських рішень // XVI Міжнародна науково-практична конференція "Інтегровані інтелектуальні робототехнічні комплекси" (ПРТК-2023). Збірник тез. – К.: НАУ, 2023. – С.296-298

5. Темніков В. О., Темніков А. В. Моделі оцінювання функціонального стану персоналу на основі перцептивних обчислень і нечіткої логіки // Матеріали XVII Міжнародної науково-технічної конференції “ABIA-2025” (22–24 квітня 2025 р., Київ). – К.:

							КАІ, 2025. – С. 18.60–18.64. 6. Темніков В.О., Темніков А.В. Аналітична модель експертного оцінювання функціонального стану // XVIII Міжнародна науково-практична конференція "Інтегровані інтелектуальні робототехнічні комплекси" (ІПРТК-2025). Збірка тез. – К.: НАУ, 2025. – С.384-385 7. Темніков В.О., Темніков А.В. Метод агрегування експертних оцінок функціонального стану персоналу // Міжнародна науково-практична конференція «Інформаційні технології та комп'ютерне моделювання». Матеріали конференції. – Івано-Франківськ: ПНУ, 2025. – С.49-50 8. Temnikov V, Temnikov A., Shcherbak T. A fuzzy-perceptual approach to candidate ranking in a multicriteria decision space // The V International Conference on Emerging Technology Trends on the Smart Industry and the Internet of Thing (TTSIT-2026). Матеріали конференції. – К.: ДТЕУ, 2026. – С. 73-75 9. Темніков В.О., Темніков А.В. Нечітка модель багатокритеріального ранжування фахівців з урахуванням динамічної невизначеності // XIX Міжнародна науково-практична конференція "Інтегровані інтелектуальні робототехнічні комплекси" (ІПРТК-2026). Збірка тез. – К.: ДУ «КАІ», 2026. – С.440-442 п. 19 Член Громадської організації «Міжнародна фундація науковців та освітян» (з 2025 р.)
496067	Теремінко Лариса Григорівна	Доцент, Основне місце	Гуманітарно-мистецький факультет	Диплом спеціаліста, Київський	25	Ділова іноземна мова	Освіта: Київський державний педагогічний інститут

		роботи		державний педагогічний інститут іноземних мов, рік закінчення: 1993, спеціальність: Іноземні мови (дві мови), Диплом кандидата наук ДК 059227, виданий 09.02.2021, Атестат доцента АД 011738, виданий 23.12.2022		іноземних мов, 1993, спеціальність – «Мова і література», кваліфікація – «Іноземні мови (дві мови)». Науковий ступінь: Кандидат педагогічних наук, 13.00.04 – «Теорія і методика професійної освіти», тема дисертації – «Формування готовності до професійної мобільності майбутніх фахівців з інженерії програмного забезпечення». Вчене звання: Доцент кафедри іноземних мов за фахом Підвищення кваліфікації: Науково-педагогічне стажування на кафедрі романо-германської філології Українсько-Польського вищого навчального закладу «Центрально-Європейський університет» на тему «Сучасні тенденції та інновації іншомовній підготовці фахівців у закладах вищої освіти» в обсягом 6 кредитів (180 годин) з 07.10.2024 по 07.12.2024 (сертифікат про проходження стажування № 535 від 09.12.2024). Види і результати професійної діяльності, згідно п. 38 Ліцензійних умов провадження освітньої діяльності: 1, 3, 4, 8, 12 п. 1 1. Tereminko L.H., Hurska O.O., Denysenko N.H. Developing higher education content teachers' ESP competence. Інноваційна педагогіка. 2024. Вип. 70. Т. 2 С. 118-121. https://doi.org/10.32782/2663-6085 (фахове видання категорії В). 2. Теремінко Л.Г. Аналіз досвіду професійної підготовки українських ІТ-фахівців в умовах війни. Інноваційна педагогіка. 2025. Вип. 80. Т. 2 С. 103–107.
--	--	--------	--	---	--	--

<https://doi.org/10.32782/2663-6085/2025/80.2.21> (фахове видання категорії В).

3. Bielova-Oleynik, Y., Mosiienko, H., Tereminko, L., Khytko, O., & Madinov, M. (2025). Implementation of advanced methods in professional engineering education. Revista online de Política e Gestão Educational. Vol. 29, p. 025016 (Electronic journal article). <https://doi.org/10.22633/rpge.v29i00.20235> (Web of Science).

4. Абсалямова, Я. В., Гурська, О. О., & Теремінко, Л. Г. Використання онлайн-тестів і флеш-карт для розширення словникового запасу студентів з англійської мови. Педагогічна академія: наукові записки. 2025. Вип. 25. (електронне видання). <https://doi.org/10.5281/zenodo.18209046> (фахове видання категорії В).

5. Tarnavska T., Glushanytsia, N., Tereminko L. Ensuring the continuity and quality of higher education under emergency conditions. Перспективи та інновації науки (Серія «Педагогіка»). 2026. Вип. 59. Т.1 2026. С. 199–209. [https://doi.org/10.52058/2786-4952-2026-1\(59\)-199-209](https://doi.org/10.52058/2786-4952-2026-1(59)-199-209) (фахове видання категорії В).

п. 3

1. Акмалдінова О.М., Гурська О.О., Теремінко Л.Г., Денисенко Н.Г., Сорокун Г.В. Professional English. Applied Mathematics : навч. посіб. Київ : НАУ, 2023. 96 с. (ISBN 978-966-932-196-1, з грифом «Рекомендовано Вченою радою Національного авіаційного університету». (Протокол № 5 від 24.05.2023 р.; 2,0 у.д.а.)

2. Акмалдінова О.М., Гурська О.О., Теремінко Л.Г., Сорокун Г.В. Professional English. Cybersecurity and Data Protection: навч. посіб.

Київ : KAI, 2025. 96 с.
(ISBN 978-966-932-097-1, з грифом
«Рекомендовано
Вченою радою
Державного
університету
«Київський
авіаційний інститут».
(Протокол № 8 від
21.05.2025 р.; 2,0
у.д.а.)

п. 4

1. Акмалдінова О.М.,
Гурська О.О.,
Теремінко Л.Г.
Professional English.
Computer Engineering:
практикум. Київ: НАУ,
2022. 60 с.

2. Гурська О.О.,
Теремінко Л.Г.
Professional English.
Методичні

рекомендації до
виконання
контрольних робіт для
здобувачів вищої
освіти ОС «Бакалавр»
заочної форми
навчання спец. 122
«Комп'ютерні науки»,
123 «Комп'ютерна
інженерія». Київ:
НАУ, 2022. 32 с.

3. Polous O.,
Mykhalchenko I.,
Tereminko L.
Marketing: Term Paper
Method Guide. K.:
NAU, 2023. 50 p.

4. Білоус Н.П., Гурська
О.О., Теремінко Л.Г.
Business English.

Методичні
рекомендації до
виконання
контрольних робіт для
здобувачів вищої
освіти ОС «Магістр»
заочної форми
навчання ІТ-
спеціальностей. Київ:
НАУ, 2023. 40 с.

5. Робоча програма
навчальної
дисципліни «Ділова
іноземна мова»
освітньо-професійної
програми «Безпека
інформаційних і
комунікаційних і
систем» підготовки
здобувачів вищої
освіти освітнього
ступеня «Магістр».
Галузь знань: F
«Інформаційні
технології».

Спеціальність: F5
«Кібербезпека та
захист інформації»
(2025 р.; 16 ст.).

6. Теремінко Л.Г.
Робоча програма
навчальної
дисципліни «Ділова
іноземна мова»
освітньо-професійної
програми «Інженерія

							програмного забезпечення» підготовки здобувачів вищої освіти освітнього ступеня «Магістр». Галузь знань: F «Інформаційні технології». Спеціальність: F2 «Інженерія програмного забезпечення» (2025 р.; 16 ст.). п. 8 Участь в імплементації проєкту освіти англійською мовою: редагування рукописів англомовних навч.-метод. посібників, практикумів, методичних рекомендацій. Відповідальний виконавець теми «Теоретико-прикладні лінгвістичні, перекладознавчі та методологічні аспекти викладання іноземних мов професійного спрямування: новітні тенденції і виклики інноваційних форм навчання» (№ 1-2022/12.01.2022). Термін роботи 24.01.2022 – 30.12.2024. п. 12 1. Гурська О.О., Теремінко Л.Г. Teaching foreign language discourse to IT students via professionally oriented projects : Current Trends and Fields of Philological Studies in the Challenging Reality: Proceedings of the International scientific conference. (Riga, 29–30 July 2022). Riga (Latvia), 2022. P. 397–401. 2. Hurska O.O., Tereminko L.H. Communication as a critical aspect of aviation safety : Aviation in the XXI-st Century – Safety in Aviation and Space Technology : materials of the tenth world congress, Kyiv, September 28–30, 2022. Kyiv, 2022. 3. Теремінко Л.Г. Додатки та сервіси як ефективний засіб вивчення іноземної мови : Лінгвістичні та методологічні аспекти викладання іноземних мов професійного
--	--	--	--	--	--	--	--

спрямування : матер.
доп. IV міжнар. наук.-
практ. конф., м. Київ,
29–30 березня 2023 р.
Київ, 2023. С. 49–50.

4. Теремінко Л.Г.
English language
training for university
teachers. Лінгвістичні
та методологічні
аспекти викладання
іноземних мов
професійного
спрямування:
матеріали V
Міжнародної науково-
практичної
конференції, м. Київ,
Україна, 28-29
березня 2024 р. С. 85–
86.
[https://flsc.nau.edu.ua/
koferentsiia-kafedry/](https://flsc.nau.edu.ua/koferentsiia-kafedry/)

5. Гурська О.О.,
Теремінко
Л.Г.Формування
аналітичних умінь та
навичок майбутніх ІТ-
фахівців у процесі
іншомовної
підготовки. The latest
information and
communication
technologies in
education: матеріали
XI Міжнар. наук.-
практ. конф., м.
Флоренція, Італія, 27–
29 листопада 2023 р.
Флоренція, 2023. С.
303–307.

6. Теремінко Л.Г.
Стратегії й переваги
активного навчання
іноземної мови.
Лінгвістичні та
методологічні аспекти
викладання іноземних
мов професійного
спрямування:
матеріали VI
Міжнародної науково-
практичної
конференції, м. Київ,
Україна, 27–28
березня 2025 р. С. 89–
90.
[https://drive.google.co
m/file/d/19kRuqvZK4C
yhSxrSIItl6w4Y4UolJO5
kd/view](https://drive.google.com/file/d/19kRuqvZK4CyhSxrSIItl6w4Y4UolJO5kd/view).

7. Теремінко Л., Litvin
I. Modern concerns of
implementing English
Medium Instruction
programs. Лінгвістичні
та методологічні
аспекти викладання
іноземних мов
професійного
спрямування :
матеріали VI
Міжнародної науково-
практичної
конференції, м. Київ,
Україна, 27–28
березня 2025 р. С. 90–
92: тези доповіді.
[https://drive.google.co
m/file/d/19kRuqvZK4C
yhSxrSIItl6w4Y4UolJO5](https://drive.google.com/file/d/19kRuqvZK4CyhSxrSIItl6w4Y4UolJO5kd/view)

[illegible]

							https://surl.li/msddjs 12. Volynets N., Syniak V., Tereminko L. Biometric Data: Protection or Vulnerability of Identity? Роль безпеки в транскордонному та міжнародному співробітництві : матеріали Міжнародної науково-практичної конференції, м. Берегове, Україна, 8–9 жовтня 2025 р. С. 25–26. https://kme.org.ua/wp-content/uploads/2025/12/role-security_conf-abstracts_ua-en-hu_elektronne-viddannya_2025.pdf 13. Sviastyn V., Tereminko L. The Role of Machine Learning in Preventing Data Breaches: Роль безпеки в транскордонному та міжнародному співробітництві : матеріали Міжнародної науково-практичної конференції, м. Берегове, Україна, 8–9 жовтня 2025 р. С. 35–36. https://kme.org.ua/wp-content/uploads/2025/12/role-security_conf-abstracts_ua-en-hu_elektronne-viddannya_2025.pdf 14. Seliuchenko Ye., Tereminko L. The Impact of Cyberculture on the Modern Educational Process : Роль безпеки в транскордонному та міжнародному співробітництві : матеріали Міжнародної науково-практичної конференції, м. Берегове, Україна, 8–9 жовтня 2025 р. С. 68. https://kme.org.ua/wp-content/uploads/2025/12/role-security_conf-abstracts_ua-en-hu_elektronne-viddannya_2025.pdf 15. Hrutsenok D., Tereminko L. The Role of AI and Digital Technologies in Shaping a Safe Environment : Роль безпеки в транскордонному та міжнародному співробітництві: матеріали Міжнародної науково-практичної конференції, м. Берегове, Україна, 8–9
--	--	--	--	--	--	--	--

								жовтня 2025 р. С. 77–78. https://kme.org.ua/wp-content/uploads/2025/12/role-security_conf-abstracts_ua-en-hu_elektronne-vydannia_2025.pdf 16. Duzhyk M., Tereminko L. Artificial Intelligence for Cybersecurity Enhancement : Роль безпеки в транскордонному та міжнародному співробітництві : матеріали Міжнародної науково-практичної конференції, м. Берегове, Україна, 8–9 жовтня 2025 р. С. 81–82. https://kme.org.ua/wp-content/uploads/2025/12/role-security_conf-abstracts_ua-en-hu_elektronne-vydannia_2025.pdf 17. Lysiuk S., Tereminko L. The Role of Google Dorking in Detecting Personal Data Leaks : Роль безпеки в транскордонному та міжнародному співробітництві : матеріали Міжнародної науково-практичної конференції, м. Берегове, Україна, 8–9 жовтня 2025 р. С. 85–86. https://kme.org.ua/wp-content/uploads/2025/12/role-security_conf-abstracts_ua-en-hu_elektronne-vydannia_2025.pdf 18. Kykhtan S., Tereminko L. Methods of Osint and Their Integration with Artificial Intelligence Technologies for Strengthening Information Security: Роль безпеки в транскордонному та міжнародному співробітництві: матеріали Міжнародної науково-практичної конференції, м. Берегове, Україна, 8–9 жовтня 2025 р. С. 116–117. https://kme.org.ua/wp-content/uploads/2025/12/role-security_conf-abstracts_ua-en-hu_elektronne-vydannia_2025.pdf 19. Verbutskyi Ye., Rabiropkh Ye., Tereminko L. Using Ai in Targeting Social Bots: Роль безпеки в
--	--	--	--	--	--	--	--	--

							транскордонному та міжнародному співробітництві: матеріали Міжнародної науково-практичної конференції, м. Берегове, Україна, 8–9 жовтня 2025 р. С. 172–173. https://kme.org.ua/wp-content/uploads/2025/12/role-security_conf-abstracts_ua-en-hu_elektronne-vydannia_2025.pdf 20. Maksymchuk I., Tereminko L. The Importance of Hygiene in Online Space : Роль безпеки в транскордонному та міжнародному співробітництві : матеріали Міжнародної науково-практичної конференції, м. Берегове, Україна, 8–9 жовтня 2025 р. С. 180–181. https://kme.org.ua/wp-content/uploads/2025/12/role-security_conf-abstracts_ua-en-hu_elektronne-vydannia_2025.pdf 21. Теремінко Л., Litvin I. Methodological Aspects of Using Digital Tools in Teaching ESP to IT Students. Лінгвістичні та методологічні аспекти викладання іноземних мов професійного спрямування: матеріали VII Міжнародної науково-практичної конференції, м. Київ, Україна, 26–27 березня 2026 р. С. 57–59. https://drive.google.com/file/d/1k333fOCd2ZaaZfqASpJ26tajB8xutAup/view
495965	Приходько Оксана Юріївна	Доцент, Основне місце роботи	Гуманітарно-мистецький факультет	Диплом спеціаліста, Рівненський державний педагогічний інститут, рік закінчення: 1995, спеціальність: Українська мова та література, Диплом магістра, Національний університет біоресурсів і природокористування України, рік закінчення:	16	Наукові комунікації у фаховій діяльності	495965 Приходько Оксана Юріївна Доцент кафедри української мови, історії та інформаційної діяльності (1 ставка), основне місце роботи Кафедра української мови, історії та інформаційної діяльності Гуманітарно-мистецького факультету Диплом кандидата філологічних наук ДК № 009794 від 17.01.2001 р.

				2025, спеціальність: 061 Журналістика, Диплом кандидата наук ДК 009794, виданий 17.01.2001, Атестат доцента 02ДЦ 000102, виданий 24.12.2003		Атестат доцента кафедри українознавства 02ДЦ № 000102 від 24.12.2003 р. Освіта: Рівненський державний педагогічний інститут, 1995 рік, спеціальність - Українська мова та література, кваліфікація - «Учитель української мови та літератури», диплом спеціаліста КН № 900140 від 16.06.1995 р. Науковий ступінь: Кандидат педагогічних наук, 13.00.02 – Теорія і методика навчання української літератури, тема дисертації - «Вивчення української літератури в школі у контексті літератур західних і східних слов'ян». Вчене звання: Доцент кафедри слов'янської філології. Підвищення кваліфікації: 1. 2024 – Одеський національний університет імені І. І. Мечникова. Тема - «Штучний інтелект та академічна добросовісність у соціогуманітарній освіті та науці». Сертифікат про стажування № 15-57- 2024, 2024 рік (6 кредитів ЄКТС/ 180 годин). 2. Державна установа «Український інститут розвитку освіти». Тема – «Експертиза навчальної літератури». Сертифікат про стажування № 831ae6d5dcdbd412cb76d 242a822c39bf, 2025 рік (0,5 кредита ЄКТС/ 15 годин). Види і результати професійної діяльності, згідно п. 38 Ліцензійних умов провадження освітньої діяльності: 1, 3, 4, 9, 12, 14, 15, 19 п. 1 1. Бойко Н., Коткова Л., Приходько О. Means and methods of objectization of emotional-evaluative
--	--	--	--	--	--	--

							semantic plans of lexical units in the ukrainian language. AD ALTA: journal of interdisciplinary research. 12/02-XXX. 2022. P. 73–80. URL: http://www.magnanimitas.cz/ADALTA/120230/papers/A_16.pdf («Scopus») 2. Vaskiv Mykola, Prykhodko Oksana, Drozdovskyi Dmytro, Bykova Olha, Haiovych Halyna, Kozachok Vira. Nasimi's Poetry in the Discourse of Turkish Renaissance: Philosophical and Aesthetical Issues. Synesis (Universidade Católica de Petrópolis, Rio de Janeiro, Brasil), 2022. V. 14, n. 2. P. 293-310. ISSN 1984-6754. URL: https://seer.ucp.br/seer/index.php/synesis/article/view/2289 («Scopus») 3. Приходько О., Литвинська С. Методологічні аспекти викладання навчальної дисципліни «Наукові комунікації у фаховій діяльності» для майбутніх фахівців. Вісник Національного авіаційного університету. Серія: Педагогіка. Психологія: зб. наук. праць. Київ : НАУ, 2023. № 22. С. 51 – 60. URL: https://jrn1.nau.edu.ua/index.php/VisnikPP/article/view/17604 4. Бойко Н., Коткова Л., Литвинська С., Приходько О., Самборин В. Evaluative potential of the component composition of phraseological units of the ukrainian language regarding indication of the world of emotions. AD ALTA: journal of interdisciplinary research. 13/01-XXXII. 2023. С. 132–137. URL: https://www.webofscience.com/wos/woscc/full-record/WOS:000925136500024 («Scopus») 5. Литвинська С., Приходько О., Сібрук А. З історії буквених позначень голосних звуків «И» / «І» в українській мові. Актуальні питання гуманітарних наук: міжвузівський збірник наукових праць
--	--	--	--	--	--	--	--

							молодих вчених Дрогобицького державного педагогічного університету імені Івана Франка. Дрогобич : Видавничий дім «Гельветика», 2024. Вип. 76. Т. 3. С. 102-107. URL: http://www.aphn-journal.in.ua/archive/76_2024/part_3/19.pdf 6. Kotkova L., Prykhodko O., Lytvynska S., Tsyhanok H., Lushchuk Y. Innovations in scientific communication: Techniques for crafting distinctive textual content. Multidisciplinary Science Journal. Vol. 6 (2024), e2024ss0732. URL: https://www.malque.pub/ojs/index.php/msj/article/view/2992 («Scopus») 7. Anastasiia Sibruk, Prykhodko Oksana, Svitlana Lytvynska, Cheripko Sergii, Hanna Onufriychuk, Viktor Sibruk The Impact Of Artificial Intelligence On Academic Writing: Linguistic And Stylistic Analysis In Higher Education. International Journal of Environmental Sciences. Vol. 11 No. 20s (2025). URL: https://theaspd.com/index.php/ijes/article/view/5613 DOI: https://doi.org/10.64252/thwys35 («Scopus»). 8. Anastasiia Sibruk, Oksana Prykhodko, Bakhytzhan Akhmetov, Serhii Cheripko, Viktor Sibruk, Chrystyna Dybik, Hanna Onufriichuk. Artificial intelligence in higher education: Opportunities and risks for student research. Joint Proceedings of the Workshops at the Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN 2025). Kyiv, Ukraine, June 20 - 22, 2025. Vol-4024. P. 318-329. URL: https://eur-ws.org/Vol-4024/ https://eur-ws.org/Vol-4024/paper21.pdf («Web of Sciences»).
--	--	--	--	--	--	--	---

							п. 3 1. Савчук Н., Приходько О. Літературне краєзнавство: науково-дослідницька робота : навчально- методичний посібник по роботі з обдарованою молоддю. Рівне: ВСП «РЕТФК НУВГП», 2023. 58 с. 2. Наукові комунікації у фаховій діяльності: навч. посіб. / Литвинська С.В., Добровольська Л.А., Дячук Т.М., Кошетар У.П., Онуфрійчук Г.І., Приходько О.Ю., Сенчило-Татліліоглу Н.О., Сібрук А.В., Стецик Х.М. Київ: НАУ, 2024. 136 с. URL: https://umk.nau.edu.ua/wp-content/uploads/2024/06/Navch.-posib.-NKFD-ost.a5Obkl-1.pdf 3. Академічна добросесність та професійна етика : навч. посіб. / Сібрук А. В., Дубик Х. М., Литвинська С.В., Онуфрійчук Г.І., Приходько О.Ю., Черіпко С. І. – Київ : ДУ «КАІ», 2025. – 140 с.
							п. 4 1. Приходько О. Ю., Воробйова Л. М. Методичні рекомендації щодо виконання науково- дослідницьких проектів. Зарубіжна література: навчальний посібник. Рівне: РМАНУМ, 2025. 62 с. URL: https://drive.google.com/file/d/1wet6H-oНауxbaqOjj4cOI_Pse183dZK1/view 2. Культура наукової мови та комунікації: практикум / уклад.: С. В. Литвинська, О. Ю. Приходько, А. В. Сібрук, Х. М. Стецик. Київ : НАУ, 2024. 48 с. URL: https://umk.nau.edu.ua/wp-content/uploads/2024/06/Praktykum_Kultura-naukovoi-movy-ta-komunikatsii_20.03.2024.pdf 3. Наукові комунікації у фаховій діяльності: практикум / уклад.: С. В. Литвинська, О. Ю. Приходько, С. І. Черіпко. – К. : ДНП «ДУ КАІ», 2025. – 52

п. 12

1. Кошетар У. П., Литвинська С. В., Приходько О. Ю. Концептуальний апарат фахової наукової комунікації. Науковий збірник «InterConf+», 28(137): за матеріалами VII Міжнародної науково-практичної конференції «Теорія і практика науки: ключові аспекти», Рим, Італія, 19-20 грудня 2022 р. С.124-135. DOI: <https://doi.org/10.51582/interconf.19-20.12.2022>.

2. Prykhodko Oksana. Genre specificity of non-fiction in modern Ukrainian literature. Hagia Sophia. Editors: Prof. Dr. Muhittin ELIAÇIK, Zhandos ALIMGEREYEV. Istanbul: Farabi Publishing House, 2022. P. 299-305. ISBN:978-625-7898-64-5. URL: https://www.ayasofyakangresli.com/_files/ugd/4ec152_5f99ee52ca70497ca83e952cf31d7b6d.pdf

3. Приходько О., Шапенко Н. Проблеми штучного інтелекту та GPT-чату в контексті академічної доброчесності здобувача вищої освіти. Аксіопсихологічні вектори розвитку сучасної освіти: збірник матеріалів Міжнародної науково-практичної конференції, м. Тернопіль, 19-20 жовтня 2023 р. Тернопіль : ТНПУ ім. В. Гнатюка, 2023. С. 67-70. URL: http://dspace.tnpu.edu.ua/bitstream/123456789/31042/1/Zbirnyk_materialiv_konferentsii.pdf

4. Приходько О. Пам'яті скарбничого просвітянського духу. Слово просвіти: всеукраїнський культурологічний тижневик. Вип. 47-48 (1232), 23 листопада –

							6 грудня, 2023. С. 13. URL: 5. Литвинська С.В., Приходько О.Ю. Формування професійно-мовленнєвої компетентності як обов'язкової складової професійної компетентності майбутнього фахівця. Інформація та соціум: збірник матеріалів VIII Міжнародної науково-практичної конференції (м. Вінниця, 02 червня 2023р.). Вінниця: ДонНУ імені Василя Стуса, 2023. С. 138–140. URL: https://jias.donnu.edu.ua/issue/view/487 https://jias.donnu.edu.ua/article/view/14575/14480 6. Приходько О. Драматична поема Лесі Українки «На полі крові» як об'єкт театральної репрезентації: соціокультурна перспектива біблійного інтертексту. Мова та культура у просторі новітніх технологій: проблеми сучасної комунікації: матеріали VI Міжнародної наукової конференції, м. Київ, 23 березня 2023 р. / Національний авіаційний університет, факультет лінгвістики та соціальних комунікацій, кафедра української мови та культури. За заг. ред. С.В. Литвинської, А.В. Сібрук. Київ : Талком, 2023. С. 94-96. URL: https://er.nau.edu.ua/handle/NAU/59448?locale=uk 7. Приходько О., Ємець А., Коновалова В. Професійна комунікація за допомогою мережі «Інтернет» як форма наукової комунікації. ПОЛІТ. Сучасні проблеми науки. Гуманітарні науки: тези доповідей XXIII Міжнародної науково-практичної конференції здобувачів вищої освіти і молодих учених:[у 2-х т.]. Т. 1 (м. Київ, 04-07 квітня 2023 р.) / [ред. кол.: Н. В. Ладогубець, А. М. Кокарева та ін.]; Національний
--	--	--	--	--	--	--	---

авіаційний
університет. Київ :
НАУ, 2023. С. 320–
321. URL:
[https://flsc.nau.edu.ua/
wp-
content/uploads/2023/
05/POLIT_TOM-
2_2023.pdf](https://flsc.nau.edu.ua/wp-content/uploads/2023/05/POLIT_TOM-2_2023.pdf)
8. Приходько О.
Ландшафт фентезі:
типологія жанру.
Збірник матеріалів
Всеукраїнської
науково-практична
конференція
«Українська
термінологія: традиції
та новації»,
присвячена 25-річчю
кафедри української
мови та культури
факультету
лінгвістики та
соціальних
комунікацій
Національного
авіаційного
університету:
матеріали
Всеукраїнської
конференції, м. Київ,
16 квітня 2024 р. /
Національний
авіаційний
університет,
факультет лінгвістики
та соціальних
комунікацій, кафедра
української мови та
культури. За заг. ред.
С. В. Литвинської.
Київ: Талком, 2024. С.
54-56.
9. Приходько О. За
покликом
просвітянського
серця. Слово просвіти:
всеукраїнський
культурологічний
тижневик. Вип. 5
(1288), 6 — 12 лютого
2025. С. 9.
10. Приходько О.
«Лісова пісня» в
модерному стилі.
Слово просвіти:
всеукраїнський
культурологічний
тижневик. Вип. 15
(1298), 17 — 23 квітня
2025. С. 15.
11. Приходько О.
Штучний інтелект у
дискурсі академічної
добросесності
освітньої і наукової
діяльності здобувачів
вищої освіти.
Матеріали VII
Міжнародної наукової
конференції «Мова та
культура у просторі
новітніх технологій:
проблеми сучасної
комунікації», м. Київ,
12 березня 2025 р.; ДУ
«Київський
авіаційний інститут» /
за заг. ред. А.В.
Сібрук. К., 2025. С. 82-

								85. 12. Приходько О., Бровінська Л. Терміни і професіоналізми в мовленні IT-фахівців. ПОЛІТ. Сучасні проблеми науки. Соціально-гуманітарні науки: тези доповідей XXV Міжнародної науково-практичної конференції здобувачів вищої освіти і молодих учених:[у 2-х т.]. Т. 2 (м. Київ, 01-04 квітня 2025 р.) / [ред. кол.: Н. І. Мельник, А. М. Кокарева та ін.]; Державний університет «Київський авіаційний інститут». – К.: KAI, 2025. С. 187–189. URL: https://drive.google.com/file/d/12uMjVNlcGb_dKHWCNPLQlGCHDNlFe5FNG/view 13. Сібрук А. В., Приходько О. Ю. Linguistic and Stylistic Features of Scientific Text. Світові виміри освітніх тенденцій: збірник наукових праць / за ред. Г. В. Межжеріної, О. Ю. Корчук ; Навчально- науковий інститут міжнародного співробітництва та освіти. Державний університет «Київський авіаційний інститут». Київ, 2025. Вип. 18. С. 249-256. URL: https://imco.nau.edu.ua/наукова-робота/ 14. Приходько О. Спинися, мить! Прекрасна ти! Театральні «Мізансцени» у фотороботах Анатолія Мізерного. Слово просвіти: всеукраїнський культурологічний тижневик. Вип. 26 (1309), 3 — 9 липня 2025. С. 14. 15. . Приходько О. Задера В. Штучний інтелект як засіб оптимізації освітньої і наукової діяльності здобувачів вищої освіти. Збірник матеріалів Всеукраїнської науково-практичної конференції з міжнародною участю «Українська термінологія: традиції та новації». м. Київ, 22 квітня 2026 р. / Державний університет
--	--	--	--	--	--	--	--	--

						«Київський авіаційний інститут», Гуманітарно-мистецький факультет, кафедра української мови, історії та інформаційної діяльності. Київ: ДУ «КАІ», 2026. С. 45 – 49. п. 14 Керівник постійно діючого студентського наукового гуртка «Актуальні проблеми наукової комунікації» п. 15 1. Робота у складі журі (заступник голови журі) фінального (III) етапу Міжнародного мовно-літературного конкурсу учнівської та студентської молоді імені Тараса Шевченка (2017 – 2025 рр.) 2. Робота в експертній раді програми «Дослідження. Освіта. Резиденції. Стипендії» Українського культурного фонду (2022 р.) п. 19 1. Член громадської організації «Рівненське обласне об'єднання ВУТ «Просвіта» ім. Тараса Шевченка», членський квиток № РВ 02458 від 09.03.2021. 2. Член громадської організації «Київське обласне об'єднання Всеукраїнського товариства «Просвіта» імені Тараса Шевченка», членський квиток № К 02078 від 07.07.2024.
--	--	--	--	--	--	--

Таблиця 3. Матриця відповідності програмних результатів навчання, освітніх компонентів, методів навчання та оцінювання

Програмні результати навчання ОП	ПРН відповідає результату навчання, визначеному стандартом вищої освіти (або охоплює його)	Обов'язкові освітні компоненти, що забезпечують ПРН	Методи навчання	Форми та методи оцінювання
ПРН26.	☐	Методи побудови та	Лекції, лабораторні	Тестування, усне

Розробляти та впроваджувати стратегії кіберстійкості систем та технологій кібербезпеки, спрямовані на захист критичної цифрової інфраструктури, підвищення стійкості інформаційних систем до атак, мінімізацію кіберризиків та розвиток ефективних механізмів реагування на кіберзагрози, необхідні для забезпечення безпечного цифрового середовища, розвитку інновацій у сфері кібербезпеки (Ціль 9 сталого розвитку), підвищення рівня захищеності міських цифрових екосистем (Ціль 11 сталого розвитку) та зміцнення інституційних механізмів протидії кіберзлочинності відповідно до принципів миру, правосуддя та ефективного управління (Ціль 16 сталого розвитку).		аналізу криптосистем	заняття, самостійна робота	опитування, письмовий контроль, екзамен
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсового проекту
		Моделювання та оптимізація безпекових процесів авіаційної галузі	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Організаційні моделі кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Аудит інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Інтелектуалізовані системи інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Інтелектуалізовані системи інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи
		Науково-дослідна практика в області систем та технологій кібербезпеки	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
ПРН25. Вирішувати задачі забезпечення та супроводу комплексних систем захисту	☐	Переддипломна практика	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік

інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки, що дозволяє вирішувати практичні завдання підвищення рівня безпекових процесів в тому числі і в сфері авіаційної безпеки.		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсового проекту
		Аудит інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Інтелектуалізовані системи інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Інтелектуалізовані системи інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи
		Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
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.	☒	Інтелектуалізовані системи інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи
		Науково-дослідна практика в області систем та технологій кібербезпеки	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		Переддипломна практика	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
		Інтелектуалізовані системи інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Аудит інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Моделювання та оптимізація	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування,

		безпекових процесів авіаційної галузі	робота	письмовий контроль, екзамен
ПРН24. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки, в тому числі в галузі авіаційної безпеки.	☐	Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
		Переддипломна практика	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		Науково-дослідна практика в області систем та технологій кібербезпеки	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		Організаційні моделі кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Аудит інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Моделювання та оптимізація безпекових процесів авіаційної галузі	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
ПРН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.	☒	Методи побудови та аналізу криптосистем	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Аудит інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний	Захист кваліфікаційної роботи

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.	☒	Інтелектуалізовані системи інформаційної безпеки	метод Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Інтелектуалізовані системи інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи
		Науково-дослідна практика в області систем та технологій кібербезпеки	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
		Переддипломна практика	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
ПРН 21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.	☒	Моделювання та оптимізація безпекових процесів авіаційної галузі	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Аудит інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
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.	☒	Методологія прикладних досліджень у сфері кібербезпеки	Лекції, практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Наукові комунікації у фаховій діяльності	Лекції, практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Переддипломна практика	Пошуковий метод, метод проблемного виконання, дослідницький	Захист звіту з практики

			метод, продуктивно- практичний метод	
		Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно- практичний метод	Захист кваліфікаційної роботи
<i>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.</i>	☒	Методи побудови та аналізу криптосистем	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Моделювання та оптимізація безпекових процесів авіаційної галузі	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Організаційні моделі кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Переддипломна практика	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно- практичний метод	Захист звіту з практики
		Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно- практичний метод	Захист кваліфікаційної роботи
<i>ПРН 18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та/або кібербезпеки.</i>	☒	Наукові комунікації у фаховій діяльності	Лекції, практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсового проекту
		Інтелектуалізовані системи інформаційної безпеки	Лекції, практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи

		Переддипломна практика	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
		Інтелектуалізовані системи інформаційної безпеки	Лекції, практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
<i>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.</i>	☒	Інтелектуалізовані системи інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи
		Науково-дослідна практика в області систем та технологій кібербезпеки	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		Переддипломна практика	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
		Інтелектуалізовані системи інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Моделювання та оптимізація безпекових процесів авіаційної галузі	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Наукові комунікації у фаховій діяльності	Лекції, практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
<i>ПРН 16. Приймати обґрунтовані</i>	☒	Кваліфікаційна робота	Пошуковий метод, метод	кваліфікаційної роботи

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.			проблемного виконання, дослідницький метод, продуктивно-практичний метод	
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Моделювання та оптимізація безпекових процесів авіаційної галузі	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Організаційні моделі кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
ПРН 15. Зрозуміло і недовозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.	☒	Наукові комунікації у фаховій діяльності	Лекції, практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсового проекту
		Моделювання та оптимізація безпекових процесів авіаційної галузі	Лекції, практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Інтелектуалізовані системи інформаційної безпеки	Лекції, практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи
		Науково-дослідна практика в області систем та технологій кібербезпеки	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		Переддипломна практика	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький	Захист кваліфікаційної роботи

			метод, продуктивно- практичний метод	
		Інтелектуалізовані системи інформаційної безпеки	Лекції, практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
<i>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.</i>	☒	Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
		Методи побудови та аналізу криптосистем	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсового проекту
		Моделювання та оптимізація безпекових процесів авіаційної галузі	Лекції, лабораторні заняття, самостійна робота	тестування, усне опитування, письмовий контроль, екзамен
		Організаційні моделі кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Переддипломна практика	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
<i>ПРН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегій і політики інформаційної безпеки та/або кібербезпеки організації.</i>	☒	Методологія прикладних досліджень у сфері кібербезпеки	Лекції, практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсового проекту
		Моделювання та оптимізація безпекових процесів авіаційної галузі	Лекції, практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Інтелектуалізовані системи інформаційної безпеки	лекції, практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Інтелектуалізовані системи інформаційної безпеки	лекції, практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової

		Науково-дослідна практика в області систем та технологій кібербезпеки	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	роботи Захист звіту з практики
		Переддипломна практика	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Наукові комунікації у фаховій діяльності	Лекції, практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
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.	☒	Моделювання та оптимізація безпекових процесів авіаційної галузі	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
		Організаційні моделі кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
ПРН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі	☒	Ділова іноземна мова	Практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Інтелектуалізовані системи інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Інтелектуалізовані системи інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи

інформаційної безпеки та/або кібербезпеки.		Науково-дослідна практика в області систем та технологій кібербезпеки	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		Переддипломна практика	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	метод, продуктивно-практичний метод Захист кваліфікаційної роботи
ПРН 2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.	☒	Наукові комунікації у фаховій діяльності	Лекції, практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Інтелектуалізовані системи інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Інтелектуалізовані системи інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи
		Науково-дослідна практика в області систем та технологій кібербезпеки	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		Переддипломна практика	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-	Захист кваліфікаційної роботи

			практичний метод	
		Моделювання та оптимізація безпекових процесів авіаційної галузі	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
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.	☒	Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
		Моделювання та оптимізація безпекових процесів авіаційної галузі	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсового проекту
		Наукові комунікації у фаховій діяльності	Лекції, практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Методи побудови та аналізу криптосистем	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
ПРН 4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.	☒	Методи побудови та аналізу криптосистем	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Моделювання та оптимізація безпекових процесів авіаційної галузі	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Організаційні моделі кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Аудит інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Інтелектуалізовані системи інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Інтелектуалізовані системи інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи

		Переддипломна практика	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
ПРН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.	☒	Ділова іноземна мова	Практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсового проекту
		Моделювання та оптимізація безпекових процесів авіаційної галузі	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Організаційні моделі кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Переддипломна практика	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
		Наукові комунікації у фаховій діяльності	Лекції, практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
ПРН 6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	☒	Методи побудови та аналізу криптосистем	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсового проекту
		Моделювання та оптимізація безпекових процесів авіаційної галузі	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен

		Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
		Аудит інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
<i>ПРН 7.</i> Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	☒	Методологія прикладних досліджень у сфері кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсового проекту
		Організаційні моделі кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
<i>ПРН 8.</i> Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	☒	Методологія прикладних досліджень у сфері кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Моделювання та оптимізація безпекових процесів авіаційної галузі	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Організаційні моделі кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Переддипломна практика	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-	Захист кваліфікаційної роботи

			практичний метод	
ПРН 9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	☒	Методи побудови та аналізу криптосистем	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсового проекту
		Аудит інформаційної безпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
ПРН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	☒	Організаційні моделі кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Кваліфікаційна робота	Пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
		Методологія прикладних досліджень у сфері кібербезпеки	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсового проекту
		Моделювання та оптимізація безпекових процесів авіаційної галузі	Лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен