НАЦІОНАЛЬНЕ АГЕНТСТВО ІЗ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	**Державне некомерційне підприємство "Державний університет "Київський авіаційний інститут"**
Освітня програма	**65513 Безпека інформаційних і комунікаційних систем**
Рівень вищої освіти	**Магістр**
Спеціальність	**125 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	**Державне некомерційне підприємство "Державний 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	**65513**
Назва ОП	**Безпека інформаційних і комунікаційних систем**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека та захист інформації**
Спеціалізація (за наявності)	*відсутня*
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 кібербезпеки**
Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП	**Кафедра технічного захисту інформації, Кафедра іноземних мов професійного спрямування, Кафедра української мови, історії та інформаційної діяльності**
Місце (адреса) провадження освітньої діяльності за ОП	**пр. Гузара Любомира, 1 Київ, Україна 03058**
Освітня програма передбачає присвоєння професійної кваліфікації	*не передбачає*
Професійна кваліфікація, яка присвоюється за ОП (за наявності)	***відсутня***
Мова (мови) викладання	**Українська**
ID гаранта ОП у ЄДЕБО	**494533**
ПІБ гаранта ОП	**Ільєнко Анна Вадимівна**
Посада гаранта ОП	**Завідувач кафедри**
Корпоративна електронна адреса гаранта ОП	**anna.ilienko@npp.kai.edu.ua**
Контактний телефон гаранта ОП	**+38(097)-381-72-00**
Додатковий телефон гаранта ОП	*відсутній*

Форми здобуття освіти на ОП	Термін навчання
заочна	1 р. 4 міс.
очна денна	1 р. 4 міс.

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

Підготовка здобувачів другого (магвстерського) рівня вищої освіти за освітньо-професійною програмою (далі – ОПП) «Безпека інформаційних і комунікаційних систем» зі спеціальності 125 «Кібербезпека та захист інформації» здійснюється випусковою кафедрою кібербезпеки. В 2000 році започатковано підготовку фахівців у галузі інформаційної безпеки та захищених інформаційних технологій та створено кафедру комп'ютеризованих систем захисту інформації Національного авіаційного університету (далі- НАУ). За цей період змінилося кілька класифікаторів спеціальностей, але кафедра продовжує підготовку висококваліфікованих і конкурентоспроможних фахівців у сфері кібербезпеки та захисту інформації. Відповідно до наказу голови комісії з реорганізації НАУ, в.о. ректора, від 31.05.2024 № 256/од «Про зміни в структурі Факультету комп'ютерних наук та технологій», було створено кафедру кібербезпеки з метою підготовки фахівців у галузі інформаційних технологій першого (бакалаврського), другого (магістерського) та третього (наукового) рівнів вищої освіти. Кафедра здійснює підготовку зі спеціальності 125 «Кібербезпека та захист інформації» за освітніми програмами, а саме: «Безпека інформаційних і комунікаційних систем» та «Управління кібербезпекою та захистом інформації».
На сьогодні кафедра в рамках спеціальності F5 «Кібербезпека та захист інформації» та галузі знань F «Інформаційні технології» здійснює підготовку фахівців освітнього ступеня «Бакалавр» та «Магістр» за освітньо-професійною програмою «Безпека інформаційних та комунікаційних систем».
Відповідно до Закону України «Про вищу освіту» від 01.07.2014р. №1556-VII (зі змінами), листа МОН від 28.04.2017р. №1/9-239, «Методичних рекомендацій до розроблення та оформлення освітньо-професійно програми», що складені відповідно до Закону України «Про освіту» від 05.09.2017р. №2145-VIII, на основі моніторингу потреб ринку праці, запитів роботодавців щодо необхідності підготовки фахівців по даній ОПП, була розроблена ОПП «Безпека інформаційних і комунікаційних систем», затверджена вченою радою НАУ (протокол № 5 від 26.06.2018). У відповідності до щорічного перегляду ОПП у 2019 році була скоригована. Нова редакція ОПП була затверджена вченою радою НАУ (протокол № 3 від 20.03.2019) і введена в дію наказом від 02.03.2019 №139/од. Після введення в дію «Положення про освітні програми НАУ» (http://surl.li/spsxtu) та з метою вдосконалення механізмів вибору дисциплін та формування індивідуальної освітньої траєкторії, врахування бачення студентства та рекомендацій роботодавців переформатовано вибіркову освітню компоненту. Відповідні зміни внесені в ОПП для здобувачів вищої освіти 2020 року вступу з 2020-2021 н.р. та затверджені вченою радою НАУ (протокол №6 від 26.08.2020) і введена в дію наказом від 27.08.2020 №317/од. Відповідно до затвердженого стандарту вищої освіти зі спеціальності 125 «Кібербезпека», який був введений в дію наказом МОН від 18.03.2021 № 332, здійснено розробку нової редакції ОПП з метою вдосконалення освітніх компонент та приведення ОПП у відповідність до затвердженого стандарту. Нова редакція затверджена вченою радою НАУ (протокол №4 від 21.04.2021) та введена наказом від 29.07.2021 № 246/од. У 2022 році згідно з наказом т.в.о. ректора від 09.02.2022 № 063/од «Про щорічний перегляд освітньо-професійних програм» було переглянуто ОПП «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти зі спеціальності 125 «Кібербезпека» (зміни внесені на підставі результатів перегляду ОПП відповідно до наказу від 08.06.2022 №154/од). Згідно з вимогами постанови КМУ від 16.12.2022 №1392 «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» було змінено назву спеціальності 125 «Кібербезпека» на 125 «Кібербезпека та захист інформації». Після щорічного перегляду, проведеного у 2023 році, ОПП «Безпека інформаційних та комунікаційних систем» переведена на спеціальність 125 «Кібербезпека та захист інформації» починаючи з 2023 року вступу та затверджено вченою радою НАУ (протокол №2 від 15.02.2023) і введена наказом від 23.02.2023 № 069/од. З урахуванням пропозицій стейкхолдерів та академічної спільноти у 2024 році було розроблено нову редакцію ОПП. Нова редакція затверджена вченою радою НАУ(протокол №4 від 17.04.2024) і введена наказом від 23.04.2024 № 166/од (підстава Рішення № 1 від 16.01.2024 засідання Науково-методичної ради НАУ), але відповідно до п.1.47 наказу голови комісії з реорганізації НАУ, в.о. ректора, від 28.03.2024 № 120/од «Про введення в дію рішень вченої ради університету від 20 березня 2024 року (протокол №3)» реалізація освітнього процесу за цією редакцією освітньої програми в 2024-2025 н. р. відтермінована у зв'язку з реорганізацією НАУ.
Згідно з наказом від 14.01.2025 №19/од «Про перегляд освітньо-професійних програм, за якими провадиться освітня діяльність КАІ» розпочався перегляд освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти. Проєкт освітньої програми для другого (магістерського) рівня вищої освіти зі спеціальності F5 «Кібербезпека та захист інформації» галузі знань F «Інформаційні технології» було розроблено робочою групою та оприлюднено для громадського обговорення на вебсайті університету https://surl.li/bgkvlm та кафедри https://surl.li/rijmou. Перегляд ОПП «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти здійснювався кафедрою кібербезпеки відповідно до внутрішніх процедур забезпечення якості освіти із залученням зацікавлених сторін. Основною метою перегляду було оновлення програми відповідно до сучасних викликів у сфері кібербезпеки, міжнародних стандартів, потреб ринку праці та рекомендацій стейкхолдерів. Робота із зацікавленими сторонами відбувалася у кілька етапів: обговорення на засіданнях кафедри – робоча група аналізувала наявну програму та ініціювала зміни (протокол № 2 від 28.01.2025, протокол № 2/1 від 03.02.2025); засідання круглого столу (27.02.2025, https://surl.li/mkrgih) – проведено обговорення за участю роботодавців, випускників та здобувачів, під час якого були надані пропозиції щодо вдосконалення ОПП; рецензування програми – отримані письмові рецензії від експертів у галузі кібербезпеки; анкетування здобувачів освіти – зібрано пропозиції щодо покращення навчального процесу, його організації та змістового наповнення (https://surl.li/gmmnoj , протокол № 4 від 27.02.2025); електронна комунікація – частина рекомендацій надходила у письмовому форматі на корпоративну пошту гаранта ОП. Розширене засідання кафедри кібербезпеки факультету комп'ютерних наук та технологій із залученням широкого кола зацікавлених сторін відбулося 11 березня 2025 року, зокрема викладачів кафедри, стейкхолдерів, випускників і здобувачів освіти

на якому було погоджено нову редакцію освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» спеціальності F5 «Кібербезпека та захист інформації» другого (магістерського) рівня вищої освіти (https://surl.li/mchnjq) та ОПП затверджена наказом від 31.03.2025 №209/од «Про введення в дію рішень Вченої ради КАІ від 26 березня 2025 року (протокол № 5)».

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	*З*	*ОД*	*З*
1 курс	2025 - 2026	120	35	13	0	0
2 курс	2024 - 2025	50	35	10	0	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	**65389 Управління кібербезпекою та захистом інформації** **65408 Системи технічного захисту інформації, автоматизація її обробки** **65410 Системи та технології кібербезпеки** **65409 Безпека інформаційних і комунікаційних систем**
другий (магістерський) рівень	**65512 Системи технічного захисту інформації, автоматизація її обробки** **65379 Системи та технології кібербезпеки** **65513 Безпека інформаційних і комунікаційних систем**
третій (освітньо-науковий/освітньо-творчий) рівень	**65364 Кібербезпека**

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 право власності, господарського відання або оперативного управління (оренда, безоплатне користування тощо)	0	0
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	*ОПП БІКС Магістр 2023 125 Кібербезпека та захист інформації.pdf*	2U113BbVUFV3RKJu7znj87O2IRYCT5l4oHORSgWiHTc=
Освітня програма	*ОПП БІКС Магістр 2025 F5 Кібербезпека та захист інформації.pdf*	nu58hjrZDWDRYXuK82hlsYozqfSHoD1FkouifSm5tI8=

Навчальний план за ОП	*НМ-14-125-1_23.pdf*	6eWKqD3XSZJsgtuciw6PSQh2TXFxmrF1++Vjo+Rq1eA=
Навчальний план за ОП	*НМ-14-125-1 з_23.pdf*	9oLNt/R33GbEUeMLQbOIPLjBh/HEHQZ6K2EFwme5EV4=
Навчальний план за ОП	*НМ-4-F5-1-2025 (денне навчання).pdf*	KNpUBJ1LMeF8c7o/ZlmvCTHh1urwQklo6fe65bS8RMs=
Навчальний план за ОП	*НМ-4-F5-1з-2025 (заочне навчання).pdf*	h5r/rbsY9BN/uLWGR+/lpQbQUGrwgOwzQch6TqOi8ZE=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*РЕЦЕНЗІЯ (Магістр)_vaibit.pdf*	EUprGd4SfnUoxt3/g037sBgi9GlroSOKzhwb75o3yyA=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Рецензія ОПП Магістр Кіберполіція.pdf*	n8n53uBl+/P8Z7stxsMnMAp2Be2p7syqSKUeJ6m3JnY=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Рецензія_UkSATSE_ОПП Магістр.pdf*	iBZTnYaxMh4d8aTnx/8zTmpTcmeo1XjE9TT2JcJHj2I=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*РЕЦЕНЗІЯ_СітонГруп_ОПП Магістр.pdf*	ExhrYoPus+vxl6tEObLpxyBBJo0c4DdFaLP19cdQ+dM=

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 від 18.03.2021 №332, затверджений Стандарт вищої освіти України (далі – Стандарт) зі спеціальності 125 «Кібербезпека» для другого (магістерського) рівня освіти (http://surl.li/hgvgvl). При розробці ОПП «Безпека інформаційних і комунікаційних систем» враховано Стандарт для другого (магістерського) рівня із галузі знань 12 «Інформаційні технології» зі спеціальності 125 «Кібербезпека».

Зміст ОПП «Безпека інформаційних і комунікаційних систем» дає можливість досягти результатів навчання, які визначені Стандартом, а саме: програмні результати навчання в ОПП «Безпека інформаційних і комунікаційних систем» повністю відповідають результатам навчання. Цілі ОПП відповідають цілям навчання. Програмні результати навчання за розробленою ОПП повністю відповідають вимогам, наведеним у Стандарті: ПР1- ПР23 (розділ VI Стандарту). Сукупність результатів навчання ПРН1-ПРН23 забезпечено обов'язковими компонентами ОПП. Матриця забезпечення програмних результатів навчання відповідними компонентами наведена у п. 5 даної ОПП. Інтегральна компетентність в рамках ОПП формується на основі узагальнення компетентнісних характеристик освітнього рівня «Магістр» та повною мірою розкривається при написанні кваліфікаційної роботи. Форма та вимоги до випускової атестації здобувачів другого (магістерського) рівня вищої освіти, приведені в Стандарті, відображені в ОПП. Таким чином, в розробленій ОПП реалізовано компетентнісний підхід відповідно до Національної рамки кваліфікацій України. Усі програмні результати навчання, зазначені в ОПП, досягаються змістовним наповненням визначених освітніх компонентів, їх обсягами та методами навчання й контролю. Достатня кількість комп'ютерної техніки, кадрового, навчально-методичного та програмного забезпечення ОПП сприяють досягненню результатів навчання, визначених Стандартом. Визначені вимоги до рівня знань, умінь, комунікацій та відповідальності магістрів повною мірою відповідають освітнім програмам провідних українських та світових ЗВО. Відповідність програмних результатів навчання, освітніх компонентів, методів навчання та оцінювання наведено у

таблиці 3.

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

Присвоєння професійних кваліфікацій в межах програми не передбачено. Разом з цим зміст ОК ("Методи побудови та аналізу криптосистем","Моніторинг та аудит кібербезпеки", "Технології захисту мережевих інфраструктур","Технології створення та застосування систем захисту кіберпростору") враховують професійний стандарт («Фахівець з питань безпеки», наказ Адміністрації Держспецзв'язку від 25.11.2022 № 715), зокрема щодо криптографічного захисту, аудиту та моніторингу, а також розроблення та впровадження комплексних систем кіберзахисту, що дозволяє забезпечити конкурентно спроможність випускників.

Чи мета освітньої програми та програмні результати навчання визначаються з урахуванням потреб заінтересованих сторін (стейкголдерів)?
- здобувачі вищої освіти та випускники програми

Інтереси здобувачів за другим (магістерським) рівнем вищої освіти були враховані під час формулювання цілей ОПП та програмних результатів навчання. Для оцінки якості навчання в 2024/2025 н. р. проведено опитування здобувачів, які навчаються за цією ОПП, щодо якості організації навчального процесу з метою виявлення проблем у навчанні та в подальшому врахувати їх зауваження/побажання. Результати анкетування відображені за посиланням https://surl.lu/pbyppn Обговорення результатів анкетування здобувачів вищої освіти щодо якості надання освітніх послуг за ОПП «Безпека інформаційних і комунікаційних систем» відображено у протоколі засідання кафедри від 27.02.2024 № 4. Відділом моніторингу якості вищої освіти КАІ проведено опитування здобувачів ВО і виконано аналіз відповідей щодо задоволеності навчання за ОП (http://surl.li/snrzfa). Відповідно до інтересів здобувачів укладаються угоди про співпрацю з роботодавцями для проведення практик і працевлаштування (http://kszi.nau.edu.ua/stejkkholderi). Здобувачі активно долучаються до обговрення проектів ОПП, а саме обговорення проекту ОПП 11.03.2024 (https://surl.li/tfklth) здобувачі Тріщун А., Величківський І. та обговорення проекту ОПП 27.02.2025 (https://surl.li/tplkby) здобувачка Маляренко С. підтримали ОП та відзначили можливість реалізації індивідуальної освітньої траєкторії студентів. Випускники висловлюють свою думку щодо подальшого розвитку ОПП, здебільшого, в усній формі при неформальному спілкуванні та приймають участь у обговоренні (27.02.2025, https://surl.li/mfvspq)

- роботодавці

Для врахування інтересів та пропозицій роботодавців щодо цілей і програмних результатів навчання ОПП «Безпека інформаційних і комунікаційних систем» проводились спільні зустрічі та круглі столи між розробниками ОПП і представниками підприємств (організацій), щодо обговорення ключових моментів організації освітнього процесу при підготовці даної освітньої програми (https://surl.li/uissqj, http://surl.li/nzqgmj; http://surl.li/yfqurn; http://surl.li/drpltn; http://surl.li/wocvdr) а саме: Державним підприємством обслуговування повітряного руху України «Украероруx», ТОВ «СІТОН ДІДЖИТАЛ», Всеукраїнської асоціації «Інформаційна безпека та інформаційні технології» та інші. Отримано відповідні позитивні рецензії роботодавців на ОП «Безпека інформаційних і комунікаційних систем». Побажання роботодавців враховувалися також при укладенні договорів про співробітництво: меморандум про співпрацю з Департаментом кіберполіції Національної поліції України, договір про співробітництво з «Алгоритм-Х»; договір про науково-технічне співробітництво ТОВ «Центр інформаційної та технічної підтримки «Сапфоріс»; договір про співробітництво з ТОВ «СІТОН ДІДЖИТАЛ», договір про співробітництво з ТОВ «АНТЕ МЕДІАМ» (03.06.2025), договір про співробітництво з «ІТ Спеціаліст» (18.06.2025) та ін. (http://kszi.nau.edu.ua/stejkkholderi).

- академічна спільнота

Інтереси академічної спільноти враховувались наступним чином: академічної спільноти КАІ – через обговорення проблем академічної свободи викладання та прийняття відповідних рішень на засіданнях кафедр, Комісії з якості факультету, Науково-методичної ради факультету; академічної спільноти взагалі – через створення умов для співпраці з представниками інших ЗВО, наукових установ, а також комунікації з представниками інших академічних установ на конференціях, під час роботи над спільними науковими дослідженнями тощо. Також інтереси академічної спільноти як стейкхолдера враховуються відповідно до: опитування викладачів, задіяних в освітньому процесі за ОП; результатів стажування в закордонних ЗВО, освітніх програмах, науково-дослідних організаціях України та провідних організаціях: Cisco Networking Academy (http://surl.li/hzmnlc); USAID «Кібербезпека критично важливої інфраструктури України», EPAM, SoftServe, Sigma Software University, ТОВ «Алгоритм-Х»; Технічно-Гуманітарна академія в Бельско-Бяла, Польща, SoftServe; ДЗВО «Університет менеджменту освіти»; ТОВ ІТ-Спецсервіс; ТОВ «ЦСК «Україна», SoftServe, GlobalLogic (http://surl.li/ngwnul). Студенти мають можливість наукового стажування за програмами академічної мобільності Еразмус+, а також приймають участь у міжнародних конференціях (http://surl.li/szqlrn).

- інші стейкхолдери

Джерелами співпраці зі стейкхолдерами щодо врахування їх пропозицій є проведення Днів відкритих дверей (http://iro.nau.edu.ua/, https://surl.lu/yhgxmv); фахові конференції, круглі столи тощо. 23–24 травня 2025 року кафедра кібербезпеки Факультету комп'ютерних наук та технологій долучилася до Фестивалю кар'єри на ВДНГ, що проходить у місті Києві. Захід проходив під гаслом «Твій перший крок у нову професійну подорож» та став справжнім майданчиком можливостей для молоді, студентів і майбутніх спеціалістів https://surl.li/ykcdrq . Кафедра

кібербезпеки КАІ прийняла участь 19 та 30 липня 2025 року у OPEN DAY https://www.facebook.com/share/p/1EQ5PPwVc5/, https://www.facebook.com/share/p/1CKRBWkyQ6/ і познайомили майбутніх студентів з напрямом кібербезпеки, розповіли, як здіснюється підготовка фахівців за ОПП. Зауваження та побажання інших стейкхолдерів враховуються під час формування переліків обов'язкових і вибіркових освітніх компонент ОПП, корегування навчальних планів, корегування робочих навчальних програм дисциплін. Надається можливість на академічну мобільність Еразмус+. Стейкхолдери також оцінюють та підписують ОПП. Публічне обговорення проєкту ОП відбувалося на офіційному сайті університету (https://surl.li/kluqsd), (https://surl.li/vsfamo).

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

Мета освітньо-професійної програми полягає у підготовці висококваліфікованих, конкурентоспроможних фахівців на глобальному ринку праці, здатних розв'язувати задачі дослідницького та інноваційного характеру у сфері кібербезпеки та захисту інформації. Програма забезпечує здобувачів фундаментальною підготовкою, що включає поглиблені теоретичні та практичні знання, уміння та навички, необхідні для ефективного виконання професійних завдань у сфері захисту інформації, зокрема з урахуванням специфіки авіаційної галузі. Здобувачі оволодівають сучасними методами, технологіями та засобами забезпечення безпеки інформаційних і комунікаційних систем, включаючи їх проєктування, впровадження та експлуатацію.
Відмінність програми – реалізація моделі підготовки фахівців в сфері безпеки інформаційних і комунікаційних систем з урахуванням потреб ІТ ринку, а також авіаційної галузі України. Мета ОПП враховує Стандарт для другого (магістерського) рівня вищої освіти зі спеціальності 125 «Кібербезпека» (http://surl.li/kevmdj) та відповідає відповідає місії КАІ, яка полягає в тому, щоб надихати і розвивати лідерів, які створюють інновації та зміцнюють лідерство України. Також ОП відповідає Стратегії розвитку КАІ на період 2025–2030 років щодо розвитку освіти, науки, інновацій та міжнародної співпраці (https://surl.li/btmbrp), що корелюється з потребами ринку праці, інтересами роботодавців та академічної спільноти.

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

Мета та програмні результати навчання за ОПП відповідають тенденціям розвитку спеціальності, що орієнтовані на розв'язання задач дослідницького та інноваційного характеру у сфері кібербезпеки та захисту інформації, в тому числі моделювання, розробка, впровадження і експлуатація програмних та програмно-апаратних комплексів та засобів захисту інформації на об'єктах критичної інфраструктури, авіаційної галузі та народного господарства .В ході розробки та перегляду ОПП було проаналізовано стан ринку праці (https://www.work.ua, https://robota.ua, https://ua.joblum.com) та виявлено потенційних стейкхолдерів. При формуванні навчального плану вказані тенденції представлені в професійних дисциплінах і в тематиці курсових та кваліфікаційних робіт. Тенденції розвитку спеціальності було проаналізовано при формуванні ОПП через аналіз навчальних планів провідних вітчизняних навчальних закладів (НТУ України «Київський політехнічний інститут імені Ігоря Сікорського», Київський національний університет імені Тараса Шевченка, Національний університет «Львівська політехніка», Київський столичний університет імені Бориса Грінченка). Цілі ОПП та програмні результати навчання відповідають тенденціям розвитку ринку праці. Вимоги та потреби провідних роботодавців ринку праці задовольняються шляхом введення в навчальний план нових вибіркових навчальних дисциплін.

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

Під час формулювання цілей та програмних результатів навчання ОПП було враховано галузевий та регіональний контекст шляхом вивчення інтересів стейкхолдерів, оскільки вони сформульовані на основі урахування результатів аналізу стану та сучасних тенденцій розвитку наукових досліджень у сфері інформаційної та кібербезпеки в Україні та в м. Києві. Провідні викладачі співпрацюються з ЗВО, науковими установами, провідними ІТ-компаніями України і м.Києва з питань інформаційної та кібербезпеки. Така співпраця дозволяє враховувати специфіку галузевої регіональної науково-технічної та кадрової політики і сучасні вимоги до майбутніх фахівців у цілях, програмах дисциплін та програмних результатах навчання. Викладачі та здобувачі беруть участь у різних міжнародних проєктах, що дозволяє підтримувати актуальність ОПП другого (магістерського) рівнів вищої освіти, враховувати тенденції розвитку спеціальності та потреби регіону і держави, зокрема це Міжнародний проєкт USAID «Кібербезпека критично важливої інфраструктури України» (http://surl.li/qzuphh, http://surl.li/cjtriq), конференція «Стратегія розбудови кадрового потенціалу України у сфері кібербезпеки та захисту інформації» (http://surl.li/jncxax).
Мета освітньої програми та програмні результати навчання формуються з урахуванням актуальних потреб ринку праці та галузевого контексту. Зокрема, набрання чинності Законом України від 17.04.2025 № 4336-IX підтверджує зростаючий попит на відповідних фахівців в галузі.

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

ОПП розроблена відповідно до потреб світового ринку праці та нових тенденцій розвитку кібербезпеки і технологій. Під час формулювання цілей та ПРН ОПП використовувався досвід вітчизняних ЗВО: НТУ України «Київський політехнічний інститут імені Ігоря Сікорського», Київський національний університет імені Тараса Шевченка, Національний університет «Львівська політехніка», Київський столичний університет імені Бориса Грінченка. За результатами аналізу ОП обрано відповідний комплекс обов'язкових дисциплін та вибіркових компонентів ОПП. Був врахований також значний досвід, який отримали викладачі кафедри кібербезпеки та технічного захисту

інформації завдяки участі у проєкті Агентства USAID «Кібербезпека критично важливої інфраструктуриУкраїни» (http://surl.li/mbzvzl), участь у літніх школах «Європейський досвід для підвищення стійкості критично важливих об'єктів в Україні» за Проєктом Еразмус+ (https://surl.li/jtayhe, https://surl.li/ilccqe, https://www.facebook.com/share/p/165cZruS2L/), SoftServe Academy (Cloud Environment Configuration and Security / Налаштування та безпека хмарних середовищ)

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

Мета освітньої програми та програмні результати навчання за спеціальністю F5 «Кібербезпека та захист інформації» формулювалися з урахуванням кращих практик та досвіду реалізації аналогічних освітніх програм провідних закордонних університетів, зокрема:
Каліфорнійського державного університету Сан-Бернардіно (California State University, San Bernardino), який є одним із визнаних центрів підготовки кадрів у сфері кібербезпеки, акредитованим за стандартами National Security Agency (NSA) та Department of Homeland Security (DHS) https://www.csusb.edu/cybersecurity;
Університету Джорджа Вашингтона (George Washington University), програма якого орієнтована на підготовку спеціалістів із глибокими знаннями в галузі прикладної криптографії, захисту комп'ютерних мереж і безпечного програмування https://cs.engineering.gwu.edu/master-science-cybersecurity-computer-science;
Канзаського державного університету (Kansas State University), де кібербезпека викладається з інтеграцією інженерного підходу, розвитку навичок аналізу ризиків, етичного хакінгу та кіберзахисту критичної інфраструктури https://engg.k-state.edu/academics/undergraduate/cybersecurity/ .
Врахування досвіду зазначених навчальних закладів дало змогу:
структурувати освітню програму відповідно до актуальних світових тенденцій у сфері кібербезпеки;
сформулювати програмні результати навчання, які охоплюють як технічні, так і управлінські компетентності, міждисциплінарний підхід, розвиток soft skills;
врахувати міжнародні стандарти, таким як NICE (National Initiative for Cybersecurity Education), ISO/IEC 27001, та врахування рекомендацій NIST;
підвищити привабливість та конкурентоспроможність випускників на міжнародному ринку праці.
Таким чином, урахування міжнародного досвіду сприяє забезпеченню високої якості освітнього процесу, професійної мобільності здобувачів вищої освіти та інтеграції освітньої програми у глобальний освітній 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)?

Об'єктами вивчення за ОП є сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; інформаційні системи (інформаційнокомунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних; інформаційні ресурси; програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; системи управління інформаційною безпекою та/або кібербезпекою; технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. Ціллю навчання за ОПП є підготовка висококваліфікованих, конкурентоспроможних фахівців на глобальному ринку праці, здатних розв'язувати задачі дослідницького та інноваційного характеру у сфері кібербезпеки та захисту інформації. Програма забезпечує здобувачів фундаментальною підготовкою, що включає поглиблені теоретичні та практичні знання, уміння та навички, необхідні для ефективного виконання професійних завдань у сфері захисту інформації, зокрема з урахуванням специфіки авіаційної галузі. Теоретичний зміст предметної області містить теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки. Програма має прикладну орієнтацію та базується на загальновідомих положеннях, результатах сучасних наукових досліджень та нових знаннях у сфері кібербезпеки,

необхідних для майбутньої професійної діяльності магістрів, здатних вирішувати певні проблеми і задачі за умови оволодіння системою компетентностей. Перелік ОК випускника ОПП дозволяє стверджувати про відповідність змісту ОПП предметній області спеціальності F5 «Кібербезпека та захист інформації». ОПП ґрунтуються на принципах студентоцентризму та індивідуально-особистісного підходу; реалізуються через навчання на основі досліджень, посилення практичної орієнтованості та творчої спрямованості у формі комбінації лекцій, практичних занять, самостійної навчальної і дослідницької роботи, розв'язування прикладних задач, виконання проєктів, навчальних та виробничих практик, курсових робіт (проектів), кваліфікаційної роботи. Освітня програма охоплює технології безпеки інформаційно-комунікаційних систем, захист мережевої інфраструктури, підходи щодо моніторингу та аудиту кібербезпеки та розробку систем захисту кіберпростору для об'єктів критичної інфраструктури, зокрема авіаційної галузі та народного господарства, відповідно до міжнародних стандартів та вимог.

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

У 2024-2025 н.р. формування індивідуальної освітньої траєкторії здобувачів ВО відбувалось згідно встановлених документів https://surl.li/usosxb, https://surl.li/yiphyn та передбачало два етапи: етап 1 – обрання вибіркових дисциплін на рівні освітньої програми за допомогою автоматизованої системи формування індивідуальної освітньої траєкторії (https://directorate.nau.edu.ua/login) та корпоративної пошти здобувача ВО ; етап 2 – можливість поглиблення індивідуалізації вибору засвідчує заповнення заяви.
У 2025-2026 н.р. формування індивідуальної освітньої траєкторії здобувачів вищої освіти в КАІ забезпечується відповідно до Положення про організацію освітнього процесу (https://surli.cc/wettwe) та Тимчасового порядку вибору навчальних дисциплін здобувачами ВО на першому (бакалаврському) та другому (магістерському) рівнях вищої освіти в КАІ в системі «Digital University» (https://surl.li/mcmhjg). Ці документи регламентують процедури вибору навчальних дисциплін (https://surl.li/xaezzr). Основним документом щодо формування індивідуальної освітньої траєкторії є індивідуальний навчальний план. Студенти мають можливість обирати дисципліни в обсязі, що становить не менше 25% (10% для регульованих спеціальностей) від загального обсягу кредитів ЄКТС ОП. При формуванні індивідуальної освітньої траєкторії здобувач також має можливість вільного вибору тем для досліджень, навчання одночасно за кількома ОП, участі в програмах академічної мобільності, а також зарахування результатів навчання, отриманих у неформальній та інформальній освіті.

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

Вибір дисциплін у 2025-2026 н.р. здійснюється через прозору та чітко визначену процедуру, яка включає етапи вибору, терміни його організації та алгоритм електронного запису через систему «Digital University» (https://cabinet.nau.edu.ua/login). Процедура формування індивідуальної освітньої траєкторії на 2024-2025 н.р. https://surl.li/sqgeps, силабуси https://surl.li/urzcyz, результати відображені на сайті кафедри https://surl.li/papseb, https://surl.lu/rptemp та університету https://surl.lt/zvjfbf.
Студенти завчасно інформуються про старт вибору через офіційні канали комунікації, зокрема через корпоративну електронну пошту, особистий кабінет у системі «Digital University», сайт та соцмережі університету. Електронний каталог вибіркових дисциплін містить повні силабуси із зазначенням результатів навчання, форм контролю та контактної інформації викладачів.
У встановлені графіком строки студент заходить до особистого кабінету, переглядає відкритий каталог із силабусами, проставляє пріоритети та підтверджує свій вибір.
Каталог вибіркових компонентів щороку переглядається науково методичною радою КАІ, що гарантує актуальність змісту, усунення дублювань і врахування рекомендацій роботодавців та трендів ринку праці. Обсяг вибіркової частини незмінно відповідає вимогам закону – не менше 25 % загальної кількості кредитів (для регульованих спеціальностей не менше 10 %). Обсяг вибіркової навчальної дисципліни на першому (бакалаврському) та другому (магістерському) рівнях вищої освіти – 4 кредити ЄКТС. У липні 2025 р. пройшов тестовий вибір навчальних дисциплін через систему «Digital University».
Каталог вибіркових освітніх компонентів КАІ складається з загальноуніверситетських і факультетських дисциплін. Факультетські вибіркові дисципліни забезпечують цільове поглиблення професійної підготовки, формують вузькогалузеві компетентності та підвищують конкурентоспроможність випускників на ринку праці. Загальноуніверситетські дисципліни покликані розширити міждисциплінарний кругозір і включає п'ять тематичних підкаталогів: підприємницька підготовка; партнерські курси, що викладаються фахівцями таких компаній, як «Прогрестех Україна», Ark Robotics, MikroTik, АТ «Антонов», Гетеборзький університет та інші, і ґрунтуються на аналізі реальних виробничих кейсів; дисципліни КАІ LABS, у межах яких студенти виконують проєктну роботу в лабораторіях університету та партнерських дослідницьких центрах; дисципліни мовної підготовки, спрямовані на формування стійких комунікативних навичок для діяльності в міжнародному середовищі; курси з розвитку soft skills, що формують соціально комунікативні та командні компетентності, необхідні для успішної професійної реалізації. Таке структурування вибіркової частини навчального плану забезпечує студентам можливість поєднувати фахову спеціалізацію з розвитком підприємницьких, мовних та міжособистісних навичок, що відповідає сучасним вимогам ринку праці та стратегічним пріоритетам університету.

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 здійснюється відповідно до Положення про організацію освітнього процесу в КАІ (https://surl.li/fanviz). В КАІ діє Положення про організацію та проведення практик здобувачів вищої освіти КАІ https://surl.li/rfwuoz Практична підготовка здобувачів в межах ОПП передбачена навчальним планом (2025-2026 н.р.): науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем (6 кредитів ЄКТС),

переддипломна практика (9 кредитів ЄКТС), що є обов’язковими ОК. Програми практик регламентують діяльність здобувачів і керівників практик (https://surl.lu/bbxbiy). Практика є важливим етапом професійної підготовки здобувачів, однією з основних складових для формування загальних і фахових компетентностей. Формулювання цілей і завдань практичної підготовки, визначення її змісту відбувається у співпраці з роботодавцями, які окреслюють реальні потреби ринку праці та необхідні уміння і навички. Базами практик можуть бути підприємства та організації в Україні та за її межами. Практики реалізовуються на підставі договорів, що підписані з КАІ (http://kszi.nau.edu.ua/stejkkholderi; http://surl.li/sgoutt; https://surl.lu/mrjgtj). Зі здобувачами проводять організаційні зустрічі щодо організації та проведення практичної підготовки (https://surl.li/kbxoha, https://surl.li/rmsvlr)

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

Упродовж усього терміну навчання за ОПП здобувачі набувають та практикують соціальні навички, важливі для сучасного фахівця для розв’язання задач дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки. Для випускників ОПП дані навички є особливо важливими, оскільки вони мають демонструвати здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності). Соціальні навички, навички критичного мислення та креативності, емоційного інтелекту, культурної обізнаності та поваги мультикультурності («SoftSkills») формуються в межах загальних компонент ОПП ОК1-2 та фахової компоненти ОК3, за рахунок підготовки доповідей, презентацій, рефератів тощо. Формуванню соціальних навичок «SoftSkills» сприяють дисципліни вільного вибору для ефективної роботи в команді та успішної кар'єри. Ці дисципліни з формування соціально-комунікативних навичок допомагають розвинути важливі компетенції для професійної діяльності (https://nau.edu.ua/ua/news/2025/7/24032.html).Участь здобувачів у диспутах та конференціях, що передбачено ОПП, передбачає активну соціальну взаємодію учасниками інформаційного простору. Сприяє цьому також простір неформальної освіти NAU HUB (https://bit.ly/3fFJKEN). Науково-педагогічні працівники кафедри, а саме доцентка Анна Ільєнко взяла участь у міжнародній програмі підвищення кваліфікації викладачів EDUPRO присвяченій розвитку SoftSkills (http://surl.li/harogw, https://surl.li/bcjwuy).

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

ОПП має чітку структуру, що забезпечує логічну взаємопов'язаність освітніх компонентів, які сприяють досягненню заявлених цілей та програмних результатів навчання. Програма складається з обов'язкових і вибіркових компонентів, які формують загальний обсяг 90 кредитів ЄКТС. Обов'язкові компоненти охоплюють дисципліни, такі як «Методологія прикладних досліджень у сфері кібербезпеки», «Моніторинг та аудит кібербезпеки», «Методи побудови та аналізу криптосистем» та інші, що забезпечують фундаментальні знання у сфері кібербезпеки. Освітні компоненти програми інтегруються в єдину систему, де кожен курс підтримує і доповнює інші. Програма спрямована на підготовку фахівців, здатних вирішувати складні задачі в сфері інформаційної безпеки. Програмні результати навчання включають вміння критично аналізувати проблеми кібербезпеки, інтегрувати знання для розв'язання складних задач та проводити дослідницьку діяльність. Освітня програма забезпечує формування загальнокультурних компетентностей через вивчення етики професійної діяльності, правових аспектів інформаційної безпеки та норм міжнародного співробітництва. Це дозволяє студентам не лише здобути професійні знання, але й розвинути критичне мислення та відповідальність у суспільств. Здобувачі програми отримують навички самостійного аналізу та визначення закономірностей суспільних процесів через практичну діяльність під час навчання. Це включає участь у проектах, дослідженнях та практиках, що сприяють розвитку аналітичних навичок в сфері кібербезпеки. Освітня програма демонструє чітку структуру, логічну взаємопов'язаність компонентів та сприяє формуванню необхідних компетентностей для успішної професійної діяльності в галузі кібербезпеки та досягнення заявленої мети і програмних результатів навчання. Всі ОК та ВК освітньої програми забезпечують якісну фахову підготовку здобувача ВО для формулювання мети, об'єкту, предмету досліджень, проведення розрахунків та експериментів в кваліфікаційній роботі (http://surl.li/qsbcmf, http://surl.li/nkkgfi).

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 розроблені загальні вимоги щодо розподілу обсягу окремих ОК в ОП (в кредитах ЄКТС) із фактичним навантаженням здобувачів (включно із самостійною роботою) відповідно до Методичних рекомендацій з розробки навчальних планів підготовки здобувачів ВО (https://bit.ly/3scifVW), що встановлюють вимоги до розрахунку достатності навчального навантаження на здобувачів відповідно до кількості кредитів та видів завдань. Один кредит ЄКТС відповідає 30 годинам загального навчального навантаження, включаючи всі види навчальної діяльності — аудиторну, самостійну, практичну тощо. У випускному семестрі до ОК віднесені переддипломна практика та кваліфікаційна робота. В ОПП використовуються наступні види аудиторних навчальних занять: лекції, лабораторні заняття, практичні заняття. Більше 50% обсягу ОПП спрямовано на забезпечення загальних та фахових компетентностей.
Обсяг кредитів для кожної ОК визначається з урахуванням типу завдань, часу на їх виконання, складності та очікуваних результатів навчання. Для перевірки відповідності між запланованим обсягом і фактичним

навантаженням у КАІ проводиться періодичне опитування здобувачів на загальноуніверситетському (https://surl.li/nffjwp, https://nau.edu.ua/ua/menu/quality/otsinyuvannya-rezultativ-yakosti-navchannya/) та кафедральному рівнях (http://surl.li/ardhgj). Це дозволяє своєчасно коригувати навчальні плани й забезпечити збалансоване 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

Структура освітньої програми забезпечує практикоорієнтованість через інтеграцію теоретичних знань і практичних навичок, що відповідають вимогам сучасного ринку праці. Програма розроблена з урахуванням потреб ІТ-індустрії та авіаційної галузі, що забезпечує випускників знаннями та вміннями, необхідними для роботи у сфері кібербезпеки та включає вивчення сучасних технологій та методів захисту інформації. Програма включає навчально-дослідницьку практику та переддипломну практику, які проводяться в реальних умовах підприємств і організацій. Це дає можливість студентам отримати досвід роботи в професійній сфері (https://surli.cc/qhsgoq, http://surl.li/zdwuef, http://surl.li/vugcut). Викладання за даною ОПП здійснюється через комбінацію лекцій, практичних занять та проектної діяльності, що сприяє глибшому розумінню матеріалу та розвитку навичок критичного мислення. Студенти активно залучаються до дослідницької діяльності, що підвищує їхню мотивацію та готовність до професійної діяльності (http://surl.li/oxnghp). Для забезпечення досягнення ПРН функціонують лабораторії та центри, зокрема: Навчальний центр «ІТ Академія» та навчально-дослідна лабораторія протидії кіберзагрозам в авіаційній галузі (https://cyberlab.nau.edu.ua/), кіберполігон Cyber Range UA (https://surl.li/mreppk, http://surl.li/sybbki), лабораторія AxxonSoft (https://surl.li/ancyop). В КАІ діє ПОЛОЖЕННЯ про дуальну форму здобуття вищої освіти в КАІ https://surl.li/dyllph. Підготовка здобувачів вищої освіти 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

ОПП сприяє набуттю здобувачами навичок і компетентностей, орієнтованих на досягнення глобальних цілей сталого розвитку до 2030 року, проголошених резолюцією Генеральної Асамблеї ООН та визначених Указом Президента України. ОПП передбачає формування ЗК абстрактного мислення, аналізу та синтезу. До змісту ОК включені питання, які забезпечують набуття здобувачами вищої освіти знань, навичок і компетентностей, направлених на досягнення Цілей сталого розвитку ООН до 2030 р. Набуття здобувачами ВО фокусуються на інноваціях та розвитку стійкої інфраструктури в сфері кібербезпеки, а також здійснює підготовку фахівців у сфері кібербезпеки, що сприяє соціальному розвитку і безпеці та є важливими аспектами для сталого розвитку суспільства. ОП забезпечує принципи якісної освіти через інтеграцію теоретичних знань з практичними навичками та набуття здобувачами ВО ІК, ЗК1-6, що дозволяє випускникам бути конкурентоспроможними на ринку праці. Освітня програма спрямована на підготовку нового покоління фахівців, здатних будувати стале майбутнє. При перегляді ОПП в 2025 році відповідну компетентність та програмний результат навчання (https://surl.gd/kjdyys)

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

Сайт приймальної комісії КАІ: https://pk.kai.edu.ua/
Правила прийому до КАІ: https://pk.kai.edu.ua/pravyla-pryiomu-do-kai-u-2025-rotsi/
Детальна інформація щодо вступу до магістратури КАІ: https://pk.kai.edu.ua/vstup/mahistratura/

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

Прийом на навчання здійснюється відповідно до Порядку прийому для здобуття вищої освіти у 2025 році зі змінами (https://zakon.rada.gov.ua/laws/show/z0312-25), Правил прийом удо КАІ у 2025 році зі змінами та Положення про приймо на навчання для здобуття ступені магістра (https://pk.kai.edu.ua/pravyla-pryiomu-do-kai-u-2025-rotsi/). Вступники, які здобули освітній рівень бакалавра, ОКР спеціаліста або ОС магістра. Всі вступники для здобуття ОС Магістр складають єдиний вступний іспит (ЄВІ - іноземна мова та тест загальної навчальної компетентності). Використовуються оцінки єдиного державного кваліфікаційного іспиту (ЄДКІ) зі спеціальності 125 «Кібербезпека та захист інформації» 2024 або 2025 р. (тільки для вступників на спеціальність F5 «Кібербезпека та захист інформації», які складали відповідний ЄДКІ 2024 або 2025 р.) або Єдине фахове вступне випробування з інформаційних технологій для всіх інших вступиків. Конкурсний бал = 0,2 × П1 + 0,2 × П2 + 0,6 × П3, де П1 - оцінка блоку з іноземної мови ЄВІ, П2 - оцінка блоку ТЗНК ЄВІ, П3 - оцінка ЄДКІ, переведена у шкалу від 100 до 200, або ЄФВВ. Передбачений вступ на основі вступних випробувань у закладі освіти замість ЄВІ та ЄФВВ для вступників з числа учасників бойових дій та осіб з особливими освітніми потребами за державним замовленням та на основі НРК7 за кошти фізичних та / або юридичних осіб. Усі вступники подають разом із заявою мотиваційний лист (https://pk.kai.edu.ua/motyvaczijnyj-lyst/).

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?

Чіткі та зрозумілі правила визнання результатів навчання, отриманих в інших закладах освіти, зокрема під час академічної мобільності, що відповідають Конвенції про визнання кваліфікацій з вищої освіти в Європейському регіоні (Лісабон, 1997 р.), є доступними для всіх учасників освітнього процесу та яких послідовно дотримуються під час реалізації освітньої програми. Ці правила висвітлюються у «Тимчасовом положенні про порядок відрахування, переривання навчання, поновлення і переведення здобувачів вищої освіти» (https://surl.li/rkpckh), «Положенні про порядок переведення (поновлення) студентів, які навчалися у вищих навчальних закладах Донецької та Луганської областей» (http://surl.li/ldmof).
Відповідно до Положення про організацію освітнього процесу https://surl.li/llzpar та Тимчасового положення про порядок відрахування, переривання навчання, поновлення і переведення здобувачів вищої освіти» (https://surl.li/rkpckh) переведення здобувачів вищої освіти на перший курс забороняється, тому здобувач вищої освіти може подати заяву про переведення тільки після першого року навчання. Він урегульовує усі аспекти організації переведення такого здобувача вищої освіти та визнання результатів навчання, отриманих в інших ЗВО, зокрема під час академічної мобільності. Основні положення розміщені на сайті КАІ у вільному доступі (https://surl.li/avwzfz).

Наведіть конкретні приклади та прийняті рішення щодо визнання результатів навчання та кваліфікацій, отриманих на інших освітніх програмах (зокрема під час академічної мобільності)

На сьогодні подібні випадки на ОПП Безпека інформаційних і комунікаційних систем не мали місця.

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, отриманих у неформальній освіті, регулюється Положенням про організацію та проведення поточного та семестрового контролю (https://is.gd/8Pghwf). Згідно п.3.34 «результати навчання осіб, які отримані у неформальному середовищі можуть бути визнані за умови порівняльного аналізу освітньої програми та отриманими документами з результатами навчання, виконанням усіх обов'язкових видів індивідуальних завдань та проходження підсумкового контролю з навчальної дисципліни для підтвердження рівня здобутих знань, умінь та інших компетентностей».
Університет зареєстровано на платформі онлайн-освіти Coursera, що надає безкоштовний доступ до багатьох курсів (https://is.gd/FudRBV).В КАІ питання визнання результатів навчання, отриманих у неформальній освіті регулюється «Положенням про порядок визнання результатів навчання, здобутих шляхом неформальної та/або інформальної освіти"
(https://nau.edu.ua/site/variables/news/2022/11/%D0%9F%D0%BE%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F.pdf) .
Інформація про можливість скористатись таким правом надається студентам під час кураторських годин.

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

На сьогодні подібні випадки на ОПП Безпека інформаційних і комунікаційних систем не мали місця.

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 на ОПП відповідає вимогам законодавства України, зокрема, Закону України «Про вищу освіту» та враховує Стандарт зі спеціальності 125 «Кібербезпека». Методи та форми навчання і викладання ОП зазначені в Положенні про організацію освітнього процесу КАІ (https://surl.li/vcabts). Навчання виконується у формі лекційних, практичних та лабораторних занять, самостійної роботи, проходження практик, виконання курсової роботи (проекту) та кваліфікаційної роботи. Використовуються словесні наочні та практичні методи, що дозволяє забезпечити формування як загальних і фахових компетенцій, так і програмних результатів навчання. Форми та методи навчання і викладання добираються викладачем самостійно з для досягнення цілей та ПРН, доцільності та студентоцентрованого підходу, і повністю узгоджуються з академічною свободою викладання. Їх відповідність ПРН представлена в РНП (http://surl.li/vargex). Застосовуються методи теоретичного, експериментального дослідження, аналізу, моделювання та прогнозування, аналізу даних, технології пошуку, обробки інформації, дискусія, презентація. Для сприяння досягнення наукових результатів у КАІ діє Наукове товариство студентів, аспірантів, докторантів та молодих вчених КАІ (http://ysa.nau.edu.ua). Підтвердженням застосування дослідницького методу є участь здобувачів у конференціях, наукові публікації (ABIA-2025 https://surl.li/xanfsn; Політ 2025 https://surl.li/msqggd; публікації студентів http://surl.li/idmzon; Survivability & Resilience – 2023 http://surl.li/bepmip; https://surl.li/galdpx).

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?

Основні напрями студентоцентрованого навчання в КАІ визначені Системою внутрішнього забезпечення якості освітньої діяльності. Навчальний процес орієнтований на студентоцентрований підхід при виборі форм і методів навчання та викладання, які наводяться в РНП дисциплін (http://surl.li/ajrlnr). Усім учасникам освітнього процесу надається доступна і зрозуміла інформація щодо цілей, змісту та ПРН, порядку та критеріїв оцінювання в межах окремих ОК. Для проведення занять залучаються провідні викладачі факультету (д.т.н., проф. Ахрамович В. М., д.т.н., проф. Міщенко А.В., к.т.н., доц Ільєнко А. В., к.т.н. Висоцька О.О.) та провідних ВНЗ (д.т.н., с.н.с. Лаптєв О. А.). Формування індивідуальної освітньої траєкторії здобувачів вищої освіти в КАІ забезпечується відповідно до Положення про організацію освітнього процесу (https://surli.cc/wettwe) та Тимчасового порядку вибору навчальних дисциплін здобувачами вищої освіти на першому (бакалаврському) та другому (магістерському) рівнях вищої освіти в КАІ в системі «Digital University».
Студентська оцінка роботи НПП є важливою для покращення якості надання освітніх послуг, впливає на рейтинг працівників та кафедр КАІ. Рівень задоволеності здобувачів методами навчання та викладання оцінюється за допомогою анкетування (http://surl.li/fbrpei). За результатами червня 2024-2025 н.р. рівень задоволеності якості освітнього процесу 84,6% https://surl.li/spkpsj (до анкетування долучилось 26 здобувачів з 35 (74,28 %).

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

Академічна свобода гарантована ЗУ «Про освіту» (https://bit.ly/3GoBOiV), Положенням про організацію освітнього процесу в КАІ (https://surl.lu/qtozuc) і полягає в педагогічній ініціативі під час провадження педагогічної, науково-педагогічної та наукової діяльності. ЗВО забезпечує поєднання навчання і досліджень під час реалізації ОПП відповідно до рівня ВО, спеціальності та цілей ОПП. Відповідно до ЗУ «Про освіту», Положення про організацію освітнього процесу в КАІ та Методичних рекомендацій до розроблення і оформлення робочих програм дисциплін (https://surl.li/wvjycs) НПП надається можливість творчо наповнювати зміст дисциплін, вносити зміни в робочі програми, обирати методи навчання для ефективного засвоєння знань, проводити заняття із застосуванням сучасних технологій, обирати самостійну форму вивчення окремих тем. В ОПП реалізується принцип академічної свободи, свободи слова та творчості, принцип толерантного ставлення до альтернативних концепцій і прикладних підходів, передбачено вільний доступ НПП до інформаційних ресурсів, баз підвищення кваліфікації і стажування. Академічна свобода здобувачів вищої освіти досягається наданням права обирати форми і методи навчання, пропонувати теми курсових робіт та проєктів, кваліфікаційних робіт, права на академічну мобільність (http://surl.li/kwbwo), можливістю навчання одночасно за декількома ОПП, отримання другої вищої освіти (https://ino.nau.edu.ua/), формуванням індивідуального навчального плану, можливістю долучатися до студентського самоврядування (http://surl.li/agvdd).

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

Повна інформація щодо цілей, змісту і очікуваних результатів навчання, порядку та критеріїв оцінювання за кожною дисципліною надається здобувачам при зустрічі наставників з академічними групами перед початком занять, а також НПП на першому аудиторному занятті з дисциплін (https://surl.lu/ayywnk). У робочих програмах навчальних дисциплін ОПП надається вся необхідна інформація щодо цілей, змісту й очікуваних результатів навчання, порядку та критеріїв оцінювання. Контрольні заходи проводяться згідно з графіком навчального процесу, який доводиться до студентів наставниками. Контрольні заходи проводяться в обсязі навчального матеріалу, визначеного робочою програмою освітніх компонент. Розроблення робочої програми навчальної дисципліни регламентується Методичними рекомендаціями до розроблення і оформлення робочої програми навчальної дисципліни денної та заочної форм навчання (http://surl.li/ahzry). Здобувач може ознайомитися з робочою програмою в електронному вигляді на сайті кафедри (http://surl.li/kuyfmf). Паперові версії робочих програм зберігаються на кафедрі.

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

У КАІ створено необхідні умови для поєднання навчальної та дослідницької роботи. Активними формами поєднання навчання та досліджень є: вирішення дослідницьких завдань при виконанні практичних і самостійних робіт, під час написання курсових робіт і проектів, кваліфікаційної роботи. ОПП передбачає набуття кожним здобувачем здатності розв'язувати складні спеціалізовані задачі та практичні проблеми в сфері кібербезпеки та захисту інформації. Кафедрою протягом 2024–2025 рр. проводились наукові дослідження в межах кафедральних науково-дослідних робіт, а саме НДР № 5-2024/18.02 «Система забезпечення кібербезпеки та стійкості об'єктів критичної інфраструктури» (http://surl.li/bseyxb). З метою поєднання навчальної та дослідницької роботи при кафедрі функціонують студентські наукові гуртки https://surl.li/nqocnm, результатом є наукові публікації студентів http://surl.li/zbaplg. Актуальність та значимість наукових досліджень і розробок НПП кафедри підтверджується участю в міжнародних науково-практичних конференціях (http://surl.li/miyepf). Інноваційні розробки кафедри включено до Каталогу «Наука та інновації» (2021) (http://kszi.nau.edu.ua/naukova-robota-g/naukovi-rozrobki). Актуальність та значимість наукових досліджень не тільки підтверджується участю у міжнародних науково-практичних конференціях, а й знаходять своє продовження у кваліфікаційних роботах. Здобувачі ВО проходять практики на підприємствах та організаціях України (http://surl.li/qkcptb, https://surl.li/igbbaj). Для підвищення ефективності навчання, проходження практики та подальшого працевлаштування підписані безоплатні угоди про співпрацю (http://kszi.nau.edu.ua/stejkkholderi).

Для сприяння досягнення наукових результатів у КАІ діє Наукове товариство студентів, аспірантів, докторантів та молодих вчених КАІ (http://ysa.nau.edu.ua). Для підтримки та заохочення молодих вчених запроваджено премії та стипендії, конкурсний відбірнаукових проєктів для молодих вчених та створено Центр організації освітньо-наукової діяльності студентів та молодих учених. Ільєнко Анна, к.т.н., доцент - стипендіат стипендії Кабінету Міністрів України для молодих вчених (постанова президії Комітету від 10 червня 2020 року № 4). У процесі реалізації освітньої програми навчальна та дослідницька діяльність інтегруються через участь студентів у командних змаганнях із кібербезпеки, що формує практичні навички, розвиває аналітичне мислення, вміння працювати в команді та закріплює теоретичні знання. Зокрема, у 2024–2025 роках студенти спеціальності брали участь у таких змаганнях: University CTF 2024 HACKTHEBOX – https://surl.lu/npdmbn; CTF Snyk 2025 – https://surl.lu/jxivnw; Cyber Apocalypse CTF 2025 HACKTHEBOX – https://surl.li/tynlgd; CYBERWARFARE 2025 – https://surl.lu/mdyoao. Участь у таких заходах не лише підвищує рівень професійної підготовки здобувачів, а й мотивує їх до дослідницької діяльності, сприяє міждисциплінарній взаємодії та поглибленому засвоєнню матеріалу навчальних дисциплін.

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

НПП оновлюють зміст освіти на основі наукових досягнень і сучасних практик у галузі кібербезпеки та захисту інформації. У КАІ діє система забезпечення якості освіти (https://bit.ly/38yquSD), рада з якості КАІ https://nau.edu.ua/ua/menu/quality/rada-z-yakosti/ одним із основних завдань якої є здійснення моніторингу та періодичного перегляду ОПП. На основі принципу академічної свободи НПП ОПП визначають, які наукові досягнення та сучасні практики слід пропонувати здобувачам під час навчання, проводять наради з групою розробників ОПП. Щорічно провідні НПП кафедри оновлюють зміст навчальних дисциплін, що знаходить відображення у робочих програмах, які щорічно розглядаються на засіданнях випускової кафедри. Науково-педагогічні працівники кафедри мають профілі в Google Scholar, ORCID з відповідними публікаціями; сертифікати та свідоцтва про підвищення кваліфікації у відповідних до ОП напрямках, що дозволяє оновлювати зміст навчальних дисциплін відповідно до вимог Положення про підвищення кваліфікації (стажування) НПП НАУ (http://surl.li/tmifep). Щорічно провідні НПП кафедри оновлюють зміст навчальних дисциплін, що знаходить відображення і у робочих програмах (http://surl.li/gpiclx), актуальність яких щорічно переглядається. Щороку оновлюється тематика кваліфікаційних робіт з урахуванням сучасних тенденцій розвитку сфери безпеки інформаційно-комунікаційних систем та мереж (http://surl.li/seuhsk).

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

Інтернаціоналізація навчання, викладання та наукових досліджень у межах ОПП КАІ здійснюється відповідно до Стратегії розвитку КАІ, положень про академічну мобільність, а також участі в міжнародних програмах і рейтингах. В освітньому процесі враховуються міжнародні освітні стандарти та кращі світові практики, зокрема за рахунок участі університету в ініціативах QS World University Rankings і Times Higher Education Rankings. Створено організаційні умови реалізації права на академічну мобільність і участі в грантових програмах HORIZON, ERASMUS+, FULLBRIGHT, MEVLANA (https://surl.li/bsdzni, https://surl.li/twmbbs, https://surl.li/tbdkvu). Здобувачі беруть участь у міжнародних онлайн-курсах, вебінарах, хакатонах (http://surl.li/qzuphh, http://surl.li/evxeuy). Доцент Висоцька О. О. пройшла стажування в Технічно-гуманітарній академії в Бельсько-Бяла (Польща). Реалізується впровадження міжнародних сертифікаційних курсів (Cisco Networking Academy http://surl.li/hzmnlc). Результати наукових досліджень кафедри публікуються в індексованих зарубіжних виданнях та презентуються на міжнародних конференціях (http://surl.li/kxnlpj). Інтернаціоналізація діяльності реалізується, зокрема, через участь здобувачів у міжнародних наукових конференціях, де вони отримують інформацію про новітні досягнення і тенденції розвитку сфери кібербезпеки, представляють результати своїх досліджень, обговорюють їх з провідними фахівцями.

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?

ПРН оцінюються згідно з Положенням про організацію освітнього процесу КАІ контрольними заходами (https://surl.li/xfvasr) та ОПП (http://surl.li/utqfsi). Вибір форми контролю за кожним ОК зумовлений його місцем у формуванні ПРН. Критерії оцінювання визначаються для ОПП загалом і для кожного її ОК окремо та фіксуються у робочих програмах навчальних дисциплін (http://surl.li/gfeawj). Контрольні заходи якості підготовки фахівців є необхідним елементом зворотного зв'язку в освітньому процесі. Вони забезпечують визначення рівня досягнення завдань навчання і дозволяють коригувати, при необхідності, хід освітнього процесу. Основними видами контролю результатів навчання здобувачів вищої освіти є вхідний, поточний, модульний, семестровий контроль та підсумкова атестація. Вхідний контроль проводиться з метою визначення рівня підготовки здобувачів вищої освіти з тих навчальних дисциплін, яким навчалися перед вивченням певної навчальної дисципліни, або загального рівня підготовки здобувача вищої освіти за попередній період навчання. Поточний контроль здійснюється науково-педагогічними працівниками у формі усного спілкування зі здобувачами вищої освіти, письмового, тестового експрес-контролю на лекціях, лабораторних, практичних, семінарських та індивідуальних заняттях і має за мету перевірку ступеня засвоєння певного навчального матеріалу, а також рівня оволодіння вміннями та навичками. Модульний (проміжний) контроль – це контроль знань та вмінь здобувачів вищої освіти після вивчення певної

частини (модуля) навчальної дисципліни. Він проводиться шляхом виконання модульної контрольної роботи, яка може мати форму тестових, аналітичних завдань тощо. Підсумковий контроль проводиться з метою оцінки результатів навчання на певному освітньому ступені рівнів вищої освіти або на окремих його завершених етапах. Підсумковий контроль включає семестровий контроль (заліки, екзамени, захист курсової роботи) та атестацію здобувачів вищої освіти. Семестровий контроль проводиться у вигляді семестрового екзамену або диференційованого заліку в обсязі навчального матеріалу, визначеного навчальною програмою конкретної навчальної дисципліни, в терміни, встановлені графіком навчального процесу. Атестація здобувачів дозволяє встановити відповідність між результатами навчання та вимогами ОПП. Атестація здобувачів ВО регламентується Положенням про атестацію здобувачів ВО (http://surl.li/iascde).

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

В КАІ чіткість та зрозумілість контрольних заходів та критеріїв оцінювання регламентуються у наступних документах: Положення про організацію освітнього процесу в КАІ (https://surl.li/xfvasr); Положенням про атестацію здобувачів ВО (http://surl.li/iascde); ОПП (http://surl.li/utqfsi); навчальних планах (http://surl.li/nbvgqv); робочих програмах навчальних дисциплін (http://surl.li/gfeawj). На навчальних заняттях викладач доводить до відома здобувачів ВО всю необхідну інформацію з навчальної дисципліни, а також інформує їх про наявність робочої навчальної програми та методичного забезпечення. Всі робочі програми навчальних дисциплін (http://surl.li/szipve) та навчальні плани (http://kszi.nau.edu.ua/osvitnij-protses/robocho-navchalni-plani) є у вільному доступі у сайті кафедри .

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

Процедура проведення контрольних заходів регулюється: Положенням про організацію освітнього процесу в КАІ (https://surl.li/xfvasr); Положенням про атестацію здобувачів ВО (http://surl.li/iascde), в яких регламентується проведення модульних контрольних робіт, диференційованих заліків та екзаменів. Усі чинні положення розташовані на сайті КАІ та є доступними для всіх учасників освітнього процесу (http://surl.li/eisxl). Графік навчального процесу, розклади заліків, екзаменів оприлюднені у відкритому доступі на офіційному вебсайті факультету у розділі Студентам (https://fcst.nau.edu.ua/), а положення наказу Про організацію освітнього процесу у 1 семестрі 2025-2026 висвітлено на сайті кафедри (http://kszi.nau.edu.ua/novini/386-pro-orhanizatsiyu-osvitnoho-protsesu-u-1-semestri-2025-2026). Також створено Google Classroom, де здобувачі вищої освіти можуть мати доступу до навчальних матеріалів з дисциплін (http://kszi.nau.edu.ua/novini/387-stvoreno-google-classroom-dlya-zdobuvachiv-bakalavratu-ta-mahistratury). Робочі програми кожної навчальної дисципліни містять розділи, що регламентують проведення поточного та підсумкового контролю, його форми, а також критерії їх оцінювання. Здобувачі ВО можуть ознайомитись із робочою програмою навчальної дисципліни на сайті кафедри (http://surl.li/gfeawj).

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

У розділі VII Стандарту для другого (магістерського) рівня вищої освіти зі спеціальності 125 «Кібербезпека» (http://surl.li/jxutqx). Форми атестації здобувачів ВО зазначено, що атестація здійснюється у формі публічного захисту кваліфікаційної роботи. ОПП передбачає атестацію у формі публічного захисту кваліфікаційної роботи (https://surl.li/fneflk, http://surl.li/utqfsi, https://surl.lt/srsmfe, https://surl.li/yagfcl). За всіма вимогами ОПП враховує Стандарт зі спеціальності 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти. Форма атестації здобувачів ВО повністю забезпечує загальні та фахові компетентності зі спеціальності, визначених цим Стандартом. Форми атестації та супутні процедури врегульовуються Положенням про атестацію здобувачів вищої освіти Національного авіаційного університету (http://surl.li/iascde), Положення про кваліфікаційні роботи (проєкти) здобувачів вищої освіти (http://surl.li/tkyzlf). Кваліфікаційні роботи здобувачів денної та заочної форм навчання за ОП оприлюднюються в репозитарії КАІ (https://er.kai.edu.ua/collections/f6acc403-8d5b-411c-ad8d-046701b2bb15).

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/xfvasr); Положенням про атестацію здобувачів вищої освіти (http://surl.li/iascde), в якому регламентується проведення модульних контрольних робіт, диференційованих заліків та екзаменів. Усі чинні положення розташовані на сайті КАІ та є доступними для всіх учасників освітнього процесу (http://surl.li/eisxl). Графік навчального процесу, розклади заліків, екзаменів оприлюднені у відкритому доступі на офіційному веб-сайті факультету у розділі Студентам (https://fcst.nau.edu.ua/) та на сайті кафедри https://surli.cc/llsxce. Робочі програми кожної навчальної дисципліни містять розділи, що регламентують проведення поточного та підсумкового контролю, його форми, а також критерії їх оцінювання. Здобувачі вищої освіти можуть ознайомитись із робочою програмою навчальної дисципліни на сайті кафедри (http://surl.li/gfeawj).

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

У КАІ вироблена чітка процедура комплектування, організації та роботи екзаменаційних комісій, яка зазначена Положенням про організацію освітнього процесу (https://surl.li/xfvasr) та Положенням про атестацію здобувачів вищої освіти (http://surl.li/iascde). Семестровий контроль з навчальної дисципліни проводить лектор, а також бере участь викладач, який проводив практичні (лабораторні) заняття. Під час екзаменаційної сесії перед складанням екзамену викладачі проводять консультації відповідно до затвердженого розкладу консультацій до екзаменів. Проведення екзаменів у КАІ здійснюється в письмовій формі. Усі форми контролю проводяться з дотриманням принципів академічної доброчесності (https://surl.li/fpfutl). З метою моніторингу дотримання учасниками освітнього процесу моральних та правових норм розроблено Декларації про дотримання академічної доброчесності науково-педагогічного працівника та здобувача вищої освіти (https://surl.li/fpfutl). Усі процедури, які стосуються запобігання та врегулювання конфлікту інтересів, здійснюються відповідно до Закону України «Про запобігання корупції». У разі виникнення конфліктів, здобувачі можуть звернутися до куратора групи, декана, президента, Студентського самоврядування (http://surl.li/neojgv), до відділу із з питань запобігання корупції (https://bit.ly/3t8Oppz) та скориставшись Скринькою довіри (https://bit.ly/454Jaog). На ОПП конфлікту інтересів не виникало. Скарг здобувачів ВО на упередженість та 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 відбувається згідно з Положенням про організацію освітнього процесу КАІ (https://surl.li/xfvasr). Ліквідувати академічну заборгованість дозволяється у терміни встановлені наказом президента про організацію освітнього процесу в парних/непарних семестрах. Повторне проходження семестрового контролю з метою ліквідації академічної заборгованості дозволяється лише до початку наступного семестру. Графік ліквідації академічної заборгованості здобувачами ВО, які мають не більше 2-х академічних заборгованостей викладено на сайті кафедри (https://surl.li/ffmpdd).Також здобувачам надається графік проведення консультацій (https://surl.lu/ljyjpo, https://surl.li/pgbyvo, https://surl.li/myqqru).
У разі повторного отримання незадовільної оцінки здобувач має право, за власною заявою, перескладати комісії, склад і термін роботи якої визначає декан факультету на підставі пропозиції кафедри. Головою та членами комісії є завідувач та викладачі кафедри, а також декан, заступники деканів за їх згодою. Також має право бути присутнім представник Студентської Ради. Оцінка, виставлена комісією з ліквідації академічної заборгованості при повторному перескладанні, є остаточною і перегляду не підлягає. Здобувач вищої освіти, який отримав під час ліквідації академічної заборгованості на комісії незадовільну оцінку, відраховується з КАІ за невиконання індивідуального навчального плану.
Прикладів повторного складання іспитів протягом існування ОП не відзначалося.

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

Згідно з Положенням про організацію освітнього процесу КАІ (https://surl.li/xfvasr) здобувач вищої освіти, який не погоджується з виставленою позитивною оцінкою, має право звернутися з письмовою апеляцією до завідувача кафедри не пізніше наступного робочого дня після оголошення результатів екзамену. Завідувач кафедри, екзаменатор з навчальної дисципліни або призначені завідувачем кафедри НПП зобов'язані розглянути апеляцію у присутності здобувача вищої освіти впродовж двох робочих днів та прийняти остаточне рішення. За результатом апеляції оцінка роботи не може бути зменшена, а тільки залишена без зміни або збільшена. Результат розгляду апеляції фіксується на письмовій роботі здобувача вищої освіти і підтверджується підписами завідувача кафедри та науково-педагогічних працівників, які брали участь в проведенні апеляції.
Прикладів перескладання іспитів комісії на ОП не було.

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

У закладі вищої освіти визначено чіткі та зрозумілі політика, стандарти і процедури дотримання академічної доброчесності, яких послідовно дотримуються усі учасники освітнього процесу під час реалізації ОПП. Заклад вищої освіти популяризує академічну доброчесність (насамперед через імплементацію цієї політики у внутрішню культуру якості) та використовує відповідні технологічні рішення як інструменти протидії порушенням академічної доброчесності. Політику, стандарти і процедури дотримання академічної доброчесності містять такі документи КАІ:
1. Кодекс честі науково-педагогічного працівника та Кодекс честі студента, що розміщені на стендах навчальних корпусів університету, а також на сайті (https://bit.ly/3mLaYIy);
2. Положення про виявлення та запобігання академічному плагіату (https://bit.ly/37A4RCE);
3. Порядок перевірки академічних та наукових текстів на плагіат введений в дію наказом ректора від 13.12.2018 № 605/од (https://bit.ly/37A4ZC8);
4. Статут КАІ (https://bit.ly/3uFpOWi);
5. Система академічної доброчесності (https://bit.ly/2ZVbHAL).
В КАІ діє Політика академічної доброчесності https://surl.lt/moafzr
На ОПП передбачена перевірка на плагіат кваліфікаційних робіт, наукових праць здобувачів вищої освіти та викладачів.

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

З 2019 року обов'язковим є перевірка кваліфікаційних робіт здобувачів вищої освіти за допомогою сервісу Unicheck, а з 2024 року через сервіс Strikeplagiarism. Перевірку кваліфікаційних робіт здійснюють відповідальні за

антиплагіат-перевірку на рівні кафедр, результати перевірки опрацьовує Експертна рада кафедри та надає рішення про допуск до захисту. В КАІ постійно ведеться роз'яснювальна робота серед здобувачів та науково-педагогічних працівників щодо академічної доброчесності. В 2024 році підписаний договір про співпрацю з ТОВ «Плагіат», що дозволяє отримувати вільний доступ до сервісу StrikePlagiarism.com (http://surl.li/pwgniu). Система є єдиною в Україні, яка підключена до внутрішніх закритих репозитаріїв університетів (понад 100 млн робіт, з них 3 млн українською) і до баз публікацій (понад 100 млн робіт), індексованих Scopus і Web of Science (https://bit.ly/3manqGG).

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

Академічна доброчесність в КАІ популяризується через постійну роз'яснювальну роботу наставників академічних груп та викладачів кафедри здобувачам ВО під час проведення занять, через пояснення правил запозичення, цитування та надання відповідних посилань. На початку навчального року під час годин корпоративної культури здобувачі ВО ознайомлюються з основними принципами дотримання академічної доброчесності. Здобувачі ВО заповнюють форму Декларації про дотримання академічної доброчесності, яка розміщена на сайті КАІ (https://bit.ly/3hHujJm). Профілактичні заходи протидії академічному плагіату закріплені у п.5 «Положення про виявлення та запобігання академічному плагіату» (https://bit.ly/37A4RCE). Інформація щодо формування академічної доброчесності в студентському середовищі висвітлюється на веб-сайті КАІ(https://bit.ly/3eppv9X) та кафедри (https://surli.cc/cqyoew). У КАІ впроваджений Кодекс честі науково-педагогічного працівника та Кодекс честі студента, що розміщені на сайті КАІ (https://bit.ly/3mLaYIy).
У вересні 2025 року було проведено організаційну зустріч зі здобувачами другого (магістерського) рівня вищої освіти та ознайомлено з питаннями академічної доброчесності (https://surl.li/ddczyj), а також здобувачі підписали у встановленій формі декларації про дотримання академічної доброчесності.

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

Існують такі регулятивні документи щодо виявлення академічної доброчесності (https://bit.ly/2ZVbHAL): Положення про виявлення та запобігання академічному плагіату (https://bit.ly/37A4RCE) та Порядок перевірки академічних та наукових текстів на плагіат (https://bit.ly/37A4ZC8). За порушення академічної доброчесності НПП, здобувачами вищої освіти встановлюється відповідальність відповідно до Закону України «Про вищу освіту». Відповідно до регулятивних документів КАІ факт виявлення плагіату в академічних текстах здобувачів освітнього ступеня «Магістр» призводить до їхньої академічної відповідальності та є підставою для: відмови у присудженні наукового ступеня, забороні враховувати публікації, у яких виявлено академічний плагіат, як опублікований результат кваліфікаційної роботи, повторного проходження оцінювання знань (складання іспиту або заліку, тощо) або відповідного освітнього компонента освітньої програми, відрахування здобувача з університету, позбавлення академічної стипендії або наданих університетом пільг з оплати навчання. Для перевірки академічних та наукових праць на плагіат у КАІ застосовується інформаційна система - StrikePlagiarism. Акти перевірки студентських робіт зберігаються в інформаційній системі та у відділі моніторингу якості вищої освіти.
Випадків недопущення здобувачів до захисту кваліфікаційної роботи внаслідок порушення правил академічної доброчесності на ОПП «Безпека інформаційних і комунікаційних систем» не було.

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

Інформація про НПП, які залучені до реалізації ОП у 2025-2026 н.р. розміщена у базі ЄДЕБО та на сайті кафедри (http://surl.li/auxlaz). Реалізацію ОП у 2025-2026 н.р. забезпечують 7 викладачів, серед яких 3 докторів технічних наук професорів та 3 кандидатів наук, доцентів та 1 кандидат технічних наук. Усі викладачі мають достатній рівень відповідності Ліцензійним умованим провадження освітньої діяльності, а також, академічну кваліфікацію (освіта, профіль наукової діяльності, публікації, підвищення кваліфікації та професійну кваліфікацію), профіль якої відповідає змісту освітніх компонентів, що викладаються.
Перелік викладачів і дисциплін (2025-2026 н.р., спеціальність F5 "Кібербезпека та захист інформації") : ОК3.1 «Методологія прикладних досліджень у сфері кібербезпеки», ОК8.1 «Технології створення та застосування систем захисту кіберпростору»: викладає д.т.н., професор кафедри Ахрамович В. М., який має значний досвід наукової роботи, зокрема в підготовці наукових кадрів. Він є членом спеціалізованої вченої ради та опонентом дисертаційних досліджень претендентів на наукові ступені. ОК4 «Методи побудови та аналізу криптосистем»: викладає гарант ОП, к.т.н., доцент, завідувач кафедри Ільєнко А. В., яка має вагомі наукові та навчально-методичні напрацювання у сфері криптографічного захисту інформації. ОК5 «Моделювання та оптимізація безпекових процесів авіаційної галузі» викладає д.т.н., проф. Міщенко А.В., який має наукові напрацювання за спеціальністю F5 "Кібербезпека та захист інформації" та практичний досвід в авіаційній сфері (2010 - 2024 р.р. - технічний директор КП Міжнародний аеропорт "Київ"(Жуляни). ОК7 «Технології захисту мережевих інфраструктур»: викладає к.т.н. Висоцька О.О., яка має наукові напрацювання та постійно підвищує кваліфікацію у сфері кібербезпеки та захисту інформації. ОК6 «Моніторинг та аудит кібербезпеки": викладає д.т.н., с.н.с., професіонал-практик Лаптєв О.А., який має значні наукові напрацювання, зокрема публікації у фахових виданнях та журналах, що індексуються в наукометричних базах та має практичний досвід у сфері кібербезпеки. Викладацький склад освітньої програми відповідає всім

кваліфікаційним вимогам, визначеним законодавством. Професійний досвід та наукові здобутки викладачів забезпечують якісну підготовку здобувачів вищої освіти та належне викладання освітніх компонентів. Процедури конкурсного добору викладачів є прозорими і дають можливість забезпечити потрібний рівень їхнього професіоналізму для успішної реалізації ОП. Під час конкурсного відбору використовуються такі нормативні документи Порядок проведення конкурсного відбору при заміщенні вакантних посад (https://nau.edu.ua/ua/news/2025/5/23974.html, https://surl.li/akrivg); Положення про підвищення кваліфікації НПП (https://surl.li/zqrrxd), (https://vchenarada.nau.edu.ua/konkurs/zrazki-ta-formi-dokumentiv-dlya-prohodzhennya-konkursu/).

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

При відборі кадрів для забезпечення ОП: враховується особистий досвід роботи НПП за профілем ОП (наявність наукових публікацій та методичних робіт, участь у конференціях, наявність стажувань та підвищення кваліфікацій, наявність практичного досвіду роботи). Необхідний рівень професіоналізму НПП забезпечується таким чином: при первинному проходженні конкурсного добору враховується наявність наукового ступеня та/або вченого звання, підвищення кваліфікації та стажування; при подальшому проходженні конкурсу враховуються конкурсні вимоги відповідно до ЗУ «Про освіту» та Порядок проведення конкурсного відбору при заміщенні вакантних посад (https://surl.li/akrivg). Специфікою конкурсного відбору в КАІ є проведення конкурсною комісією співбесід з кожним кандидатом. До конкурсу/співбесід допускаються кандидати, які виконали умови участі в конкурсі. Унікальною практикою КАІ є залучення до складу конкурсної комісії зовнішніх експертів/практиків з досвідом, що відповідає профілю кафедри. Мета залучення експертів - встановлення рівня актуальності фахової компетенстності викладачів. Прозорість процедури підтверджується відкритим конкурсом, оголошення про який публікується на офіційному сайті КАІ (https://nau.edu.ua/ua/news/2025/5/23974.html) та порталі вакансій robota.ua (https://robota.ua/company2336366). Відсутність обмежень за статтю, віком, релігійними чи політичними переконаннями забезпечує недискримінаційний характер процедури та рівний доступ для всіх кандидатів.

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 залучає роботодавців до реалізації освітнього процесу, використовуючи їхній потенціал для проведення занять, стажування НПП, а також розвиває форми співпраці: спільна робота при розробці та реалізації ОП; рецензування ОП та її періодичний перегляд (ТОВ "СІТОН ДІДЖИТАЛ", ДП Украероруx https://surl.li/vabiad, ТОВ «Алгорітм-Х» http://surl.li/thfzza, Департамент кіберполіції УПК https://surl.li/mchnjq); проходження практик (https://surl.li/crofns, https://surl.gd/qrmdnq, http://surl.li/yfifbc); підвищення кваліфікації НПП (http://surl.li/mlfgwf, http://surl.li/vcenhj, http://surl.li/tfajnx, https://surl.gd/zxdcvk, https://surl.gd/leovly); участь здобувачів у освітніх онлайн-вебінарах (http://surl.li/ncfbdc, http://surl.li/evxeuy).
На кафедрі існує практика залучення до занять за ОПП професіоналів-практиків і представників роботодавців. Наприклад: 06.05.2024 Ризики та проблеми безпеки в глибинних мережах http://surl.li/svlkrf; квітень-травень 2024 року лекції від експертів ІТ-галузі http://surl.li/nnsvyk; 13.09.2024 – Україна у світовій кібервійні https://surli.cc/udhqxr; 24.09.2024 року – Побудова кар'єри: від ЦРУ до засновника стартапу з кібербезпеки http://surl.li/wqhhok; 07.10.2024 Linkos Group http://surl.li/hnubjd; 17.12.2024 – Seeton Group LLC https://surl.li/mfinuq; 22.11.2024 – гостьова Департамент Кіберполіції https://surl.li/luyzly; 20.03.2025, 26.03.2026 - лекції Linkos Group https:/surl.gd/tnxhjx; 24.04.2025 - Ernst & Young https://surl.li/vfkora; 29.09.2025 - IT-specialist https://surl.li/mudsey.

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

Розвиток професійної компетентності викладачів є стратегічним пріоритетом КАІ (розділ 5.3 Стратегії КАІ https://surl.lu/nskcfo). Стимулюючий характер має щорічне рейтингування НПП, кафедр та факультетів https://surl.lu/zxbkts. Процедури підвищення кваліфікації та стажування НПП регламентує «Положення про підвищення кваліфікації НПП та педагогічних працівників НАУ» (http://surl.li/rupzww). НПП мають можливість стажування у рамках програми Erasmus+, Mevlana (https://bit.ly/41lAxEX). НПП мають можливість підвищити кваліфікацію під час стажувань згідно двосторонніх угод про співпрацю (http://surl.li/rsqufy). НПП кафедри приймають активну участь у закордонних конференціях (http://surl.li/rgrytp). Підтвердження виконання підвищення кваліфікації зафіксовано НПП у базі ЄДЕБО та на сайті кафедри (фахове підвищення кваліфікації: https://surl.li/ralxai; https://surli.cc/rwqcot; http://surl.li/hzmnlc; http://surl.li/ppxujd; http://surl.li/tsqtjk; http://surl.li/yjzana; http://surl.li/ngwnul; http://surl.li/vstuvi), Cisco Networking Academy (https://surl.gd/ahoita, https://surli.cc/rgrtom, https://surl.li/evecpx). Також викладачі для розвитку професійної майстерності та softskill приймають участь у курсах-інтенсивах TEACHERS SMART UP (http://surl.li/qekuwu, http://surl.li/hforkl, https://surl.gd/wvgzdp), SoftServe (http://surl.li/wvtdxs, http://surl.li/wljazm), GlobalLogic Україна (http://surl.li/bpwjxq), участь у воркшопах та заходах (https://surl.li/wbqnjm, https://surl.li/kwqcew, https://surl.li/qbayxy, https://surl.li/csyztb).

Наведіть конкретні приклади заохочення розвитку викладацької майстерності

Система заходів стимулювання розвитку викладацької майстерності НПП КАІ передбачає матеріальні та моральні

заохочення і регламентується: Статутом (http://bit.ly/3Xz3ev8); Колективним договором (https://nau.edu.ua/site/variables/news/2024/12/Kolektyvnyi%20dohovir%202024-2025.pdf), Положенням про преміювання працівників КАІ (https://drive.google.com/file/d/1AtiOsFtmMVTsuNsEJtY64WBxMM5l9G0m/view) Також в КАІ діє Положення про порядок надання матеріальної допомоги працівникам КАІ (https://drive.google.com/file/d/1HzSObyT4WEYDIEuzeF1m0SH1fzL-P2XT/view). Система нематеріального заохочення НПП реалізується через нагородження грамотами та подяками від завідувача кафедри, декана факультету, президента університету залежно від внеску у розвиток кафедри та університету, а також через представлення до заохочувальних відзнак МОН. Для стимулювання розвитку викладацької майстерності в КАІ запроваджено: конкурс наукових проєктів для молодих вчених (http://surl.li/hgwvdn); премії та стипендії для молодих учених (http://surl.li/usssmt). З нагоди 90-річчя КАІ (НАУ) відзнаки за вагому роботу та внесок у розвиток університету отримали його працівники (http://surl.li/jlylgt). Ільєнко А.В. стала стипендіаткою стипендії КМУ для молодих вчених (2020-2022), а 15.12.2022 Ільєнко А.В. отримала подяку МОН.

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 дозволяють реалізовувати освітній процес за ОП у т.ч. в умовах дистанційного та змішаного навчання. Інфраструктура об'єднує 12 навчальних корпусів, що включають спеціалізовані лабораторії, обладнані відповідно сучасних вимог до організації освітнього процесу, 12 гуртожитків, Авіаційний медичний центр, профілакторій, ЦКМ, ІОЦ, Навчально-спортивний оздоровчий центр, Науковотехнічну бібліотеку, видавництво https://youtu.be/rnN4z2f0qrE. Наявний бібліотечний фонд за спеціальністю відповідає чинним Ліцензійним умовам і щорічно поповнюється літературою. У бібліотеці організовано доступ здобувачів до каталогів міжнародних наукометричних баз, серед них Web of Science, Scopus, JStor. Навчальні приміщення та лабораторії кафедр укомплектовані необхідним обладнанням, у наявності точки бездротового доступу до мережі Інтернет, в лекційних аудиторіях є мультимедійні проектори. Для забезпечення досягнення ПРН функціонують лабораторії та центри: Навчальний центр «ІТ Академія» та НДЛ протидії кіберзагрозам в авіаційній галузі (https://cyberlab.nau.edu.ua/), а також кіберполігоні Cyber Range UA (https://surl.li/emdkif, http://surl.li/vevapn, http://surl.li/vphylw) та лабораторії AxxonSoft https://surl.li/tisexh. Здобувачі мають вільний доступ до навчально-методичного забезпечення ОПП на сайті кафедри, а саме робочих програм (http://surl.li/yowffl), електронної бібліотеки кафедри (http://surl.li/amwcaz), репозитарію https://surl.li/ihbzws, а також матеріали розміщуються у GoogleClassroom для кожного ОК.

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

Задоволення інтересів та потреб студентства відбувається у різноманітних сферах: професійний, гуманітарний, культурно-творчий розвиток та спортивний напрям, Викладачі та студенти КАІ мають безкоштовний доступ до платфом Udemy https://udemy.com та «Prometheus» http://surl.li/uwbnwa. КАІ має доступ до найбільшої у світі бази даних рефератів та цитування рецензованої літератури Scopus. Наукове товариство студентів, аспірантів, докторантів та молодих вчених НАУ-хаб організує зустрічі з успішними професіоналами https://bit.ly/3Z52gYP. Починаючи з 2015 р. КАІ щороку подає аналітичний звіт з результатами анкетування студентів щодо вивчення стану використання державної мови та оцінки якості навчання https://bit.ly/3lQgrm8. Контроль якості результатів навчання здійснюється на рівнях університету, факультетів і кафедр http://surl.li/neyeue, що дозволяє враховувати думку студентів для забезпечення якості освіти. Кафедрою проводиться опитування здобувачів http://surl.li/neyeue. Також НПП кафедр залучають здобувачів до проведення наукових досліджень http://surl.li/eyjzsn, участь у REX IT FES та JOB EXPO http://surl.li/cjxaes, http://surl.li/ajtkop, у змаганнях з кібербезпеки http://surl.li/tcmtbp, https://surl.li/jruzww, https://surl.li/sltzcw, https://surl.li/vklnfv, відвідування виставки з кібербезпеки http://surl.li/cjfvfn, InfoSec Ukraine 2025 https://surl.li/fnsqpr, SheCyberHub (https://surl.li/hcnyjg) Врахування потреб відбувається завдяки роботі студентського самоврядування, органом якого є Студентська рада.

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

Безпечність освітнього середовища для життя та здоров'я здобувачів забезпечується через інструктажі щодо норм техніки безпеки життєдіяльності, правил поведінки напередодні канікул та свят, правил поведінки в умовах повітряної тривоги (https://surl.li/zaisez). Щорічно в КАІ проводяться навчальні заходи з цивільної оборони та пожежної безпеки, надання домедичної допомоги. Всі здобувачі ознайомлені з Алгоритмом дій за сигналом цивільного захист «Повітряна тривога» (наказ ректора №310/од від 29.08.2023) (http://surl.li/qdzbuc) . Площа укриттів становить 7858,7 м2, що дозволяє одночасно вмістити 13097 осіб, відповідно до норми 0,63 м2 на одну особу. На годинах корпоративної культури проводяться бесіди з профілактики недопущення правопорушень у студентському середовищі, консультації з правил етичного кодексу в КАІ. На кафедрі затверджено план виховної роботи на перше півріччя 2025-2026 н.р. https://surl.lu/cqwhct. Необхідну допомогу за потреби можуть надати професійні психологи-практики КАІ. Функціонують Відділ безпекової діяльності, Авіаційний медичний центр , функціонує кабінет прихолога https://surl.lu/iulzlb , що здійснює організацію, діагностику і тренінгові заняття просвітницької та профілактичної роботи, розробляє заходи щодо профілактики булінгу, а також є відділ взаємодії

зі студентами https://surl.lt/emvqqz. Введено в дію Положення про запобігання та протидію булінгу, мобінгу, кібербулінгу, харасменту в КАІ https://bit.ly/3B86qV5.

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.

Механізми підтримки здобувачів реалізуються через максимальну поінформованість здобувачів за допомогою офіційного сайту КАІ (https://nau.edu.ua/), факультету (https://fcst.nau.edu.ua/), кафедри http://kszi.nau.edu.ua/), Facebook сторінка кафедри з розміщенням всієї актуальної інформації для здобувачів (https://www.facebook.com/profile.php?id=61575738521270), а також посилання на сайти усіх підрозділів університету. Механізми освітньої, організаційної, інформаційної, консультативної та соціальної підтримки здобувачів вищої освіти реалізуються в системі кафедра-факультет-університет. Освітня підтримка сконцентрована в межах кафедри та розподілена за функціями серед НПП, що викладають навчальні дисципліни, гаранта ОП (https://bit.ly/2LpTDri), членів робочої групи ОП, завідувача кафедри. Організаційна підтримка здобувачів освіти реалізується у взаємодії зі структурними підрозділами факультету (деканат, Студентська рада) та університету (навчальні та наукові частини, відділ по роботі зі студентами (http://surl.li/eittx). Інформаційна підтримка забезпечується через офіційні канали розповсюдження інформації – сайт університету, факультету, кафедри, корпоративну пошту КАІ, класи по дисциплінам у Google Suite Classroom (https://surl.li/nmkkzo), репозиторій КАІ (https://er.kai.edu.ua/communities/98276bb8-b6c0-49f8-97e6-55203235ff38), он-лайн бібліотеку КАІ (https://lib.nau.edu.ua/), електронні джерела інформації кафедри (сайт кафедри http://kszi.nau.edu.ua/ та офіційна сторінка Facebook кафедри https://www.facebook.com/profile.php?id=61575738521270). Консультативну підтримку забезпечують наставники академічних груп (http://kszi.nau.edu.ua/vikhovnarobota-menu/nastavniki-akademichnikh-grup), старший наставник кафедри, гарант освітньої програми, завідувач кафедри, декан факультету. Соціальна підтримка реалізується через соціально-гуманітарний напрямок роботи зі студентами: наставник – старший наставник кафедри – старший наставник на факультеті. Зворотній зв'язок зі студентами кафедра має за допомогою опитувань, корпоративної пошти та корпоративних Google-чатів.
Результати опитування здобувачів викладаються на сайті КАІ (http://surl.li/agvaw) та на сайті кафедри (http://surl.li/khocia). На основі аналізу інформації студентських мереж, а також результатів зустрічей зі студентським активом кафедри, опитувань (запроваджених кафедрою та університетом), кафедра обговорю на кафедрі і впроваджує шляхи їх усунення (http://surl.li/lximna).
Також в КАІ діє Положення про винагороду від президента КАІ, яке визначає винагороду для здобувачів КАІ, які мають визначні успіхи та помітні здобутки у всіх сферах діяльності, з метою матеріального та морального заохочення і стимулювання їх відмінного навчання, розвитку наукових та творчих здібностей (https://nau.edu.ua/site/variables/news/2025/2/Polozhennia%20vynahoroda.pdf).

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)

В КАІ створено достатні умови щодо реалізації права на освіту для осіб з особливими освітніми потребами https://nau.edu.ua/ua/menu/quality/inklyuzivna-osvita/ . В КАІ діє Політика рівності, інклюзії та доступності https://surl.li/vxkdig. Для організації безбар'єрного доступу до будівель та приміщень в КАІ затверджено план-графік виконання робіт (http://surl.li/amerk), видано Розпорядження «Про закріплення аудиторій для осіб з особливими освітніми потребами під час освітнього процесу» (http://surl.li/dmxvw). Відповідно до медикосоціальних показань за наявності обмежень життєдіяльності особи, з особливими освітніми потребами, мають право на спеціальний навчально-реабілітаційний супровід і вільний доступ до інфраструктури КАІ, у т.ч. безперешкодний доступ до навчально-методичного забезпечення, бібліотечних ресурсів, наукометричних баз даних, надання їм фахової консультаційної підтримки, а також через належне технічне оснащення аудиторного фонду та гуртожитків. На ОП конкретних прикладів навчання здобувачів з особливими освітніми потребами не було.

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 в КАІ базується на принципах дотримання демократичних цінностей, свободи, справедливості, рівності прав і можливостей, толерантності, недискримінації, відкритості та прозорості. У КАІ застосовуються політика та процедури вирішення конфліктних ситуацій (зокрема пов'язаних із сексуальними домаганнями, дискримінацією та/або корупцією тощо), які є доступними для всіх учасників освітнього процесу та яких послідовно дотримуються тому числі під час реалізації ОП. Вирішення конфліктних ситуацій в КАІ регулюється Положенням про запобігання та протидію булінгу, мобінгу, кібербулінгу, харасменту в НАУ (https://bit.ly/3EWndwT). В КАІ організовано відділ з питань запобігання та виявлення корупції https://bit.ly/3Lmf86M, роботу якого спрямовано на розвиток чесності, добросовісності, прозорості та відкритості надання освітніх послуг. Для розгляду справ пов'язаних з корупцією функціонує Комісія з оцінки корупційних ризиків КАІ https://bit.ly/3HELozP . Повідомити про правопорушення чи написати скаргу можливо на електронну скриньку довіри https://bit.ly/3C4IOkT. За час реалізації ОП випадків конфліктних ситуацій, в тому числі пов'язаних із сексуальними домаганнями, дискримінацією та корупцією, не було.

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 ОПП в КАІ відбувається у відповідності до «Положення про освітні програми» (https://bit.ly/30GU2DO), а також з урахуванням «Положення про гаранта освітньої програми» (https://bit.ly/35rvR4u).

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

Перегляд ОП відбувається в результаті періодичного моніторингу з метою удосконалення як окремих компонент ОП так і всієї програми. Моніторинг здійснюється раз на рік з урахуванням конкурсних показників та результатів навчання (https://surl.li/fdrqle, http://surl.li/tpbtmc, http://surl.li/mijhll). Критеріями, за якими відбувається перегляд ОП, формуються у результаті зворотного зв'язку із НПП, здобувачами ВО і роботодавцями та внаслідок прогнозування розвитку галузі та потреб суспільства. Моніторинг та періодичний перегляд ОП також здійснюється з метою встановлення відповідності їх структури та змісту вимогам законодавчої та нормативної бази, що регулює якість освіти, вимоги ринку праці до якості фахівців, сформованості загальних та фахових компетенцій, освітніх потреб здобувачів вищої освіти. Процедура моніторингу ОП проводиться відповідно до «Положення про освітні програми НАУ» (https://bit.ly/30GU2DO) та процедури забезпеченя якості КАІ https://nau.edu.ua/ua/menu/quality/quality-procedures.html. На основі затвердженого Стандарту зі спеціальності 125 «Кібербезпека» (від 18.03.2021р.), здійснено розробку нової редакції ОПП. Нова редакція затверджена вченою радою та введена наказом ректора від 29.07.2021 №246/од. У 2022 році згідно з наказом т.в.о. ректора від 09.02.2022 № 063/од «Про щорічний перегляд освітньо-професійних програм» був проведений перегляд освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти зі спеціальності 125 «Кібербезпека» (зміни внесені на підставі результатів перегляду освітньої програми відповідно до наказу ректора від 08.06.2022 №154/од). Після щорічного перегляду, проведеного у 2023 році (http://surl.li/mijhll), ОП переведена на спеціальність «Кібербезпека та захист інформації» починаючи з 2023 року вступу та затверджено вченою радою НАУ і введена наказом ректора від 23.02.2023 №069/од.
У 2024 році було розроблено нову редакцію ОП, але реалізація освітнього процесу зо цією редакцією освітньої програми в 2024-2025 році відтермінована у зв'язку з реорганізацією НАУ (http://surl.li/xegqtn, http://surl.li/qxoixe)
У 2025 році було розроблено та погоджено нову редакцію ОП 11.03.2025 (https://surl.li/djeail). 6.02.2025 року було розпочато обговорення проекту ОП «Безпека інформаційних і комунікаційних систем» с пеціальності F5 "Кібербезпека та захист інформації"(https://surl.li/bjumdh). Робота із зацікавленими сторонами відбувалася у кілька етапів: обговорення на засіданнях кафедри (протокол №2 від 28.01.2025, протокол №2/1 від 03.02.2025); засідання круглого столу (27.02.2025, https://surl.li/mkrgih); рецензування програми – отримані письмові рецензії від експертів у галузі кібербезпеки; анкетування здобувачів освіти (https://surl.li/gmmnoj , протокол №4 від 27.02.2025).

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

Здобувачі ВО безпосередньо та через органи студентського самоврядування залучені до процесу періодичного перегляду ОП. Здобувачі входять до складу робочої групи з розроблення ОП. Здобувачі обговорюють ОП на засіданнях Студентської ради (ОП,2025 погоджено Студентською радою факультету протокол № 25/1-п-ФКНТ від 10.03.2025). Здобувачі входять до складу Вченої ради факультету та вченої ради КАІ (НАУ). Здобувачі також беруть участь у процесі перегляду ОП: під час анонімного онлайн-опитування (https://surl.li/plwkqa); - висловлюючи свої пропозиції викладачам та під час зустрічей з кураторами; через студентське самоврядування (https://nau.edu.ua/ua/menu/studentu/sr-nau.html), яке зобов'язане аналізувати та узагальнювати зауваження та пропозиції здобувачів вищої освіти щодо організації освітнього процесу і звертатися до адміністрації з пропозиціями щодо їх вирішення. Залучення здобувачів відбувається безпосередньо та через органи студентського самоврядування: участь в опитуваннях щодо змісту ОП та задоволення якістю викладання, формування пропозицій до переліку вибіркових дисциплін, наприклад здобувачі приймали участь у круглому столі щодо обговорення ОП (https://surl.li/mkrgih, http://surl.li/zjqnqu) та розширених засіданнях кафедри (http://surl.li/zwvnmm) . Опитування відображено за посиланнями (https://surl.li/djeail, http://surl.li/bfwnck) Студенти також можуть взяти участь в публічному обговоренні проєктів ОП (https://surl.li/bjumdh, http://surl.li/saocik, http://surl.li/ljmrgq)

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

Вирішальна роль у процесах функціонування внутрішньої системи забезпечення якості освітньої діяльності (ВСЗЯ) КАІ, належить студентському самоврядуванню (https://nau.edu.ua/ua/menu/studentu/sr-nau.html), діяльність якого впливає на основні освітні, фінансово-господарські та інші процеси КАІ. Залучення здобувачів до участі в усіх видах діяльності ВСЗЯ КАІ дозволяє не тільки отримати сигнали про слабкі або сильні сторони функціонування, а й повною мірою використовувати механізми для найбільш ефективного розкриття внутрішнього потенціалу самих здобувачів.
Студентське самоврядування бере участь у процедурі внутрішнього забезпечення якості ОП та має можливість впливати на процеси реалізації ОП через присутність представників студентства серед членів низки комісій та рад

кафедрального та факультетського рівня: Вчена рада факультету, Науково-технічна рада факультету, засідання випускової кафедри, тощо. Голова студентської ради факультету приймає участь у погодженні ОП та навчальних планів ОП. Здобувачі входять до складу робочої групи з розроблення ОП: - під час опитування; - участь в обговренні ОПП; - через студентське самоврядування, яке зобов'язане аналізувати та узагальнювати зауваження та пропозиції здобувачів щодо організації освітнього процесу і звертатися до адміністрації з пропозиціями щодо їх вирішення. Студенти також можуть взяти участь в публічному обговоренні проєктів освітніх програм на сайті КАІ та кафедри (https://surl.li/bjumdh, http://surl.li/saocik, http://surl.li/ljmrgq)

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 залучені до процесу таким чином: представники стейкхолдерів є членами робочої групи з розробки та перегляду ОП, що зафіксовано в протоколах засіданнях кафедри, ОП та висвітлено на сайті КАІ; під час стажування на підприємствах стейкхолдерів НПП отримують найсучаснішу інформацію і досвід роботи від стейкхолдерів, обговорюють впровадження отриманої інформації в освітній процес; під час практики відбувається зворотній зв'язок із стейкхолдерами-керівниками практики щодо оволодіння компетенціями здобувачами та змісту ОП; під час робочих зустрічей НПП зі стейкхолдерами, обговорюються питання життєвого циклу ОП; відгуки від стейкхолдерів та пропозиції щодо якості ОП висловлюють переважно усно та під час круглих столів процесі обговорення (https://surl.li/rablgv, https://surl.li/pvwhhz). Задля забезпечення якості підготовки здобувачів другого (магістерського) рівня вищої освіти та у рамках підписаних договорів з потенційними роботодавцями (http://kszi.nau.edu.ua/stejkkholderi) студенти мають можливість проходити практику у виробничому середивищі (http://surl.li/bbympv, https://surl.lu/ouptrf) та приймати участь у освітніх онлайн-вебінарах у рамках проєкту проєкту USAID «Кібербезпека критично важливої інфраструктури України» (http://surl.li/ubezob). Приклади залучення роботодавців до перегляду ОП http://surl.li/tgjipf, http://surl.li/zcmhyd, http://surl.li/rjctea, http://surl.li/ifszia.

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'єрного шляху та траєкторій працевлаштування випускників ОП здійснюється в межах факультету та кафедри: пошук та надання інформації про вакансії, організація зустрічей зі потенційними-роботодавцями (наприклад , участь у кар'єрному онлайн фестивалі REX IT FEST (http://surl.li/cjxaes), консультації щодо напрямів діяльності та вимог компаній-працедавців; підготовка інформаційних матеріалів та участь в організації заходів університету, спрямованих на працевлаштування випускників). За підтримки Інституту неперервної освіти (http://surl.li/hnwvol) щорічно в КАІ проводяться заходи: «Час авіаційної кар'єри», «Злітна смуга», «Ярмарок вакансій», «День кар'єри», «Освіта та кар'єра 20 ХХ» та ін., де випускники можуть отримати інформацію від роботодавців щодо вакансій, а КАІ визначається з реальними потребами ринку праці. Щодо відслідковування кар'єрного шляху та траєкторій працевлаштування випускників ОП існують механізми збирання та врахування інформації: випускники заповнюють анкети, вказують інформацію про працевлаштування, а також пропозиції та зауваження; збирання інформації про випускників через керівників їх кваліфікаційних робіт та кураторів. Спілкування з випускниками та відображення їх досягнень на сайті кафедри у розділі «Наші випускники» (http://surl.li/xebrjy). Ведеться постійний збір інформації щодо працевлаштування випускників шляхом анкетування за встановленою формою (https://surl.li/axwyfh).

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

Внутрішня система забезпечення якості в КАІ реалізується через виконання наступних процедур (https://bit.ly/3kDEmzU): розроблення стратегії забезпечення якості освітньої діяльності та вищої освіти; організації системи забезпечення якості освітньої діяльності та вищої освіти; перегляду ОП з визначеною періодичністю та постійним моніторингом; формування системи відповідальності всіх структурних підрозділів та співробітників за забезпечення якості; залучення здобувачів вищої освіти до забезпечення якості; щорічного оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті, на інформаційних стендах; забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників; забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи здобувачів вищої освіти, за кожною ОП; забезпечення наявності інформаційних систем для ефективного управління освітнім процесом; забезпечення публічності інформації про освітні програми, ступені вищої освіти та кваліфікації; забезпечення дотримання академічної доброчесності працівниками та здобувачами вищої освіти, у тому числі створення і забезпечення функціонування ефективної системи запобігання та виявлення академічного плагіату; втілення політики в сфері якості, її моніторингу та перегляду. Процедури внутрішнього забезпечення якості здійснюються на підставі Документованої процедури «Порядок проведення внутрішніх аудитів якості освітньої діяльності» https://bit.ly/3B6cTzG .
21 березня 2024 року кафедра кібербезпеки (на той час кафедра комп'ютеризованих систем захисту інформації), де реалізовувалась дана ОП, успішно пройшла внутрішній аудит, що відбувався згідно наказу ректора від 12.09.2023 №334/од (http://surl.li/tmyvrr).

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 враховані під час удосконалення цієї ОП?

За результатами акредитації ОП у вересні 2018 року було отримано сертифікат про акредитацію за другим (магістерським) рівнем вищої освіти (http://surl.li/nbzjyh). З урахуванням наданих рекомендацій здійснені наступні заходи:
1. Посилені вимоги до професійної активності викладачів. Результати наукової та професійної активності викладачів впродовж останніх 5 років (http://surl.li/xczsjg, http://surl.li/yiuesd).
2. В процесі перегляду ОП кожного року роботодавці та здобувачі освіти залучались до її обговорення (https://surli.cc/qcoflm, http://surl.li/uwxnmp), (http://surl.li/cjjzvs), (http://surl.li/eqzsor).
4. Розширено коло співпраці з партнерами кафедри, а саме заключено нові угоди для проведення практик та підвищення кваліфікації НПП (http://kszi.nau.edu.ua/stejkkholderi)
5. Проводилося анкетування здобувачів освіти (http://surl.li/ozkjur).

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

В академічній спільноті закладу вищої освіти сформована культура якості, яка сприяє постійному розвитку освітньої програми та освітньої діяльності за цією програмою (https://bit.ly/3s1LXwc). Серед учасників академічної спільноти проводяться опитування, що стосуються проблем забезпечення якості освіти в КАІ та за ОП (http://kszi.nau.edu.ua/osvitnij-protses/anketuvannya-zdobuvachiv). Укладаються договори з підприємствами – базами практик (http://kszi.nau.edu.ua/stejkkholderi). Здобувачі вищої освіти регулярно ознайомлюються з організацією виробничих процесів в компаніях потенційних роботодавців та проводяться організаційні зустрічі щодо проведення виробничих практик для студентів спеціальності F5 "Кібербезпека та захист інформації" (https://surl.li/qtbjes). На кафедрі нарощується база даних установ, підприємств, організацій – потенційних роботодавців. Засідання кафедр та Вчених рад факультетів та КАІ присвячуються питанням якості ОП та процедурам її забезпечення. Системно проводиться робота щодо ознайомлення учасників академічної спільноти з новими тенденціями у цьому напрямі. З метою формування загальної культури якості освітнього процесу в університеті створено Раду з якості КАІ (https://bit.ly/38p2jHz, https://surl.li/ykteyq) як колегіального дорадчого органу, який координує діяльність підрозділів університету, спрямованого на забезпечення ефективного функціонування та удосконалення внутрішньої системи забезпечення якості вищої освіти та освітньої діяльності.

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

Формування культури якості освіти в КАІ– це комплексний процес, який охоплює всі аспекти діяльності та передбачає активну участь викладачів, студентів, адміністрації. Відповідно до Положення про систему забезпечення якості вищої освіти та освітньої діяльності (surl.li/ooxzol) організація внутрішнього забезпечення якості вищої освіти в КАІ здійснюється на п’яти рівнях. На першому рівні здійснюються соціологічні опитування здобувачів вищої освіти. Другий рівень організації системи внутрішнього забезпечення якості вищої освіти в КАІ здійснюється викладачами кафедри при безпосередньому керівництві гаранта освітньої програми та завідувача кафедри. Третій рівень організації системи внутрішнього забезпечення якості вищої освіти у КАІ реалізується на факультеті під безпосереднім керівництвом декана. На четвертому рівні системи внутрішнього забезпечення якості вищої освіти у КАІ структурними підрозділами університету, відділом моніторингу якості вищої освіти та Радою з якості університету здійснюються процедури і заходи, які свідчать про дотримання вимог до забезпечення якості вищої освіти (https://nau.edu.ua/ua/menu/quality/rada-z-yakosti/). На п’ятому рівні системи внутрішнього забезпечення якості вищої освіти в КАІ діяльність наглядової ради, вченої ради, президента спрямовані на постійне покращення здатності університету виконувати вимоги усіх зацікавлених сторін до якості вищої освіти на основі результатів вивчення задоволеності її якістю випускників КАІ та роботодавців.

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?

В КАІ чітко прописані правила і процедури, що регулюють права і обов’язки всіх учасників освітнього процесу, розміщені у відкритому доступі: Статут університету (https://bit.ly/3lCt4Bo); Стратегія КАІ (https://surl.lt/egueer); Колективний договір (https://surl.li/zrbwuy); Правила внутрішнього трудового розпорядку (https://bit.ly/3rGLqBP); Положення про організацію освітнього процесу (https://surl.li/cqfhsn); Положення про виявлення та запобігання академічному плагіату (https://bit.ly/3gu1OPG); Положення про атестацію здобувачів вищої освіти (https://surl.li/vtbumh); Положення про кваліфікаційні роботи (проєкти) здобувачів вищої освіти (https://surl.li/qfasvx); Положення про запобігання та протидію булінгу, мобінгу, харасменту (https://surl.lu/imwobe) тощо. В КАІ діє Положення про комісію з питань етики та врегулювання скарг https://surl.li/txpfem

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

Посилання на веб-сторінку ЗВО з проєктами нормативних документів (https://nau.edu.ua/ua/menu/quality/proekti/proekti-normativnih-dokumentiv.html, https://nau.edu.ua/ua/menu/quality/proekti/), освітніх програм (https://nau.edu.ua/ua/menu/quality/proekti/proekti-

osvitno-profesiynih-program/) та перегляд ОПП на сайті кафедри (https://surl.li/jagfce, http://surl.li/zmaakd)

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 КАІ своєчасно оприлюднено інформацію щодо освітньо-професійну програму «Безпека інформаційниїх і комунікаційних систем» (https://bit.ly/3Kh9STH) та сайті кафедри кібербезпеки (http://surl.li/rbmudd). Також на офіційному сайті КАІ розміщена вкладка «Забезпечення якості освіти», яку в свою чергу розділено на Проєкти нормативних документів (https://cutt.ly/2RDT4OO) та Проєкти освітньо-професійних програм (https://cutt.ly/QRDT2IT), На сайті кафедри присутня інформація щодо навчальних планів (http://surl.li/nyazhb), робочі програми (http://surl.li/ndhvaz). На кожного викладача створено окрему сторінку, де відображена вся інформація про НПП (http://surl.li/oupwyz).

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП?

Сильні сторони: ОП реалізується в КАІ, який є провідним галузевим закладом вищої освіти країни, що дає підстави для проведення перспективних міждисциплінарних досліджень відповідно до актуальних запитів вітчизняного і світового ринків; собливістю ОП є реалізація моделі підготовки фахівців в сфері безпеки інформаційних і комунікаційних систем з урахуванням потреб ІТ ринку, а також авіаційної галузі України.У ОП немає аналогів серед ЗВО України щодо врахування галузевого контексту функціонування авіаційного сектору. Постійно здійснюється щорічний перегляд ОП, а саме здійснюється актуалізація складу стейкхолдерів з метою підкрекреслення унікальності освітньої програми та залучення здобувачів до перегляду ОП. Регулярно, щорічно проводиться анкетування здобувачів вищої освіти. На кафедрі створено базу випускників з метою збирання інформації щодо кар'єрного шляху випускників та розширено бази потенційних роботодавців, а інформацію про успішних випускників розміщено на веб-сторінці кафедри. Кафедра має високий рівень виконання кваліфікаційних робіт: усі роботи містять актуальну тематику, практичну цінність, готовий програмний продукт/модуль; результати робіт апробовані у наукових виданнях та конференціях.
Налагоджена робота зі стейкхолдерами: укладені угоди про співпрацю, стажування викладачів відбувається на базі стейкхолдерів, студенти проходять виробничу практику на базі стейкхолдерів, з подальшим працевлаштуванням; здійснюється професійна підготовка за програмами академії Cisco; на постійній основі здійснюється залучення здобувачів та провідних науково-педгогічних працівників до участі у вебінарах від проєкту USAID. Налагоджена система кадрового забезпечення: у 2019 р. на кафедрі захищено одну кандидатську дисертацію (Висоцька О. О.) та у 2022 р. захист дисертаційної роботи на здобуття ступеня доктора філософії зі спеціальності 122 - Комп'ютерні науки (Галата Л. П.),
У 2024-205 н.р. здобувачі третього (освітньо-наукового) рівня ВО Педченко Є.М. та Петляк Н.С. захистили дисертації на здобуття ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 125 – Кібербезпека (https://surl.li/xolbax , https://surl.li/mgibci).
У 2023 р. доцент Висоцька О. О. отримали сертифікат про володіння іноземною мовою на рівні В2; викладачі кафедри мають наукові публікації, у тому числі у виданнях, що входять до світових наукометричних баз Scopus, Web of Science та ін. із залучення студентів до участі в міжнародних науково-технічних конференціях., досвід практичної діяльності за фахом тощо. Постійно оновлюється електронна бібліотека кафедри на сайті кафедри з вільним доступом здобувачів вищої освіти.
Слабкі сторони ОП: 1) відсутність програм подвійних дипломів і дуальної освіти; 2) в умовах воєнного стану належного поширення серед здобувачів вищої освіти та НПП не отримала практика академічної мобільності.

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

До перспектив розвитку освітньої програми «Безпека інформаційних і комунікаційних систем» упродовж найближчих трьох років слід віднести:
1) Поглиблення співпраці з роботодавцями та галузевими партнерами — залучення до довготривалої взаємодії провідних фахівців ІТ-компаній і підприємств, розширення бази роботодавців для забезпечення якісної практичної підготовки здобувачів, організації стажувань науково-педагогічних працівників, а також подальший розвиток партнерств із підприємствами авіаційної галузі для посилення авіаційної складової освітньої програми.
2) Розвиток міжнародного співробітництва та академічної мобільності — активізація участі здобувачів і викладачів у програмах академічної мобільності, зокрема Erasmus+, Horizon Europe, налагодження співпраці з європейськими закладами вищої освіти, створення спільних навчальних курсів і програм подвійних дипломів.
3) Розширення практичної складової навчання та впровадження елементів дуальної освіти — розвиток взаємодії зі стейкхолдерами й потенційними роботодавцями, розширення можливостей для проходження виробничих практик, виконання реальних виробничих завдань, а також корегування тем курсових і кваліфікаційних робіт відповідно до актуальних потреб галузі.

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:

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	*РП Ділова іноземна мова.pdf*	uH1vwDko6zAy5331Z2dQzvnltgJPJeZ5Jir16iSldVw=	*Мультимедійний комплекс(ноутбук, проектор, екран), доступ до мережі інтернет. Програмне забезпечення: ліценз. Google GSuite for Education (Google Classroom, Google Meet, Google форми / документи / таблиці / презентації).*
Наукові комунікації у фаховій діяльності	навчальна дисципліна	*РП_Наук комунікації у фаховій діяльності.pdf*	baccs8uUXvK7FNoiUIu4CvVmfVabnd6Nw5WEJH1LXVM=	*Мультимедійний комплекс(ноутбук, проектор, екран), доступ до мережі інтернет. Програмне забезпечення: ліценз. Google GSuite for Education (Google Classroom, Google Meet, Google форми / документи / таблиці / презентації).*
Методологія прикладних досліджень у сфері кібербезпеки	навчальна дисципліна	*РП_Методологія прикладних досліджень у сфері КБ.pdf*	2eZdLnLpZJs007onLmxI72R18I1w4VrPTndaKyV3Qdc=	*Мультимедійний комплекс(ноутбук, проектор, екран), доступ до мережі інтернет. Програмне забезпечення: ліценз. Google GSuite for Education (Google Classroom, Google Meet, Google форми / документи / таблиці / презентації).*
Курсовий проєкт з дисципліни Методологія прикладних досліджень у сфері кібербезпеки	курсова робота (проект)	*КП_Методологія прикладних досліджень у сфері кібербезпеки.pdf*	A8zQwIfchpMVQOj6aZBX9vldQ0RwHJQZQ7N//Hy1S50=	*Мультимедійний комплекс(ноутбук, проектор, екран), доступ до мережі інтернет. Програмне забезпечення: ліценз. Google GSuite for Education (Google Classroom, Google Meet, Google форми / документи / таблиці / презентації).*
Методи побудови та аналізу криптосистем	навчальна дисципліна	*РП_Методи побудови та АКС.pdf*	q//cYiWJGVoMoL+HSbyQEOEYQShJz/qlPiKB4p+aWos=	*Мультимедійний комплекс(ноутбук, проектор, екран), доступ до мережі інтернет. Програмне забезпечення: ліценз. Google GSuite for Education (Google Classroom, Google Meet, Google форми / документи / таблиці / презентації). Криптографічний пакет OpenSSL, Microsoft Visual Studio Community Edition.*
Моделювання та оптимізація безпекових процесів авіаційної галузі	навчальна дисципліна	*РП_Моделювання_та_оптимізація_безпекових-процесів.pdf*	V7xB2XuYgL8rikBWjFQt849bIthou/bjKgu2D9W6C8o=	*Мультимедійний комплекс(ноутбук, проектор, екран), доступ до мережі інтернет. Програмне забезпечення: ліценз. Google GSuite for Education (Google Classroom, Google Meet, Google форми / документи / таблиці / презентації). Криптографічний пакет OpenSSL, Microsoft Visual Studio Community Edition. Спеціалізоване МТЗ: Скануючий приймач «IC-R6» - 1 шт.; Скануючий приймач «AR-5000» - 1 шт.; Скануючий приймач «AR-8600» - 1 шт.; Пошуковий комплекс «Digi Scan Labs» - 1 шт.; Пошуковий комплекс ST-031 «Піранья» - 1 шт.; Нелінійний радіолокатор «NR-μ» - 1 шт.; Біометричний контролер доступу «Seven C-771» - 1 шт.; Генератор «SRC-300A» (багатофункціональний засіб блокування мобільних пристроїв) – 1 шт.; Мікрофон направленої дії «Супер вухо - 100» - 1 шт.; АТС «PEEINTN» - 1 шт.; IP-шифратор «CryptoIP-448» - 2 шт.; Навчальний стенд дослідження охоронних систем 1- шт.; ППК ОП «Дунай» 16/32 – 3 шт.; Ретрополятор «Дунай Р-1000» - 1 шт.; ПК «Satel» - 1 шт.; ППК «ВБД 6-12» - 1 шт.; Навчальний комплект охоронної системи INTEGRA 64 WSR – 1 шт.; Навчальний стенд дослідження систем відеоспостереження -1 шт.; Програматор комплексу відеонагляду – 1 шт.; Пульт керування системою відеонагляду Panasonik CN161 – 1 шт.; Камера Panasonik WV-CW960 – 1 шт.Комутатор 3COM – 1 шт.; Комутатор SRW208P – 1 шт.; Комутатор VM-42 – 1 шт.; Зчитувач даних SAGEM MA 520 – 1 шт.; Пристрій цифрового запису відеоданих WY HD220 – 1 шт. ; Аналого-цифровий перетворювач B480 – 2 шт.; DSP камера відеонагляду з кронштейном – 1 шт.; Камера NVL-5500 – 1 шт.; Камера NVC-180BH – 1 шт.; Камера Panasonik WV-CF294 – 1 шт.; Камера Samsung SNC-B2315P – 1 шт.; Камера WyY N-202 – 1 шт.; Монітор виведення даних LD2000/6 – 1 шт.; Екран TS180 – 1 шт.*
Моніторинг та аудит кібербезпеки	навчальна дисципліна	*РП_Моніторинг та аудит КБ.pdf*	GIGmMShJT1AwWAH/bYg8OLClDJj+cXCGyq63DMHgq90=	*Мультимедійний комплекс(ноутбук, проектор, екран), доступ до мережі інтернет. Програмне забезпечення: ліценз. Google GSuite for Education (Google*

				Classroom, Google Meet, Google форми / документи / таблиці / презентації).
Захист комунікаційних мереж засобами Cisco	навчальна дисципліна	*РП_Захист комунікац мереж засобами CISCO.pdf*	iZcoAx4FJ+0099djQUEEpYIub9WglUplzwlszJQShKw=	*Мультимедійний комплекс(ноутбук, проектор, екран), доступ до мережі інтернет. Програмне забезпечення: ліценз. Google GSuite for Education (Google Classroom, Google Meet, Google форми / документи / таблиці / презентації). Пропрієтарне ліцензоване програмне забезпечення - емулятор «Cisco Packet Tracer».*
Технології створення та застосування систем захисту кіберпростору	навчальна дисципліна	*РП_Технології створення та застосування систем захисту КБ.pdf*	pHlbk8DmVHqQMsdmWm0pAP064eWYOLFxOFDlmSIVxr0=	*Мультимедійний комплекс(ноутбук, проектор, екран), доступ до мережі інтернет. Програмне забезпечення: ліценз. Google GSuite for Education (Google Classroom, Google Meet, Google форми / документи / таблиці / презентації).*
Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	курсова робота (проект)	*КР_Технології створення та застосування систем захисту кіберпростору.pdf*	fr4EU/pLQSK71UKYOBQ9vdTmMrzgK8TsX6WHAYoWF+w=	*Мультимедійний комплекс(ноутбук, проектор, екран), доступ до мережі інтернет. Програмне забезпечення: ліценз. Google GSuite for Education (Google Classroom, Google Meet, Google форми / документи / таблиці / презентації).*
Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	практика	*РП_Науково-дослідна практика (актуалізована).pdf*	5je80iJUBNJyojmMw1zumC55rWiaYFb+EZalwoBuLl8=	*В залежності від бази практики*
Переддипломна практика	практика	*РП_Переддипломна практика (актуалізована).pdf*	tuSANOT26C3iUmgoSn8zT6LQil7BQdVTuSo3AbpS2gQ=	*В залежності від бази практики та від теми кваліфікаційної роботи*
Кваліфікаційна робота	підсумкова атестація	*Положення_про_кваліфікаційні_роботи_НАУ_2024.pdf*	gdnPqqxyW5Dr5jdNT/fbwURm83i8kmmpg/hMLrTBv1g=	*Залежно від теми кваліфікаційної роботи*

* 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

ID 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)
496067	Теремінко Лариса Григорівна	Доцент, Основне місце роботи	Факультет психології, комунікацій та перекладу	Диплом спеціаліста, Київський 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	24	Ділова іноземна мова	Освіта: 1. Київський державний педагогічний інститут іноземних мов, 1993 р., спеціальність «Іноземні мови (дві мови)», кваліфікація «Вчитель англійської та німецької мов» диплом КЖ № 011998, виданий 26 червня 1993 р. 2. Кандидат педагогічних наук, спеціальність 13.00.04 – теорія і методика професійної освіти, диплом ДК № 059227, виданий 09.02.2021. Тема дисертації: «Формування готовності до професійної мобільності майбутніх фахівців з інженерії програмного забезпечення». 3. Атестат доцента АД № 011738, виданий 23.12.2022, доцент кафедри іноземних мов за фахом. Підвищення кваліфікації: Підвищення кваліфікації: Куявський університет, м. Влоцлавек (Республіка Польща). Тема: Актуальні зміни та інновації у підготовці сучасних філологів (в обсязі 180 годин) з 06.09.2021 - 17.10.2021. Сертифікат № FSI-61730-KSW від 17.10.2021р. Українсько-Польський вищий навчальний заклад «Центрально-Європейський університет», м. Київ. Тема: Сучасні тенденції та інновації в іншомовній підготовці фахівців у

							закладах вищої освіти (в обсязі 180 годин) з 07.10.2024 - 07.12.2024. Довідка № 535 від 09.12.2024р. Асоціація інноваційної та цифрової освіти. Тема: Штучний інтелект в освіті (в обсязі 15 годин). Сертифікат № 17871773 від 02.12.2024р. Види і результати професійної діяльності: п.1 1. Гурська О.О., Теремінко Л.Г., Акмалдінова В.Є. Інтеграція загальнопрофесійної та іншомовної підготовки як основа формування професійно важливих якостей майбутніх ІТ-фахівців у закладі вищої технічної освіти. Вісник Національного авіаційного університету. Серія: Педагогіка. Психологія: зб. наук. праць. К.: НАУ, 2021. Вип. 1(18). С. 37-48. (Index Copernicus International) 2. Hurska O.O., Tereminko L.H., Denysenko N.H. Developing higher education content teachers' ESP competence. Інноваційна педагогіка. 2024. Вип. 70. Т.2 С. 118-121. (Index Copernicus International) 3. Гурська, О. О., Білоус, Н. П., Теремінко, Л. Г. Переклад архаїзмів історичного роману «Айвенго» .Актуальні питання гуманітарних наук: міжвузівський зб. наук. праць молодих вчених Дрогобицького державного педагогічного університету імені Івана Франка. Дрогобич: ВД «Гельветика», 2021. Вип. 38. Том 1. С. 104-109. (Index Copernicus International). 4. Гурська, О. О., Білоус, Н. П., Теремінко, Л. Г. Переклад історизмів роману В. Скотта "Айвенго". Науковий вісник Міжнародного гуманітарного університету. Серія: Філологія : наук. зб. Одеса: ВД «Гельветика», 2021. №49. Том 2. С. 139-142. (Index Copernicus International). 5. Білоус Н.П., Подсєвак К.С., Теремінко Л.Г. Історично маркована лексика роману В. Скотта "Айвенго" як засіб історичної стилізації художнього тексту. Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Філологія. Журналістика. Одеса: ВД "Гельветика", 2021. Том 32 (71). №3. Ч.2. С. 7-11. (Index Copernicus International) 6. Bobrytska, V. I, Luzik, E. V., Skyrda, T. S., Tereminko, L. H., Hurska, O. O. (2021). Fostering Tertiary Student Professional Mobility Skills via Convergence of the Professional Mobility and Foreign Language Learning. European Journal of Educational Research, 10 (4), 1919–1936. (Scopus). 7. Теремінко Л.Г. Аналіз досвіду професійної підготовки українських ІТ-фахівців в умовах війни. Інноваційна педагогіка. 2025. Вип. 80. Т. 2 С. 103–107 (Index Copernicus

							International). 8. 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. e025016 (Web of Science). п.3 1. Акмалдінова О.М., Гурська О.О., Теремінко Л.Г., Денисенко Н.Г., Сорокун Г.В., Professional English. Applied Mathematics: навчальний посібник для здобувачів вищої освіти ОС «Бакалавр» спеціальності 113 «Прикладна математика». К.: НАУ, 2023. 96 с. (1,2 авт.арк. на автора). 2. Акмалдінова О.М., Гурська О.О., Теремінко Л.Г., Сорокун Г.В., Professional English. Cybersecurity and Data Protection: навчальний посібник для здобувачів вищої освіти ОС «Бакалавр» спеціальності 125 «Кібербезпека та захист інформації». К.: КАІ, 2025. 96 с. (1,5 авт.арк. на автора). п.4 1. 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». К.: НАУ, 2022. 32 с. 2. Marketing: Term Paper Method Guide for higher education seekers of bachelor`s degree specialty 075 "Marketing" / O. Polous, I. Mykhalchenko, L. Tereminko. K.: NAU, 2022. 48 p. 3. Гурська, О. О., Білоус, Н.П., Теремінко, Л.Г. Business English. Методичні рекомендації до виконання контроль¬них робіт для здобувачів вищої освіти ОС «Магістр» заочної форми навчання ІТ-спеціальностей. К.: НАУ, 2023. 40 с." п.5 Кандидат педагогічних наук наук, 2021, 13.00.04 – теорія і методика професійної освіти. Тема "Формування готовності до професійної мобільності майбутніх фахівців з інженерії програмного забезпечення"" п.12 1. Гурська, О. О., Теремінко, Л. Г. Сучасні тенденції в підготовці майбутніх філологів. Current Changes and Innovations in Training Modern Philologists: abstracts of the Internship Proceedings. (Wloclawek, 6 September – 17 October 2021.). P. 28–31. 2. 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). P. 397–401.
3. Гурська, О. О., Теремінко, Л. Г., Будко, Л. В. (2023). Формування англомовної компетентності майбутніх авіаційних фахівців у цифровому освітньому середовищі закладів вищої освіти. АВІА-2023: матеріали XVI Міжнар. наук.-техн. конф., м. Київ, Україна, 18-20 квітня 2023 р. С. 34.13-34.17
4. 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. С. 303-306.
5. Теремінко Л.Г. Англійська мова професійного спрямування як засіб формування готовності до професійної мобільності майбутніх ІТ-фахівців : Лінгвістичні та методологічні аспекти викладання іноземних мов професійного спрямування : матер. доп. ІІІ міжнар. наук.-практ. конф., м. Київ, 31 березня 2021 р. Київ, 2021. С. 51–53.
6. Теремінко Л.Г. Додатки та сервіси як ефективний засіб вивчення іноземної мови : Лінгвістичні та методологічні аспекти викладання іноземних мов професійного спрямування : матер. доп. ІV міжнар. наук.-практ. конф., м. Київ, 29–30 березня 2023 р. Київ, 2023. С. 49–50.
7. 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: тези доповіді.
8. 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: тези доповіді.
9. 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.
10. Yevtushenko A., Teremінko L. Cybersecurity in the context of cyber resilience: Ukrainian experience. Кібербезпека в транскордонному співробітництві: матеріали Міжнародної науково-практичної конференції, м. Берегове, Україна, 15–16 жовтня 2024 р. С. 32-33:

							тези доповіді. 11. Теремінко Л., Ярош А., Євтушенко А.: Сучасні практики у сфері кібербезпеки. Кібербезпека в транскордонному співробітництві: матеріали Міжнародної науково-практичної конференції, м. Берегове, Україна, 15–16 жовтня 2024 р. С. 48-49: тези доповіді. 12. Tererеminko L.H. Analysing the research on future aviation industry specialists' foreign language training. Авіа-2025: матеріали XVII Міжнародної науково-технічної конференції, м. Київ, Україна, 22-24 квітня 2025 р. С. 32.12–32.16: тези доповіді. 13. Теремінко Л.Г. Професійна підготовка ІТ фахівців в умовах війни: педагогічно-порівняльний аспект. Психолого-педагогічний супровід професійного розвитку суб'єктів педагогічної освіти і освіти дорослих у сучасних реаліях України: матеріали звітної науково-практичної конференції Інституту педагогічної освіти і освіти дорослих імені Івана Зязюна НАПН України за 2024 рік, м. Київ, Україна, 22-24 квітня 2025 р.: тези доповіді.
494468	Ахрамович Володимир Миколайович	Професор, Основне місце роботи	Факультет комп'ютерних наук та технологій	Диплом спеціаліста, Київський ордена 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	Технології створення та застосування систем захисту кіберпростору	Освіта: 1. Київський політехнічний інститут, 1980 р. спеціальність - Технологія машинобудування, металорізальні верстати та інструменти, кваліфікація – Інженер – механік. 2. Доктор технічних наук, 05.13.21 – Системи захисту інформації (диплом доктора наук ДД № 011778 від 29.06.2021), тема дисертації - «Методологічні основи забезпечення захисту інформації в соціальних мережах». 3. Професор кафедри кібербезпеки (атестат професора АП №004630 від 23.12.2022) Підвищення кваліфікації: 1. Доктор технічних наук, 05.13.21 – Системи захисту інформації, тема дисертації «Методологічні основи забезпечення захисту інформації в соціальних мережах». Диплом доктора наук ДД № 011778, виданий 29.06.2021 р. 2.International Historical Biographical Institute (Dubai-New York-Rome-Jerusalem-Beljing)lJ. Тема «Підвищення кваліфікації: Studying Exerience and Professional Achivements for Forming a Successful Personality and Transforming of the World». Термін 18.02.2022-23.04.2022рр. Сертифікат (6 кредитів ЄКТС). Види і результати професійної діяльності: п.1 1.Akhramovych V., Pepa Y., Zahynei1 A., Akhramovych V.,Dzyuba T., Danylov I. Method for calculating the information security indicator in social media with considerationof the path durationbetween clients.

							Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska" – IAPGOS. 2024. Volume № 14. №1. pp. 71-77. Scopus. ISSN: 2083-0157. DOI: https://doi.org/10.35784/iapgos.5720. 2.Akhramovych V., Lehominova S., Stefurak O., Akhramovych V., Chuprun S., 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, №.6, pp.1-19, 2024. DOI: https://doi.org/10.5815/ijcnis.2024.06.01. Scopus. Q1. ISSN: 2074-9090. 3.Akhramovych V., Shuklin G., Pepa Y., Muzhanova T., Zozuli S. Devising a procedure to determine the level of informational space security in social networks considering interrelations among users. Східно-Європейський ЖУРНАЛ передових технологій. Харків. 2022 № 1/9 (115). pp. 63-74. URL: https://journals.uran.ua/eejet/article/view/252135 DOI: https://doi.org/10.15587/1729-4061.2022.252135. Scopus, Q2. ISSN: 1729-3774. 4.Khrashchevskyi R., Klobukov V., Kozlovskyi V., Akhramovych V., Lazarenko S. Method of calculating information protection from mutual influence of users in social networks. International Journal of Computer Network and Information Security (IJCNIS). 2023. Vol. 15, № 5. pp. 27-40. DOI: https://doi.org/10.5815/ijcnis.2023.05.03. Scopus, Q1. ISSN: 2074-9090. 5.Ахрамович В., Ахрамович В. Кількісна оцінка ймовірності функціонування системи захисту без протиправних дій. Кібербезпека та захист критичної інфраструктури. 2024. Том. 12. №. 2 (23) pp. 257-267. DOI: https://doi.org/10.20535/2411-1031.2024.12.2.315745. ISSN: 2411-1031. п.5 Доктор технічних наук, 05.13.21 – Системи захисту інформації, тема дисертації «Методологічні основи забезпечення захисту інформації в соціальних мережах». ДД № 011778, виданий 29.06.2021 р. п.7 1. Член разової спеціалізованої ради ДФ 26.861.008 при захисті дисертації на здобуття наукового ступеня доктор філософії Бржевської Зореслави Михайлівна – «Методика оцінки достовірності інформації в умовах інформаційного протиборства». 2021 р. 2. Опонент при захисті дисертації на здобуття наукового ступеня доктор філософії Урденко Олександра Георгійовича «Моделювання та управління інформаційною безпекою підприємства в умовах цифрової трансформації» 2021р. 3. Член разової спеціалізованої ради при

							захисті дисертації на здобуття наукового ступеня доктор філософії Марченка Віталія Вікторовича «Метод виявлення шкідливих процесів в інформаційній системі підприємства на основі ідентифікації та діагностування станів логічних об'єктів»». 2023 р. 4. 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 інфрастуктури держави», ДСК. 2024 р. 5. . Відгук на автореферат дисертації "Методи забезпечення резильєнтності організаційно-технічних систем" Коробейнікова Федора Олександровича, представленої на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації» 2024р. 6. Член разової спеціалізованої ради при захисті дисертації на здобуття наукового ступеня доктор філософії Педченка Євгена Максимовича – «Методи та моделі оцінювання стану кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури». 2025 р. (https://vchenarada.nau.edu.ua/2025/05/02/spetsializovana-vchena-rada-z-pravom-prijnyattya-do-rozglyadu-ta-provedennya-zahistu-disertatsiyi-pedchenka-yevgena-maksimovicha-na-zdobuttya-stupenya-doktora-filosofiyi-z-galuzi-znan-12-informatsijni/) 7. Член спеціалізованої ради Д.26.062.01. Державного університету ""Київський авіаційни інститут"" (https://mon.gov.ua/npa/pro-zatverdzhennia-rishen-atestatsiinoi-kolehii-ministerstva) п.12 12) наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п'яти публікацій: 1. Vitalii Savchenko, Volodymyr Akhramovych, Taras Dzyuba, Serhii Laptiev, Nataliia. Lukova-Chuiko, Tetiana Laptieva. Methodology for Calculating Information Protection from Parameters of its Distribution in Social Networks. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT). Conference Proceedings. December 15-16, 2021. Kyiv, Ukraine. Pp. 99-105. http://atit.ieee.org.ua/wp-content/uploads/2021/12/Program-ATIT-2021-02-14.12.21.pdf 2. Vitalii Savchenko, Volodymyr Akhramovych, Oleksander Matsko, Ivan Havryliuk Method of Calculation of Information

							Protection from Clusterization Ratio in Social Networks. Proceedings of the 3rd International Conference on Information Security and Information Technologies (ISecIT 2021) co-located with 1st International Forum "Digital Reality" (DRForum 2021) Odesa, Ukraine, September 13-19, 2021.-pp. 24-31. (Scopus). 3. Volodymyr Akhramovych, Vadym Akhramovych, Viktor Ivankin, Oleh Stefaruk. Detection of black holes in the manet network // Science and society: modern trends in a changing world. Proceedings of the 5th International scientific and practical conference. MDPC Publishing. Vienna, Austria. 2024. Pp. 136-143. 4. Volodymyr Akhramovych, Vadym Akhramovych, Roman Prydybailo, Serhiy Chuprun. Methods of detecting DOS attacks. // European congress of scientific achievements. Proceedings of the 4th International scientific and practical conference. Barca Academy Publishing. Barcelona, Spain. 2024. Pp. 155-161. 5. Volodymyr Akhramovych, Vadym Akhramovych, Viktor Ivankin. Wireless network attacks which are permanent infrastructures are dynamic in nature // Perspectives of contemporary science: theory and practice. Proceedings of the 3rd International scientific and practical conference. SPC "Sci-conf.com.ua". Lviv, Ukraine. 2024. Pp. 398-404.
495965	Приходько Оксана Юріївна	Доцент, Основне місце роботи	Факультет психології, комунікацій та перекладу	Диплом спеціаліста, Рівненський державний педагогічний інститут, рік закінчення: 1995, спеціальність: Українська мова та література, Диплом кандидата наук ДК 009794, виданий 17.01.2001, Атестат доцента 02ДЦ 000102, виданий 24.12.2003	16	Наукові комунікації у фаховій діяльності	Освіта: Рівненський державний педагогічний інститут, 1995 рік, кваліфікація спеціаліста «Учитель української мови та літератури», диплом з відзнакою КН № 900140 від 16 червня 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: 2020 – Університет менеджменту освіти НАПН України, «Організація дистанційного навчання у закладах освіти», 7 кредитів ЄКТС (210 год.), СП 35830447/1065-20 2022 – Clarivate. Тема «Research Smarter: Огляд літератури на відмінно». 2024 – Одеський національний університет імені І. І. Мечникова, «Штучний інтелект та академічна доброчесність у соціогуманітарній освіті та науці», 6 кредитів ЄКТС (180 год.), № 15-57-2024, 2025 – Державна установа «Український інститут розвитку освіти», "Експертиза навчальної літератури", 0,5 кредитів ЄКТС (15 год.), Серійний номер сертифікату 831ae6d5dcbd412cb76d242a822c39bf Види і результати професійної діяльності:

							п. 1. Публікації у періодичних наукових фахових виданнях України категорії Б: 1. 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 2. 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://jrnl.nau.edu.ua/index.php/VisnikPP/article/view/17604 3. 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. Публікації у виданнях, що входить до наукометричної бази Web of Science, Scopus) 1. 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/thwyjs35 (видання індексовано в наукометричній базі «Scopus»). 2. 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://ceur-ws.org/Vol-4024/ https://ceur-ws.org/Vol-4024/paper21.pdf (видання індексовано в наукометричній базі «Web of Sciences»). 3. Kotkova L., Prykhodko O.,

							Lytvynska S., Tsyhanok H., Lushchyk 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 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 5. 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 6. 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 П. 3 1. Академічна доброчесність 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. 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-Татліоґлу 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.Савчук Н., Приходько О. Літературне краєзнавство: науково-дослідницька робота : навчально-методичний посібник по роботі з обдарованою молоддю. Рівне: ВСП «РЕТФК НУВГП», 2023. 58 с. П.4 1. Наукові комунікації у фаховій діяльності: практикум / уклад.: С. В. Литвинська, О. Ю. Приходько, С. І. Черіпко. – К. : ДНП «ДУ КАІ», 2025. – 52 с. 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. Приходько О. Ю., Воробйова Л. М. Методичні рекомендації до виконання та захисту науково-дослідницьких проєктів із зарубіжної літератури. Рівне: РМАНУМ, 2023. 62 с. П.9 Член експертної групи з української мови (Наказ МОН № 1636 від 20.11.2024) П.12 1. Приходько О. За покликом просвітянського серця. Слово просвіти: всеукраїнський культурологічний тижневик. Вип. 5 (1288), 6 — 12 лютого 2025. С. 9. 2. Приходько О. «Лісова пісня» в модерному стилі. Слово просвіти: всеукраїнський культурологічний тижневик. Вип. 15 (1298), 17 — 23 квітня 2025. С. 15. 3. Приходько О. Штучний інтелект у дискурсі академічної доброчесності 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. 4. Приходько О., Бровінська Л. Терміни і професіоналізми в мовленні ІТ-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. Кокарєва та ін.]; Державний університет «Київський авіаційний інститут». – К.: КАІ, 2025. С. 187–189. URL: https://drive.google.com/file/d/12uMjVNIcGbdKHWCNPLQlGCHDNlFe5FNG/view 5. 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/ 6. 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. 7. 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. 8. 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 9. Приходько О. Пам'яті скарбничого просвітянського духу. Слово просвіти: всеукраїнський культурологічний тижневик. Вип. 47-48 (1232), 23 листопада – 6 грудня, 2023. С. 13. URL: 10. 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, 02червня 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 11. 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 12. 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. Кокарєва 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 13. Prykhodko Oksana. Genre specifity 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.ayasofyakongresi.com/_files/ugd/4ec152_5f99ee52ca70497ca83e952cf31d7b6d.pdf 14. Приходько О. Ю. Науково-дослідницька робота учня-члена МАН в умовах цифровізації освітнього простору. Збірник наукових праць «Актуальні проблеми в системі освіти: загальноосвітній заклад середньої освіти – доуніверситетська підготовка – заклад вищої освіти». Київ : НАУ, 2021. Вип. 1. С. 208–211. URL: https://jrnl.nau.edu.ua/index.php/APSE/article/view/15867 15. Приходько О. «На полі крові» Лесі Українки: сценічне втілення у Рівному. Слово просвіти. Вип. 11 (1115), 18-24 березня, 2021. С. 8. URL: http://slovoprosvity.org/2021/03/29/na-poli-krovi-lesi-ukrainky-stsenichne-vtilennia-v-rivnomu/ 16. Приходько О. Аристократ духу або Добрий геній української книги. Слово просвіти. Вип. 46-47 (1150-1151), 18-30 листопада, 2021. С. 13. URL: http://slovoprosvity.org/wp-content/uploads/2021/11/46-47-1150-1151-18-30-lystopada-2021.pdf П.14 Керівник постійно діючого студентського наукового гуртка «Актуальні проблеми наукової комунікації» П.15 1. Робота у складі журі (заступник голови журі) фінального (ІІІ) 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 Член громадської організації «Київське обласне об'єднання Всеукраїнського товариства «Просвіта» імені Тараса Шевченка», членський квиток № К 02078 від 07.07.2024 Член громадської організації «Рівненське обласне об'єднання ВУТ «Просвіта» ім. Тараса

							Шевченка», членський квиток № РВ 02458 від 09.03.2021
494563	Лаптєв Олександр Анатолійович	Професор, Сумісництво	Факультет комп'ютерних наук та технологій	Диплом спеціаліста, Київське вище військове авіаційне інженерне училище, рік закінчення: 1986, спеціальність: Авіаційне обладнання, Диплом доктора наук ДД 010230, виданий 24.09.2020, Диплом кандидата наук ДК 013189, виданий 13.02.2002, Атестат старшого наукового співробітника (старшого дослідника) АС 004851, виданий 15.12.2005	6	Моніторинг та аудит кібербезпеки	Освіта: 1. Київське вище військове авіаційне училище 1986р., спеціальність - інженер-електрик, кваліфікація - інженер по авіаційному обладнанню. 2. Науковий ступінь: Доктор технічних наук 05.13.21 - Системи захситу інформації, тема дисертації: Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації. Диплом ДД №010230, від 29 вересня 2020 року 3. Атестат старшого наукового співробітника (старшого дослідника) АС 004851, виданий 15.12.2005 Підвищення кваліфікації: 1. Курси підвищення кваліфікації за програмою USADI-« Advanced Malware», з 11 червня 2022 р. по 31 серпня 2022 р., в обсязі 6 кредітів-180 годин. 2. Участь у науково-практичному семінарі «Сучасні інформаційні технології в освіті та наукових дослідженнях» Документи: СертифікатN° АСN°120-82 з 25 травня по 10 червня 2022 р., (в обсязі 108 годин). 3. Участі у науково-практичному семінарі «Цифрові технології в освітніх та наукових дослідженнях СертифікатN° N°55/2023 з 31 травня по 13 червня 2022 р., (в обсязі 108 годин). 4. Стажування у Державному науково-дослідному інституті кібербезпеки та захисту інформації, з 22.01.2024 р. по 05.04.2024р., в Види і результати професійної діяльності: п.1 1. Laptiev, O.,Sobchuk, V.,Subach, I.,Barabash, A.,Salanda, I. The Method of Detecting Radio Signals Using the Approximation of Spectral Function. CEUR Workshop Proceedings, 2022, 3384, pp. 52–61. 0,7 ум.друк.арк./власний внесок 0,15 авторських аркушів, 2. Valentyn Sobchuk , Iryna Zelenska and Oleksandr Laptiev. Algorithm for solution of systems of singularly perturbed differential equations with a differential turning point. Bulletin of the Polish Academy of Sciences Technical Sciences, Vol.71, No 3, 2023, Article number: e145682 . DOI: 10.24425/bpasts.2023.145682 WoS. Scopus. 0,9 ум.друк.арк. /власний внесок 0,25 авторських аркушів, 3. Barabash, O., Sobchuk, V., Musienko, A., Laptiev, O., Bohomia, V., Kopytko, S. (2023). System Analysis and Method of Ensuring Functional Sustainability of the Information System of a Critical Infrastructure Object. In: Zgurovsky, M., Pankratova, N. (eds) System Analysis and Artificial

							Intelligence . Studies in Computational Intelligence, vol 1107. P. 177-192, Springer, Cham. https://doi.org/10.1007/978-3-031-37450-0_11 1,1 ум.друк.арк./власний внесок 0,25 авторських аркушів. 4. Valentyn Sobchuk, Iryna Zelenska and Oleksandr Laptiev. Algorithm for solution of systems of singularly perturbed differential equations with a differential turning point. Bulletin of the Polish Academy of Sciences Technical Sciences, Vol.71, No 3, 2023, Article number: e145682 https://doi.org/10.24425/bpasts.2023.145682 WoS 5. Serhii Yevseiev & Yuliia Khokhlachova & Serhii Ostapov & Oleksandr Laptiev et al, 2023. ""Models of socio-cyber-physical systems security,"" Monographs, PC TECHNOLOGY CENTER, number 978-617-7319-72-5.redif, December. DOI: https://doi.org/10.15587/978-617-7319-72-5 https://www.scopus.com/record/display.uri?eid=2-s2.0-85180372745&origin=resultslist 6. Barabash, O., Sobchuk, V., Musienko, A., Laptiev, O., Bohomia, V., Kopytko, S. System Analysis and Method of Ensuring Functional Sustainability of the Information System of a Critical Infrastructure Object. In: Zgurovsky, M., Pankratova, N. (eds) System Analysis and Artificial Intelligence . Studies in Computational Intelligence. 2023. vol 1107. P.177-192, Springer, Cham. DOI: https://doi.org/10.1007/978-3-031-37450-0_11 7. Boryseiko, O.; Laptiev, O.; Perehuda, O.; Ryzhov, A. Optimizing Energy Conversion in a Piezo Disk Using a Controlled Supply of Electrical Load. Axioms. 2023. Volume12, Issue 12, 1074. DOI: https://doi.org/10.3390/axioms12121074 Q1 8. Barabash O., Sobchuk V., Sobchuk A., Musienko A., & Laptiev O. Algorithms for synthesis of functionally stable wireless sensor network. Advanced Information Systems. 2025. 9(1), P. 70–79. https://doi.org/10.20998/2522-9052.2025.1.08" п.2 1. Реєстраційний номер заявки u 2025 01071 дата 13/03/2025 Погасій С.С., Лаптєв О.А., Меленті Є.О. Голдобін С.М., Грунович В.О., назва Багатофункціональний пристрій детонації. 2. Реєстраційний номер заявки u 2025 01070 дата 13/03/2025 Погасій С.С., Лаптєв О.А., Меленті Є.О. Голдобін С.М., Грунович В.О., назва Універсальна автономна роботизована мобільна платформа подвійного призначення. 3. Реєстраційний номер заявки u 2025 02351 дата 20/05/2025 Погасій С.С., Лаптєв О.А., Меленті Є.О. Голдобін С.М., Грунович В.О., назва Комплекс для

							керованої передачі короткочасного імпульсу радіосигналу п.3 1. Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov and others/ Synergy of building cybersecurity systems. Kharkiv. Publisher PC TECHNOLOGY CENTER. 2021 – 188 с. 18,8 ум.друк.арк./власний внесок 3,3 авторських аркушів. ISBN 978-617-7319-31-2 (on-line). ISBN 978-617-7319-32-9 (print). DOI: https://doi.org/10.15587/978-617-7319-31-2 https://monograph.com.ua/pctc/catalog/book/64 https://commons.wikimedia.org/wiki/File:SYNERGY_OF_BUILDING_CYBERSECURITY_SYSTEMS.pdf 2. Лаптєв О.А., Кузавков В.В., Хорошко В.О. Підручник «Системи пошуку засобів негласного зняття акустичної інформації» – К. Міленіум. 2023 – 282 с. https://www.researchgate.net/publication/368925556_SISTEMI_POSUKU_ZASOBIV_NEGLASNOGO_ZDOBUTTA_AKUSTICNOI_INFORMACII 3.Пазковскі Т., Собчук В., Лаптєв О. Кібербезпека: глосарій- Львів-Новий Світ-2000, 2024.- 244 с. ISBN 978-966-418-456-1 УДК 005.336.2:004.72.56.52(045) https://www.researchgate.net/publication/382564216_Kiberbezpeka_glosarij 4.Лаптєв О.А., Хорошко В.О. Виявлення, локалізація та обробка сигналів засобів негласного знімання інформації.-К. Міленіум, 2024.- 350 с. ISBN 978-966-8063-82-3 УДК 004.056.53:534.4 https://www.researchgate.net/publication/384598539_Viavlennalokalizacia_ta_obrobka_signaliv_zasobiv_neglasnogo_otrimanna_movnoi_informacii" п.4 1.Laptiev O., Savchenko V., Shuklin G., Stefurak O. Detection and blocking of means of illegal obtaining of information at objects of information activity.Kyiv/ SUT. 2020. – p.125 http://www.dut.edu.ua/uploads/l_2034_30494170.pdf. Власний внесок 3,36 авторських аркушів. 2.Лаптєв О.А., Савченко В.А., Шуклін Г.В. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності. К. ДУТ. 2020– 126 с. http://www.dut.edu.ua/uploads/l_2031_50136601.pdf. Власний внесок 3,36 авторських аркушів 3. Лаптєв О.А., Наконечний В.С., Толюпа С.В., Сайко В.Г., Щебланін Ю.М. Методичні вказівки до лабораторних робіт з дисципліни «Програмні методи захисту інформації» – Київ, 2022. 86 с. 4. Програмно-апаратне забезпечення та захист мобільних пристроїв : методичні вказівки до лабораторних робіт

							[Електронний ресурс] / укладачі О. А. Лаптєв, Т. О. Гришанович, Я. В. Жолоб, О. К. Жигаревич. ВНУ ім. Лесі Українки. Електронні текстові дані (1 файл: 859 КБ). Луцьк : ВНУ ім. Лесі Українки, 2022. 99 с. URI: https://evnuir.vnu.edu.ua/handle/123456789/21574 5. Наконечний В.С., Толюпа С.В., Сайко В.Г., Лаптєв О.А., Щебланін Ю.М., Фесенко А.О. Методичні вказівки до лабораторних робіт з дисципліни «Технології забезпечення кібербезпеки» – Київ, 2023. 148 с. 6. Методичні вказівки до лабораторних робіт з дисципліни ""Комплексні системи захисту інформації""[Електронний ресурс] : для студентів спец. 125 ""Кібербезпека та захист інформації""/ уклад.: О. А. Лаптєв [та ін.] ;; Нац. техн. ун-т ""Харків. політехн. ін-т"". – Електрон. текст. дані. – Харків, 2023. – 105 с. – URI: http://repository.kpi.kharkov.ua/handle/KhPI-Press/63875. 7. Браіловський М.М., Лаптєв О.А., Наконечний В.С., Ткач Ю.М., Хорошко В.О. «Нормативно-правове забезпечення інформаційної безпеки». Методичні рекомендації до виконання практичних робіт для здобувачів освітнього ступеня «Бакалавр» спеціальності 125 «Кібербезпека та захист інформації»: КНУТШ, 2024.– 59 с. 8. Лаптєв О.А.,Наконечний В.С.,Толюпа С.В.,Браіловський М.М.,Щебланін Ю.М.Методичні вказівки до лабораторних робіт «Безпека критичної інформаційної інфраструктури» К: КНУ імені Тараса Шевченка, 2024 -195 с." п. 5 Доктор технічних наук, 05.13.21. Системи захисту інформації, тема дисертації: Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації. Диплом ДД №010230, Міністерство освіти і науки України, від 29 вересня 2020 року п.6 Ахрамович Володимир Миколайович, доктор технічних наук,05.13.21- Системи захисту інформації, тема дисертації: Методологічні основи захисту інформації у соціальних мережах, ДД №011778, Міністерство освіти і науки України, від 29 червня 2021 року п.7 1.СРД 26.861.06; по захисту дисертацій на здобуття наукового ступеня доктора (кандидата) технічних наук за спеціальностями: 21.05.01 – Інформаційна безпека держави (технічні науки); 05.13.21 – Системи захисту інформації (технічні науки). 2. СРД 64.052.01; по захисту дисертацій на здобуття наукового ступеня доктора

							(кандидата) технічних наук за спеціальностями: 05.13.21 – Системи захисту інформації (технічні науки). 05.13.05 – Комп'ютерні системи та компоненти." п.8 Член редакційної колегії: 1.Наукового журналу Students Magazine on Computing and Communications (SMCC) http://pubs.ressi.id/index.php/SMCC/about/editorialTeam 2.Наукового журналу : «Сучасний захист інформації» https://journals.dut.edu.ua/index.php/dataprotect/about/editorialTeam 3.Наукового журналу : «Безпека інформаційних систем і технологій» https://ists.knu.ua//about 4. Наукового журналу «Прикладні проблеми комп'ютерних наук, безпеки та математики» https://apcssm.vnu.edu.ua/index.php/Journalone/about/editorialTeam" п.12 1. Oleksandr Laptiev, Serhii Yevseiev, Andrii Trystan, Valerii Chystov, Olha Matiushchenko and Iryna Zakharchenko. Solving the Problem of Convergence of the Results of Analog Signals Conversion in the Process of Aircraft Control. 2022 IEEE Third International Conference on System Analysis & Intelligent Computing (SAIC), 04-07 Oktober, Kyiv, Ukraine. p. 118-124. 2. Oleksiy Kapustyan,Valentyn Sobchuk,Taras Yusypiv, Oleksandr Laptiev; Irina Shestak; Kateryna Zinchenko. Robust Stability of Limit Regimes in Distributed Signal Transmission RD Systems.2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), 15-17 December 2022, Kyiv, Ukraine, 2022. pp.168 – 172 DOI: 10.1109/ATIT58178.2022.10024228 https://ieeexplore.ieee.org/document/10024228 3. Oleksandr Laptiev, Andrii Musienko, Volodymyr Nakonechnyi, Andrii Sobchuk, Sergii Gakhov, Serhii Kopytko. Algorithm for Recognition of Network Traffic Anomalies Based on Artificial Intelligence. 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications. June 8-10, 2023, Ankara, Turkey. DOI: 10.1109/HORA58378.2023.10156702 Scopus. https://www.scopus.com/record/display.uri?eid=2-s2.0-85165707546&origin=resultslist&sort=plf-f 4. V. Sobchuk, O. Laptiev, I. Tsyganivska and V. Zhuravlev. Application of Finite Partially Ordered Sets in the Determination of Production Chain Planning Strategy. 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). October 26-28, Ankara, Turkiye, 2023, pp. 1-6 DOI: 10.1109/ISMSIT58785.2023.1

							0304945. 5. Oleksandr Laptiev, Vitalii Savchenko, Alla Kobozieva, Anatolii Salii Development of a method for detecting deviations in the nature of traffic from the elements of the communication network. VIII Міжнародна науково-практична конференція. «Проблеми кібербезпеки інформаційно-комунікаційних систем», м. Київ, 11 квітня 2025 року.КНУ імені Тараса Шевченка. С.111-117. 6. Bobok Ivan, Kobozieva Alla, Laptiev Oleksandr, Speranskyy Viktor. A Universal Method of Digital Content Integrity Expertise 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications, ICHORA 2025. Ankara 23-24 May 2025, Code 209351 http://doi.org/10.1109/ICHORA65333.2025.11017283" п.19 Асоційований член «Східноєвропейсого наукового товариства» .Посвідчення ES 0007 від 03.03.2021р https://clarity-project.info/edr/43181535 п.20 Технічний директор ЗАО ХК «Бліц Інформ» з 2004 по 2018 рр.
494547	Міщенко Андрій Віталійович	Професор, Основне місце роботи	Факультет комп'ютерних наук та технологій	Диплом спеціаліста, Київське вище військове авіаційне інженерне училище, рік закінчення: 1989, 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, Атестат доцента 02ДЦ 014434, виданий 16.06.2005, Атестат професора АП 000463, виданий 05.07.2018	15	Моделювання та оптимізація безпекових процесів авіаційної галузі	Освіта: 1. Київське вище військове авіаційне-інженерне училище, 1989 р., спеціальність – «Авіаційне обладнання літальних апаратів», 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 діяльнвстю», диплом магістра КВ № 3563604 від 28.02.2009 р. 4. Доктор технічних наук, 21.05.01 – «Інформаційна безпека держави», тема дисертації – «Методологічні та організаційно-технічні основи забезпечення інформаційної безпеки авіатранспортного комплексу України». 5. Професор кафедри засобів захисту інформації (атестат - АП № 000463 від 05.07.2018). 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). Види і результати професійної діяльності: п.1 1. Міщенко А.В., Курило О.В., Золотухіна О.А. Нечітка модель оцінки ризиків інформаційної безпеки та підтримки рівня захищеності ERP-систем. Телекомунікаційні та інформаційні технології. К.:ДУТ. 2020. № 1 (66). С.142-151 (Категорія В). 2. 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 Б). 3. 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 Б). 4. 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]. 5. Міщенко А.В., Іщенко Н.Ф., Ліщиновська Н.О., Скрипник Л.Р. Безпека держави в енергонезалежності об'єктів критичної інфраструктури. Наука і техніка сьогодні. 2023. №.2(16) С. 401-416. doi: 10.52058/2786-6025-2023-2(16)-401-415 [in Ukrainian]. https://doi.org/10.52058/2786-6025-2023-2(16)-401-415 [Google Scholar]. 6. 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). 7. 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 Б). 8. Корченко, О. Г., Козловський, В. В., Міщенко, А. В., & Терейковський, О. І. (2025). ВИЗНАЧЕННЯ ФУНКЦІОНАЛЬНИХ ВИМОГ ДО МУЛЬТИМОДАЛЬНОЇ СИСТЕМИ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ ПЕРСОНАЛУ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ З ВИКОРИСТАННЯМ UML-ДІАГРАМ ПРЕЦЕДЕНТІВ. Сучасний захист інформації, (2), 68-75. (Категорія Б). п.3 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. (6 авторських аркушів) п.7 Член спеціалізованої ради Д.26.062.01 Державного університету "Київський авіаційний інститут" (https://mon.gov.ua/npa/pro-zatverdzhennia-rishen-atestatsiinoi-kolehii-ministerstva) п.12 1. Mishchenko A. Criteria for evaluating the effectiveness of the decision support system / Kozlovskiy V., Mishchenko A. // Strategy of Quality in Industry and Education: XIII International Conference, June 5-8, 2020.: Proceed. of the Conf. – Varna, Bulgaria, 2020. – Vol. 1. – P. 343-351. 2. 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. 3. 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. 4. 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).

							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).
494533	Ільєнко Анна Вадимівна	Завідувач кафедри, Основне місце роботи	Факультет комп'ютерних наук та технологій	Диплом 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 12ДЦ 042200, виданий 28.04.2015	15	Методи побудови та аналізу криптосистем	Освіта: 1. Національний авіаційний університет, 2009 р., спеціальність – «Захист інформації в комп'ютерних системах та мережах», кваліфікація – «науковий співробітник (безпека підприємств, установ та організацій)» 2. Кандидат технічних наук, 05.13.21 – Системи захисту інформації, тема дисертації «Методи підвищення ефективності захищених інформаційно-комунікаційних систем на основі ідентифікації кодових конструкцій». 3.Доцент кафедри комп'ютеризованих систем захисту інформації (атестат - 12ДЦ № 042200 від 28.04.2015 р.) Підвищення кваліфікації: 1. Літня школа 2025 у рамках проєкту Еразмус+ модуль Жан Моне «Європейський досвід для підвищення стійкості критично важливих об'єктів в Україні». Термін 21 липня-08 серпня 2025 р.. Сертифікат (4 кредита ЄКТС). 2. 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). 3. ТОВ «АЛГОРІТМ-Х». Термін 15.10.2020р. - 15.12.2020 р. Тема - «Сучасні підходи щодо побудови систем захисту інформаційних мереж». Звіт про стажування (180 годин/6 кредитів ЄКТС). 4. Softserve. Тема «Підвищення кваліфікації: Вдосконалення викладання у вищій освіті: інституційний та індивідуальний виміри». Термін 22.12.2022р. Сертифікат (0,067 кредита ЄКТС). 5. Sigma Software University. Тема «Практичні кейси проєктного навчання, створення e-learning курсу». Термін 28.01.2023р. Сертифікат (1 кредит ЄКТС). 5. Проєкт Еразмус+ №: 101085825 - ERASMUS-JMO-2022-MODULE. Тема «Європейський досвід для підвищення стійкості критично важливих об'єктів в Україні». Термін 25.04.2023р. Сертифікат (0,05 кредита ЄКТС). 6. EPAM та IT Ukraine Association. Тема: «Teachers Internship: Deep Dive into AWS (Amazon Web Services)». Термін липень 2023р. Сертифікат (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 (0,067 кредита ЄКТС). 9. GlobalLogic Education. Тема «IT-інструменти для викладачів». Термін липень-серпень 2023 р. Сертифікат (0,6 кредита ЄКТС) 10.SoftServe. Тема «Tech Summer Bootcamp for Teachers -2023». Термін липень-серпень 2023 р. Сертифікат (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 (3 кредита ЄКТС). 12. Sigma Software University. Sigma Software University: Teachers Smart Up: Winter Edition 3.0 2024 / Тренди в IT. Термін: 22-26 січня 2024 Сертифікат (1 кредит ЄКТС) Види і результати професійної діяльності: п.1 1. Ільєнко А.В. Сучасний стан забезпечення кібернетичної безпеки цивільної авіації України та світу / А.В. Ільєнко, С.С. Ільєнко, Д.С. Кваша//Кібербезпека: освіта, наука, техніка. – 2020. – Т.5 № 9. – С. 24-36. (фахове видання категорії В) 2. Anna Ilyenko, Sergii Ilyenko, Svitlana Kazmirchuk, Olena Prokopenko and Yana Mazur, The Improvement of Digital Signature Algorithm Based on Elliptic Curve Cryptography, Advances in Intelligent Systems and Computing. – Volume 1247. – 6 August 2020. – pp.327-337. Available at: https://link.springer.com/chapter/10.1007/978-3-030-55506-1_30. (Scopus) 3. Anna Ilyenko, Sergii Ilyenko, Svitlana Kazmirchuk, Yakovenko Olesya, Marharyta Herasymenko and Maksim Iavich, Improved Gentry's Fully Homomorphic Encryption Scheme: Design, Implementation and Performance Evaluation, CEUR Workshop Proceedings (Proceedings of the International Workshop on Cyber Hygiene co-located with 1st International Conference on Cyber Hygiene and Conflict Management in Global Information Networks). –Volume 2654. – 19 August 2020. – pp.72-83. Available at: http://ceur-ws.org/Vol-2654/ (Scopus) 4. Anna Ilyenko A Biometric Asymmetric Cryptosystem Software Module Based On Convolutional Neural Networks / Anna Ilyeko, Sergii Ilyenko, Marharyta Herasymenko// International

							Journal of Computer Network and Information Security. – V. 13, №6. – 2021. – P. 1-12. (Scopus) 5. Ільєнко А.В. Програмний модуль відслідковування помилок у високонавантажених веб-додатках на базі використання авторського алгоритму логеру / С.С.Ільєнко, Д.С.Сташевський // Кібербезпека: освіта, наука, техніка. – 2021. – Т.3 (№ 11). – С. 61-72. (фахове видання категорії В) 6. 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) 7. 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) 8. 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) 9. 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) 10. 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) 11. Ільєнко А.В.. Програмний модуль автентифікації з використанням удосконаленої схеми Меркле-Демґарда /А.В.Ільєнко, Л.П., Галата, М.М.Арєшков, О.В.Дубчак // Безпека інформації, 2024. – Р.399 – 406. (https://doi.org/10.18372/2225-5036.30.20361) 12. Ільєнко А.В. Системний підхід до безпеки вебдодатків: аналіз загроз та методи кіберзахисту / А.В.Ільєнко, Л.П., Галата, Д.Спис, О.В.Дубчак// Захист інформації, 2024. - С. 277-293 (https://doi.org/10.18372/2410-7840.26.20022) 13. Гулак, Н., Ільєнко, А., & Дубчак, О. (2025). ПРАКТИЧНІ АСПЕКТИ

							ВИКОРИСТАННЯ КРИПТОГРАФІЧНИХ МЕТОДІВ ДЛЯ ЗАХИСТУ БАЗ ДАНИХ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(28), 246–258. https://doi.org/10.28925/2663-4023.2025.28.786 п.2 1. Пат. 146770 Україна, МПК G09C 1/00,H04K 1/00. Спосіб гомоморфної процедури шифрування та дешифрування інформації на основі використання додаткових параметрів/ Ільєнко С.С., Ільєнко А.В.: заявник та патентовласник Нац. авіац. ун-т. – № u202005681; Заявл. 03.09.2020; Опубл. 18.03.2021, Бюл. № 11. – 4 с. 2. Пат.149227 Україна, МПК G09C 1/00,H04K 1/00. Спосіб автентифікації на основі використання еліптичних кривих/ Ільєнко С.С., Ільєнко А.В.: заявник та патентовласник Нац. авіац. ун-т. – № u202102943; Заявл. 01.06.2021; Опубл. 28.10.2021, Бюл. № 43. – 3 с. п.3 1. Методи та засоби забезпечення резервування авіоніки : монографія / В. П. Захарченко, С. В. Єнчев, С. С. Ільєнко, С. С. Товкач, А. В. Ільєнко; ред.: В. М. Воробйов; Національний авіаційний університет// монографія. – К.: НАУ, 2020. – 276 с. (Ільєнко А.В. - 1,5 автор. аркушу) ISBN 978-966-932-140-4 п.4 1.Ільєнко А.В. Методи побудови та аналізу криптосистем / А.В.Ільєнко , С.С.Ільєнко, О.О.Висоцька// Лабораторний практикум для студентів освітньо-професійної програми «Безпека інформаційних і комунікаційних систем». – К.: НАУ, 2020. – 48 с. 2.Ільєнко А.В. Прикладна криптологія/ А.В.Ільєнко// Лабораторний практикум для студентів. – К.: НАУ, 2022. – 60 с. 3. Ільєнко А.В. Прикладна криптологія // Лабораторний практикум для студентів. – К.: НАУ, 2022. – 60 с. 4. Робоча програма та НМК «Методи побудови та аналізу криптосистем» ОС Магістр. 5. Робоча програма та НМК «Прикладна криптологія» ОС Бакалавр. п.7 Вчений секретар спеціальзованої вченої ради Д.26.062.01. Державного університету ""Київський авіаційни інститут"" (https://mon.gov.ua/npa/pro-zatverdzhennia-rishen-atestatsiinoi-kolehii-ministerstva) п.8 1. НДР №43/09.01.09 «Інформаційна технологія організації імітаційного полігону захисту критичних інформаційних ресурсів».

							Термін виконання - 01.09.2019р. – 30.06.2021р. (науковий керівник). 2. НДР № 5-2024/18.02 «Система забезпечення кібербезпеки та стійкості об'єктів критичної інфраструктури». Термін виконання - 01.03.2024р. – 30.06.2026р. (науковий керівник) п.12 1. Ilyenko A.V. Modern approach to cybersecurity of computer-integrated aviation systems / Ilyenko S.S, Kvasha D.S., Ilyenko A.V.// Aviation in the XXI-st century. Safety in aviation and space technologies: the nine world congress, 22-24 of September 2020: abstracts. – K., 2020. – V.1. (матеріали Міжнародної конференції) 2. Ilyenko A.V. Software module for authentication using neural network / Anna Ilyenko, Marharyta Herasymenko// Проблеми кібербезпеки інформаційно-телекомунікаційних систем: IV Міжнародна науково-практична конференція, 15-16 квітня 2021 р.: тези доп. – К., 2021. – С. 12-13. (матеріали Міжнародної конференції) 3. 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) 4. 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) 5. 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) 6. 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. 7. 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. 8. 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. 9. 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. 10. 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. 11. 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. 12. Ільєнко А. В., Ахрамович В. В. Методика дослідження захищеності кіберпростору соціальних платформ від кількості співтовариств // ABIA-2025: XVII Міжнар. наук.-техн. конф., 22–24 квіт. 2025 р.: тези доп. – Київ: КАІ, 2025. – С. 14.12–14.14. 13. Ільєнко А. В., Гулак Н. К., Дубчак О. В. Застосування криптографічних методів для захисту баз даних від несанкціонованого доступу // ABIA-2025: XVII Міжнар. наук.-техн. конф., 22–24 квіт. 2025 р.: тези доп. – Київ: КАІ, 2025. – С. 14.6–14.8. 14. Ільєнко А. В., Ільєнко С. С., Галата Л. П. Модуль захисту авіаційних інформаційно-комунікаційних систем на основі комбінованих моделей ML // ABIA-2025: XVII Міжнар. наук.-техн. конф., 22–24 квіт. 2025 р.: тези доп. – Київ: КАІ, 2025. – С. 14.9–14.11. 15. Ільєнко А.В., Дубчак О.В. Аналіз атак і засобів убезпечення data link layer // Комп'ютерні системи та мережеві технології: XVI міжнародна науково-технічна конференція, 25-28 березня 2025 р.: тези доп. – К., 2025. – С. 35-37. п.14 Керівник постійно діючого студентського наукового гуртка «Криптографічні методи захисту інформації» (підготовка здобувачів до участі у міжнародних наукових конференціях) п.19 Участь у професійних об'єднаннях: ITeachers SoftServe Community

							(01.09.2023) http://kszi.nau.edu.ua/novini/352-zaviduvach-kafedri-kiberbezpeki-doluchilasya-do-mizhnarodnoji-programi-edupro-vid-softserve; http://kszi.nau.edu.ua/novini/219-uchast-u-zustrichi-iteachers-meet-up-na-temu-kiberbezpeki
494468	Ахрамович Володимир Миколайович	Професор, Основне місце роботи	Факультет комп'ютерних наук та технологій	Диплом спеціаліста, Київський ордена 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: 1. Київський політехнічний інститут, 1980 р. спеціальність - Технологія машинобудування, металорізальні верстати та інструменти, кваліфікація – Інженер – механік. 2. Доктор технічних наук, 05.13.21 – Системи захисту інформації (диплом доктора наук ДД № 011778 від 29.06.2021), тема дисертації - «Методологічні основи забезпечення захисту інформації в соціальних мережах». 3. Професор кафедри кібербезпеки (атестат професора АП №004630 від 23.12.2022) Підвищення кваліфікації: 1. Доктор технічних наук, 05.13.21 – Системи захисту інформації, тема дисертації «Методологічні основи забезпечення захисту інформації в соціальних мережах». Диплом доктора наук ДД № 011778, виданий 29.06.2021 р. 2.International Historical Biographical Institute (Dubai-New York-Rome-Jerusalem-Beljing)lJ. Тема «Підвищення кваліфікації: Studying Exerience and Professional Achivements for Forming a Successful Personality and Transforming of the World». Термін 18.02.2022-23.04.2022рр. Сертифікат (6 кредитів ЄКТС). Види і результати професійної діяльності: п.1 1. Pavlo Shchypanskyi, Vitalii Savchenko, Volodymyr Akhramovych, Tetiana Muzshanova, Svitlana Lehominova, Volodymyr Chegrenets.The Model of Secure Social Networks Activity Based on Graph Theory/ International Journal of Innovative Technology and Exploring Engineering (IJITEE)ISSN: 2278-3075,Volume-9 Issue-4, February 2020 Pp 1803-1810. https://www.ijitee.org/download/volume-9-issue-4. (Scopus) 2. 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/ijetae0423_03. (Scopus, квартіль Q2). 3. Vitalii Savchenko, VolodymyrAkhramovych, Alina Tushych, Irina Sribna, Ihor Vlasov. Analysis of Social Network Parameters and the Likelihood of its Construction/International Journal of Emerging Trends

							in Engineering Research ISSN 2347 -3983, Volume 8.No. 2,February2020 Pp. 271-276. http://www.warse.org/ IJETER/static/pdf/ file/ijeter05822020.pdf. (Scopus) 4. Laptiev O., Savchenko V., , Kotenko A., Akhramovych V., Samosyuk V., Shuklin G., , Biehun A. Method of Determining Trust and Protection of Personal Data in Social Networks. International Journal of Communication Networks and Information Security (IJCNIS) 2021. № 1, April 2021. Pp. 15-21, Scopus, квартіль Q2. 5. Vitalii Savchenko, Volodymyr Akhramovych, Taras Dzyuba, Serhii Laptiev, Nataliia. Lukova-Chuiko, Tetiana Laptieva. Methodology for Calculating Information Protection from Parameters of its Distribution in Social Networks. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT). Conference Proceedings. December 15-16, 2021. Kyiv, Ukraine. Pp. 99-105. http://atit.ieee.org.ua/wp-content/uploads/2021/12/Program-ATIT-2021-02-14.12.21.pdf. . – (Scopus). 6. Vitalii Savchenko, Volodymyr Akhramovych, Oleksander Matsko, Ivan Havryliuk Method of Calculation of Information Protection from Clusterization Ratio in Social Networks. Proceedings of the 3rd International Conference on Information Security and Information Technologies (ISecIT 2021) co-located with 1st International Forum ""Digital Reality"" (DRForum 2021) Odesa, Ukraine, September 13-19, 2021.-pp. 24-31. (Scopus). 7. 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 Srodowiska, 2024. – 14(1). – PP. 71–77. (Scopus). 8. Serhii Yevseiev, Yuliia Khokhlachova, Serhii Ostapov, Oleksandr Laptiev, Olha Korol, Stanislav Milevskyi, Oleksandr Milov, Serhii Pohasii, Yevgen Melenti, Hrebeniuk 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 Yerhidzei, 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. (Scopus). 9. R. Khrashchevskyi, V. Klobukov, V. Kozlovskyi, 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, квартіль Q1). 10. Volodymyr Akhramovych, Yuriy Pepa, Anton Zahynei1, Vadym Akhramovych, Taras Dzyuba, Ihor Danylov. Method for calculating the information security indicator in social media with considerationof the path durationbetween 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) 11. 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, квартіль Q1). 12. Ахрамович В. М., Лаптєв О. А., Ахрамович В. В. Метод розрахунку захисту інформації у соціальних мережах в умовах нечітких множин // Безпека інформації. – 2024. – Т. 30, № 3. – С. 358–364. 13. Вадим. Ахрамович, Володимир. Ахрамович. Метод розрахунку показника захисту інформації ком'ютера в умовах невизначеності. Information Technology and Security.January-June 2025. Vol. 13. Iss. 1(24) pp. 55-68. п.5 Доктор технічних наук, 05.13.21 – Системи захисту інформації, тема дисертації «Методологічні основи забезпечення захисту інформації в соціальних мережах». ДД № 011778, виданий 29.06.2021 р. п.7 1. Член разової спеціалізованої ради ДФ 26.861.008 при захисті дисертації на здобуття наукового ступеня доктор філософії Бржевської Зореслави Михайлівна – «Методика оцінки достовірності інформації в умовах інформаційного протиборства». 2021 р. 2. Опонент при захисті дисертації на здобуття наукового ступеня доктор філософії Урденко Олександра Георгійовича «Моделювання та управління інформаційною безпекою підприємства в умовах цифрової трансформації» 2021р. 3. Член разової спеціалізованої ради при захисті дисертації на здобуття наукового ступеня доктор філософії Марченка Віталія Вікторовича «Метод

							виявлення шкідливих процесів в інформаційній системі підприємства на основі ідентифікації та діагностування станів логічних об'єктів»». 2023 р. 4. 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 інфрастуктури держави», ДСК. 2024 р. 5. . Відгук на автореферат дисертації ""Методи забезпечення резильєнтності організаційно-технічних систем"" Коробейнікова Федора Олександровича, представленої на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації» 2024р. 6. Член разової спеціалізованої ради при захисті дисертації на здобуття наукового ступеня доктор філософії Педченка Євгена Максимовича – «Методи та моделі оцінювання стану кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури». 2025 р. (https://vchenarada.nau.edu.ua/2025/05/02/spetsializovana-vchena-rada-z-pravom-prijnyattya-do-rozglyadu-ta-provedennya-zahistu-disertatsiyi-pedchenka-yevgena-maksimovicha-na-zdobuttya-stupenya-doktora-filosofiyi-z-galuzi-znan-12-informatsijni/) 7. Член спеціалізованої ради Д.26.062.01. Державного університету ""Київський авіаційни інститут"" (https://mon.gov.ua/npa/pro-zatverdzhennia-rishen-atestatsiinoi-kolehii-ministerstva) п.12 1. Vitalii Savchenko, Volodymyr Akhramovych, Taras Dzyuba, Serhii Laptiev, Nataliia. Lukova-Chuiko, Tetiana Laptieva. Methodology for Calculating Information Protection from Parameters of its Distribution in Social Networks. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT). Conference Proceedings. December 15-16, 2021. Kyiv, Ukraine. Pp. 99-105. http://atit.ieee.org.ua/wp-content/uploads/2021/12/Program-ATIT-2021-02-14.12.21.pdf 2. Vitalii Savchenko, Volodymyr Akhramovych, Oleksander Matsko, Ivan Havryliuk Method of Calculation of Information Protection from Clusterization Ratio in Social Networks. Proceedings of the 3rd International Conference on Information Security and Information Technologies (ISecIT 2021) co-located with 1st International Forum ""Digital Reality"" (DRForum 2021) Odesa, Ukraine, September 13-19, 2021.-pp. 24-31. (Scopus). 3. Volodymyr Akhramovych,

							Vadym Akhramovych, Viktor Ivankin, Oleh Stefaruk. Detection of black holes in the manet network // Science and society: modern trends in a changing world. Proceedings of the 5th International scientific and practical conference. MDPC Publishing. Vienna, Austria. 2024. Pp. 136-143. 4. Volodymyr Akhramovych, Vadym Akhramovych, Roman Prydybailo, Serhiy Chuprun. Methods of detecting DOS attacks. // European congress of scientific achievements. Proceedings of the 4th International scientific and practical conference. Barca Academy Publishing. Barcelona, Spain. 2024. Pp. 155-161. 5. Volodymyr Akhramovych, Vadym Akhramovych, Viktor Ivankin. Wireless network attacks which are permanent infrastructures are dynamic in nature // Perspectives of contemporary science: theory and practice. Proceedings of the 3rd International scientific and practical conference. SPC "Sci-conf.com.ua". Lviv, Ukraine. 2024. Pp. 398-404.
494698	Висоцька Олена Олександрівна	Доцент, Основне місце роботи	Факультет комп'ютерних наук та технологій	Диплом спеціаліста, Київський міжнародний університет цивільної авіації, рік закінчення: 1998, спеціальність: 091501 Комп'ютерні та інтелектуальні системи та мережі, Диплом кандидата наук ДК 056616, виданий 14.05.2020	25	Захист комунікаційних мереж засобами Cisco	Освіта: 1. Диплом спеціаліста з відзнакою КВ №10616376, Київський міжнародний університет цивільної авіації, 1998 р., спеціальність: "Комп'ютерні та інтелектуальні системи та мережі", кваліфікація: інженер-системотехнік. 2.Диплом кандидата технічних наук ДК №056616 від 14 травня 2020 р. за спеціальністю 05.13.21 – "Системи захисту інформації". Тема дисертації: "Методи біометричної автентифікації користувачів інформаційних систем за їх клавіатурним та рукописним почерком" Підвищення кваліфікації: 1)Національний авіаційний університет, Захист кандидатської дисертації за спеціальністю 05.13. 21 «Системи захисту інформації», Диплом: ДК №056616 від 14 травня 2020 р. 2) Технічно-Гуманітарна Академія в Бєльско-Бяла, Польща (Akademia Techniczno-Humanistyczna w Bielsku-Białej (University of Bielsko-Biala), Polska), 15.11.2021 р. - 13.12.2021 р., програма: «Комп'ютеризовані системи захисту інформації» («Systemy Komputeryzowane Ochrony Informacji»), кількість модулів: 7, кількість годин: 300, Сертифікат: Nr K18/13-01-4/2021 від 13.12.2021р. 3)SoftServe|Academy, Назва курсу: Cloud Environment Configuration and Security / Налаштування та безпека хмарних середовищ, термін проведення: 09 лютого 2024 – 10 квітня 2024, кількість годин: 120 год., кількість кредитів: 4 кредити, Сертифікат: Серія IE № 17738/2024 від 10.04.2024 р. Види і результати професійної діяльності:

							п.1 1.A. Davydenko, O. Vysotska, T. Shmelova, «Methods of Primary Processing Handwriting Samples at User Authentication Using a Probabilistic Neural Network», Proceedings of the International Workshop on Cyber Hygiene co-located with 1st International Conference on Cyber Hygiene and Conflict Management in Global Information Networks, vol. 2654, pp. 723-735, 2020. (Scopus) 2. Anatolii Davydenko, Oleksandr Korchenko, Olena Vysotska, Ihor Ivanchenko. “Model and method for identification of functional security profile”, Proceedings of the 3rd International Conference on Information Security and Information Technologies (ISecIT 2021) co-located with 1st International Forum ""Digital Reality"" (DRForum 2021), vol. 3200, pp. 274-280, 2021. (Scopus) 3. Висоцька О. Виділення обличчя людини у відеопотоці для контролю за дотриманням співробітниками стану безпеки в процесі роботи та навчання / О. Висоцька, А. Давиденко, В. Христевич // Захист інформації. 2022. – Том 24, №2. – С. 94-107. DOI: https://doi.org/10.18372/2410-7840.24.16934 (фахове видання категорії В, Index Copernicus) 4. Vysotska O. Modeling the mindfulness people's function based on the recognition of biometric parameters by artificial intelligence elements / O. Vysotska, A. Davydenko, O. Potenko // Radioelectronic and computer systems. 2023. – No 3 – P. 136-149. DOI: https://doi.org/10.32620/reks.2023.3.11 (фахове видання категорії А, Scopus) 5. Давиденко А. Дослідження взаємозв'язків між семантичними параметрами для галузі безпеки систем доступу / А. Давиденко, О. Висоцька, М. Пригара, В. Бичков // Захист інформації. 2024. – Том 26, №1. – С. 21-29. DOI: https://doi.org/10.18372/2410-7840.26.18821 (фахове видання категорії В, Index Copernicus) 6. Anatolii Davydenko, Oleksandr Korchenko, Mykhailo Prygara, Olena Vysotska, Volodymyr Shcherbyna. ""Analysis of The Relationship Between Semantic Parameters In The Development Of The Security Function Of Access System."" 2024 IEEE 5th International Conference on Advanced Trends in Information Theory (ATIT). IEEE, 2024. (Scopus, подано до друку)" п.4 Лабораторний практикум: 1.А.В. Ільєнко, С.С.Ільєнко, О.О.Висоцька. Методи побудови та аналізу криптосистем. Лабораторний практикум для студентів освітньо-професійної програми «Безпека інформаційних і комунікаційних систем». – К.: НАУ, 2020. – 48 с. Робочі програми навчальних дисциплін:

							1. Безпека інформаційно-комунікаційних систем та мереж. 2. Бази даних та знань. 3. Сучасні технології забезпечення кібербезпеки. 4. Технології безпечного доступу. 5. Інформаційно-аналітичні системи." п.5 Захист дисертації на тему "Методи біометричної автентифікації користувачів інформаційних систем за їх клавіатурним та рукописним почерком" за спеціальністю 05.13.21 – "Системи захисту інформації". Диплом кандидата технічних наук ДК №056616 від 14 травня 2020 р. за спеціальністю "Системи захисту інформації". п.12 1. O. Vysotska, A. Davydenko, «Biometric technologies in Cybersecurity», AVIATION IN THE XXI-st CENTURY: World Congress, Kyiv, 2020. Online: https://conference.nau.edu.ua/index.php/Congress/Congress2020/paper/view/7873/6486 2. Нестерук А.О. Система біометричної автентифікації користувачів комп'ютерних систем / Нестерук А.О., Висоцька О.О. // Materials of the XVI International scientific and practical Conference Scientific horizons - 2020, September 30 - October 7, 2020: Sheffield. Science and education LTD – P. 66-69. 3. Микитенко О.А. Ентропійна стеганографічна система захисту повідомлень в комп'ютерних мережах / Микитенко О.А., Висоцька О.О. // Материали за XVI международна научна практична конференция «Образованието и науката на XXI век – 2020», 15 - 22 октомври 2020 г.: София: «Бял ГРАД-БГ», С. 59-61. 4. Корченко О.Г. Аналіз топології інформаційної безпеки українського національного гріду / Корченко О.Г., Давиденко А.М., Висоцька О.О. // 13-а Всеукраїнська науково-практична конференція "Стан та удосконалення безпеки інформаційно-телекомунікаційних систем" (SITS' 2021). Збірник тез наукових доповідей (24-26 червня 2021 р.). – Миколаїв – Коблево, 2021. – С. 18-21. 5. Висоцька О.О. "Підтримка технології єдиного входу шляхом використання двофакторної автентифікації користувачів інформаційно-телекомунікаційних систем" / Висоцька О.О., Давиденко А.М. // VII Міжнародна науково-практична конференція "Перспективні напрями захисту інформації". Матеріали VII Міжнародної науково-практичної конференції (30 серпня – 03 вересня 2021 р.). – Одеса, 2021. – С. 16-19. 6. Davydenko Anatolii. "Model and method for identification of functional security profile" / Davydenko Anatolii, Korchenko

							Oleksandr, Vysotska Olena, Ivanchenko Ihor // Міжнародна науково-практична конференція “Інформаційна безпека та інформаційні технології”. Матеріали конференції (13-19 вересня 2021 р.). – Харків – Одеса, 2021. – С. 286-292. (Scopus) 7. Shaban Maxim. “Functional security profile settings model” / Shaban Maxim, Vysotska Olena, Vyshnevska Natalia, Shcherbyna Volodymyr. // XI міжнародна науково-технічна конференція “ITSec: Безпека інформаційних технологій”. Матеріали XI міжнародної науково-технічної конференції (1-6 жовтня 2021 р.). – Анталія (Туреччина), 2021. – С. 41-43. 8. Шапочка О. О. “Дослідження проблематики кібератак типу DDoS та можливі шляхи підвищення ефективності захисту від них” / Шапочка О. О., Висоцька О.О. // II Міжнародна наукова конференція “Розвиток наукової думки постіндустріального суспільства: сучасний дискурс”. Матеріали II Міжнародної наукової конференції, Т. 1 (8 жовтня, 2021 р.). – Дніпро, 2021. – С. 86-88. 9. Бацмай Б. В. “Методи застосування систем автентифікації користувача за клавіатурним почерком” / Бацмай Б. В., Висоцька О.О. (Науковий керівник) // II Міжнародна студентська наукова конференція “Актуальні питання та перспективи проведення наукових досліджень”. Матеріали II Міжнародної студентської наукової конференції, Т.2 (8 жовтня 2021р.). – Кременчук, 2021. – С. 17-20. 10. Vysotska Olena. “Increasing the level of security of information systems by using the event module with the implementation of event correlation” / Vysotska Olena, Davydenko Anatolii // Національний університет “Львівська політехніка”. VIII Міжнародна науково-технічна конференція “Захист інформації і безпека інформаційних систем”. Матеріали VIII Міжнародної науково-технічної конференції (11–12 листопада 2021 р.). – Львів, 2021. – С. 73-74. 11. Zubilevych Anton. “Single sign-on technology in the process of authentication in web applicationson” / Zubilevych Anton, Vysotska Olena // Національний університет “Львівська політехніка”. VIII Міжнародна науково-технічна конференція “Захист інформації і безпека інформаційних систем”. Матеріали VIII Міжнародної науково-технічної конференції (11–12 листопада 2021 р.). – Львів, 2021. – С. 23-24. 12. Vysotska Olena. “Dodatkowe uwierzytelnianie uprawnionych użytkowników według geometrii ich twarzy w

systemach informatycznych wykorzystujących technologię single sign-on" / Vysotska Olena, Davydenko Anatolii // XI edycja Konferencji "Inżynier XXI wieku". Part of the Monograph "Przetwarzanie, transmisja i bezpieczeństwo informacji" (10 grudnia 2021). – Bielsko – Biała, Polska, 2021. – S. 257-268. DOI: https://doi.org/10.53052/9788366249868.27
13. Висоцька О.О., "Удосконалена система автентифікації в організації з використанням віддаленого доступу" / Висоцька О.О., Цевельов Є.О. // XVII Международна научна практична конференция "Бъдещето въпроси от света на науката - 2021". Материали XVII Международна научна практична конференция, Vol. 1 (17 - 25 декември 2021 р.). –София, 2021. – С. 83-85.
14. Джежело М.В., "Удосконалення комплексу кіберзахисту системи управління контентом вебресурсу підприємства" / Джежело М.В., Висоцька О.О., Батрак О.Г. // 1st International Scientific and Practical Conference "Modern directions and movements in science". Proceedings of the 1st International Scientific and Practical Conference, №127 (October 6-8, 2022). – LUXEMBOURG, 2022. – С. 271-275. https://archive.interconf.center/index.php/conference-proceeding/article/download/1422/1450
15. Корченко О. Г. "Аналіз інформаційних компонент систем розмежування доступу" / Корченко О. Г., Давиденко А. М., Висоцька О. О., Щербина В. П. // "Актуальні питання забезпечення кібербезпеки та захисту інформації". Колективна монографія за заг. наук. ред. А.М. Давиденко. – Київ: Європейський університет, 2023. – С. 19-30.
16. Давиденко А. "Формування навичок фіксації деструктивної дезінформації в кіберпросторі під час занять для студентів спеціальності «Кібербезпека»" / Давиденко А., Висоцька О., Потенко О. // Європейський університет. IX міжнародна науково-практична конференція «Актуальні питання забезпечення кібербезпеки та захисту інформації». Матеріали IX міжнародної науково-практичної конференції (30 березня 2023 р.). – Київ, 2023. – С.35-37.
17. Давиденко Анатолій. "Фіксація деструктивної дезінформації в кіберпросторі за участі студентів спеціальності «Кібербезпека»" / Давиденко Анатолій, Висоцька Олена // Національний авіаційний університет. XII міжнародна науково-технічна конференція «ITSec: Безпека інформаційних технологій». Матеріали XII міжнародної науково-технічної конференції (2-4 травня 2023 р.). – Ужгород, 2023. – С.19-21.

18. Давиденко А.М. “Тестування згорткової нейронної мережі при розпізнаванні зображень обличь” / Давиденко А.М., Висоцька О.О., Суліма О.А. // Національний університет «Чернігівська політехніка». XIII міжнародна науково-практична конференція «Комплексне забезпечення якості технологічних процесів та систем». Матеріали XIII міжнародної науково-практичної конференції (25–26 травня 2023 р.). Том 2. – Чернігів, 2023. – С.233-235.
19. Davydenko Anatolii. “Developing a software application for the protection of information systems based on the analysis of graphic images” / Davydenko Anatolii, Vysotska Olena and Potenko Oleksandr // Національний університет “Львівська політехніка”. IX Міжнародна науково-технічна конференція “Захист інформації і безпека інформаційних систем”. Матеріали IX Міжнародної науково-технічної конференції (25–26 травня 2023 р.). – Львів, 2023. – С. 122-123.
20. Давиденко А. М. “Захист інформаційних систем на основі аналізу графічних зображень” / Давиденко А. М., Висоцька О. О., Потенко О. С. // Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Науково-практична конференція «Кібербезпека енергетики». Матеріали науково-практичної конференції (31 травня 2023 р.). – Київ, 2023. – С.74-77.
21. Котирло П.І. “Використання спаму як способу поширення пропаганди в соціальних мережах” / Котирло П.І., Висоцька О.О. // Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Міжнародна науково-практична конференція «Живучість та резильєнтність – 2023» («Survivability & Resilience – 2023»). Збірник матеріалів конференції (19 жовтня 2023 р.). – Київ, 2023. – С.131-132.
22. Сулима О.А. “Використання дворівневої моделі доступу” / Сулима О.А., Висоцька О.О., Скворцов С.О. // Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Науково-практична конференція «Використання блокчейн технологій в енергетиці – 2024». Збірник матеріалів конференції (5 червня 2024 р.). – Київ, 2024. – С.28-29.
23. Хукаленко Б.А. “Аналіз використання сучасних методів біометричної автентифікації у менеджерах паролів” / Хукаленко Б.А., Висоцька О. О. // The 3rd International scientific and practical conference “Current trends in scientific research development”: Proceedings of the 3rd International scientific and practical conference (October 17-19, 2024). – BoScience Publisher, Boston, USA, 2024. – С.137-

143. https://sci-conf.com.ua/wp-content/uploads/2024/10/CURRENT-TRENDS-IN-SCIENTIFIC-RESEARCH-DEVELOPMENT-17-19.10.2024.pdf
24. Vjatcheslav Dzecina. “ Inspection of critical properties of subsystems of an smart home ” / Vjatcheslav Dzecina, Olena Vysotska // International Scientific Conference “Innovations and New Directions in Scientific Research”: Proceedings of the International Scientific Conference (October 14, 2024). – Manchester, UK: Bookmundo, 2024. – P. 111-112. https://researcheurope.org/wp-content/uploads/2024/10/re-14.10.2024.pdf.
25. Olesya Kotchenko. “Analysis of advantages and disadvantages of harm assessment tools” / Olesya Kotchenko, Olena Vysotska // International Scientific Conference “Innovations and New Directions in Scientific Research”: Proceedings of the International Scientific Conference (October 14, 2024). – Manchester, UK: Bookmundo, 2024. – P. 113-114. https://researcheurope.org/wp-content/uploads/2024/10/re-14.10.2024.pdf.
26. Борщ А.А. “Методи моніторингу мережевого трафіку з метою виявлення та блокування зовнішнього вторгнення в комп'ютерні системи” / Борщ А.А., Висоцька О. О. // Міжнародна науково-практична інтернет-конференція “Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення”: Матеріали міжнародної науково-практичної інтернет-конференції, Випуск 92 (м. Тернопіль, Україна, м. Ополе, 12 Польща, 12-13 листопада 2024 р.). – ГО “Наукова спільнота”, WSZIA w Opolu. Тернопіль, 2024. http://www.konferenciaonline.org.ua/ua/article/id-1933/
27. Безпалий О.Р. “Дослідження можливостей використання сучасних технологій для двофакторної аутентифікації на основі біометричних параметрів” / Безпалий О.Р., Висоцька О.О. (Науковий керівник) // 6 Міжнародна студентська наукова конференція. “Тренди та перспективи розвитку мультидисциплінарних досліджень”: Матеріали 6 міжнародної студентської наукової конференції (м. Кременчук, 11 жовтня 2024 рік). – ГО “Молодіжна наукова ліга”.— Вінниця: ТОВ “УКРЛОГОС Груп”, 2024. – С.107-109. https://archive.liga.science/index.php/conference-proceedings/issue/view/inter-11.10.2024/98
28. Миловидов В.Ю. “Актуальність та проблематика фішингових атак на освітні структури” / Миловидов В.Ю., Висоцька О.О. (Науковий керівник) // VII Міжнародна студентська

							наукова конференція “Діджиталізація науки як виклик сьогодення”: Матеріали VII Міжнародної студентської наукової конференції (м. Полтава, 25.10.2024). – ГО “Молодіжна наукова ліга”.— Вінниця: ТОВ “УКРЛОГОС Груп”, 2024. – С. 552-555. https://archive.liga.science/index.php/conference-proceedings/issue/view/inter-25.10.2024/101 29. Погоріла В. М. “Аналіз архітектури програмних застосунків з метою виявлення вразливостей пов ’язаних з використанням штучного інтелекту” / Погоріла В. М., Висоцька О.О. (Науковий керівник) // VI Всеукраїнська студентська наукова конференція «Науковий простір: аналіз, сучасний стан, тренди та перспективи»: Матеріали VI Всеукраїнської студентської наукової конференції (м. Київ, 18 жовтня, 2024 рік)). – ГО “Молодіжна наукова ліга”.— Вінниця: ТОВ “УКРЛОГОС Груп”, 2024. – С. 337-340. https://archive.liga.science/index.php/conference-proceedings/issue/view/ukr-18.10.2024/100 30. Висоцька О.О. “Дослідження вразливостей автоматизованих систем пов’язаних з використанням штучного інтелекту” / Висоцька О.О., Давиденко А.М. // Національний університет «Чернігівська політехніка». XV міжнародна науково-практична конференція «Комплексне забезпечення якості технологічних процесів та систем». Матеріали XIII міжнародної науково-практичної конференції (22–23 травня 2025 р.). Том 2. – Чернігів, 2025. – С.298-300. 31. Давиденко Анатолій. “Дослідження методів розпізнавання обличчя” / Анатолій Давиденко, Олена Висоцька, Михайло Пригара, Володимир Щербина // Західноукраїнський національний університет - Державний університет інформаційно-комунікаційних технологій. XIV міжнародна науково-технічна конференція «ITSec: Безпека інформаційних технологій». Матеріали XIV міжнародної науково-технічної конференції (22-24 травня 2025 р.). – Тернопіль, 2025. – С.58-59. 32. Висоцька О.О. “Виявлення фішингових сайтів за допомогою нейронних мереж” / Висоцька О.О. // Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Науково-практична конференція «Кібербезпека енергетики». Матеріали конференції (28 травня 2025 р.). – Київ, 2025. – С.81-82." п.19 Назва: Громадська організація «Асоціація спеціалістів кібербезпеки» Дата входження до складу: 22.06.2025 Опис діяльності: Зміцнення

							кібербезпеки через активний обмін досвідом, знаннями та інноваційними рішеннями між фахівцями галузі.

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**
ПРН 25. Вміння: - здійснювати організацію функціонування інформаційно-комунікаційної систем: формувати опис автоматизованої системи та середовища її функціонування, визначати склад апаратного та програмного забезпечення, здійснювати аналіз обчислювальних процесів та технологій обробки інформації, аналіз складу та характеристик існуючої системи захисту з використанням засобів Cisco. - знати спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки інформаційних мереж; - проєктувати захищені (з урахуванням загроз) інформаційні мережі з використанням сучасних методів та технологій забезпечення інформаційної безпеки та/або кібербезпеки.	☐	Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист курсової роботи
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	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
ПРН 23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.	☒	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
		Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист курсової роботи
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	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

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.	☒	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 у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист курсової роботи
		Технології створення та застосування систем захисту кіберпростору	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
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
		Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист курсової роботи
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	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
		Методи побудови та аналізу криптосистем	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
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, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Курсовий проєкт з дисципліни Методологія прикладних досліджень у сфері кібербезпеки	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист курсового проекту
		Моделювання та оптимізація безпекових процесів авіаційної галузі	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	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

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.	☒	Моделювання та оптимізація безпекових процесів авіаційної галузі	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	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
		Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист курсової роботи
ПРН 18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.	☒	Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист курсової роботи
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	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
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.	☒	Методологія прикладних досліджень у сфері кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Курсовий проєкт з дисципліни Методологія прикладних досліджень у сфері кібербезпеки	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист курсового проекту
		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
		Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист курсової роботи
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	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	практичні 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
		Ділова іноземна мова	практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
ПРН 16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.	☒	Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	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
		Моделювання та оптимізація безпекових процесів авіаційної галузі	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист курсової роботи
		Кваліфікаційна робота	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
ПРН 15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.	☒	Наукові комунікації у фаховій діяльності	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
		Моделювання та оптимізація безпекових процесів авіаційної галузі	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист курсової роботи
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	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
ПРН 24. Вміння: - проєктувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної	☐	Методи побудови та аналізу криптосистем	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		Переддипломна практика	пошуковий метод, метод	Захист звіту з практики

та/або кібербезпеки; - вирішувати задачі практичного застосування в своїй професійній діяльності криптографічних алгоритмів, протоколів та криптосистем для забезпечення належного рівня інформаційної та кібербезпеки в інформаційно-телекомунікаційних системах; - розробляти та впроваджувати криптографічні системи і використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.			проблемного виконання, дослідницький метод, продуктивно-практичний метод	
		Кваліфікаційна робота	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
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.	☒	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 у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		Методи побудови та аналізу криптосистем	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
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.	☒	Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	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
ПРН 11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	☒	Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист курсової роботи
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	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
		Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
ПРН 12. Досліджувати, розробляти та впроваджувати методи	☒	Кваліфікаційна робота	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-	Захист кваліфікаційної роботи

і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.			практичний метод	
		Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	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
ПРН 1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	☒	Ділова іноземна мова	практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Наукові комунікації у фаховій діяльності	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
		Курсовий проєкт з дисципліни Методологія прикладних досліджень у сфері кібербезпеки	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист курсового проекту
		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
		Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист курсової роботи
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	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
ПРН 2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.	☒	Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	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
		Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист курсової роботи
		Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен

		Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Ділова іноземна мова	практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Наукові комунікації у фаховій діяльності	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
		Курсовий проєкт з дисципліни Методологія прикладних досліджень у сфері кібербезпеки	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист курсового проекту
		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
ПРН 3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	☒	Методологія прикладних досліджень у сфері кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Курсовий проєкт з дисципліни Методологія прикладних досліджень у сфері кібербезпеки	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист курсового проекту
		Методи побудови та аналізу криптосистем	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	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
ПРН 4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.	☒	Моделювання та оптимізація безпекових процесів авіаційної галузі	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист курсової роботи
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	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
		Методи побудови та аналізу криптосистем	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
ПРН 5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних	☒	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
		Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік

наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.		Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист курсової роботи
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	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
		Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
ПРН 6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	☒	Моделювання та оптимізація безпекових процесів авіаційної галузі	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист курсової роботи
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	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
		Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
ПРН 7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	☒	Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	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
ПРН 8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	☒	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 у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		Курсова робота з	пошуковий метод, метод	Захист курсової роботи

		дисципліни Технології створення та застосування систем захисту кіберпростору	проблемного виконання, дослідницький метод, продуктивно-практичний метод	
		Технології створення та застосування систем захисту кіберпростору	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
		Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
ПРН 9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	☒	Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	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
ПРН 10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	☒	Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	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