

**ВІДОМОСТІ**  
про самооцінювання освітньої програми

Заклад вищої освіти	<b>Національний авіаційний університет</b>
Освітня програма	<b>59297 Безпека інформаційних і комунікаційних систем</b>
Рівень вищої освіти	<b>Магістр</b>
Спеціальність	<b>125 Кібербезпека та захист інформації</b>

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:*

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

## Загальні відомості

### 1. Інформація про ЗВО (ВСП ЗВО)

Реєстраційний номер ЗВО у ЄДЕБО	<b>183</b>
Повна назва ЗВО	<b>Національний авіаційний університет</b>
Ідентифікаційний код ЗВО	<b>01132330</b>
ПІБ керівника ЗВО	<b>Семенова Ксенія Ігорівна</b>
Посилання на офіційний веб-сайт ЗВО	<b><a href="http://www.nau.edu.ua">http://www.nau.edu.ua</a></b>

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

<https://registry.edbo.gov.ua/university/183>

### 3. Загальна інформація про ОП, яка подається на акредитацію

ID освітньої програми в ЄДЕБО	<b>59297</b>
Назва ОП	<b>Безпека інформаційних і комунікаційних систем</b>
Галузь знань	<b>12 Інформаційні технології</b>
Спеціальність	<b>125 Кібербезпека та захист інформації</b>
Спеціалізація (за наявності)	<i>відсутня</i>
Рівень вищої освіти	<b>Магістр</b>
Тип освітньої програми	<b>Освітньо-професійна</b>
Вступ на освітню програму здійснюється на основі ступеня (рівня)	<b>Бакалавр, Магістр (ОКР «спеціаліст»)</b>
Структурний підрозділ (кафедра або інший підрозділ), відповідальний за реалізацію ОП	<b>Кафедра кібербезпеки Факультет комп'ютерних наук та технологій</b>
Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП	<b>кафедра іноземних мов професійного спрямування (факультет лінгвістики та соціальних комунікацій), кафедри української мови та культури факультет лінгвістики та соціальних комунікацій), кафедра кібербезпеки (факультет комп'ютерних наук та технологій), кафедра технічного захисту інформації (факультет комп'ютерних наук та технологій)</b>
Місце (адреса) провадження освітньої діяльності за ОП	<b>Національний авіаційний університет Україна, 03058, м.Київ, просп. Гузара Любомира, 1</b>
Освітня програма передбачає присвоєння професійної кваліфікації	<i>не передбачає</i>
Професійна кваліфікація, яка присвоюється за ОП (за наявності)	<b><i>відсутня</i></b>
Мова (мови) викладання	<b>Українська</b>
ID гаранта ОП у ЄДЕБО	<b>13973</b>
ПІБ гаранта ОП	<b>Ільєнко Анна Вадимівна</b>
Посада гаранта ОП	<b>Завідувач кафедри (1 ставка)</b>
Корпоративна електронна адреса гаранта ОП	<b><a href="mailto:anna.ilienko@npp.nau.edu.ua">anna.ilienko@npp.nau.edu.ua</a></b>
Контактний телефон гаранта ОП	<b>+38(097)-381-72-00</b>
Додатковий телефон гаранта ОП	<b>+38(044)-408-18-09</b>

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 вищої освіти з освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» спеціальності 125 «Кібербезпека та захист інформації» здійснюється випусковою кафедрою кібербезпеки. Початок підготовки фахівців у галузі інформаційної безпеки та захищених інформаційних технологій лежить у 2000 році, разом зі створенням кафедри, тоді кафедри комп'ютеризованих систем захисту інформації Національного авіаційного університету. За цей час змінилося кілька класифікаторів спеціальностей, але кафедра продовжує готувати висококваліфікованих, конкурентоспроможних фахівців у сфері кібербезпеки та захисту інформації. Наказом голови комісії з реорганізації НАУ, в.о. ректора від 31.05.2024 №256/од 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 за спеціальністю 125 «Кібербезпека та захист інформації» за освітніми програмами: «Безпека інформаційних і комунікаційних систем» та «Управління кібербезпекою та захистом інформації».

Відповідно до постанови Кабінету Міністрів України від 27.08.2010 р. №787 «Про затвердження переліку спеціальностей, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційними рівнями спеціаліста і магістра» в рамках галузі знань «Інформаційна безпека» здійснюється підготовка фахівців за освітньо-кваліфікаційними рівнями «Спеціаліст» та «Магістр» за спеціальністю 7/8.17010101 «Безпека інформаційних та комунікаційних систем».

Наказом Міністерства освіти і науки України №1039 від 25.07.2013 «Про затвердження і введення в дію складових галузевих стандартів вищої освіти із спеціальностей освітньо-кваліфікаційного рівня «Магістр» галузі знань 1701 «Інформаційна безпека», затверджені складові галузевих стандартів вищої освіти України (освітньо-кваліфікаційні характеристики (ОКХ) та освітньо-професійні програми (ОПП) підготовки фахівців освітньо-кваліфікаційного рівня «Магістр» галузі знань 1701 «Інформаційна безпека» за спеціальністю 8.17010101 «Безпека інформаційних та комунікаційних систем».

У квітні 2015 р. постановою Кабінету Міністрів України № 266 були проведені зміни шифрів і найменувань галузі знань і відповідно кодів і найменувань спеціальності. Відтепер кафедра в рамках 125 спеціальності «Кібербезпека» та галузі знань 12 «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 України від 28.04.2017р. №1/9-239, «Методичних рекомендацій до розроблення та оформлення освітньо-професійної 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 ОП, була розроблена ОП «Безпека інформаційних і комунікаційних систем», затверджена Вченою радою НАУ (протокол №5 від 26.06.2018р.). У відповідності до щорічного перегляду ОПП у 2019 році була скоригована. Нова редакція ОП була затверджена Вченою радою НАУ(протокол №3 від 20.03.2019р.) та введена в дію наказом ректора №139/од від 02.03.2019р.

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 вибірково освітню компоненту. Відповідні зміни внесені в ОП для здобувачів вищої освіти 2020 року вступу з 2020-2021 н.о. та затверджені Вченою радою НАУ(протокол №6 від 26.08.2020р.) та введена в дію наказом ректора №317/од від 27.08.2020р.

На основі затвердженого стандарту вищої освіти за спеціальністю 125 «Кібербезпека», який був введений в дію Наказом МОН України від 18.03.2021р. №332, здійснено розробку нової редакції ОП з метою вдосконалення освітніх компонент та приведення ОП у відповідність до затвердженого стандарту. Нова редакція затверджена Вченою радою НАУ(протокол №4 від 21.04.2021р.) та введена наказом ректора №246/од від 29.07.2021р. У 2022 році згідно з наказом т.в.о. ректора № 063/од від 09.02.2022 р. «Про щорічний перегляд освітньо-професійних програм» був проведений перегляд освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти за спеціальністю 125 «Кібербезпека» (зміни внесені на підставі результатів перегляду освітньої програми відповідно до наказу ректора від 08.06.2022 №154/од).

Відповідно до постанови Кабінету Міністрів України від 16.12.2022 р. №1392 «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» було проведено зміну назви спеціальності, а саме з «Кібербезпека» на «Кібербезпека та захист інформації». Після щорічного перегляду, проведеного у 2023 році, ОП «Безпека інформаційних та комунікаційних систем» переведена на спеціальність «Кібербезпека та захист інформації» починаючи з 2023 року вступу та затверджено Вченою радою НАУ(протокол №2 від 15.02.2023р.) та введена наказом ректора №069/од від 23.02.2023р. З врахуванням пропозицій стейкхолдерів та академічної спільноти у 2024 році було розроблено нову редакцію ОП. Нова редакція затверджена Вченою радою НАУ(протокол №4 від 17.04.2024р.) та введена наказом ректора №166/од від 23.04.2024р. (підстава Рішення № 1 засідання Науково-методичної ради НАУ від 16.01.2024), 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 році відтермінована у зв'язку з реорганізацією Національного авіаційного університету.

#### 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	Обсяг набору на	Контингент студентів на відповідному році навчання	У тому числі іноземців
--------------	-------------------------	-----------------	--	------------------------

я	відбувся набір здобувачів відповідного року навчання	ОП у відповідно му навчально му році	станом на 1 жовтня поточного навчального року			
			ОД	З	ОД	З
1 курс	2024 - 2025	60	40	12	0	0
2 курс	2023 - 2024	60	38	9	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	<b>59194 Системи та технології кібербезпеки</b> <b>59198 Безпека інформаційних і комунікаційних систем</b> <b>59199 Системи технічного захисту інформації, автоматизація її обробки</b> <b>59327 Управління кібербезпекою та захистом інформації</b> <b>59436 Управління інформаційною безпекою</b>
другий (магістерський) рівень	<b>59297 Безпека інформаційних і комунікаційних систем</b> <b>59440 Адміністративний менеджмент у сфері захисту інформації</b> <b>59298 Системи технічного захисту інформації, автоматизація її обробки</b> <b>59328 Системи та технології кібербезпеки</b>
третій (освітньо-науковий/освітньо-творчий) рівень	<b>59092 Кібербезпека</b>

## 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	3993	0

Примітка. Для ЗВО із ВСП інформація зазначається:

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

## 8. Документи щодо ОП

Документ	Назва файла	Хеш файла
Освітня програма	<i>ОПП БІКС Магістр 2023 125 Кібербезпека та захист інформації.pdf</i>	2U113BbVUFV3RKJu7znj87O2IRYCT5l4oHORSgWiHTc =
Освітня програма	<i>ОПП БІКС Магістр 2024 125 Кібербезпека та захист інформації.pdf</i>	UNiKTAAnRdWU9AznGiXDicSDg2HmGAL/cvv/SfzJ5BN Y=
Навчальний план за ОП	<i>Навчальний_план_ОС_Магістр_2_023.pdf</i>	6eWKqD3XSZJsgtuciw6PSQh2TXFxmrf1++Vj0+Rq1eA=
Навчальний план за ОП	<i>Навчальний_план_ОС_Магістр_3_аоч_2023.pdf</i>	9oLNt/R33GbEUeMLQbOIPJh/HEHQZ6K2EFwme5E V4=
Матеріали від ЗВО: пропозиції та рекомендації	<i>Рецензія ОПП Магістр _1.pdf</i>	Ohjac5GPQ+9NCa5PEPpPdDuN4kXEzM8PnNsvatimsSw =

від роботодавців, таблиця відповідності публікацій наукових керівників напрямом (тематикам) досліджень аспірантів (для ОП третього рівня освіти)		
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямом (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	<i>Рецензія ОПП Магістр_2.pdf</i>	AwSue2Ui+5id6bcNcH46FNfGKWhBGHAL3Ol51M4nkc =
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямом (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	<i>Рецензія ОПП Магістр_3.pdf</i>	PxflLv2svCyIJrymsfjR/Ng7yBYjlpJj687dk9On8/4=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямом (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	<i>Рецензія ОПП Магістр_4.pdf</i>	FPckl2GIUVo+xB1uGuvtvqr5LE976mLs16RQd+S19rM=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямом (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	<i>Рецензія ОПП Магістр_5.pdf</i>	EbJqwlURMgo1/82mYraDhUVrkdz592fVoV5ktGBjhqc=

## 1. Проектування 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 №332 від 18.03.2021 р. Міністерством Освіти і Науки України затверджений Стандарт вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня освіти (<http://surl.li/hgvgl>). При розробці ОП «Безпека інформаційних і комунікаційних систем» враховано Стандарт вищої освіти України другого (магістерського) рівня, галузі знань 12 «Інформаційні технології», спеціальність 125 «Кібербезпека» (Стандарт вищої освіти затверджено і введено в дію наказом Міністерства освіти і науки України від 18.03.2021 р. № 332). Зміст ОП «Безпека інформаційних і комунікаційних систем» дає можливість досягти результатів навчання, які визначені Стандартом вищої освіти, а саме: програмні результати навчання в ОП «Безпека інформаційних і комунікаційних систем» повністю відповідають результатам навчання. Цілі ОП відповідають цілям навчання. Програмні результати навчання за розробленою ОП повністю відповідають вимогам, наведеним у стандарті вищої освіти: ПР1- ПР23 (розділ VI Стандарту). Сукупність результатів навчання ПРН1-ПРН23 забезпечено обов'язковими компонентами ОП. Матриця забезпечення програмних результатів навчання відповідними компонентами наведена у п. 5 даної ОП. Інтегральна компетентність в рамках ОП 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) ступеня вищої освіти, приведені в стандарті, відображені в ОП. Таким чином, в розробленій ОП реалізовано компетентнісний підхід відповідно до Національної рамки кваліфікацій України. Усі програмні результати навчання, зазначені в ОП, досягаються змістовним наповненням визначених освітніх компонентів, їх обсягами та методами навчання й контролю. Достатня кількість комп'ютерної техніки, кадрового, навчально-методичного та програмного забезпечення ОП 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)?**

Зміст освітньої програми не враховує вимоги наявних професійних стандартів.

У рамках щорічного перегляду проведеного у 2023 році, ОП переведена на спеціальність «Кібербезпека та захист інформації» починаючи з 2023 року вступу та затверджено Вченою радою НАУ (протокол №2 від 15.02.2023р.) та введена наказом ректора №069/од від 23.02.2023р. та відповідає затвердженому професійному стандарту «Фахівець з питань безпеки», який затверджений наказом Адміністрації Держспецзв'язку від 25.11.2022 №715 (<http://surl.li/jfsfuc>)

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

### **- здобувачі вищої освіти та випускники програми**

Інтереси здобувачів за другим рівнем вищої освіти були враховані під час формулювання цілей ОП та програмних результатів навчання. Для оцінки якості навчання в 2023/2024 навчальному році було проведено опитування здобувачів 2 курсу щодо якості організації навчального процесу, що навчаються за цією ОП, з тим, щоб визначити проблеми у навчанні та врахувати їх зауваження/побажання. Обговорення результатів анкетування здобувачів вищої освіти щодо якості надання освітніх послуг за ОП «Безпека інформаційних і комунікаційних систем» відображено протоколом засідання кафедри від 19.03.2024 року № 13 (<http://kszi.nau.edu.ua/novini/229-rezultati-anketuvannya-zdobuvachiv-vishchoji-osviti-2023-2024-n-r>). Відділом забезпечення якості НАУ 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/stejjkholderi>). На щорічному обговоренні ОП (<http://surl.li/tadxlw>) здобувачі вищої освіти Трішун А., Величківський І. підтримали ОП та відзначили можливість реалізації індивідуальної освітньої траєкторії студентів за рахунок широкого переліку вибіркового компонентів, які забезпечують отримання необхідних практичних навиків у сфері кібербезпеки необхідних для майбутньої професійної діяльності. Випускники висловлюють свою думку щодо подальшого розвитку ОП, здебільшого, в усній формі при неформальному спілкуванні.

### **- роботодавці**

Для врахування інтересів та пропозицій роботодавців щодо цілей і програмних результатів навчання ОП «Безпека інформаційних і комунікаційних систем» проводились спільні зустрічі та круглі столи між розробниками ОП і представниками підприємств (організацій), щодо обговорення ключових моментів організації освітнього процесу при підготовці даної освітньої програми (<http://surl.li/nzqgmj>; <http://surl.li/yfqurn>; <http://surl.li/drpltn>; <http://surl.li/wocvdr>) а саме: Державним підприємством обслуговування повітряного руху України «Укранерорух», Департамент кіберзахисту Адміністрації Держспецзв'язку, ТОВ «Алгоритм-Х» 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 ГРУП» та ін. (<http://kszi.nau.edu.ua/stejjkholderi>).

### **- академічна спільнота**

Інтереси академічної спільноти враховувалися наступним чином: академічної спільноти НАУ – через обговорення проблем академічної свободи викладання та прийняття відповідних рішень на засіданнях кафедр, Комісії з якості факультету, Науково-методичної ради факультету та НАУ; 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» (<http://surl.li/azokkr>); Технічно-Гуманітарна академія в Бельско-Бяла, Польща, SoftServe; ДЗВО «Університет менеджменту освіти»; ТОВ IT-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: та Днів професій в НАУ (<http://iro.nau.edu.ua/>); фахові конференції, круглі столи тощо. Зауваження та побажання інших стейкхолдерів враховуються під час формування переліків обов'язкових і вибіркового освітніх компонент ОП, корегування навчальних планів, корегування робочих навчальних програм дисциплін. Надається можливість на академічну мобільність Еразмус+. Стейкхолдери також оцінюють та підписують ОП. Публічне обговорення проекту ОП відбувалося на офіційному сайті університету (<http://surl.li/iejjnx>), (<http://surl.li/phoqag>).

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

Мета освітньо-професійної програми полягає в підготовці висококваліфікованих, конкурентоспроможних фахівців

на глобальному ринку праці, здатних розв'язувати задачі дослідницького та інноваційного характеру у сфері кібербезпеки та захисту інформації, забезпечення здобувачів вищої освіти фундаментальною підготовкою у вигляді поглиблених теоретичних і практичних знань, умінь та навичок, достатніх для ефективного виконання завдань відповідного рівня професійної діяльності в сфері захисту інформації та з урахуванням специфіки авіаційної галузі; оволодіння студентами знаннями, вміннями та навичками з проектування, експлуатації та впровадження сучасних технологій, методів та засобів забезпечення безпеки інформаційних і комунікаційних систем задля позитивного внеску у розвитку суспільства на національному та міжнародному рівнях через генерацію нових знань та інноваційних ідей з урахуванням потреб ІТ ринку, а також авіаційної галузі України. Відмінність програми – реалізація моделі підготовки фахівців в сфері безпеки інформаційних і комунікаційних систем з урахуванням потреб ІТ ринку, а також авіаційної галузі України.

Мета ОП враховує стандарту ВО України для другого (магістерського) рівня за спеціальністю 125 «Кібербезпека» (<http://surl.li/kevmdj>), Стратегії розвитку НАУ (<http://surl.li/uruizn>) та Статуту університету (<http://surl.li/xsskiw>), 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 ОП 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 ОП 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 ОП 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 ОП 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 ОП 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 співпрацюють 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 ОП 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>). Зокрема доцент кафедри Петренко А.Б. та асистент Телющенко В.А. прийняли участь у першій конференції «Стратегія розбудови кадрового потенціалу України у сфері кібербезпеки та захисту інформації» у межах форуму «Кібер Україна» (<http://surl.li/jnscxh>). 26 вересня 2023 року к.т.н., доцент Петренко Андрій Борисович прийняв участь у офлайн зустрічі Діалог "Сучасний спеціаліст із кібербезпеки — хто він?" (<http://surl.li/shrdpr>).

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

ОП розроблена відповідно до потреб світового ринку праці та нових тенденцій розвитку електроенергетичних систем і технологій. Під час формулювання цілей та програмних результатів навчання (ПРН) ОП 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 ОП. Був врахований також значний досвід, який отримали викладачі кафедри кібербезпеки та технічного захисту інформації завдяки участі у проєкті Агентства USAID "Кібербезпека критично важливої інфраструктури України", зокрема, підвищення кваліфікації у 2022 р. в літній школі доцента кафедри Ільєнко А.В., які були організовані у межах цього проєкту (<http://surl.li/mbzvzl>)

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

Мета освітньої програми та програмні результати навчання формулювалися з урахуванням досвіду аналогічних іноземних освітніх програм, а саме Каліфорнійський державний університет Сан-Бернардіно <https://www.csusb.edu/cybersecurity> Університет Джорджа Вашингтона <https://cs.engineering.gwu.edu/master-science-cybersecurity-computer-science> Канзаський державний університет <https://engg.k-state.edu/academics/undergraduate/cybersecurity/> Це забезпечує відповідність світовим стандартам і підвищує конкурентоспроможність випускників на міжнародному ринку праці.

## 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 (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; системи управління інформаційною безпекою та/або кібербезпекою; технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. Ціллю навчання за ОП є підготовка високваліфікованих фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки.

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 ОП дозволяє стверджувати про відповідність змісту ОП предметній області спеціальності 125 "Кібербезпека та захист інформації". Освітньо-професійна програма ґрунтується на принципах студентоцентризму та індивідуально-особистісного підходу; реалізується через навчання на основі досліджень, посилення практичної орієнтованості та творчої спрямованості у формі комбінації лекцій, практичних занять, самостійної навчальної і дослідницької роботи, розв'язування прикладних задач, виконання проєктів, навчальних та виробничих практик, курсових робіт (проєктів), кваліфікаційної роботи. Осним фокусом програми є загальна вища освіта в галузі «Інформаційні технології» з поглибленою спеціалізованою підготовкою в сфері інформаційної та кібербезпеки, в тому числі моделювання, розробка, впровадження і експлуатація програмних та програмно-апаратних комплексів та засобів захисту інформації на об'єктах критичної інфраструктури, авіаційної галузі та народного господарства.

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

Основний документ формування індивідуальної освітньої траєкторії здобувача вищої освіти (ВО) – індивідуальний навчальний план (ІНП), що формується відповідно: Положення про формування індивідуальної освітньої траєкторії здобувача вищої освіти в НАУ (<http://surl.li/uuyqyjg>); Положення про індивідуальний навчальний план (<https://bit.ly/3NuWiIl>); Положення про організацію освітнього процесу в НАУ (<https://bit.ly/3skHoPP>); Положення про організацію самостійної роботи (<https://bit.ly/3GncZnG>). У НАУ визначено порядок та процедуру формування індивідуальної освітньої траєкторії (<http://surl.li/pvjzwc>). Згідно <https://bit.ly/2YrWdtz> вільний вибір здобувача ВО вибіркових дисциплін (<http://surl.li/sakubu>) передбачає два послідовні 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. Здобувачі ВО мають право: вільно обирати ВК в обсязі не менше 25% від загальної кількості кредитів ЄКТС та факультативні дисципліни; навчатися одночасно за кількома ОП, індивідуальним графіком; академічну мобільність; зарахування кредитів з неформальної освіти; пропонувати свої теми курсових та кваліфікаційних робіт, бази практик. Для даної ОП ІНП містить перелік, кредитів та контрольні заходи щодо ОК, до яких входять обов'язкові 66 кредитів та вибіркові ОК 24 кредитів ЄКТС.

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



Вибіркові дисципліни здобувачів ВО надають можливість більш повного забезпечення відповідності освітніх кваліфікаційних вимог ринку праці, ефективного використання можливостей університету і його навчальних підрозділів, здійснення поглибленої підготовки за ОП, що забезпечується через формування індивідуальної освітньої траєкторії. Вільний вибір здобувачами ВО навчальних дисциплін визначено в Положенні про формування індивідуальної освітньої траєкторії здобувача вищої освіти в НАУ (<http://surl.li/wbaikx>). Переліки вибіркових дисциплін переглядаються випусковою кафедрою щорічно до початку процедури їх вибору, з урахуванням пропозицій здобувачів ВО, науково-педагогічних працівників, інших кафедр/факультетів/інститутів та стейкхолдерів. При формуванні переліку враховуються сучасні тенденції і спеціальності кібербезпека та захист інформації, результати наукових досліджень (<http://surl.li/cvfsjq>). Вибіркові ОК обираються здобувачем індивідуально із запропонованого каталогу (<http://surl.li/wcqvof>) з урахуванням особистих уподобань та перспектив майбутньої професійної діяльності. Процедура вибору здобувачами дисциплін включають: інформування здобувачів про перелік та зміст ВК, що виносяться на вибір й вивчатимуться в наступному навчальному році (<http://surl.li/pazsmf>); ознайомлення з порядком, термінами та особливостями процесу обрання, Покроковою інструкцією для роботи в «Автоматизованій системі формування індивідуальної освітньої траєкторії здобувача вищої освіти» (АСФІОТ) (<http://surl.li/wmazfx>), консультування, за необхідності; обрання через АСФІОТ вибіркових ОК; проведення коригування з метою виконання умов щодо мінімальної кількості здобувачів ВО, які можуть бути записані на дисципліну. Результати обрання здобувачами ВО вибіркових дисциплін затверджуються на засіданні випускової кафедри та публікуються на сайті кафедри (<http://surl.li/ltsvrl>). Розпорядження декана про затвердження обраних ОК за кожною ОП на кожен курс і семестр передається до навчально-методичного відділу університету. Обрані здобувачами ВК включаються до робочого плану та індивідуального навчального плану та є обов'язковими для вивчення.

### **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 НАУ (<https://bit.ly/3LerL3O>). Розроблено Положення про організацію та проведення практик (<https://bit.ly/35KD9UF>). Практична підготовка здобувачів в межах ОП передбачена навчальним планом: науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем (4,5 кредити ЄКТС), переддипломна практика (6 кредитів ЄКТС), що є обов'язковими ОК. Програми практик регламентують діяльність здобувачів і керівників практик (<http://surl.li/xmmhpi>; <http://surl.li/fwclcz>). 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 реалізуються на підставі договорів, що підписані з НАУ (<http://kszi.nau.edu.ua/stejjkholderi>; <http://surl.li/sgoutt>).

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

Упродовж усього терміну навчання за ОП 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 ОП 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 ОП ОК1-2 та фахової компоненти ОК3, за рахунок підготовки доповідей, презентацій, рефератів тощо. Формуванню соціальних навичок «SoftSkills» сприяють дисципліни вільного вибору, в тому числі дисциплін поза межами спеціальності, а саме «Філософські проблеми наукового пізнання» та «Захист особистих немайнових прав в інформаційному суспільстві» (<http://surl.li/jfrzxe>). Участь здобувачів у диспутах та конференціях, що передбачено ОП, 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 та старша викладачка Олена Прокопенко взяли участь у міжнародній програмі підвищення кваліфікації викладачів EDUPRO (EDUCATOR PROFICIENCY PROGRAM) присвяченій розвитку soft skills (<http://surl.li/harogw>).

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

ОП 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 "Ділова іноземна мова", "Методологія прикладних досліджень у сфері кібербезпеки", "Моніторинг та аудит кібербезпеки" 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 суспільстві. 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)?**

В НАУ 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 в НАУ (<https://bit.ly/3scifVW>), що встановлюють вимоги до розрахунку достатності навчального навантаження на здобувачів відповідно до кількості кредитів та видів завдань. Загальна кількість ОК (дисциплін, курсових робіт і практик) становить не більше 16 на навчальний рік. У випускному семестрі до ОК віднесені переддипломна практика та кваліфікаційна робота. В ОП використовуються наступні види аудиторних навчальних занять: лекції, лабораторні заняття, практичні заняття. Максимальний загальний навчальний час здобувачів ВО протягом тижня з усіх видів навчальної роботи, включаючи самостійну, не перевищує 1,5 кредитів ЄКТС або 45 годин (при шестиденному тижні). Більше 50% обсягу ОП спрямовано на забезпечення загальних та фахових компетентностей. Для коригування фактичного навантаження здобувачів ВО періодичне опитування проводиться на загальноуніверситетському рівні (<http://surl.li/eniif>, <https://nau.edu.ua/ua/menu/quality/otsinyuvannya-rezultativ-yakosti-navchannya/>) та на кафедрі (<http://surl.li/ardhgj>).

### **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 форму 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 IT-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, налагодити контакти з потенційними роботодавцями та адаптуватися до вимог ринку (<http://surl.li/zdwuef>, <http://surl.li/vugcut>). Викладання за даною ОП 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 програмних результатів навчання на базі факультеті функціонують лабораторії та центри, зокрема: Навчальний центр «IT Академія» та навчально-дослідна лабораторія протидії кіберзагрозам в авіаційній галузі (<https://cyberlab.nau.edu.ua/>), а також кіберполігон Cyber Range UA (<http://surl.li/sybbki>). 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**

ОП 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. ОП передбачає формування ЗК абстрактного мислення, аналізу та синтезу. До змісту ОК 1-9 включені питання, які забезпечують набуття здобувачами вищої освіти знань, навичок і компетентностей, направлених на досягнення Цілей сталого розвитку ООН до 2030 р. відповідно до наказу ректора 063/од від 09.02.2022 (<http://surl.li/hkbgfi>). Набуття здобувачами ВО ФК1-10 та додаткових ФК11,12 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 та процвітаюче майбутнє.

### **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 НАУ: <http://pk.nau.edu.ua>

Правила прийому до НАУ у 2024 році: <https://pk.nau.edu.ua/pravylyl-priyomu-do-nau-u-2024-rotsi/>

Положення про Приймальну комісію НАУ : <https://pk.nau.edu.ua/wp-content/uploads/2021/12/Polozhennia-pro-prymalnu-komisiiu-NAU.pdf>

Положення про фахову атестаційну комісію : <https://pk.nau.edu.ua/wp-content/uploads/2021/12/Polozhennia-pro-fakhovu-atestatsiinu-komisiiu-NAU.pdf>

Положення про апеляційну комісію: <https://pk.nau.edu.ua/wp-content/uploads/2021/12/Polozhennia-pro-apeliatsiinu-komisiiu-NAU.pdf>

Вартість підготовки фахівців на 24/25 навч. рік : <https://pk.nau.edu.ua/vartist-navchannia-bakalavr-mahistr/>

Положення про порядок організації набору та навчання (стажування) іноземних громадян та осіб без громадянства у Національному авіаційному університеті : <http://surl.li/wyeree>

Правила прийому на навчання за освітньою програмою є чіткими та зрозумілими, не містять дискримінаційних положень та оприлюднені на офіційному веб-сайті закладу вищої освіти.

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

Прийом вступників на навчання за ОПП здійснюється відповідно до Умов вступу та Правил прийому на навчання в НАУ в 2024 (<https://pk.nau.edu.ua/pravylyl-priyomu-do-nau-u-2024-rotsi/>). Для конкурсного відбору на навчання для здобуття ступеня магістра у 2024 році на основі НРК6 та НРК7 зараховуються бал (бали): 1) для вступу на спеціальності галузі знань 12 «Інформаційні технології»: ЄВІ 2023 або 2024 років та єдиного державного кваліфікаційного іспиту (ЄДКІ) зі спеціальності 125 «Кибербезпека та захист інформації» 2024 року (тільки для вступників на спеціальність 125 «Кибербезпека та захист інформації», які склали відповідний ЄДКІ 2024 року); ЄВІ 2023 або 2024 років та ЄФВВ 2024 року (крім вступників на спеціальність 125 «Кибербезпека та захист інформації», які склали відповідний ЄДКІ 2024 року).

## **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 НАУ» (<http://surl.li/grmp>), «Положенні про порядок переведення (поновлення) студентів, які навчалися у вищих навчальних закладах Донецької та Луганської областей, на навчання до НАУ» (<http://surl.li/ldmof>), Положення про видачу та облік академічних довідок (<http://surl.li/lfshd>)

Відповідно до Положення про порядок відрахування, переривання навчання, поновлення і переведення осіб, які навчаються у закладах вищої освіти, та надання їм академічної відпустки (<http://surl.li/jbohjs>) та «Тимчасового положення про порядок відрахування, переривання навчання, поновлення і переведення здобувачів вищої освіти НАУ» (<http://surl.li/grmp>) переведення здобувачів вищої освіти на перший курс забороняється, тому здобувач вищої освіти може подати заяву про переведення тільки після першого року навчання. Цей документ розміщений на сайті НАУ у вільному доступі. Він урегулює усі аспекти організації переведення такого здобувача вищої освіти та визнання результатів навчання, отриманих в інших ЗВО, зокрема під час академічної мобільності.

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

За 2019-2024 р.р. на ОП другого (магістерського) рівня вищої освіти випадків поновлення студентів, що на навчання з інших ЗВО не було.

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

В НАУ питання визнання результатів навчання, отриманих у неформальній освіті регулюється «Положенням про порядок визнання результатів навчання, здобутих шляхом неформальної та/або інформальної освіти Національного авіаційного університету» (<https://bit.ly/3C8sjUY>).

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

Практики застосування не було.

## **4. Навчання і викладання за освітньою програмою**

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

Освітній процес на ОП відповідає вимогам законодавства України, зокрема, Закону України "Про вищу освіту" та враховує стандарт вищої освіти другого (магістерського) рівня для спеціальності 125 Кібербезпека. Методи та форми навчання і викладання ОП зазначені в Положенні про організацію освітнього процесу в НАУ (<https://bit.ly/2KytNAS>). Навчання виконується у формі лекційних, практичних та лабораторних занять, самостійної роботи, проходження практик, виконання курсової роботи (проєкту) та кваліфікаційної роботи. Використовуються словесні наочні та практичні методи. Синтез цих методів та форм навчання дозволяє забезпечити формування як загальних і фахових компетенцій, так і програмних результатів навчання. Форми та методи навчання і викладання добираються викладачем самостійно з міркувань досягнення визначених у ОП цілей та ПРН, доцільності та студентоцентрованого підходу, і повністю узгоджуються з академічною свободою викладання. Їх відповідність ПРН представлена в робочих програмах дисциплін (<http://surl.li/vargex>). Застосовуються методи теоретичного, експериментального дослідження, аналізу, моделювання та прогнозування, аналізу даних, технології пошуку, обробки інформації, дискусія, презентація. Підтвердженням застосування дослідницького методу є участь здобувачів у конференціях, наукові публікації (<http://surl.li/idmzon> <http://surl.li/bermip>). Для сприяння досягнення наукових результатів у НАУ діє Наукове товариство студентів, аспірантів, докторантів та молодих вчених НАУ (<http://ysa.nau.edu.ua>).

**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 НАУ визначені Системою внутрішнього забезпечення якості освітньої діяльності. Навчальний процес орієнтований на студентоцентрований підхід при виборі форм і методів навчання та викладання, які наводяться в робочих програмах і силабусах навчальних дисциплін (<http://surl.li/ajrlnr>), (<http://surl.li/mbzxdn>). 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 досвідчені спеціалісти – провідні викладачі кафедри (к.т.н. Ільєнко А.В.) та провідних ВНЗ (д.т.н.Толюпа С.В., д.т.н. Терейковська Л.О., к.т.н. Пархоменко І.І.). Формування індивідуальної освітньої траєкторії здобувачів ВО здійснюється шляхом обрання здобувачами вибіркового дисциплін відповідно до нормативних документів з використанням автоматизованої системи (<http://surl.li/axrqgh>). Результати обрання вибіркового дисциплін здобувачами ВО затверджується на засіданні кафедри (<http://surl.li/qkkjxi>) та відображається на сайті кафедри (<http://surl.li/jidpfg>). Студентська оцінка роботи НПП є важливою для покращення якості надання освітніх послуг, впливає на рейтинг працівників та кафедр університету. Рівень задоволеності здобувачів методами навчання та викладання оцінюється за допомогою анкетування (<http://surl.li/fbrpei>). В НАУ діє Положення про рейтингове оцінювання діяльності НПП та навчально-наукового структурного підрозділу НАУ (<http://surl.li/czmse>).

**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/3GoVOiV>), Положенням про організацію освітнього процесу в НАУ (<https://bit.ly/34EkCch>) і полягає в педагогічній ініціативі під час провадження педагогічної, науково-педагогічної та наукової діяльності. ЗВО забезпечує поєднання навчання і досліджень під час реалізації ОП відповідно до рівня ВО, спеціальності та цілей ОП. Відповідно до ЗУ «Про освіту», Положення про організацію освітнього процесу в НАУ та Методичних рекомендацій до розроблення і оформлення робочих програм дисциплін (<https://bit.ly/3utAEjZ>) 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 ОП 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 ОП, 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 (<http://surl.li/ijoeeg>). У робочих програмах навчальних дисциплін ОП 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/kuymfm>). Паперові версії робочих програм

зберігаються на кафедрі та в навчальному відділі НАУ.

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

В Університеті 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. ОП передбачає набуття кожним здобувачем здатності розв'язувати складні спеціалізовані задачі та практичні проблеми в сфері кібербезпеки та захисту інформації. Кафедрою проводяться наукові дослідження в межах, 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, результатом є наукові публікації студентів (<http://surl.li/zbaapl>). Актуальність та значимість наукових досліджень і розробок НПП кафедри підтверджується участю в міжнародних науково-практичних конференціях (<http://surl.li/miyepf>). Інноваційні розробки кафедри комп'ютеризованих систем захисту включено до Каталогу «Наука та інновації» (2021) Національного авіаційного університету. Дані розробки впроваджені в навчальний процес підготовки здобувачів вищої освіти ОП «Безпека інформаційних і комунікаційних систем» (<http://surl.li/tqcfgi>; <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/qkscptb>). З метою підвищення ефективності результатів навчання, для проходження виробничої практики і подальшого працевлаштування на безоплатній основі підписані Угоди про співпрацю (<http://kszi.nau.edu.ua/stejjkholderi>). Для сприяння досягнення наукових результатів у НАУ діє Наукове товариство студентів, аспірантів, докторантів та молодих вчених НАУ (<http://ysa.nau.edu.ua>). Для підтримки та заохочення молодих вчених запроваджено премії та стипендії (<http://surl.li/kckwkb>; <http://surl.li/qtrtjm>), конкурсний відбір наукових проектів для молодих вчених та створено Центр організації освітньо-наукової діяльності студентів та молодих учених. Ільєнко Анна, к.т.н., доцент кафедри стипендіат стипендії Кабінету Міністрів України для молодих вчених (<http://surl.li/gtkpkh>; постанова президії Комітету від 10 червня 2020 року № 4).

### **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 відповідній галузі. У НАУ діє система забезпечення якості освіти (<https://bit.ly/38yquSD>), одним із основних завдань якої є здійснення моніторингу та періодичного перегляду ОП. На основі принципу академічної свободи НПП ОП визначають, які наукові досягнення та сучасні практики слід пропонувати здобувачам під час навчання, проводять наради з групою розробників ОП. Щорічно провідні НПП кафедри оновлюють зміст навчальних дисциплін, що знаходять відображення у робочих програмах, які щорічно розглядаються на засіданнях випускової кафедри автоматизації та енергоменеджменту. 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/tmfep>). Щорічно провідні НПП кафедри оновлюють зміст навчальних дисциплін, що знаходять 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 інформаційних 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 діяльності визначається Стратегією розвитку НАУ, Стратегією інтернаціоналізації співробітництва в галузі освіти (<https://nau.edu.ua/ua/menu/un%D1%96versitet/pro-un%D1%96versitet.html>), Положенням про порядок набору та навчання іноземних громадян (<https://bit.ly/3os9x50>), співпрацею із зарубіжними ЗВО (<https://bit.ly/3uutKei>). Впроваджується програма входження НАУ у світові рейтинги QS World University Rankings та Times Higher Education World University Rankings. Створено організаційні умови реалізації права на академічну мобільність і участі в грантових програмах HORIZON, ERASMUS+, FULLBRIGHT, MEVLANA (<https://bit.ly/3otLhzk>). Викладачі проходять підвищення кваліфікації в закордонних закладах ВО (Технічно-Гуманітарна академія в Бельско-Бяла, Польща, доцент Висоцька О.О.) та міжнародній програмі Cisco Networking Academy (<http://surl.li/hzmnlc>); публікують результати досліджень в зарубіжних наукових виданнях, беруть участь у 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. Також здобувачі беруть участь у дистанційних вебінарах, що організуються у межах проекту USAID «Кібербезпека критично важливої інфраструктури України» (<http://surl.li/qzuphh>, <http://surl.li/evxeuy>).

## **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 та проведення поточного і семестрового контролю НАУ контрольними заходами (<https://bit.ly/3B8ng6g>) та ПРН, передбачених ОП (<http://surl.li/utqfsi>). Вибір форми контролю за кожним ОК зумовлений його місцем у формуванні ПРН. Критерії оцінювання визначаються для ОП 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 ОП. Атестація здобувачів ВО регламентується Положенням про атестацію здобувачів ВО Національного авіаційного університету (<http://surl.li/iascde>).

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

В Національному авіаційному університеті чіткість та зрозумілість контрольних заходів та критеріїв оцінювання регламентуються у наступних документах: Положення про організацію освітнього процесу в НАУ (<https://bit.ly/3scxzBW>); Положенням про атестацію здобувачів ВО Національного авіаційного університету (<http://surl.li/iascde>); ОП (<http://surl.li/utqfsi>); навчальних планах (<http://surl.li/nbvqgv>); робочих програмах навчальних дисциплін (<http://surl.li/gfeawj>) та силабусах навчальних дисциплін (<http://surl.li/uhthoe>). 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 (силабуси) за НП є у вільному доступі у сайті кафедри (<http://surl.li/szipve>, <http://surl.li/vtezn>).

### **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 НАУ (<https://bit.ly/3Huiouh>); Положенням про організацію та проведення поточного і семестрового контролю (<https://bit.ly/3rvHT9j>), в якому регламентується проведення модульних контрольних робіт, диференційованих заліків та екзаменів. Усі чинні положення розташовані на сайті НАУ 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/>). 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 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 стандарті вищої освіти України для другого (магістерського) рівня за спеціальністю 125 «Кібербезпека» (<http://surl.li/jxutqx>) у розділі VII. Форми атестації здобувачів вищої освіти зазначено, що атестація здійснюється у формі публічного захисту кваліфікаційної роботи. ОП передбачає атестацію у формі публічного захисту кваліфікаційної роботи (<http://surl.li/utqfsi>). За всіма вимогами ОП відповідає Стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти. Форма атестації здобувачів ВО повністю забезпечує загальні та фахові компетентності за спеціальністю, визначених цим Стандартом. Форми атестації та супутні процедури врегульовуються Положенням про атестацію здобувачів ВО Національного авіаційного університету (<http://surl.li/iascde>), Положенням про кваліфікаційні роботи (проекти) здобувачів вищої освіти Національного авіаційного університету (<http://surl.li/tkyzlf>). Кваліфікаційні роботи здобувачів за ОП оприлюднюються в репозитарії НАУ (<https://er.nau.edu.ua/handle/NAU/41559>).

### **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 НАУ (<https://bit.ly/3Huiouh>); Положенням про організацію та проведення поточного і семестрового контролю

(<https://bit.ly/3rvHT9j>), в якому регламентується проведення модульних контрольних робіт, диференційованих заліків та екзаменів. Усі чинні положення розташовані на сайті НАУ 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/>). 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**

В університеті вироблена чітка процедура комплектування, організації та роботи екзаменаційних комісій, яка зазначена Положенням про організацію освітнього процесу та Положенням про атестацію ЗВО. 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 НАУ здійснюється в письмовій формі. Усі форми контролю проводяться з дотриманням принципів академічної доброчесності (<https://bit.ly/34AwnRo>). З метою моніторингу дотримання учасниками освітнього процесу моральних та правових норм розроблено Декларації про дотримання академічної доброчесності науково-педагогічного працівника та здобувача вищої освіти НАУ (<https://bit.ly/34AwnRo>). 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, ректора, Студентського самоврядування (<http://surl.li/neojgv>), до відділу із питань запобігання корупції (<https://bit.ly/3t8Oppz>), та скориставшись Скринькою довіри (<https://bit.ly/454Jaog>). На ОП конфлікту інтересів не виникало. Скарг здобувачів ВО на упередженість та необ'єктивність екзаменаторів не було.

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

Порядок повторного проходження контрольних заходів відбувається згідно з Положенням про організацію та проведення поточного і семестрового контролю НАУ. Ліквідувати академічну заборгованість дозволяється у терміни встановлені наказом ректора про організацію освітнього процесу в парних/непарних семестрах. Повторне проходження семестрового контролю з метою ліквідації академічної заборгованості дозволяється лише до початку наступного семестру (<https://bit.ly/3oqZoWi>). Якщо при перескладанні здобувач отримав незадовільну підсумкову семестрову оцінку, він має право за заявою перескласти комісії, яку формує декан факультету на підставі пропозицій відповідних кафедр і затверджує склад та термін ліквідації академічних заборгованостей. 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 університету за невиконання індивідуального навчального плану. Прикладів повторного складання іспитів протягом існування ОП не відзначалося.

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

Порядок оскарження процедури та результатів проведення контрольних заходів регулюється «Положенням про організацію та проведення поточного і семестрового контролю», зокрема пп. 2.32-2.34 (<https://bit.ly/3oqZoWi>). 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 ОП. 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 НАУ:

1. Кодекс честі науково-педагогічного працівника та Кодекс честі студента Національного авіаційного університету, що розміщені на стендах навчальних корпусів університету, а також на сайті (<https://bit.ly/3mLaYIy>);
2. Положення про виявлення та запобігання академічному плагіату в Національному авіаційному університеті, затверджено на засіданні Вченої ради (<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 НАУ (<https://bit.ly/3uFpOWi>);
5. Система академічної доброчесності в НАУ (<https://bit.ly/2ZVbHAL>). В НАУ був проведений аналіз впровадження системи академічної доброчесності (<https://bit.ly/2LqvVed>). На ОП 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. 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 НАУ 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 НАУ 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 НАУ (<https://bit.ly/3hHujJm>). Профілактичні заходи протидії академічному плагіату закріплені у п.5 «Положення про виявлення та запобігання академічному плагіату в НАУ» (<https://bit.ly/37A4RCE>). Інформація щодо формування академічної доброчесності в студентському середовищі висвітлюється на веб-сайті НАУ (<https://bit.ly/3errv9X>). У НАУ впроваджений Кодекс честі науково-педагогічного працівника та Кодекс честі студента, що розміщені на стендах навчальних корпусів університету, а також на сайті (<https://bit.ly/3mLaYIy>). Метою кодексу є формування в університеті демократичних взаємин з високим ступенем етичної гідності між студентами, науково-педагогічними працівниками, співробітниками і адміністрацією та розвиток корпоративної культури університетського співтовариства.

### **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 недоброчесності: Положення про виявлення та запобігання академічному плагіату в НАУ (<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 НАУ факт виявлення плагіату в академічних текстах здобувачів різного освітньо-кваліфікаційного ступеня призводить до їхньої академічної відповідальності та є підставою для: відмови у присудженні наукового ступеня, заборони 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 НАУ застосовується інформаційна система - Unicheck. Акти перевірки студентських робіт зберігаються на кафедрі та у відділі моніторингу якості вищої освіти. Випадків недопущення здобувачів до захисту кваліфікаційної роботи внаслідок порушення правил академічної доброчесності на ОП «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 розміщена у базі ЄДЕБО та на сайті кафедри (<http://surl.li/auxlaz>). 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 (<http://surl.li/qejqdk>); Положення про конкурс на посаду керівника структурного підрозділу (<http://surl.li/zlgzjw>); Положення про підвищення кваліфікації НПП НАУ (<http://surl.li/wintzj>). Науково-педагогічні працівники, залучені до забезпечення ОП, мають відповідні публікації та підвищення кваліфікації, що відповідають освітньому компоненту, який вони викладають.



**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 за профілем ОП наукових публікацій та методичних робіт, участь у конференціях, наявність стажувань та підвищення кваліфікацій, наявність практичного досвіду роботи). Необхідний рівень професіоналізму НПП ОП 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 затвердженого Вченою радою НАУ «Порядку проведення конкурсного відбору при заміщенні вакантних посад НПП та укладання з ними трудових договорів (контрактів) у НАУ» (<https://bit.ly/znXrfuR>). Серед кандидатів обираються претенденти, які мають відповідний рівень освіти, науковий ступінь та/або вчене звання відповідно до профілю ОП, стаж науково-педагогічної роботи та викладають навчальні дисципліни на високому науково-методичному рівні, що має підтверджуватися висновком кафедри про проведення відкритого заняття; навчально-методичні праці, які використовуються в освітньому процесі та наукові праці, опубліковані у фахових наукових виданнях (<http://surl.li/vcvzfp>). Конкурсний відбувається прозоро із запрошенням адміністрації університету та всіх охочих <http://surl.li/spyqlc>

**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 їх потенціал для проведенні занять, стажування НПП, розвиває форми співпраці: - спільна робота при розробці та реалізації ОП; - рецензування ОП та її періодичний перегляд (<http://surl.li/thfzza>); - проходження здобувачами ВО практик (<http://surl.li/yfifbc>); - підвищення кваліфікації та стажування НПП (<http://surl.li/mlfgwf>, <http://surl.li/vcenhj>, <http://surl.li/tfajnx>); - участь здобувачів у освітніх онлайн-вебінарах від проєкту USAID «Кибербезпека критично важливої інфраструктури України» (<http://surl.li/nfbc>, <http://surl.li/evxeuy>). На кафедрі існує практика залучення до аудиторних занять за ОП професіоналів-практиків, представників роботодавців. Наприклад, 6 травня 2024 року відбулася онлайн-лекція доцента і директора магістерської програми зі штучного інтелекту в Наньянському технологічному університеті Dr. Adams Wai-Kin Kong на тему Ризики та проблеми безпеки в глибинних мережах (<http://surl.li/svlkrf>), протягом квітня-травня 2024 року відбулися 7 лекцій від провідних експертів ІТ-галузі <http://surl.li/nnsvyk>. 26 квітня 2024 року відбулася лекція від представників компанії GigaTrans <http://surl.li/euurm>. 13 вересня 2024 р. лекція на тему Україна у світовій кібервійні; 24 вересня 2024 року - Побудова кар'єри: від ЦРУ до засновника страталу з кібербезпеки <http://surl.li/wqhhok>. В рамках дисципліни Методи побудови та аналізу криптосистем 7 жовтня 2024 року відбулася лекція від навчального центру Linkos Group <http://surl.li/hnubjd>.

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

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>) тощо. НПП мають можливість підвищити кваліфікацію під час стажувань згідно двосторонніх угод про співпрацю (<http://surl.li/rsqfy>). НПП кафедри проходили приймали активну участь у закордонних конференціях (<http://surl.li/rgryp>). Підтвердження виконання підвищення кваліфікації зафіксовано НПП у базі ЄДЕБО та на сайті кафедри (<http://surl.li/hzmnlc>; <http://surl.li/ppxujd>; <http://surl.li/tofmgp>; <http://surl.li/azokkr>; <http://surl.li/tsqtjk>; <http://surl.li/yjzana>; <http://surl.li/npujcd>; <http://surl.li/ngwnul>; <http://surl.li/vstuvi>). Наприклад, у рамках освітнього проєкту Агентства USAID "Кибербезпека критично важливої інфраструктури України" викладач кафедри 2022 рр. підвищила кваліфікацію в обсязі 180 кредитів ЄКТС, пройшовши програму «Cybersecurity Summer Instructor Training Program» (<http://surl.li/snghte>). Також викладачі приймають участь у курсах-інтенсивах TEACHERS SMART UP (<http://surl.li/qekuwu>, <http://surl.li/hforkl>, <http://surl.li/tfajnx>), у вебінарах від компанії SoftServe (<http://surl.li/wvtdxs>, <http://surl.li/wljazm>), а також у рамках договору про партнерство та ділове співробітництво між університетом та компанією «GlobalLogic Україна» приймають участь у курсах (<http://surl.li/bpwjxq>).

**Наведіть конкретні приклади заохочення розвитку викладацької майстерності**

Система заходів стимулювання розвитку викладацької майстерності НПП НАУ передбачає матеріальні та моральні заохочення і регламентується: Статутом (<http://bit.ly/3Xz3ev8>), Колективним договором НАУ (Положення про порядок заохочення осіб, які працюють, навчаються (<https://bit.ly/3pvJ58A>)). НАУ сприяє розвитку викладацької майстерності, створює умови для підвищення якості виконання професійних обов'язків, підвищення мотивації, збільшення кількості публікацій у періодичних виданнях, що індексуються у наукометричних базах Scopus та Web of Science, шляхом використання системи заохочень у вигляді преміювань відповідно до Положення про преміювання працівників <http://surl.li/scwjlf>. Система заохочення НПП нематеріального характеру реалізується через нагородження грамотами, подяками від завідувача кафедри, декана факультету, ректора університету в залежності від міри вкладу в розвиток та представлення до заохочувальних відзнак МОН України (<http://surl.li/bdqir>). Для стимулювання розвитку майстерності НПП в університеті запроваджено: конкурс наукових проєктів для молодих вчених (<http://surl.li/hgwwdn>), премії та стипендії для молодих учених (<http://surl.li/ussmt>). З нагоди 90-річчя Національного авіаційного університету отримали відзнаки за їхню вагомую роботу та внесок у розвиток університету (<http://surl.li/jlylgt>). Ільєнко Анна стипендіат стипендії Кабінету Міністрів України для молодих вчених (<http://surl.li/gtkpkh>), 15 грудня 2022 року Доцент кафедри Ільєнко А.В. отримала подяку МОН (<http://surl.li/pwyutg>).

## 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 НАУ дозволяють реалізовувати освітній процес за ОП у т.ч. в умовах дистанційного та змішаного навчання. Інфраструктура об'єднує 11 навчальних корпусів, що включають спеціалізовані лабораторії, обладнані відповідно сучасних вимог до організації освітнього процесу, 12 гуртожитків, Центр харчування, Авіаційний медичний центр, профілакторій, ЦКМ, ІОЦ, Навчально-спортивний оздоровчий центр, Науковотехнічну бібліотеку, видавництво. 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 програмних результатів навчання на базі Факультету комп'ютерних наук та технологій функціонують лабораторії та центри, зокрема: Навчальний центр «ІТ Академія» та навчально-дослідна лабораторія протидії кіберзагрозам в авіаційній галузі (<https://cyberlab.nau.edu.ua/>), а також кіберполігон Cyber Range UA (<http://surl.li/vevapn>, <http://surl.li/vphylw>). Здобувачі мають вільний доступ до навчально-методичного забезпечення ОП на сайті кафедри, а саме робочих програм (<http://surl.li/yowffl>) та силабусів (<http://surl.li/gywplm>), а також електронної бібліотеки кафедри (<http://surl.li/amwcaz>).

### **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 розвиток, гуманітарний розвиток, спортивний напрям, культурно-творчий розвиток. Викладачі та студенти мають безкоштовний доступ до платформи Udemy <https://udemy.com>. Для студентів НАУ є додаткова онлайн-можливість для самоосвіти на платформі «Prometheus» <http://surl.li/uwbnwa>. НАУ 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. НАУ 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/ejzsn>, участі у міжнародному освітньому проєкті з кібербезпеки <http://surl.li/aghlpz>, участь у REX IT FES <http://surl.li/cjxae>, у змаганнях з кібербезпеки <http://surl.li/tcmtbp>, відвідування виставки з кібербезпеки <http://surl.li/cjfvfn>, участь у JOB EXPO <http://surl.li/ajtkor>. 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 БЖД, правил поведінки напередодні канікул та свят, що засвідчується листами ознайомлення, правил поведінки в умовах повітряної тривоги. Щорічно в НАУ проводяться навчальні заходи з цивільної оборони та пожежної безпеки, надання домедичної допомоги. На годинах корпоративної культури проводяться бесіди з профілактики недопущення правопорушень у студентському середовищі, консультації з правил етичного кодексу в НАУ. Необхідну допомогу за потреби можуть надати професійні психологи-практики ФЛІСК НАУ. Функціонують Відділ безпекової діяльності, Авіаційний медичний центр, у відділі по роботі зі студентами функціонує сектор психолого-педагогічної роботи <http://bit.ly/411jOa8>, що здійснює організацію, діагностику і тренінгові заняття просвітницької та профілактичної роботи, розробляє заходи щодо профілактики булінгу. Введено в дію Положення про запобігання та протидію булінгу, мобінгу, кібербулінгу, харасменту в НАУ <https://bit.ly/3B86qV5>. Для співробітників проводяться тренування щодо дій у разі оголошення сигналу «Повітряна тривога» (<https://bit.ly/3Cw3R1q>). Всі здобувачі та співробітники ознайомлені з Інструкцією щодо дій персоналу Національного авіаційного університету у разі виникнення надзвичайних ситуацій, затвердженою наказом ректора № 222/од від 26.07.2022 та Алгоритмом дій за сигналом цивільного захисту «Повітряна тривога», затвердженим наказом ректора №310/од від 29.08.2023 (<http://surl.li/qdzbc>).

### **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 НАУ (<https://nau.edu.ua/>), факультету (<https://fcst.nau.edu.ua/>) та кафедри <http://kszi.nau.edu.ua/>

), а також посилання на сайти усіх підрозділів університету. Механізми освітньої, організаційної, інформаційної, консультативної та соціальної підтримки здобувачів вищої освіти реалізуються в системі кафедра-факультету-університет. Освітня підтримка сконцентрована в межах кафедри та розподілена за функціями серед НПП навчальних дисциплін, 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, проректор з гуманітарної політики та інновацій, відділ по роботі зі студентами (<http://surl.li/eittx>)). Інформаційна підтримка забезпечується через офіційні канали розповсюдження інформації – сайт університету, факультету, кафедри, корпоративну пошту НАУ, класи по дисциплінам у Google Suite Classroom, репозиторій НАУ, он-лайн бібліотеку НАУ, електронні джерела інформації кафедри. Консультативну підтримку забезпечують наставники академічних груп (<http://kszi.nau.edu.ua/vikhovna-robita-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 аналізу студентських Telegram-каналів. Результати опитування здобувачів викладаються на сайті НАУ (<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 формує перелік зауважень та проблем і впроваджує шляхи їх усунення (<http://surl.li/lximna>).

### **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 НАУ створено достатні умови щодо реалізації права на освіту для осіб з особливими освітніми потребами <https://nau.edu.ua/ua/menu/quality/inklyuzivna-osvita/> на основі: «Концепції організації інклюзивного навчання в НАУ» (<https://cutt.ly/kCZlv9L>). Для організації безбар'єрного доступу до будівель та приміщень в НАУ 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/dmxxvw>). 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 НАУ, 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 НАУ базується на принципах дотримання демократичних цінностей, свободи, справедливості, рівності прав і можливостей, толерантності, недискримінації, відкритості та прозорості. В НАУ 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 НАУ регулюється Положенням про запобігання та протидію булінгу, мобінгу, кібербулінгу, харасменту в НАУ (<https://bit.ly/3EWndwT>); Положенням про Раду з гуманітарних питань НАУ та Положенням про комісію з правопорушень НАУ. В НАУ організовано Відділ з питань запобігання та виявлення корупції <https://bit.ly/3Lmf86M>, який діє відповідно до Антикорупційної програми НАУ <https://bit.ly/3EcJgQX>, спрямованої на розвиток чесності, добросовісності, прозорості та відкритості надання освітніх послуг. Для розгляду справ пов'язаних з корупцією функціонує Комісія з оцінки корупційних ризиків НАУ <https://bit.ly/3NELozP>. Повідомити про правопорушення чи написати скаргу можливо на електронну скриньку довіри <https://bit.ly/3C4IOkT>, або на скриньку довіри у першому корпусі НАУ. 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 ОП в НАУ відбувається у відповідності до "Положення про освітні програми Національного авіаційного університету" (<https://bit.ly/3oGU2DO>), 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 ціллю удосконалення як окремих компонент ОП

так і всієї програми. Моніторинг здійснюється раз на рік з урахуванням конкурсних показників та результатів навчання (<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 систему забезпечення якості вищої освіти та освітньої діяльності НАУ» (<https://bit.ly/3nkkq5j>) та "Положення про освітні програми НАУ" (<https://bit.ly/3oGU2DO>). На основі затвердженого стандарту вищої освіти за спеціальністю 125 «Кібербезпека» (від 18.03.2021р.), здійснено розробку нової редакції ОП. Нова редакція затверджена Вченою радою НАУ та введена наказом ректора №246/од від 29.07.2021р. У 2022 році згідно з наказом т.в.о. ректора № 063/од від 09.02.2022 р. «Про щорічний перегляд освітньо-професійних програм» був проведений перегляд освітньо-професійної програми «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти за спеціальністю 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 та введена наказом ректора №069/од від 23.02.2023р.

З врахуванням пропозицій стейкхолдерів та академічної спільноти у 2024 році було розроблено нову редакцію ОП (<http://surl.li/xegqtn>, <http://surl.li/qxoixe>). Основними пропозиціями та зауваженнями представників заінтересованих сторін в результаті обговорення ОП у 2024 році були наступні: зміна складу стейкхолдерів з метою підкреслити унікальність ОП; внести коригування в п. 2.1. ціль освітньо-професійної програми, а саме врахувати авіаційну складову при підготовці здобувачів; внести в п.3.3. освітньої програми фокус ОП; Внести в п. 3.4. освітньої програми відмінність, а саме особливість програми. Нова редакція затверджена Вченою радою НАУ та введена наказом ректора №166/од від 23.04.2024р., 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 році відтермінована у зв'язку з реорганізацією Національного авіаційного університету.

### **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 погоджено Студентською радою факультету протокол №24/3-п від 20.03.2024 р.). Здобувачі входять до складу Вченої ради факультету та Вченої ради НАУ. Здобувачі також беруть участь у процесі перегляду ОП: під час анонімного онлайн-опитування (<https://nau.edu.ua/ua/menu/quality/otsinyuvannya-rezultativ-yakosti-navchannya/>); - висловлюючи свої пропозиції викладачам та під час зустрічей з кураторами; через студентське самоврядування (<http://surl.li/bdqag>), 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 вибіркового дисциплін, наприклад здобувачі приймали участь у круглому столі щодо обговорення ОП (<http://surl.li/zjqnqu>) та розширених засіданнях кафедри (<http://surl.li/zwvnm>). Опитування на кафедральному рівні відображено на (<http://surl.li/bfwnc>) Студенти також можуть взяти участь в публічному обговоренні проєктів освітніх програм на сайті НАУ (<http://surl.li/saocik>, <http://surl.li/ljmrqg>)

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

Вирішальна роль у процесах функціонування внутрішньої системи забезпечення якості освітньої діяльності (ВСЗЯ) НАУ, належить студентському самоврядуванню (<https://bit.ly/3pVVJOo>), діяльність якого впливає на основні освітні, фінансово-господарські та інші процеси НАУ. Залучення здобувачів до участі в усіх видах діяльності ВСЗЯ НАУ 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; - висловлюючи пропозиції викладачам та через кураторів; - 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 НАУ (<http://surl.li/saocik>, <http://surl.li/ljmrqg>)

### **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 НАУ; 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; стейкхолдери, які беруть участь в ЕК, дають оцінку якості кваліфікаційних робіт та висловлюють свої побажання щодо покращення освітнього процесу за ОП; відгуки від стейкхолдерів та пропозиції щодо якості ОП висловлюють переважно усно. Задля забезпечення якості підготовки здобувачів другого (магістерського) рівня вищої освіти та у рамках підписаних договорів з потенційними роботодавцями (<http://kszi.nau.edu.ua/stejkholderi>) студенти мають можливість проходити практику у виробничому середовищі (<http://surl.li/bbympv>) та приймати участь у освітніх онлайн-вебінарах у рамках проекту проекту USAID «Кибербезпека критично важливої інфраструктури України» (<http://surl.li/ubezob>). Приклади залучення роботодавців до перегляду ОП <http://surl.li/tgiipf>, <http://surl.li/zcmhyd> та <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/cjxae>), 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/hnwwol>) щорічно в НАУ проводяться заходи: «Час авіаційної кар'єри», «Злітна смуга», «Ярмарок вакансій», «День кар'єри», «Освіта та кар'єра 20 XX» та ін., де випускники можуть отримати інформацію від роботодавців щодо вакансій, а НАУ 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 найкращими 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 (<http://kszi.nau.edu.ua/osvitnij-protses/monitoring-pratsevlashtuvannya>).

### **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 НАУ 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 Національного авіаційного університету" <https://bit.ly/3V6cTzG>.

21 березня 2024 року тоді ще кафедра комп'ютеризованих систем захисту інформації Факультету кібербезпеки та програмної інженерії, де реалізовувалась дана ОП, успішно пройшла внутрішній аудит, що відбувався згідно наказу ректора від 12.09.2023 №334/од (<http://surl.li/tmyvrr>). В процесі проведення аудиту були визначені сильні сторони кафедри та визначені можливості щодо поліпшення роботи. Виявлені невідповідності і коригувальні дії були занесені в "Журнал обліку невідповідностей, коригувальних і запобіжних дій". Керівником групи аудиту на основі відповідних документів проведена оцінка результативності виконання коригувальних дій кафедри. Коригувальні дії визнані достатніми.

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

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 наведені в таблиці 2 (<http://surl.li/xczsjg>, <http://surl.li/yiuesd>).
2. В процесі перегляду ОП кожного року роботодавці та здобувачі освіти залучались до її обговорення (<http://surl.li/uwxnmp>), (<http://surl.li/cjzvs>), (<http://surl.li/eqzsr>).
4. Розширено коло співпраці з партнерами кафедри, а саме заключено нові угоди для проведення практик та

- підвищення кваліфікації НПП (<http://kszi.nau.edu.ua/stejjkholderi>)  
5. Проводилося анкетування здобувачів освіти (<http://surl.li/ozkjur>).  
6. Оновлені переліки вибіркових компонентів ОП (<http://surl.li/rwqeeek>).

### **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 НАУ. Укладаються договори з підприємствами – базами практик (<https://bit.ly/3ovezOl>). Здобувачі вищої освіти регулярно ознайомлюються з організацією виробничих процесів в компаніях потенційних роботодавців (<http://kszi.nau.edu.ua/stejjkholderi>). На кафедрі нарощується база даних установ, підприємств, організацій – потенційних роботодавців. Засідання кафедр та Вчених рад факультетів та НАУ 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 рішенням Вченої ради НАУ (протокол №8 від 27.11.2019 р.) схвалено створення Ради з якості НАУ (<https://bit.ly/38p2jHz>) як колегіальнодорадчого органу, який координує діяльність підрозділів університету, спрямовану 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 НАУ – 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 Національного авіаційного університету" (<https://bit.ly/3mrg6ciA>) організація внутрішнього забезпечення якості вищої освіти в НАУ здійснюється на п'яти рівнях. На першому рівні здійснюються соціологічні опитування здобувачів вищої освіти. Другий рівень організації системи внутрішнього забезпечення якості вищої освіти в НАУ здійснюється викладачами кафедри при безпосередньому керівництві гаранта освітньої програми та завідувача кафедри. Третій рівень організації системи внутрішнього забезпечення якості вищої освіти у НАУ реалізується на факультеті під безпосереднім керівництвом декана. На четвертому рівні системи внутрішнього забезпечення якості вищої освіти у НАУ 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. На п'ятому рівні системи внутрішнього забезпечення якості вищої освіти в НАУ діяльність Наглядової ради, Вченої Ради, ректора спрямовані на постійне покращення здатності Університету виконувати вимоги усіх зацікавлених сторін до якості вищої освіти на основі результатів вивчення задоволеності її якістю випускників Університету 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 НАУ чітко прописані правила і процедури, що регулюють права і обов'язки всіх учасників освітнього процесу, розміщені у відкритому доступі: Статут університету (<https://bit.ly/3lCt4Vo>); Правила внутрішнього трудового розпорядку (<https://bit.ly/3rGLqBP>); Положення про організацію освітнього процесу (<https://bit.ly/3gzhe4Q>); Положення про виявлення та запобігання академічному плагіату (<https://bit.ly/3gu1OPG>); Положення про організацію та проведення поточного і семестрового контролю (<https://bit.ly/3gsueJw>); Положення про запобігання та протидію булінгу, мобінгу, харасменту (<http://surl.li/bdviq>) тощо.

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

Посилання на веб-сторінку ЗВО з проектами нормативних документів, освітніх програм (<https://bit.ly/3Z4UCNY>) та перегляд ОП на сайті кафедри (<http://surl.li/zmaakd>), (<http://surl.li/vjrfha>), (<http://surl.li/kuuwfv>).

### **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 веб-сайті НАУ своєчасно оприлюднено інформацію щодо освітньо-професійну програму «Безпека інформаційних і комунікаційних систем» (<https://bit.ly/3Kh9STH>) та сайті кафедри кібербезпеки (<http://surl.li/rbmudd>). Також на офіційному сайті НАУ розміщена вкладка «Забезпечення якості світи», яку в свою чергу розділено на Проекти нормативних документів (<https://cutt.ly/2RDT4OO>) та Проекти

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>), порядок формування індивідуальної освітньої траєкторії (<http://surl.li/hcrfqs>). 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: ОП реалізується в НАУ, 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 підкреслення унікальності освітньої програми та залучення здобувачів до перегляду/актуалізації освітньої програми. Регулярно, щорічно проводиться анкетування здобувачів вищої освіти щодо якості організації навчального процесу ОП, що відображається в протоколах кафедри та на сайті кафедри. 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 та можуть бути впроваджені у виробничий процес; в роботах використовується сучасне програмне забезпечення, методи та засоби захисту інформації, всі роботи відповідають профілю підготовки. 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-педагогічних працівників до участі у вебінарах від проєкту USAID. Налагоджена система кадрового забезпечення: у 2019 р. на кафедрі захищено 1 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 2023 р. доцент Висоцька О.О. отримали сертифікат про володіння іноземною мовою на рівні B2; 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 адаптивного карантину та 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 ОП «Безпека інформаційних і комунікаційних систем» слід віднести: 1). постійний моніторинг результатів наукових досліджень та розвитку новітніх технологій у сфері кібербезпеки та захисту інформації; 2) щорічний перегляд та оновлення навчальних планів і робочих програм дисциплін професійної підготовки та вибіркових дисциплін з метою приведення їх складу і змісту у відповідність до науково-технологічного досягнень та поточних потреб суспільства; 3) залучення до навчального процесу провідних фахівців ІТ-компаній (підприємств) та розширення бази роботодавців з метою здійснення практичної підготовки здобувачів, стажування провідних НПП та подальший розвиток співпраці з провідними підприємствами в авіаційній галузі для посилення авіаційної складової ОП; 4) підвищення наукового потенціалу кафедри шляхом збільшення публікацій результатів наукових досліджень у виданнях, що входять до визнаних науково-метричних баз даних, зокрема Scopus та Web of Science; 5) систематичне підвищення кваліфікації викладачів кафедри в провідних ІТ-компаніях в сфері захисту інформації та шляхом участі у міжнародних проєктах; 6) розвиток міжнародної співпраці кафедри шляхом налагодження відносин з закордонними освітніми та науковими установами з метою співробітництва у галузі освіти та наукових досліджень; з метою співробітництва у галузі освіти та наукових досліджень, активізації отримання викладачами кафедри сертифікатів з мовної освіти рівня B2, участі в організації та проведенні міжнародних науково-практичних конференцій в Україні та за кордоном; 7) подальше вдосконалення навчально-методичного забезпечення дисциплін; 8) залучення здобувачів до виконання науково-дослідних робіт кафедри у напрямках реалізації захищених інформаційних систем та мереж.

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: 09.10.2024 р.



**Таблиця 1.** Інформація про освітні компоненти ОП

Назва освітнього компонента	Вид освітнього компонента	Силабус або інші навчально-методичні матеріали		Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього*
		Назва файла	Хеш файла	
ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	практика	<i>Науково-дослідна практика_2021 (актуалізація 2023).pdf</i>	UvRJeb8SbSqxruru79ZhQpoc9CEBU3isE meV16dqipo=	<i>В залежності від бази практики</i>
ОК12.Переддипломна практика	практика	<i>Переддипломна практика_2021 (актуалізація 2023).pdf</i>	WjVJjQJWesX47CHBoCc5oIBSLSauJSaCq5BH5C3kX4I=	<i>В залежності від бази практики та від теми кваліфікаційної роботи</i>
ОК13.Кваліфікаційна робота	підсумкова атестація	<i>Положення про кваліфікаційні роботи здобувачів ВО НАУ_compressed (1).pdf</i>	nRLlusJSiOuU8EggyHupTUCNuXYUObW/qiPwNV9VqVs=	<i>Залежно від теми кваліфікаційної роботи</i>
ОК4.Курсовий проект з дисципліни <i>Методологія прикладних досліджень у сфері кібербезпеки</i>	курсорова робота (проект)	<i>КП_Методологія прикладних досліджень у сфері кібербезпеки.pdf</i>	rpBWoi9rQthhuq+/eSxFX8mixt46StpTCV F0+C24mOo=	<i>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)</i>
ОК1.Ділова іноземна мова	навчальна дисципліна	<i>РП Ділова іноземна мова.pdf</i>	uH1vwDk06zAy5331Z2dQzvnltgJPJeZ5Jir16iSldVw=	<i>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)</i>
ОК2.Наукові комунікації у фаховій діяльності	навчальна дисципліна	<i>РП_Наук комунікації у фаховій діяльності.pdf</i>	baccs8uUXvK7FNoiUIu4CvVmfVabnd6Nw5WEJH1LXVM=	<i>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)</i>
ОК3.Методологія прикладних досліджень у сфері кібербезпеки	навчальна дисципліна	<i>РПП_Методологія прикладних досліджень у сфері кібербезпеки.pdf</i>	qzBxXnsU7jFl4c/hALCRY8F6tZnHItTo86Orc3pP5oo=	<i>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)</i>
ОК5.Методи побудови та аналізу криптосистем	навчальна дисципліна	<i>РПП_Методи побудови та аналізу криптосистем.pdf</i>	OoIfOA7G1ELECsituLpDuDpWpQPPLAAjN/ddCzf5Oew=	<i>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); MS Visual Studio Community</i>
ОК6.Моделювання та оптимізація безпечових процесів	навчальна дисципліна	<i>РП_Моделювання та оптимізація безпекових-</i>	FIDJ2rpm4JxgMUIdM3GVSPft72wgrfvY OwZF55U4oM=	<i>Мультимедійний комплекс (ноутбук, проектор, екран), доступ до мережі інтернет.</i>

авіаційної галузі		<i>процесів(2023).pdf</i>		Програмне забезпечення: ліценз. Google GSuite for Education (Google Classroom, Google Meet, Google форми / документи / таблиці / презентації); лабораторне обладнання
ОК7.Моніторинг та аудит кібербезпеки	навчальна дисципліна	<i>РП Моніторинг та аудит кібербезпеки.pdf</i>	66lTz3WVm9caF1vZHZVbLLVovB2sDiUuRTMyDBv44HE=	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)
ОК8.Захист комунікаційних мереж засобами Cisco	навчальна дисципліна	<i>РП Захист комунікац мереж засобами CISCO.pdf</i>	NNzowUO3z3s9bM+RNc5cEnjM6WEuw8W7lQuJp8A96tyo=	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); Packet Tracer
ОК9.Технології створення та застосування систем захисту кіберпростору	навчальна дисципліна	<i>РНП Технолог створ та застосув КБ (актуалізована).pdf</i>	UOTAGsmKMqKfvW MiN3uB9uknY4FN3xSXCsxTcDKok8=	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)
ОК10Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	курсорова робота (проект)	<i>КР Технології створення та застосування систем захисту кіберпростору.pdf</i>	6ciuk2kbsYIYuLvZoUgb//yHMZEahub3ggbr1vdqRY=	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)

\* 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

<b>ID викладача</b>	<b>ПІБ</b>	<b>Посада</b>	<b>Структурний підрозділ</b>	<b>Кваліфікація викладача</b>	<b>Стаж</b>	<b>Навчальні дисципліни, що їх викладає викладач на ОП</b>	<b>Обґрунтування відповідності освітньому компоненту (кваліфікація, професійний досвід, наукові публікації)</b>
78328	Шульга Тетяна Валеріївна	Старший викладач (0,75 ставки), Основне місце роботи	Факультет лінгвістики та соціальних комунікацій	Диплом спеціаліста, Київський державний лінгвістичний університет, рік закінчення: 2000, спеціальність: 030502 Мова та література (англійська мова). Психологія	23	ОК1.Ділова іноземна мова	Освіта: Київський державний лінгвістичний університет, 2000 р., спеціальність – «Мова та література (англійська мова). Психологія», кваліфікація – «філолог, викладач англійської мови та зарубіжної літератури, практичний психолог» Аспірантура Інституту психології ім. Г.С.Костюка АПН України,

спеціальність:  
19.00.01 “Загальна психологія, історія психології”. Тема “Психологічні особливості наративної самопрезентації особистості”, 2009р.

Підвищення кваліфікації:  
1. Українсько-Польський вищий навчальний заклад Центрально-Європейський університет, кафедра романо-германської філології. Термін 02.10.23-30.11.2023р. Тема: «Лінгвістичні та методологічні аспекти викладання іноземних мов». Довідка про стажування № 428 від 01.12.2023. (6 кредитів ЄКТС).

2. Українсько-Польський вищий навчальний заклад Центрально-Європейський університет, кафедра романо-германської філології. Термін 21.10.19-20.11.19 р. Тема: «Лінгвістичні та методологічні аспекти викладання іноземних мов». Довідка про стажування № 1170 від 21.11.2019.

3. Оксфордський захід з професійного розвитку ELTOS , Онлайн-конференція з викладання англійської мови, Oxford University Press. Тема підвищення кваліфікації: “Playful pathways: the power of learning through play for all ages. Multimodal literacy in ELT. Developing contemporary communication skills. Empower your students for exam success”. Термін 25.04.24. Сертифікат (0.13 кредитів ЄКТС).

4. Оксфордський захід з професійного розвитку ELTOS , Онлайн-конференція з викладання англійської мови, Oxford University Press. Тема підвищення кваліфікації: “Technology and creativity: preparing yourself for the future classroom». «Transition skills in

Higher Education». «Pronunciation priorities for the global English classroom», Термін 26.04.24. Сертифікат (0.13 кредитів ЄКТС)  
5. Оксфордський захід з професійного розвитку ELTOS, Онлайн-конференція з викладання англійської мови, Oxford University Press. Тема підвищення кваліфікації: “Building bridges: intercultural competence and citizenship”. “Language teachers unite”. “Discovering the melody in spoken English”. Термін 27.04.24. Сертифікат (0.13 кредитів ЄКТС)

Види і результати професійної діяльності 1, 3, 4, 8, 12

п. 1  
1. Budko L.V., Maksymovych G.O., Shulga T.V. Content and language integrated learning model in teaching a foreign language in a non-language university // Інноваційна педагогіка. – 2024. Вип. № 67. Т.1. С.127-131. (фахове видання категорії В)  
2. Denysenko N.H., Maksymovych G.O., Shulga T.V. Distance learning technologies in teaching a foreign language. // Інноваційна педагогіка. – 2023. Вип. №58. Т.1. С.211-214. (фахове видання категорії В)  
3. Maksymovych G. O., Shulga T.V., Yurchenko S.O. On the importance of civil aviation staff's auditory competence in the context of flight safety. // Інноваційна педагогіка. – 2022. Вип. 48. Том 2. С.154-158. (фахове видання категорії В)  
3. Maksymovych G.O., Shulga T.V., Yurchenko S.O. Language competence as an underlying factor of flight safety culture. // Інноваційна педагогіка. – 2021. Вип. №35. С.150-156. (фахове видання категорії В)  
4. Максимович Г.О., Кодола Р.М., Шульга Т.В. Подолання

мовного бар'єру  
льотного і  
диспетчерського  
складу у стресових  
ситуаціях.  
Інноваційна  
педагогіка. – 2020. –  
№28. – С.184-187.  
(фахове видання  
категорії В)  
5. Kresan O.D., Shulga  
T.V. Reflection of a  
personality's experience  
and perception of life  
events in oral and  
written narrations.  
Danish Scientific  
Journal. – 2019. –  
Vol.2. – №22. P. 72-74.

п.3  
1. Акмалдінова О.М.,  
Кравчук О.Ю.,  
Максимович Г.О.,  
Шульга Т.В.  
Professional English.  
Automated Control  
Systems: Навчальний  
посібник. –К.: НАУ,  
2019. – 200 с. ISBN  
978-966-932-020-9

п. 4  
1. Акмалдінова О.М.,  
Максимович Г.О.,  
Шульга Т.В.  
Professional English.  
Electricity. Electric  
Power System:  
практикум для  
здобувачів вищої  
освіти ОС «Бакалавр»  
спеціальності 141  
«Електроенергетика,  
електротехніка та  
електромеханіка». –  
К.: НАУ, 2024. 80с.  
2. Акмалдінова О.М.,  
Максимович Г.О.,  
Шульга Т.В.  
Professional English.  
Concept of Energy.  
Mechanical  
Engineering :  
практикум для  
здобувачів вищої  
освіти ОС «Бакалавр»  
спеціальності 142  
«Енергетичне  
машинобудування». –  
К. : НАУ, 2022. – 85с.  
3. Акмалдінова О.М.,  
Будко Л.В., Шульга  
Т.В. Professional  
English. Fundamentals  
of helicopter design:  
практикум для  
здобувачів вищої  
освіти ОС «Бакалавр»  
спеціальності 134  
«Авіаційна та ракетно-  
космічна техніка». –  
К.: НАУ, 2021. – 68с.  
4. Акмалдінова О.М.,  
Максимович Г.О.,  
Шульга Т.В.  
Professional English.  
Energy saving.  
Практикум для  
студентів  
спеціальності 141

«Електроенергетика, електротехніка та електромеханіка». – К.: НАУ, 2020. – 80с.

п. 8

8.1.НДР «Теоретико-прикладні лінгвістичні, перекладознавчі та методологічні аспекти викладання іноземних мов професійного спрямування: новітні тенденції і виклики інноваційних форм навчання». Термін виконання - 24.01.2022 - 30.12.2024р. (виконавець)

п.12.

12.1. Шульга Т.В. Використання СНАТГРТ у навчанні іноземної мови: виклики та перспективи // Лінгвістичні та методологічні аспекти викладання іноземних мов професійного спрямування: V Міжнародна науково-практична конференція, 28-29 березня 2024 р.: тези доповіді. – К., 2024. – С. 91-92. (матеріали Міжнародної конференції)

12.2. Шульга.Т. Podcasting in teaching english for specific purposes // Лінгвістичні та методологічні аспекти викладання іноземних мов професійного спрямування: IV Міжнародна науково-практична конференція, 29-30.05.2023 р.: тези доповіді. – К., 2023 – С.51-52. (матеріали Міжнародної конференції)

12.3. Shulga T.V. Language training of aviation specialists within a content-oriented approach. / Maksymovych G.O., Shulga T.V.// Aviation in the XXI-st century: the 10th World Congress, September 28-30, 2022: abstracts.– К., 2022. – Режим доступу: <https://conference.nau.edu.ua/index.php/Congress/Congress2022/paper/viewFile/8586/7178> (матеріали Міжнародної конференції)

12.4. Шульга Т.В.

							<p>Змішане навчання інозем-ної мови у ВНЗ: виклики та перспективи //Лінгвістичні та методологічні аспекти викладання іноземних мов професійного спрямування: III міжнародна науково-практична конференція, 31 березня 2021р.: тези доповіді. – К., 2021. – С.55-56. (матеріали Міжнародної конференції)</p> <p>12.5. Шульга Т.В. New strategies of teaching Aviation English within competency-based approach // Лінгвістичні та методологічні аспекти викладання іноземних мов професійного спрямування: II міжнародна науково-практична конференція, 25-26 березня 2020р.: тези доповіді. – К., 2020. – С. 79-80. (матеріали Міжнародної конференції)</p> <p>12.6. Шульга Т.В. Особливості компетентнісного підходу у сучасній освіті// Лінгвістичні та методологічні аспекти викладання іноземних мов професійного спрямування: I міжнародна науково-практична конференція, 20 березня 2019 р.: тези доповіді. – К., 2019. – С. 83. (матеріали Міжнародної конференції)</p> <p>12.7. Шульга Т.В. Нове покоління авіаційних спеціалістів (NGAP): особливості мовної підготовки / Акмалдінова О.М., Будко Л.В., Шульга Т.В. // Актуальні проблеми іншомовної підготовки фахівців у сфері національної безпеки: міжвузівська науково-методична конференція, 16 квітня 2019 р.: тези доповіді. – К., 2019. – С. 5-7. (матеріали конференції)</p>
52366	Толупа Сергій Васильович	Професор (0,5 ставки), Сумісництво	Факультет комп'ютерних наук та технологій	Диплом спеціаліста, Київське вище інженерне радіотехнічне училище ППО, рік закінчення: 1986, спеціальність:	16	ОК9.Технології створення та застосування систем захисту кіберпростору	Освіта: Київське вище інженерне радіотехнічне училище ППО ім. Pokришкіна А.І., 1986р., спеціальність - автоматизовані системи управління, кваліфікація - інженер

Автоматизован  
і системи  
управління,  
Диплом  
доктора наук  
ДД 000091,  
виданий  
10.11.2011,  
Диплом  
кандидата наук  
КН 012091,  
виданий  
10.12.1996,  
Атестат  
доцента ДЦ  
005016,  
виданий  
20.06.2002,  
Атестат  
професора  
12ПР 008351,  
виданий  
25.01.2013

електронної техніки.  
Науковий ступінь:  
Доктор технічних наук  
05.12.02 -  
Телекомунікаційні  
системи та мережі,  
тема дисертації  
«Дослідження  
функціонування  
інфокомунікаційних  
мереж нового  
покоління на основі  
інтелектуальних  
технологій».  
Вчене звання:  
професор кафедри  
безпеки  
інформаційних  
технологій.  
Підвищення  
кваліфікації:  
1. ТОВ «ДЕПС  
СЕЛЮШЕНЗ».  
Сертифікат про  
підвищення  
кваліфікації серія DP  
№000131 від  
31.12.2020р.  
2. Certificate of  
completion Incident  
response within the  
2021 Cybersecurity  
Summer Training  
Program under the  
USAID Project.  
3. Навчання на курсах  
USAID Project “  
Cybersecurity for  
Critical Infrastructure  
in Ukraine” (за  
програмою «Malware  
Analysis») 18 October –  
1 December 2021.  
4. Навчання на курсах  
USAID Project "Audit  
and Risk Management"  
within the 2022  
Cybersecurity Summer  
Instructor Training  
Program under the  
USAID Cybersecurity  
for Critical  
Infrastructure in  
Ukraine Activity. 11 July  
– 31 August 2022.  
5. Стажування  
Державний НДІ  
технологій  
кібербезпеки та  
захисту інформації 6  
кредитів 180 годин з  
22.01.2024 по  
05.04.2024р.  
Сертифікат.

Навчальні посібники  
та монографії:  
1. Толюпа С.В., Бучик  
С.С., Лукова-Чуйко  
Н.В., Фесенко А.О.  
Системи технічного  
захисту інформації. .  
Навчальний посібник.  
- К.: Формат, 2022. –  
386 с.  
2. Толюпа С.В.,  
Браіловський М.М.,  
Наконечний В.С.,  
Сайко В.Г.  
Мікропроцесорні  
системи на



мікроконтролерах.  
Навчальний посібник.  
– К: КНУ імені Тараса  
Шевченка, 2022. – с.  
298.

3. Толюпа С.В.,  
Політанський Р.Л.,  
Лісінський В.В.  
Управління інформа-  
ційною безпекою.  
Навчальний посібник.  
За заг. ред. Толюпи  
С.В. – Чернів-ці. ЧНУ  
імені Юрія Федь-  
ковича. 2021р. – с.  
486.

4. Лукова-Чуйко Н.В.  
Системи виявлення  
вторгнень та  
функціональна  
стійкість розподілених  
інформаційних систем  
до кібернетичних  
загроз. // Н.В.  
Лукова-Чуйко, В.С.  
Наконечний, Толюпа  
С.В., М.М.

Браїловський //  
Монографія К.:  
Формат, 2021. – 407 с.

5. Наконечний В.С.  
Методи та засоби  
підвищення  
ефективності  
функціонування  
радіотехнічних систем  
розпізнавання  
багатопозиційного  
базування. / В.С.  
Наконечний, С.В.  
Толюпа, В.А.  
Дружинін, Н.В.  
Лукова-Чуйко. //  
Монографія. Київ. -  
К.: Формат. 2019. –  
237 с.

6. Толюпа С.В.,  
Штаненко С.С.,  
Османов Р.Н. Методи  
та засоби захисту  
інформації в  
кіберпросторі.  
Навчальний посібник.  
За заг. ред. С.В.  
Толюпи. – К.: ВІТІ.  
2024р. – С. 335.

7. Бучик С.С., Толюпа  
С.В., Шестак Я.В.  
Програмні технології  
програмування в  
інформаційній  
безпеці. Лабораторний  
практикум. –  
Житомир: ФОП  
Кирилюк І.В., ПП  
«Рута», 2023. – 50с.

Публікації за  
тематикою  
дисципліни:

1. Штаненко С.С.,  
Самохвалов Ю.Я.,  
Толюпа С.В. Підхід до  
виявлення помилок та  
відновлення  
правильного  
функціонування  
програмних засобів  
сучасних систем  
управління,

реалізованих за принципом «система на кристалі».  
Наукоємні технології.  
– К.: НАУ, 2023. – № 2 (58). – с. 376-384.  
<https://doi.org/10.18372/2310-5461.58.17655>.

2. Мостовий В.С., Толюпа С.В., Шевченко А.М.  
Optimization of the dynamic parameters of an object in a mathematical model of seismo-acoustic monitoring of natural and engineering objects. Наукоємні технології. – К.: НАУ, 2023. – № 2 (58). – С. 412-422.  
<https://doi.org/10.18372/2310-5461.58.17647>.

3. Штаненко С. С., Самохвалов Ю. Я., Толюпа С. В.  
Методичний підхід до відновлення правильного функціонування вбудованих систем на рівні програмованої елементної бази. Системи і технології зв'язку, інформатизації та кібербезпеки. ВІТІ № 3 – 2023. С.171-181.  
<https://doi.org/10.58254/viti.3.2023.19.171>.

4. Толюпа С.В., Бучик С.С., Лукова-Чуйко Н.В., Штаненко С.С.  
Математична модель проектних відносин загроз та множин системи захисту інформаційної мережі. Вісник університету «Україна» «Інфокомунікаційні та комп'ютерні технології». №1(03), 2022. С. 121-132.  
<https://visn-icct.uu.edu.ua/index.php/icct/article/view/79>

5. S. Toliupa, S. Laptiev.  
The methodology for evaluating the functional stability of the protection system of special networks. Наукоємні технології. – К.: НАУ, 2022. – № 3. – С 130-142.  
<https://jrn1.nau.edu.ua/index.php/SBT/article/view/16900>

6. Толюпа С.В., Штаненко С.С.)  
Методика проектування роботизованих систем в базі САПР INTEL QUARTUS PRIME. Збірник наукових праць Військового інституту

телекомунікацій та інформатизації імені Героїв Крут Випуск № 1. 2021р. с. 56-66.

7. Сергій Толюпа, Іван Пархоменко, Людмила Терейковська, Володимир Квасніков Побудова систем виявлення кібератак за допомогою прихованої марківської моделі. Науковий журнал НУ "Чернігівська політехніка" Технічні науки та технології, 2021. №1(23) – с. 89-96.

8. С. Толюпа, І. Пархоменко, С. Штаненко. Модель системи протидії вторгненням в інформаційних системах. Інфокомунікаційні технології та електронна інженерія. №1. 2021. С. 86-95.

9. Лукова-Чуйко Н.В., Толюпа С.В., Погасій С.С., Лаптева Т.О., Лаптев С.О. Удосконалення моделі захисту інформації в соціальних мережах. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К.: ВІКНУ, Вип. 73, 2021. С. 88 – 103.

10. Толюпа С.В., Наконечний В.С., Штаненко С.С. Алгоритм протидії кібератакам на основі стеганографічних методів технології SOFT TEMPEST. Збірник наукових праць Військового інституту телекомунікацій та інформатизації імені Героїв Крут Випуск № 1. 2020р. с. 56-66.

11. S. Toliupa, V. Nakonechnyi A. Trush. To increase the energy efficiency of radio equipment based on the use of modulation by orthogonal harmonic carriers. Automatyka, Pomiaru w Gospodarce i Ochronie Środowiska IAPGOŚ 2020; 9 (1): 24-27. Google Scholar. Poland.

12. Толюпа С.В., Наконечний В.С. Проблеми захисту критично важливих об'єктів інфраструктури Безпека

інформаційних систем і технологій. Том 1 № 2 (2020). с. 57-65

13. Serhii Toliupa , Oleksandr Pliushch , Ivan Parkhomenko. Побудова систем виявлення атак в інформаційних мережах на нейромережових структурах. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка" том 2 №10. 2020. с. 169-183.

14. Толупа С. В., Пархоменко І. І., Кириленко А. І., Вадис К. А. «Захист корпоративної інформації на мобільних пристроях.», Збірник наукових праць «Моделювання та інформаційні системи в економіці», КНЕУ, 2020. №99 – С. 151 – 161.  
<https://ir.kneu.edu.ua:443/handle/2010/35488>

15. Толупа С. В., Одарченко Р. С., Пархоменко І. І., Даков С.Ю. «Виявлення атак в корпоративній мережі за допомогою правил нечіткої логіки», Науковий журнал. – К.: НАУ, 2020. – № 4 (48). – С 470-477.  
DOI: 10.18372/2310-5461.48.15125

16. Толупа С.В., Плющ О.Г., Пархоменко І.І. «Побудова систем виявлення вторгнень в інформаційно-телекомунікаційну мережу на основі методів інтелектуального розподілу даних», Збірник наукових праць «Військового інституту Київського національного університету імені Тараса Шевченка.», К.: ВІКНУ, 2020. № 68 - С. 80-89.  
<https://doi.org/10.17721/2519-481X/2020/68-09>

#### SCOPUS

1. L. A. Komarova, V. G. Saiko, V. S. Nakonechnyi, S. V. Toliupa, R. V. Ziubina. Quality Assurance of Data Transmission in Queuing Networks. International Journal of Engineering and Advanced Technology

(IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-2, December, 2019. Scopus.

2. Pliushch, O., Toliupa, S., Vyshnivskiy, V., Rybydajlo, A. Book Chapter. Springer International Publishing (Verlag). Studying of Useful Signal Impact on Convergence Parameters of the Gradient Signal Processing Algorithm for Adaptive Antenna Arrays that Obviates Reference Signal Presence. Lecture Notes on Data Engineering and Communications Technologies, 2021, 69, crp. 267–286.

3. Buchyk, S., Toliupa, S., Lukova-Chuiko, N., Khomenko, O., Serpinskyi, Y. (2023). Applied Steganographic System for Hiding Textual Information on Audio Files. Emerging Networking in the Digital Transformation Age. Lecture Notes in Electrical Engineering, vol 965. Springer, Cham. [https://doi.org/10.1007/978-3-031-24963-1\\_18](https://doi.org/10.1007/978-3-031-24963-1_18). Scopus

4. Shtanenko S., Samokhvalov Y., Toliupa S., Silko, O. (2023). The Approach to Assessment of Technical Condition of Microprocessor Systems that Are Implemented on Integrated Circuits with a Programmable Structure. Emerging Networking in the Digital Transformation Age. Lecture Notes in Electrical Engineering, vol 965. Springer, Cham. [https://doi.org/10.1007/978-3-031-24963-1\\_28](https://doi.org/10.1007/978-3-031-24963-1_28) Scopus.

5. Shestak Y., Toliupa S., Shevchenko A., Torchylo, A., Onyigwang O.J. Data Pro-cessing Centre's Cyberattack Protection Directions on the Base of Neural Network Algorithms. CEUR Workshop Proceedings, 2023, 3347, pp. 212–221. Scopus

6. Khusainov P., Toliupa S., Bakanov V., Shtanenko S. Substantial formulation of the task of improving the information model of decision-making in

the prompt (crisis) response to cyber incidents. Proceedings - 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2022, 2022, стр. 287–290.

7. Buchyk S., Toliupa S., Symonychenko Y., Symonychenko A., Platonenko A. (2021) Improvement of Steganographic Methods based on the Analysis of Image Color Models. Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine, pp. 117–124. URL: <http://ceur-ws.org/Vol-2923/paper13.pdf>.

8. Saiko V., Toliupa S., Nakonechnyi V., Kotov M., Astapenya V. Method of determining the angular orientation of small satellites in orbit. (2021) Improvement of Steganographic Methods based on the Analysis of Image Color Models. Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine, pp. 224–233. URL: <http://ceur-ws.org/Vol-2923/paper13.pdf>.

9. Zhurakovskiy B., Toliupa S., Otrokh S., Dudarieva H., Zhurakovskiy V. Coding for information systems security and viability. Conference Paper. CEUR Workshop Proceedings this link is disabled, 2021, 2859, стр. 71–84.

10. Toliupa S., Nakonechnyi V., Kotov M., Solodovnyk V. RF signals encryption with AES in WDID. Conference Paper. CEUR Workshop Proceedings this link is disabled, 2021, 2845, стр. 96–105.

11. Toliupa S., Tereikovska L., Tereikovskiy I., Doszhanova A., Alimseitova Z. Procedure for Adapting a Neural Network to Eye Iris Recognition. Conference Paper. 2020 IEEE International Conference on

Problems of Infocommunications Science and Technology, PIC S and T 2020 - Proceedingsthis link is disabled, 2021, crp. 167–171, 9468020.  
12. Saiko V., Toliupa S., Nakonechnyi V., Brailovskyi M. Models of Improving the Efficiency of Radio Communication Systems Using the Terrahert Range. Conference Paper. 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020 - Proceedingsthis link is disabled, 2021, crp. 192–196, 9468022.  
13. Zhurakovskiy B., Toliupa S., Otrokh S., Dudarieva H., Zhurakovskiy V. Coding for information systems security and viability. CEUR Workshop Proceedingsthis link is disabled, 2021, 2859, crp. 71–84.  
14. Toliupa S., Tereikovskiy I., Tereikovska L., Mussiraliyeva S., Bagitova K. Deep Neural Network Model for Recognition of Speaker's Emotion. Conference Paper. 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020 - Proceedingsthis link is disabled, 2021, crp. 172–176, 9468017.  
15. Tereikovskiy I., Subach I., Tereikovskiy O., Tereikovska L., Toliupa S., & Nakonechnyi, V. (2020). Parameter Definition for Multilayer Perceptron Intended for Speaker Identification (pp. 227–231). Institute of Electrical and Electronics Engineers (IEEE). Scopus. <https://doi.org/10.1109/atit49449.2019.9030504>.  
16. Toliupa S., Tereikovska L., Korystin O., Chernyshev D., & Tereikovskiy I. (2020). Low-Resource Convolution Neural Network for Keyboard

Recognition of the User (pp. 222–226). Institute of Electrical and Electronics Engineers (IEEE). Scopus. <https://doi.org/10.1109/atit49449.2019.9030437>.

17. Pliushch O., Vyshnivskiy V., Toliupa S., Rybydajlo A. (2020). Utilization of Clipper Circuits to Improve Efficiency of the Gradient Signal Processing Algorithm for Adaptive Antenna Arrays (pp. 191–194). Institute of Electrical and Electronics Engineers (IEEE). Scopus. <https://doi.org/10.1109/atit49449.2019.9030529>.

18. Toliupa S., Nakonechnyi V., Kotov M., Solodovnyk V. RF signals encryption with AES in WDID. CEUR Workshop Proceedings, 2021, 2845, стр. 96–105.

19. Toliupa S., Korchenko O., Tereikovskiy I., Tereikovskiy O. Determination of signs of information and psychological influence in the tone of sound sequences. ATIT 2020 - Proceedings: 2020 2nd IEEE International Conference on Advanced Trends in Information Theory, 2020, стр. 276–280, 9349302.

20. Oleksandr Pliushch, Serhii Toliupa, Viktor Vyshnivskiy, Anatolii Rybydajlo. Studying of Useful Signal Impact on Convergence Parameters of the Gradient Signal Processing Algorithm for Adaptive Antenna Arrays that Obviates Reference Signal Presence. Springer. Chapter 11. 2021. - C. 234-245.

21. Nakonechnyi V., Toliupa S., Saiko V., Ghno G.S.N., Hussain A.K. Blockchain Implementation in the Protection System of Banking System During Online Banking Operations. Conference of Open Innovation Association, FRUCT, 2024, страницы 492–500.

22. Alnuaimy A.N.H., Jawad A.M., Abdulkareem S.A.,



							<p>Ivanchenko S., Toliupa S. BM3D Denoising Algorithms for Medical Image. Conference of Open Innovation Association, FRUCT, 2024, страницы 135–141.</p> <p>23. Zhurakovskiy B., Poltorak V., Toliupa S., Pliushch O., Platonenko A. Processing and Analyzing Images based on a Neural Network. CEUR Workshop Proceedings <a href="#">Эта ссылка отключена.</a>, 2024, 3654, страницы 125–136</p> <p>24. Koriakov I., Pliushch O., Toliupa S. Performing Data Cipherring with the Help of Digital Filters. CEUR Workshop Proceedings, 2024, 3654, страницы 491–496</p>
176132	Приходько Оксана Юріївна	Доцент (1 ставка), Основне місце роботи	Факультет лінгвістики та соціальних комунікацій	<p>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</p>	14	ОК2.Наукові комунікації у фаховій діяльності	<p>Освіта: Рівненський державний педагогічний інститут, 1995 рік, кваліфікація спеціаліста «Учитель української мови та літератури», диплом з відзнакою КН № 900140 від 16 червня 1995 р.</p> <p>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».</p> <p>Вчене звання: доцент кафедри слов'янської філології.</p> <p>Підвищення кваліфікації:</p> <ol style="list-style-type: none"> <li>Університет менеджменту освіти НАПН України. Термін 27.01.2020 - 26.06. 2020. Освітньо-професійна програма «Організація дистанційного навчання у закладах освіти». Свідоцтво про підвищення кваліфікації СП 35830447/1065-20 (7 кредитів ЄКТС).</li> <li>Clarivate. Тема «Research Smarter: Огляд літератури на відмінно». Термін 24.05.2022 р. Сертифікат (0,033 кредити ЄКТС).</li> </ol> <p>Види і результати професійної діяльності 1, 3, 4, 12, 14, 15, 19</p>

п. 1  
1. Приходько О. Ю. Психоевристика й герменевтична інтерпретація травми як чинника художнього світу (на матеріалі української та польської малої прози другої половини XIX – початку XX ст.). Султанівські читання : зб. наук. праць. Івано-Франківськ : Державний вищий навчальний заклад «Прикарпатський національний університет імені Василя Стефаника», 2019. Вип. VIII. С. 25–34. (Категорія В).  
2. Приходько О. Ю. Підручник із української літератури у проєкції на Нову українську школу. Проблеми сучасного підручника : зб. наук. праць. Київ: Педагогічна думка, 2019. Вип. 22. С. 238–249. (Категорія В).  
3. Приходько О. У пошуках онтологічної реальності: британський постпостмодерністський роман (Рецензія на монографію: Дроздовський Д. І. Проблемно-тематичні комплекси й філософсько-естетичні параметри британського постпостмодерністського роману: [моногр.]. Київ: Саміт-книга, 2020. 448 с.). Філологічний дискурс: зб. наук. праць. Хмельницький, 2020. Вип. 10. С. 314 – 316. (Категорія В).  
4. Prykhodko Oksana Superstructure And Hegemony In Milan Kundera's «The Joke» And Post-Postmodern Cultural Texts. Modern philology: promising and priority areas for scientific researches: collective monograph. Lviv-Torun : Liha-Pres, 2020. P. 159 – 175. Видання входить до наукометричної бази SENSE.  
5. Приходько О. Метод проєктів як технологія інноваційного викладання української мови у вищій школі. Актуальні питання гуманітарних наук:

міжвузівський збірник наукових праць молодих вчених Дрогобицького державного педагогічного університету імені Івана Франка.  
Дрогобич : Видавничий дім «Гельветика», 2020. Вип. 27. С. 165 – 168. (Категорія В).  
6. Dmytro Drozdovskyi, Petro Ivanushyn, Oksana Prykhodko. The Irish Experience of Identity Representation: M. J. Hyland's "Carry Me Down". Journal of History Culture and Art Research. 2020. Вип. 9 (4). 262-275. URL: <http://kutaksam.karabuk.edu.tr/index.php/ilk/article/view/2784> (Web of Sciences)  
7. Приходько О. Ю. Драматична поема Лесі Українки «На полі крові як об'єкт сценічної інтерпретації: інтермедіальний аналіз. Міжвузівський збірник наукових праць молодих вчених Дрогобицького державного педагогічного університету імені Івана Франка «Актуальні питання гуманітарних наук». Дрогобич : Видавничий дім «Гельветика», 2021. Вип. 8. С. 116 – 120. (Категорія В).  
Vaskiv Mykola, Prykhodko Oksana, Drozdovskyi Dmytro, Vukova 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> (Web of Sciences)  
9. 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](http://www.magnanimitas.cz/ADALTA/120230/papers/A_16.pdf) (Web of Sciences)

10. 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> (Web of Sciences)

11. Приходько О., Литвинська С. Методологічні аспекти викладання навчальної дисципліни «Наукові комунікації у фаховій діяльності» для майбутніх фахівців. Вісник Національного авіаційного університету. Серія: Педагогіка. Психологія: зб. наук. праць. Київ : НАУ, 2023. № 22. С. 51 – 60. URL:

<https://jrn1.nau.edu.ua/index.php/VisnikPP/article/view/17604> (Категорія В)

12. Kotkova L., Prykhodko O., Lytvynska S., Tsyhanok H., Lushchik Y. Innovations in scientific communication: Techniques for crafting distinctive textual content. Multidisciplinary Science Journal. Vol. 6 (2024), e2024ss0732. URL:

<https://www.malquepub/ojs/index.php/msj/article/view/2992> (Scopus)

п. 3  
Наукові комунікації у фаховій діяльності: навч. посіб. / Литвинська С.В., Добровольська Л.А., Дячук Т.М., Кошетар У.П., Онуфрійчук Г.І., Приходько О.Ю., Сенчило-Татліліоглу Н.О., Сібрук А.В., Стецик Х.М. Київ: НАУ, 2024. 136 с. URL: <https://umk.nau.edu.ua/wp->

content/uploads/2024/06/Navch.-posib.-NKFD-ost.a5Obkl-1.pdf

п. 4  
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-naukovoii-movy-ta-komunikatsii\\_20.03.2024.pdf](https://umk.nau.edu.ua/wp-content/uploads/2024/06/Praktykum_Kultura-naukovoii-movy-ta-komunikatsii_20.03.2024.pdf)

п. 12  
1. Приходько О. Ю. Професіограма вчителя української мови й літератури в контексті Нової української школи. Дивослово. 2019. № 2 (743). С. 15–21.  
2. Приходько О. Ю. Особливості професійної підготовки майбутніх учителів-філологів у формуванні дослідницької компетентності учнів-членів МАН. Актуальні проблеми вищої професійної освіти : Матеріали VII Міжнародної науково-практичної конференції (м. Київ, 22 березня 2019 року). Київ : НАУ. С. 117. URL : [www.kppro.nau.edu.ua/confer.php](http://www.kppro.nau.edu.ua/confer.php)  
3. Приходько О. Ю. Жанрові особливості літератури факту на прикладі повісті Г. Хоткевича «Тарас Шевченко». Research of different directions of development of philological sciences in Ukraine and EU: збірник матеріалів міжнародної науково-практичної конференції (Romania, Baia Mare, Технічний університет Клуж-Напока, 20-21 вересня 2019 р.). Baia Mare, Romania, 2019. С. 91 – 94.  
4. Prykhodko Oksana Superstructure And Hegemony In Milan Kundera's «The Joke» And Post-Postmodern Cultural Texts / Oksana Prihodko // Modern philology: promising and priority areas for scientific researches: collective

monograph. Lviv-Torun : Liha-Pres, 2020. P. 159 – 175.

5. Приходько О. Нон-фікшн, література факту, документальна література : до проблеми жанру. Актуальні проблеми літературознавчої термінології : зб. наук. праць. Рівне : РДГУ, 2020. Вип.3. С. 91 – 94.

6. Приходько О. Технології дистанційного навчання у процесі підготовки до ЗНО з української мови та літератури : зб. наук. праць матеріалів VI Всеукраїнської науково-практичної конференції «Актуальні проблеми в системі освіти: заклад загальної середньої освіти – доуніверситетська підготовка – заклад вищої освіти», 9 червня 2020 р., м. Київ, Національний авіаційний університет. Київ: НАУ, 2020. С. 123-130. URL: [http://www.iidot.nau.edu.ua/images/docs/conference/aktualni\\_problemy/zbirka\\_conf\\_2020.pdf](http://www.iidot.nau.edu.ua/images/docs/conference/aktualni_problemy/zbirka_conf_2020.pdf)

7. Приходько О. Технології дистанційного навчання у процесі викладання української мови. : зб. наук. праць матеріалів I Всеукраїнської науково-практичної конференції «Дистанційна освіта в Україні: інноваційні, нормативно-правові, педагогічні аспекти», 16 червня 2020 р., м. Київ, Національний авіаційний університет. Київ: НАУ, 2020. С. 109-111. URL: [http://www.iidot.nau.edu.ua/images/docs/conference/conf\\_distance/16.06.2020/%D0%97%D0%B1%D1%96%D1%80%D0%BA%D0%B0%20%D1%82%D0%B5%D0%B7\\_%D0%94%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D1%86%D1%96%D0%B9%D0%BD%D0%B0%20%D0%BE%D1%81%D0%B2%D1%96%D1%82%D0%Vo\\_2020.pdf](http://www.iidot.nau.edu.ua/images/docs/conference/conf_distance/16.06.2020/%D0%97%D0%B1%D1%96%D1%80%D0%BA%D0%B0%20%D1%82%D0%B5%D0%B7_%D0%94%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D1%86%D1%96%D0%B9%D0%BD%D0%B0%20%D0%BE%D1%81%D0%B2%D1%96%D1%82%D0%Vo_2020.pdf)

8. 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-polikrovi-lesi-ukrainkytsenichne-vtillennia-v-rivnomu/>

9. 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://jrnل.nau.edu.ua/index.php/APSE/article/view/15867>

10. 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>

11. Prykhodko Oksana. Genre specificity of non-fiction in modern Ukrainian literature. Hagia Sophia. Editors: Prof. Dr. Muhittin ELIACIK, 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](https://www.ayasofyakongresi.com/_files/ugd/4ec152_5f99ee52ca70497ca83e952cf31d7b6d.pdf)

12. 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>

13. 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](https://er.nau.edu.ua/handle/NAU/59448?locale=uk)

14. Приходько О.,  
Ємець А., Коновалова  
В. Професійна  
комунікація за  
допомогою мережі  
«Інтернет» як форма  
наукової комунікації.  
ПОЛІТ. Сучасні  
проблеми науки.  
Гуманітарні науки:  
тези доповідей XXIII  
Міжнародної науково-  
практичної  
конференції  
здобувачів вищої  
освіти і молодих  
учених:[у 2-х т.]. Т. 1  
(м. Київ, 04-07 квітня  
2023 р.) / [ред. кол.:  
Н. В. Ладогубець, А.  
М. Кокарева та ін.];  
Національний  
авіаційний  
університет. Київ :  
НАУ, 2023. С. 320–  
321. URL:  
[https://flsc.nau.edu.ua/  
wp-  
content/uploads/2023/  
05/POLIT\\_TOM-  
2\\_2023.pdf](https://flsc.nau.edu.ua/wp-content/uploads/2023/05/POLIT_TOM-2_2023.pdf)

15. Приходько О.,  
Шапенко Н.  
Проблеми штучного  
інтелекту та GPT-чату  
в контексті  
академічної  
добросовісності  
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/12345678  
9/31042/1/Zbirnyk\\_ma  
terialiv\\_konferentsii.pdf](http://dspace.tnpu.edu.ua/bitstream/123456789/31042/1/Zbirnyk_materialiv_konferentsii.pdf)

16. Приходько О.  
Пам'яті скарбничого  
просвітянського духу.  
Слово просвіти:  
всеукраїнський  
культурологічний  
тижневик. Вип. 47-48  
(1232), 23 листопада –  
6 грудня, 2023. С. 13.  
URL:

17. 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/issue/view/487)  
[https://jias.donnu.edu.  
ua/article/view/14575/1  
4480](https://jias.donnu.edu.ua/article/view/14575/14480)

18. 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.

						<p>діючого студентського наукового гуртка «Актуальні проблеми наукової комунікації»</p> <p>п. 15</p> <p>1. Робота у складі журі (заступник голови журі) фінального (III) етапу Міжнародного мовно-літературного конкурсу учнівської та студентської молоді імені Тараса Шевченка (2017 – 2024 рр.)</p> <p>2. Робота у складі журі IV етапу Всеукраїнської учнівської олімпіади з української мови та літератури (2014 – 2020 рр.)</p> <p>3. Робота у складі журі (голова журі) II етапу конкурсу-захисту науково-дослідницьких робіт Малої академії наук України в секції «Українська література» (2016 – 202 рр.).</p> <p>4. Робота у складі журі (голова журі) Всеукраїнської олімпіади Національного авіаційного університету для професійної орієнтації вступників на основі повної загальної середньої освіти з української мови та літератури (2017 – 2020 рр.)</p> <p>5. Робота в експертній раді програми «Дослідження. Освіта. Резиденції. Стипендії» Українського культурного фонду (2022 р.)</p> <p>п. 19</p> <p>Член громадської організації «Київське обласне об'єднання Всеукраїнського товариства «Просвіта» імені Тараса Шевченка»</p> <p>Член громадської організації «Рівненське обласне об'єднання ВУТ «Просвіта» ім. Тараса Шевченка»</p>	
236435	Дубчак Олена Вікторівна	Старший викладач (1 ставка), Основне місце роботи	Факультет комп'ютерних наук та технологій	Диплом спеціаліста, Київський інститут інженерів цивільної авіації, рік закінчення: 1981, спеціальність: Автоматизован	22	OK8.Захист комунікаційних мереж засобами Cisco	Освіта: Київський інститут інженерів цивільної авіації, 1981 р., спеціальність "Автоматизовані системи управління", кваліфікація – інженер-системотехнік Підвищення кваліфікації:

і системи  
управління

1. Cisco Networking Academy, 03.2019 - 05.2019, " Introduction to Cyber security", Сертифікат Cisco Networking Academy. (3 кредити ЄКТС, 90 год)
  2. Cisco Networking Academy, 05.2020 - 01.2021, " Academy Orientation"; "Introduction to IoT"; "Introduction to Packet Tracer"; "Instructor Professional Development", Сертифікати Cisco Networking Academy (3 кредити ЄКТС, 90 год)
  3. Cisco Networking Academy, 05.2022 - 06.2023, " Academy Orientation"; "#BeCyberSmart"; "Instructor Professional Development", Сертифікати Cisco Networking Academy (3 кредити ЄКТС, 90 год)
  4. Cisco Networking Academy, 06.2023 - 01.2024, "Instructor Professional Development", Сертифікати Cisco Networking Academy (1,5 кредити ЄКТС (45 год)
- Наявність досвіду професійної діяльності: інженер - програміст 2-ї к. (1994-2001 рр), провідний інженер - програміст (2001-2002 рр)

<http://kszi.nau.edu.ua/kadrovij-sklad/39-vukladachi/88-dubchakov>

Види і результати професійної діяльності 1, 3, 4, 10,12, 14, 19, 20:

п.1.

1. Дубчак О.В. Безпека ОС Windows/О.В. Дубчак, А.К. Голестанех, Я.С. Мазур// News of Science and Education. – 2019. - №14.- С.54-57. (наукометрична платформа Google Scholar)
2. Дубчак О.В Алгоритм організації функціонування розподіленої СППР в умовах великого навантаження /О.В. Дубчак, Н.К. Гулак // Scientific Periodical Journal "SWorldJournal"/ SWorld & D.A. Tsenov

Academy of Economics, Svishtov, Bulgaria, - 2024. – Issue 24 (Part 1, March 2024). – P.111 – 119. (наукометрична база Index Copernicus) (Загалом: понад 20 публікацій (фахові видання)

п.3.  
Профіль науковця на порталі НБУВ  
<http://irbis-nbuv.gov.ua/ASUA/1262057>

1. Василенко В.С.  
Цілісність та доступність об'єктів в інформаційних мережах / В.С.Василенко, О.Я.Матов, О.В.Дубчак // Монографія. – Київ: ІПРІ НАН України, 2014. – 428 с. (Загалом: наявність 5 монографій (у співавторстві))

п.4.  
1. Дубчак О.В. Основи програмування. Лабораторний практикум для здобувачів вищої освіти спеціальності «Кібербезпека»/О.В. Дубчак// Лабораторний практикум.- Електронний ресурс. – 2023. – 40 с.  
2. Дубчак О.В. Основи мережевих технологій. Лабораторний практикум для здобувачів вищої освіти спеціальності «Кібербезпека»/О.В. Дубчак// Лабораторний практикум.- Електронний ресурс для слухачів Cisco Networking Academy “Networking Essentials 2.0”. - 2024. – 36 с.  
3. Дубчак О.В. Методичні рекомендації щодо виконання та оформлення домашнього завдання/контрольної роботи з дисципліни "Основи мережевих технологій" для студентів спеціальності "Кібербезпека" ОПП 125.1 "Безпека інформаційних і комунікаційних систем"/О.В. Дубчак// Методичні рекомендації.- Електронний ресурс для слухачів Cisco Networking Academy

“Networking Essentials 2.0”. – 2024. – 9 с.

4. Дубчак О.В.Захист комунікаційних мереж засобами Cisco. Лабораторний практикум для здобувачів вищої освіти спеціальності «Кібербезпека»/О.В.Дубчак// Лабораторний практикум.- Електронний ресурс. - 2023. – 44 с.

5. Дубчак О.В. Захист комунікаційних мереж засобами Cisco. Методичні рекомендації щодо виконання та оформлення розрахунко-графічної роботи для здобувачів вищої освіти спеціальності «Кібербезпека та захист інформації»/О.В.Дубчак// Методичні рекомендації.- Електронний ресурс. – 2024. – 10 с.

8 робочих програм, 3 силябуси з дисциплін, що викладаються, зокрема:

- 1.Основи програмування
2. Основи мережевих технологій
3. Захист комунікаційних мереж засобами Cisco
4. Вступ до Інтернету речей
5. Методологічні засади кібербезпеки

п.10  
Участь у міжнародних освітніх проектах:  
Cisco Networking Academy, Instructor

п.12.  
Наявність 30-ти апробаційних публікацій у матеріалах міжнародних науково-практичних конференцій, зокрема:

- 1.Дубчак О.В. Аналіз загроз електронному листуванню/ О.В. Дубчак, Є.С. Мікуліч // Materials of XV Intenational Research And Practice Conference «Trends of Modern Science – 2019», 31.05.19 – 07.06.19. – Sheffield (UK): “Science&Education Ltd”. - V.14.- P.23-25.
2. Дубчак О.В. Регулятивні

принципи галузі кібербезпеки / О.В. Дубчак, А.К. Голестанех // Наукові праці Другої міжнар. наук.-практ. конф. «Сучасні тенденції розвитку інформаційних систем і телекомунікаційних технологій», 19 грудня 2019 р. (Київ, Україна). – К. : НУХТ, 2019. – С. 122-123.

3. Дубчак О.В. Технології забезпечення віддаленого доступу / О.В. Дубчак, А.А. Карабут // Cutting-Edge Science – 2020: XVI International Scientific And Practice Conference, 30.04.20 – 07.05.20: тези доп. – Sheffield (UK): “Science&Education Ltd”. - V.8.- P.53-55.

4. Дубчак О.В. Засоби захисту мобільних додатків / О.В. Дубчак, А.К.Голестанех // Nauka i inowacja – 2021: XVII międzynarodowej naukowo-praktycznej konferencji, 7-15 października 2021 r.: abstracts. – Przemysł (Polska), 2021. – V.1. – P. 30-32.

5. Дубчак О.В. Використання розширених ACL обладнання Cisco для забезпечення LAN від зовнішніх загроз / О.В. Дубчак, С.І. Ожерельєв, І.А.Кравчук // CSNT-2021: XIII міжнар. наук.-практ. конф., 15-17 квітня 2021:тези доп. - К., 2021. - С.32-33.

6. Дубчак О.В. Аналіз засобів системного програмування / О.В. Дубчак, Є.О. Галич, В.Г. Павленко // Сучасні тенденції розвитку системного програмування-2022: наук.-практ. конф., 23-24 листопада 2022.:тези доп.-К., 2022.-С.78-80.

7. Дубчак О.В. Аналіз уразливостей веббраузера / О.В. Дубчак, О.О. Левченко, І.А. Кравчук // CSNT-2023: XIV міжнародна науково-практична конференція, 13-14 квітня 2023:тези доп. - К., 2023. - С.84-85.

8. Дубчак О.В. Засоби протидії вебвідстеженню / О.В.

Дубчак, О.О.  
Левченко, Я.С. Мазур  
// CSNT-2023: XIV  
міжнародна науково-  
практична  
конференція, 13-14  
квітня 2023:тези доп. -  
К., 2023 .- С.86-87.  
9. Дубчак О.В.  
Використання  
технології штучного  
інтелекту для  
убезпечення  
комунікаційних  
мереж / О.В. Дубчак,  
Н.К. Гулак// CSNT-  
2024: XV міжнародна  
науково-практична  
конференція, 25-26  
квітня 2024:тези доп. -  
К., 2024 .- С.53-54.  
10. Дубчак О.В.  
Аналіз засобів захисту  
Wi-Fi роутерів / О.В.  
Дубчак, Є.С.  
Тимофіїв// CSNT-  
2024: XV міжнародна  
науково-практична  
конференція, 25-26  
квітня 2024:тези доп. -  
К., 2024 .- С.55-56.  
11. Дубчак О.В.  
Проблеми захисту  
конфіденційності  
користувача  
веббраузерів / О.В.  
Дубчак,  
О.О.Левченко// CSNT-  
2024: XV міжнародна  
науково-практична  
конференція, 25-26  
квітня 2024:тези доп. -  
К., 2024 .- С.56-57.

п. 14  
Керівництво СНГ  
"Технології  
програмування та  
методи захисту  
інформації" -  
підготовка студентів  
до участі в науково-  
практичних  
конференціях;  
наявність понад 15  
публікацій зі  
студентами у  
матеріалах  
міжнародних науково-  
практичних  
конференцій,  
зокрема:  
1. Дубчак О.В. Аналіз  
характеристик  
мікросервісної  
архітектури / О.В.  
Дубчак, А.О.  
Поліщук// Materialy  
XV mezinárodní  
vědecko - praktická  
konference «Aktuální  
vymoženosti vědy -  
2019», 22.06.19 –  
30.06.19. - Praha, 2019.  
- V.8.- С. 39-41.  
2 Дубчак О.В. Аналіз  
засобів захисту  
програмного  
забезпечення/ О.В.  
Дубчак, П.Д  
Панченко. //Наукові

						<p>праці Другої міжнар. наук.-практ. конф. «Сучасні тенденції розвитку інформаційних систем і телекомунікаційних технологій», 19 грудня 2019 р. (Київ, Україна). – К. : НУХТ, 2019. – С. 128-129.</p> <p>3. Дубчак О.В. Проблема некоректної автентифікації користувачів веб-застосунків / О.В. Дубчак, А.А. Карабут, І.А. Кравчук// Europejska nauka XXI powieka – 2020: XVI miesdzynarodowa naukowo-praktyczna konferencja, 7-15 pazdziernika 2020 r.: abstracts. – Przemysl (Polska), 2020. – V.3. – P. 84-86.</p> <p>4. Дубчак О.В. Автентифікація складових мікросервісної архітектури під час їх комунікації / О.В. Дубчак, А.О. Поліщук// CSNT-2021: XIII міжнародна науково-практична конференція, 15-17 квітня 2021: тези доп. - К., 2021. - С.34-35.</p> <p>5. Дубчак О.В. Аналіз засобів системного програмування / О.В. Дубчак, Є.О. Галич, В.Г. Павленко // Сучасні тенденції розвитку системного програмування-2022: наук.-практ. конф., 23-24 листопада 2022.: тези доп.-К., 2022.-С.78-80.</p> <p>6. Дубчак О.В. Аналіз засобів захисту Wi-Fi роутерів / О.В. Дубчак, Є.С. Тимофіїв// CSNT-2024: XV міжнародна науково-практична конференція, 25-26 квітня 2024: тези доп. - К., 2024. - С.55-56.</p> <p>п.19 Участь у професійних об'єднаннях: IT Ukraine Association</p> <p>п. 20 Досвід практичної роботи: інженер - програміст 2-ї кат. (1994-2001 рр), провідний інженер - програміст (2001-2002 рр)</p>	
20717	Гулак Наталія Костянтинівна	Доцент (1 ставка), Основне місце роботи	Факультет комп'ютерних наук та технологій	Диплом спеціаліста, Харківський інститут радіоелектроніки, рік	22	ОК7.Моніторинг та аудит кібербезпеки	Освіта: Харківський інститут радіоелектроніки, спеціальність "Електронні прилади",



закінчення:  
1975,  
спеціальність:  
Електронні  
прилади,  
Диплом  
кандидата наук  
ДК 002486,  
виданий  
22.12.2011

кваліфікація "Інженер  
електронної техніки"  
Науковий ступінь:  
Кандидат технічних  
наук, 05.13.06-  
Інформаційні  
технології, тема  
"Методи підвищення  
ступення стиску  
відеоданих в  
інформаційних  
системах кодування  
зображень"  
Підвищення  
кваліфікації:  
НАПН України ДЗВО  
"Університет  
менеджменту освіти",  
11.01.2021-11.06.2021  
р., "Цифрові  
технології в  
освітньому  
процесі"свідотство СП  
35830447/0844-21,  
180 год (6 кредитів)

[http://kszi.nau.edu.ua/  
kadrovij-sklad/39-  
vukladachi/140-gulak-  
nataliya-kostyantynivna](http://kszi.nau.edu.ua/kadrovij-sklad/39-vukladachi/140-gulak-nataliya-kostyantynivna)

Види і результати  
професійної  
діяльності 1, 3, 4,  
10,12,13, 20

п.1.  
1.1. Гулак Н.К.  
Автоматизація модуля  
інформаційних  
активів /Н.К. Гулак,  
А.А. Майстренко  
//Інформаційні  
технології та  
суспільство. – 2024. –  
Том №1(12) – С. 46-50.  
ISSN: 2786-5460 DOI:  
[https://doi.org/10.3268  
9/maur.it](https://doi.org/10.32689/maur.it) (фахове  
видання категорії В)  
1.2. Гулак Н.К.  
Алгоритм організації  
функціонування  
розподіленої СППР в  
умовах великого  
навантаження/Н.К.  
Гулак, О.В. Дубчак //  
Scientific Periodical  
Journal  
"SWorldJournal"//  
SWorld & D.A. Tsenov  
Academy of Economics,  
Svishtov, Bulgaria. -  
2024. – Issue 24 (Part 1,  
March 2024). – P.111 –  
119.  
[https://www.sworldjou  
rnal.com/index.php/sw  
j/article/ view/swj24-  
00-058](https://www.sworldjournal.com/index.php/swj/article/view/swj24-00-058) (фахове  
видання категорії В)

п.3  
3.1.Gulak N. Decision  
support system in  
conditions of the heavy  
load /N. Gulak, O.  
Yakovenko // Projekt  
interdyscyplinary  
projektem XXI wieku:  
Monografia. Tom 1. –

Akademia Techniczno-  
Humanistyczna w  
Bielsku-Bialej, 2019. -  
Vol. 2. - PP. 71-76.

п.4.  
4.1. Гулак Н.К.  
Електроніка / Н.К.  
Гулак, Н.Є. Фролова //  
Лабораторний  
практикум для  
студентів  
спеціальності: 125  
"Кібербезпека". – К.:  
НАУ, 2019. – 72 с.

4.2. Гулак Н.К.  
Комплект  
лабораторних робіт з  
дисципліни  
"Операційні системи  
та технології їх  
захисту", 2020 - 48 с. -  
Електронний ресурс  
для студентів CISCO  
NETWORKING  
ACADEMY "Linux  
Essentials"

4.3. Гулак Н.К.  
Комплект лекцій з  
"Операційні системи  
та технології їх  
захисту", 2022 - 180 с.  
- Електронний ресурс  
для студентів CISCO  
NETWORKING  
ACADEMY "Linux  
Essentials"

4.4. Гулак Н.К.  
Комплект лекцій з  
дисципліни  
«Операційні системи  
та технології їх  
захисту» Електронний  
ресурс для студентів  
CISCO NETWORKING  
ACADEMY "Linux  
Unhatched", 2023 -  
157с.

4.5. Гулак Н.К.  
Комплект  
лабораторних робіт з  
дисципліни  
"Операційні системи  
та технології їх  
захисту".  
Електронний ресурс  
для студентів CISCO  
NETWORKING  
ACADEMY "Linux  
Unhatched", 2023 -35 с.

п.10  
Участь у міжнародних  
освітніх проєктах:  
Cisco Networking  
Academy, Instructor

п.12  
12.1. Gulak N. An  
optimal synthesis  
structure of a  
distributed decision  
support system as a  
task for nonlinear  
mathematical  
programming /N.  
Gulak, O. Yakovenko, A.  
Yakovenko// X  
Міжнародна науково-  
практична  
конференція  
«Комплексне

забезпечення якості технологічних процесів та систем», 28 - зоквітня 2020 р.: Чернігів, НУ «Чернігівська політехніка». – Т.2. – С.151-156. ISBN 978-617-7571-90-1(наукометрична база Index Copernicus)

12.2. Gulak N. Experience in using of CISCO Networking Academy materials in cyber security bachelor training / N. Gulak, A. Elizarov, H. Dubchak // XXIII International Scientific and Practical Conference "Theory, practice and science", April 27 – 30, 2021. - Tokyo, Japan. –P. 392-396. ISBN – 978-1-63848-669-5 (наукометрична база Google Scholar)

12.3 Gulak N. System of making decision of the heavy loading / N. Gulak // XXV Міжнародна науково-практична конференція «Implementation of modern science and practice» 11-14 травня 2021. - Варна, Болгарія. – С. 138-141. ISBN - 978-1-63848-660-2 (наукометрична платформа Google Scholar)

12.4. Гулак Н.К. Програмний застосунок для захищеного управління користувачами та їх ресурсами /Н.К. Гулак, Я.Р. Сідлецький // XXXVII Міжнародна науково-практична конференція «Modern ways of solving the latest problems in science», 20-23 вересня 2022 р., Варна, Болгарія. – С-488-490. (матеріали Міжнародної конференції)

12.5. Гулак Н.К. Програмний модуль аналізу активності і вразливостей для захисту інформаційних активів. /М.М. Прус, Н.К. Гулак // XXXVII Міжнародна науково-практична конференція «Modern ways of solving the latest problems in science», 20-23 вересня 2022 р., Варна, Болгарія. – С.

473-476. (матеріали Міжнародної конференції)  
12.6. Гулак Н.К. Система безпечного VPN-з'єднання моделлю Zero Trust /Н.К. Гулак, О.Р. Сідлецький // XXXVII Міжнародна науково-практична конференція «Modern ways of solving the latest problems in science», 20-23 вересня 2022 р., Варна, Болгарія. – С- 485-487. (матеріали Міжнародної конференції)  
12.7. Gulak N. Information security breach incident processing module of ISMS / N. Gulak, B. Nosan // V міжнародної науково-практичної конференції “Modern and global methods of the development of scientific thought” (PCSITS-2022), 25-28 жовтня 2022 р., Флоренція, Італія. – С. 570-572. (матеріали Міжнародної конференції)  
12.8. Гулак Н.К. Використання біометричних методів для багатофакторної аутентифікації/ Н.К. Гулак, А.В. Клименко //V International Scientific and Practical Conference "Trends in science regarding the creation of new teaching methods", October 16-18, 2023, Madrid, Spain. - С. 179-181. (матеріали Міжнародної конференції)  
12.9. Гулак Н.К. Аналіз загроз та інцидентів в сфері кібербезпеки під час повномасштабного вторгнення зі сторони росії /Н.К. Гулак, М.О. Котляр//V International Scientific and Practical Conference "Trends in science regarding the creation of new teaching methods", October 16-18, 2023, Madrid, Spain. - С. 182-184. (матеріали Міжнародної конференції)  
12.10. Гулак Н.К. Захист інформації у вебзастосунках методами криптографії /Н.К. Гулак, М.В. Лось //V International Scientific

						<p>and Practical Conference "Trends in science regarding the creation of new teaching methods", October 16-18, 2023, Madrid, Spain. - С. 184 - 186. (матеріали Міжнародної конференції)</p> <p>12.11. Гулак Н.К. Захист інформації у вебзастосунках методами криптографії /Н.К. Гулак, М.В. Лось //V International Scientific and Practical Conference "Trends in science regarding the creation of new teaching methods", October 16-18, 2023, Madrid, Spain. - С. 184 - 186. (матеріали Міжнародної конференції)</p> <p>12.12. Гулак Н.К. Використання технології штучного інтелекту для забезпечення комунікаційних мереж/ О.В. Дубчак, Н.К. Гулак// CSNT-2024: XV міжнародна науково-практична конференція, 25-26 квітня 2024:тези доп. - К., 2024 .- С.53-54. (матеріали Міжнародної конференції)</p> <p>п.13 Discipline Operating systems and technologies for their protection (81 година)</p> <p>п.20. 8 років КВО «Київський радіозавод» інженер-технолог цеху мікроелектроніки</p>	
13973	Льенко Анна Вадимівна	Завідувач кафедри (1 ставка), Основне місце роботи	Факультет комп`ютерних наук та технологій	<p>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</p>	14	ОК5.Методи побудови та аналізу криптосистем	<p>Освіта: Національний авіаційний університет, 2009 р., спеціальність – «Захист інформації в комп`ютерних системах та мережах», кваліфікація – «науковий співробітник (безпека підприємств, установ та організацій)» Науковий ступінь: Кандидат технічних наук, 05.13.21 – Системи захисту інформації, тема дисертації «Методи підвищення ефективності захищених інформаційно-комунікаційних систем на основі</p>

ідентифікації кодових конструкцій».

Вчене звання: Доцент кафедри комп'ютеризованих систем захисту інформації.

Підвищення кваліфікації:

1. ТОВ «АЛГОРИТМ-Х». Термін 01.10.2021р. - 30.11.2021 р. Звіт про стажування (6 кредитів 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 (6 кредитів ЄКТС).
3. Softserve. Тема «Підвищення кваліфікації: Вдосконалення викладання у вищій освіті: інституційний та індивідуальний виміри». Термін 22.12.2022р. Сертифікат (0,067 кредита ЄКТС).
4. 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. Літня школа 2023 у рамках проєкту Еразмус+ модуль Жан Моне «Європейський досвід для підвищення стійкості критично важливих об'єктів в Україні». Термін 17.07.2023р. – 04.08.2023 р. Сертифікат (4 кредита ЄКТС).
7. EPAM та IT Ukraine Association. Тема: «Teachers Internship: Deep Dive into AWS (Amazon Web Services)». Термін липень 2023р. Сертифікат (2 кредита ЄКТС).

5. Sigma Software

University i 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 «ІТ-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. Teachers Smart Up: Winter Edition 3.0 2024 / Тренди в ІТ. Термін: 22-26 січня 2024 Сертифікат (1 кредит ЄКТС)

13. Sigma Software University. Teachers' Smart Up: Summer Edition 2024 Термін: 22-27 липня 2024 Сертифікат (1 кредит ЄКТС)

14. SoftServe Academy Tech Summer for Educators: AI Edition. Термін: 23 липення - 13 серпня 2024 Сертифікат (1 кредит ЄКТС)

<http://kszi.nau.edu.ua/kadrovij-sklad/39-vukladachi/87-ilenkoav>

Види і результати професійної діяльності 1, 2, 3, 4, 8, 12, 14, 19

п. 1  
1. Ilyenko A. Digital signature authentication scheme with message recovery based on the use of

elliptic curve / Svitlana Kazmirchuk, Ilyenko Anna // Advances in Intelligent Systems and Computing. – V. 938. – 2019. – P. 279-288. (Scopus)

2. ЛЬЕНКО А.В. Сучасний стан забезпечення кібернетичної безпеки цивільної авіації України та світу / А.В. ЛЬЕНКО, С.С. ЛЬЕНКО, Д.С. Кваша//Кібербезпека: освіта, наука, техніка. – 2020. – Т.5 № 9. – С. 24-36. (фахове видання категорії В)

3. 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](https://link.springer.com/chapter/10.1007/978-3-030-55506-1_30). (Scopus)

4. 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)

5. Anna Ilyenko A Biometric Asymmetric Cryptosystem Software Module Based On Convolutional Neural Networks / Anna Ilyenko, Sergii Ilyenko, Marharyta Herasymenko// International Journal of Computer Network and Information Security. – V. 13, №6. – 2021. – P.



1-12. (Scopus)  
6. Лєнко А.В.  
Програмний модуль  
вїдслїдковування  
помилку у  
високонавантажених  
вєб-додатках на базї  
використання  
авторського  
алгоритму логєру /  
С.С.Лєнко,  
Д.С.Сташєвський //  
Кїбербезпека: освїта,  
наука, технїка. – 2021.  
– Т.3 (№ 11). – С. 61-  
72. (фахове видання  
катєгорї В)  
7. 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)  
8. Лєнко А., Лєнко  
С.,Кваша Д., Мазур Я.  
Практичнї пїдходи  
щодо виявлення  
вразливостей в  
їнформаційно-  
телекомунїкаційних  
мережах //  
Кїбербезпека: освїта,  
наука, технїка. – 2023.  
– Т.3 № 19. – С. 46-56.  
(фахове видання  
катєгорї В)  
9. 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](https://ceur-ws.org/Vol-3550/short5.pdf).  
(Scopus)

п. 2  
1. Пат. 137706 Україна,  
МПК G09C 1/00, H04K  
1/00. Спосїб  
формування та  
верифїкації  
електронно-  
цифрового пїдпису з  
використанням  
додаткових  
криптографїчних  
алгоритмїв / Лєнко  
С.С., Лєнко А.В.:

заявник та патентовласник Нац. авіац. ун-т. – № u201902702; Заявл. 20.03.2019; Опубл. 11.11.2019, Бюл. № 21/2019. – 5 с.  
2. Пат. 137707 Україна, МПК G09C 1/00, H04K 1/00. Спосіб формування та верифікації електронно-цифрового підпису з відновленням на основі використання еліптичних кривих / Льєнко С.С., Льєнко А.В.: заявник та патентовласник Нац. авіац. ун-т. – № u201902703; Заявл. 20.03.2019; Опубл. 11.11.2019, Бюл. № 21/2019. – 5 с.  
3. Пат. 146770 Україна, МПК G09C 1/00, H04K 1/00. Спосіб гомоморфної процедури шифрування та дешифрування інформації на основі використання додаткових параметрів/ Льєнко С.С., Льєнко А.В.: заявник та патентовласник Нац. авіац. ун-т. – № u202005681; Заявл. 03.09.2020; Опубл. 18.03.2021, Бюл. № 11. – 4 с.  
4. Пат. 149227 Україна, МПК G09C 1/00, H04K 1/00. Спосіб автентифікації на основі використання еліптичних кривих/ Льєнко С.С., Льєнко А.В.: заявник та патентовласник Нац. авіац. ун-т. – № u202102943; Заявл. 01.06.2021; Опубл. 28.10.2021, Бюл. № 43. – 3 с.

п. 3  
3.1. Льєнко С.С., Захарченко В.П., Єнчев С.В., Льєнко А.В. Функціональні автоматизовані системи та комплекси повітряних суден: Навчальний посібник. – К.: НАУ, 2019. – 160 с. ISBN 978-966-932-118-3  
3.2. Методи та засоби забезпечення резервування авіоніки : монографія / В. П. Захарченко, С. В. Єнчев, С. С. Льєнко, С. С. Товкач, А. В. Льєнко; ред.: В. М. Воробйов; Національний

авіаційний  
університет//  
монографія. – К.:  
НАУ, 2020. – 276 с.  
ISBN 978-966-932-  
140-4

п. 4

1. Ільєнко А.В.  
Технологія організації  
інфраструктури  
відкритих ключів  
/А.В.Ільєнко ,  
С.В.Казмірчук,  
О.О.Висоцька //  
Лабораторний  
практикум для  
студентів освітньо-  
професійної програми  
«Безпека  
інформаційних і  
комунікаційних  
систем». – К.: НАУ,  
2019. – 32 с.
2. 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 кому-  
нікаційних систем». –  
К.: НАУ, 2020. – 48 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 «Технології  
організації  
інфраструктури  
відкритих ключів» ОС  
Магістр
6. Робоча програма та  
НМК «Прикладна  
криптологія» ОС  
Бакалавр

п. 8

- 8.1. НДР  
№116/09.01.09  
«Криптографічні  
методи захисту в  
сучасних  
інформаційно-  
комунікаційних  
системах та мережах»  
Термін виконання -  
01.09.2018р. –  
30.06.2019р.  
(відповідальний  
виконавець)
- 8.2. НДР  
№43/09.01.09  
«Інформаційна  
технологія організації  
імігаційного полігону  
захисту критичних

інформаційних ресурсів». Термін виконання - 01.09.2019р. – 30.06.2021р. (науковий керівник)  
8.3. 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.  
12.1. Puyenko A.V. Method of formation and verification of electronic digital signature with using additional cryptographic algorithms / Puyenko S.S., Puyenko A.V// Авіа-2019: XIV міжнародна науково-технічна конференція, 23-25 квітня 2019 р.: тези доп. – К., 2019. – С. 1.8-1.10. (матеріали Міжнародної конференції)  
12.2. Puyenko A.V. Modern approach to cybersecurity of computer-integrated aviation systems / Puyenko S.S, Kvasha D.S., Puyenko A.V.// Aviation in the XXI-st century. Safety in aviation and space technologies: the nine world congress, 22-24 of September 2020: abstracts. – К., 2020. – V.1. (матеріали Міжнародної конференції)  
12.3. Puyenko A.V. Software module for authentication using neural network / Anna Puyenko, 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)  
12.4. 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)

12.5. 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)

12.6. 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)

12.7. 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.

12.8. 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. –

						<p>С.45-48. 12.9. Льюенко А.В. Підхід щодо перевірки цифрових сертифікатів з використанням технології blockchain / А.В. Льюенко, С.С. Льюенко, О.Л. Яковенко // CSNT-2024: XV міжнародна науково-практична конференція, 25-26 квітня 2024: тези доп. - К., 2024. - С.74-75. 12.10. Льюенко А.В. Застосування засобів штучного інтелекту у кібербезпеці / А.В. Льюенко, 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.</p> <p>п. 14 Керівництво СНГ " Криптографічні методи захисту інформації" (підготовка студентів до участі в науково-практичних конференціях)</p> <p>п.19 Участь у професійних об'єднаннях: ITeachers SoftServe Community</p>
75317	Швець Валеріян Анатолійович	Доцент (1 ставка), Основне місце роботи	Факультет комп'ютерних наук та технологій	<p>Диплом спеціаліста, Київський інститут інженерів цивільної авіації, рік закінчення: 1986, спеціальність: Техексплуатація авіаційного радіоелектронного обладнання, Диплом кандидата наук КН 013178, виданий 31.01.1997, Атестація доцента ДЦ 005673, виданий 17.10.2002</p>	34	<p>ОК6. Моделювання та оптимізація безпекових процесів авіаційної галузі</p> <p>Освіта: Київський інститут інженерів цивільної авіації, 1986 р., спеціальність - «Техексплуатація авіаційного радіоелектронного обладнання», кваліфікація – «Радіоінженер». Науковий ступінь: Кандидат технічних наук, 05.12.04 – Радіолокація і радіонавігація, тема дисертації «Исследование и разработка целочисленных квазигармонических базисов спектрального анализа в задачах обнаружения-измерения доплеровско-импульсных радиолокационных сигналов». Вчене звання: Доцент кафедри радіоелектроніки. Підвищення кваліфікації: ТОВ «Новелл Консалтинг».</p>

Термін 01.10.2021р. - 4.12.2021 р. Звіт про стажування (6 кредитів ЄКТС).

Види і результати професійної діяльності 1, 3, 6, 8, 12, 19

п. 1

1. Shvets V., Ilnytska S., Kutsenko O. Chapter 14. Application of Computer Modelling in Adaptive Compensation of Interferences on Global Navigation Satellite Systems // Cases on Modern Computer Systems in Aviation. IGI Global, 2019. – pp. 339 – 380 (Scopus)

2. Shvets V. A. Antenna array as a constructive element of increasing cyber-security of network satellite system receivers [Текст] / V. A. Shvets, V. P. Kharchenko // Proceedings of the National Aviation University, N 1 (74), 2018. pp. 30 – 37. (фахове видання категорії B)

3. Shvets V. A. Method of evaluation of the electric field level of dangerous signals to gnss receivers [Текст] / V. A. Shvets, V. P. Kharchenko // Proceedings of the National Aviation University, N 2 (75), 2018. pp. 7–12. (фахове видання категорії B)

4. Shvets V. A. Information threats to the global navigation satellite system and how to eliminate them [Text] / V. A. Shvets // Sciences of Europe, Vol. 1, №35 (2019). – Praha, Czech Republic: Global Science Center LP, 2019. pp. 61 – 73.

5. Shvets V. A. Radio receiver for the monitoring of the radionavigation field of global navigating satellite systems [Text] / V. A. Shvets // Sciences of Europe, Vol. 1, №36 (2019). – Praha, Czech Republic: Global Science Center LP, 2019. pp. 54 – 64.

6. Швець, В. і Мелешко, Т. 2023. Оцінка заводо захищеності когерентного прийому сигналів з багатопозиційною

фазовою маніпуляцією при наявності нефлюктуаційних завад. Measuring and computing devices in technological processes. 2 (чер 2023), 167–178. (фахове видання категорії В)

п. 3

1. Shvets V., Ilynska S., Kutsenko O. Chapter 14. Application of Computer Modelling in Adaptive Compensation of Interferences on Global Navigation Satellite Systems // Cases on Modern Computer Systems in Aviation. IGI Global, 2019. – pp. 339 – 380

п.6.

20 червня 2024 року.  
Мелешко Тетяна Вікторівна, дис. на ступінь к.т.н.  
Методика оцінки завадостійкості прийому дискретних сигналів з багатопозиційною фазовою маніпуляцією в умовах впливу нефлюктуаційних завад, 05.12.13 – «Радіотехнічні пристрої та засоби телекомунікацій»

п. 8

1. Науковий керівник НДР «Каркас» № 0120U000029т 2020-2021 рр.  
2. Науковий керівник НДР «Графіт» № 0120U000028т 2020-2021 рр.

п. 12

1. Швець В. А. Заходи захисту навігаційної інформації в мережових супутникових системах [Текст] / В. А. Швець, Т. В. Мелешко // ITSec: Безпека інформаційних технологій: IX міжнародна науково-технічна конференція, 22-27 березня 2019 р. – К.: НАУ, 2019. – С. 34 – 35. (матеріали Міжнародної конференції)  
2. Швець В. А. Напрями забезпечення доступності і цілісності інформації глобальних навігаційних супутникових систем



[Текст] / В. А. Швець, Т. В. Мелешко // International Trends in Science and Technology: Proceedings of the XXI International Scientific and Practical Conference, January 31, 2020, Warsaw, Poland. – RS Global Sp. z O.O. Scholarly Publisher. Warsaw, Poland 2020. С. 29 – 36. (матеріали Міжнародної конференції)

3. Швець В. А. Методика оцінки рівня електричного поля небезпечних сигналів в заходах захисту інформації глобальних навігаційних супутникових систем [Текст] / В. А. Швець, Т. В. Мелешко // International Trends in Science and Technology: Proceedings of the XXII International Scientific and Practical Conference, February 28, 2020, Warsaw, Poland. – RS Global Sp. z O.O. Scholarly Publisher. Warsaw, Poland 2020. С. 36 – 40. (матеріали Міжнародної конференції)

4. Швець В. А., Мелешко Т. В. Пристрій визначення напрямку на джерело завади для безпілотного літального апарату / В. А. Швець, Т. В. Мелешко // Aviation in the XXI-st century 2022: World Congress, September 28 – 30, 2022: abstracts. – Kyiv (Ukraine), 2022. Р 2.4.4 – 2.4.7. (матеріали Міжнародної конференції)

5. Швець В. А., Мелешко Т. В. Малогабаритна антена UHF – S - діапазону для безпілотних літальних апаратів / XVI Міжнарод. наук.-техн. конф. «АВІА-2023», (Київ, 18-20 квітня 2023 р.). М-во освіти і науки України, Київ, 2023 р. С. 214 -218. (матеріали Міжнародної конференції)

п. 19 Науковий консультант з створення CRPA компанія Data Science

							(з 1.06. 2023 р. – по теперішній час)
52366	Толюпа Сергій Васильович	Професор (0,5 ставки), Сумісництво	Факультет комп'ютерних наук та технологій	<p>Диплом спеціаліста, Київське вище інженерне радіотехнічне училище ППО, рік закінчення: 1986, спеціальність: Автоматизовані системи управління, Диплом доктора наук ДД 000091, виданий 10.11.2011, Диплом кандидата наук КН 012091, виданий 10.12.1996, Аттестат доцента ДЦ 005016, виданий 20.06.2002, Аттестат професора 12ПР 008351, виданий 25.01.2013</p>	16	ОКЗ.Методологія прикладних досліджень у сфері кібербезпеки	<p>Освіта: Київське вище інженерне радіотехнічне училище ППО ім. Pokришкіна А.І., 1986р., спеціальність - автоматизовані системи управління, кваліфікація - інженер електронної техніки. Науковий ступінь: Доктор технічних наук 05.12.02 - Телекомунікаційні системи та мережі, тема дисертації «Дослідження функціонування інфокомунікаційних мереж нового покоління на основі інтелектуальних технологій». Вчене звання: професор кафедри безпеки інформаційних технологій. Підвищення кваліфікації: 1. ТОВ «ДЕПС СЕЛЮШЕНЗ». Сертифікат про підвищення кваліфікації серія DP №000131 від 31.12.2020р. 2. Certificate of completion Incident response within the 2021 Cybersecurity Summer Training Program under the USAID Project. 3. Навчання на курсах USAID Project "Cybersecurity for Critical Infrastructure in Ukraine" (за програмою «Malware Analysis») 18 October – 1 December 2021. 4. Навчання на курсах USAID Project "Audit and Risk Management" within the 2022 Cybersecurity Summer Instructor Training Program under the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. 11 July – 31 August 2022. 5. Стажування Державний НДІ технологій кібербезпеки та захисту інформації 6 кредитів 180 годин з 22.01.2024 по 05.04.2024р. Сертифікат.</p> <p>Навчальні посібники та монографії: 1. Толюпа С.В., Бучик С.С., Лукова-Чуйко Н.В., Фесенко А.О.</p>

Системи технічного захисту інформації. .  
Навчальний посібник.  
- К.: Формат, 2022. – 386 с.

2. Толюпа С.В., Браїловський М.М., Наконечний В.С., Сайко В.Г.  
Мікропроцесорні системи на мікроконтролерах.  
Навчальний посібник.  
– К: КНУ імені Тараса Шевченка, 2022. – с. 298.

3. Толюпа С.В., Політанський Р.Л., Лісінський В.В.  
Управління інформаційною безпекою.  
Навчальний посібник.  
За заг. ред. Толюпи С.В. – Чернівці. ЧНУ імені Юрія Федьковича. 2021р. – с. 486.

4. Лукова-Чуйко Н.В.  
Системи виявлення вторгнень та функціональна стійкість розподілених інформаційних систем до кібернетичних загроз. // Н.В. Лукова-Чуйко, В.С. Наконечний, Толюпа С.В., М.М. Браїловський // Монографія К.: Формат, 2021. – 407 с.

5. Наконечний В.С.  
Методи та засоби підвищення ефективності функціонування радіотехнічних систем розпізнавання багатопозиційного базування. / В.С. Наконечний, С.В. Толюпа, В.А. Дружинін, Н.В. Лукова-Чуйко. // Монографія. Київ. - К.: Формат. 2019. – 237 с.

6. Толюпа С.В., Штаненко С.С., Османов Р.Н. Методи та засоби захисту інформації в кіберпросторі.  
Навчальний посібник.  
За заг. ред. С.В. Толюпи. – К.: ВІПІ. 2024р. – С. 335.

7. Бучик С.С., Толюпа С.В., Шестак Я.В.  
Програмні технології програмування в інформаційній безпеці. Лабораторний практикум. – Житомир: ФОП Кирилюк І.В., ПП «Рута», 2023. – 50с.

Публікації за тематикою дисципліни:

1. Штаненко С.С., Самохвалов Ю.Я., Толюпа С.В. Підхід до виявлення помилок та відновлення правильного функціонування програмних засобів сучасних систем управління, реалізованих за принципом «система на кристалі». Наукоємні технології. – К.: НАУ, 2023. – № 2 (58). – с. 376-384. <https://doi.org/10.18372/2310-5461.58.17655>.

2. Мостовий В.С., Толюпа С.В., Шевченко А.М. Optimization of the dynamic parameters of an object in a mathematical model of seismo-acoustic monitoring of natural and engineering objects. Наукоємні технології. – К.: НАУ, 2023. – № 2 (58). – С. 412-422. <https://doi.org/10.18372/2310-5461.58.17647>.

3. Штаненко С. С., Самохвалов Ю. Я., Толюпа С. В. Методичний підхід до відновлення правильного функціонування вбудованих систем на рівні програмованої елементної бази. Системи і технології зв'язку, інформатизації та кібербезпеки. ВІТІ № 3 – 2023. С.171-181. <https://doi.org/10.58254/viti.3.2023.19.171>.

4. Толюпа С.В., Бучик С.С., Лукова-Чуйко Н.В., Штаненко С.С. Математична модель проектних відносин загроз та множин системи захисту інформаційної мережі. Вісник університету «Україна» «Інфокомунікаційні та комп'ютерні технології». №1(03), 2022. С. 121-132. <https://visn-icct.uu.edu.ua/index.php/icct/article/view/79>

5. S. Toliupa, S. Laptiev. The methodology for evaluating the functional stability of the protection system of special networks. Наукоємні технології. – К.: НАУ, 2022. – № 3. – С 130-142. <https://jrnل.nau.edu.ua/index.php/SBT/article>

/view/16900  
6. Толюпа С.В.,  
Штаненко С.С.  
)Методика  
проектування  
роботизованих систем  
в базі САПР INTEL  
QUARTUS PRIME.  
Збірник наукових  
праць Військового  
інституту  
телекомунікацій та  
інформатизації імені  
Героїв Крут Випуск №  
1. 2021р. с. 56-66.  
7. Сергій Толюпа, Іван  
Пархоменко,  
Людмила  
Терейковська,  
Володимир Квасніков  
Побудова систем  
виявлення кібератак  
за допомогою  
прихованої  
марківської моделі.  
Науковий журнал НУ  
"Чернігівська  
політехніка" Технічні  
науки та технології ,  
2021. №1(23) – с. 89-  
96.  
8. С. Толюпа, І.  
Пархоменко, С.  
Штаненко. Модель  
системи протидії  
вторгненням в  
інформаційних  
системах.  
Інфокомунікаційні  
технології та  
електронна інженерія.  
№1. 2021. С. 86-95.  
9. Лукова-Чуйко Н.В.,  
Толюпа С.В., Погасій  
С.С., Лаптева Т.О.,  
Лаптев С.О.  
Удосконалення моделі  
захисту інформації в  
соціальних мережах.  
Збірник наукових  
праць Військового  
інституту Київського  
національного  
університету імені  
Тараса Шевченка. К.:  
ВІКНУ, Вип. 73, 2021.  
С. 88 – 103.  
10. Толюпа С.В.,  
Наконечний В.С.,  
Штаненко С.С.  
Алгоритм протидії  
кібератакам на основі  
стеганографічних  
методів технології  
SOFT TEMPEST.  
Збірник наукових  
праць Військового  
інституту  
телекомунікацій та  
інформатизації імені  
Героїв Крут Випуск №  
1. 2020р. с. 56-66.  
11. S. Toliupa, V.  
Nakonechnyi A. Trush.  
To increase the energy  
efficiency of radio  
equipment based on the  
use of modulation by  
orthogonal harmonic  
carriers. Automatyka,  
Pomiary w Gospodarce

i Ochronie Środowiska IAPGOŚ 2020; 9 (1): 24-27. Google Scholar. Poland.

12. Толюпа С.В., Наконечний В.С. Проблеми захисту критично важливих об'єктів інфраструктури Безпека інформаційних систем і технологій. Том 1 № 2 (2020). с. 57-65

13. Serhii Toliupa, Oleksandr Pliushch, Ivan Parkhomenko. Побудова систем виявлення атак в інформаційних мережах на нейромережових структурах. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка" том 2 №10. 2020. с. 169-183.

14. Толюпа С. В., Пархоменко І. І., Кириленко А. І., Вадис К. А. «Захист корпоративної інформації на мобільних пристроях.», Збірник наукових праць «Моделювання та інформаційні системи в економіці», КНЕУ, 2020. №99 – С. 151 – 161.  
<https://ir.kneu.edu.ua:443/handle/2010/35488>

15. Толюпа С. В., Одарченко Р. С., Пархоменко І. І., Даков С.Ю. «Виявлення атак в корпоративній мережі за допомогою правил нечіткої логіки», Науковий журнал. – К.: НАУ, 2020. – № 4 (48). – С 470-477. DOI: 10.18372/2310-5461.48.15125

16. Толюпа С.В., Плющ О.Г., Пархоменко І.І. «Побудова систем виявлення вторгнень в інформаційно-телекомунікаційну мережу на основі методів інтелектуального розподілу даних», Збірник наукових праць «Військового інституту Київського національного університету імені Тараса Шевченка.», К.: ВІКНУ, 2020. № 68 - С. 80-89.  
<https://doi.org/10.17721/2519-481X/2020/68-09>

SCOPUS

1. L. A. Komarova, V. G. Saiko, V. S. Nakonechnyi, S. V. Toliupa, R. V. Ziubina. Quality Assurance of Data Transmission in Queuing Networks. International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-2, December, 2019. Scopus.
2. Pliushch, O., Toliupa, S., Vyshnivskiy, V., Rybydajlo, A. Book Chapter. Springer International Publishing (Verlag). Studying of Useful Signal Impact on Convergence Parameters of the Gradient Signal Processing Algorithm for Adaptive Antenna Arrays that Obviates Reference Signal Presence. Lecture Notes on Data Engineering and Communications Technologies, 2021, 69, crp. 267–286.
3. Buchyk, S., Toliupa, S., Lukova-Chuiko, N., Khomenko, O., Serpinskiy, Y. (2023). Applied Steganographic System for Hiding Textual Information on Audio Files. Emerging Networking in the Digital Transformation Age. Lecture Notes in Electrical Engineering, vol 965. Springer, Cham.  
[https://doi.org/10.1007/978-3-031-24963-1\\_18](https://doi.org/10.1007/978-3-031-24963-1_18). Scopus
4. Shtanenko S., Samokhvalov Y., Toliupa S., Silko, O. (2023). The Approach to Assessment of Technical Condition of Microprocessor Systems that Are Implemented on Integrated Circuits with a Programmable Structure. Emerging Networking in the Digital Transformation Age. Lecture Notes in Electrical Engineering, vol 965. Springer, Cham.  
[https://doi.org/10.1007/978-3-031-24963-1\\_28](https://doi.org/10.1007/978-3-031-24963-1_28) Scopus.
5. Shestak Y., Toliupa S., Shevchenko A., Torchylo, A., Onyigwang O.J. Data Pro-cessing Centre's Cyberattack Protection Directions on the Base of Neural Network

Algorithms. CEUR Workshop Proceedings, 2023, 3347, pp. 212–221. Scopus

6. Khusainov P., Toliupa S., Bakanov V., Shtanenko S. Substantial formulation of the task of improving the information model of decision-making in the prompt (crisis) response to cyber incidents. Proceedings - 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2022, 2022, сrp. 287–290.

7. Buchyk S., Toliupa S., Symonychenko Y., Symonychenko A., Platonenko A. (2021) Improvement of Steganographic Methods based on the Analysis of Image Color Models. Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine, pp. 117 –124. URL: <http://ceur-ws.org/Vol-2923/paper13.pdf>.

8. Saiko V., Toliupa S., Nakonechnyi V., Kotov M., Astapenya V. Method of determining the angular orientation of small satellites in orbit. (2021) Improvement of Steganographic Methods based on the Analysis of Image Color Models. Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine, pp. 224 –233. URL: <http://ceur-ws.org/Vol-2923/paper13.pdf>.

9. Zhurakovskiy B., Toliupa S., Otrokh S., Dudarieva H., Zhurakovskiy V. Coding for information systems security and viability. Conference Paper. CEUR Workshop Proceedings this link is disabled, 2021, 2859, сrp. 71–84.

10. Toliupa S., Nakonechnyi V., Kotov M., Solodovnyk V. RF signals encryption with AES in WDID. Conference Paper. CEUR Workshop Proceedings this link is disabled, 2021, 2845, сrp. 96–105.



11. Toliupa S., Tereikovska L., Tereikovskiy I., Doszhanova A., Alimseitova Z. Procedure for Adapting a Neural Network to Eye Iris Recognition. Conference Paper. 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020 - Proceedingsthis link is disabled, 2021, crp. 167–171, 9468020.

12. Saiko V., Toliupa S., Nakonechnyi V., Brailovskiy M. Models of Improving the Efficiency of Radio Communication Systems Using the Terrahert Range. Conference Paper. 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020 - Proceedingsthis link is disabled, 2021, crp. 192–196, 9468022.

13. Zhurakovskiy B., Toliupa S., Otrokh S., Dudarieva H., Zhurakovskiy V. Coding for information systems security and viability. CEUR Workshop Proceedingsthis link is disabled, 2021, 2859, crp. 71–84.

14. Toliupa S., Tereikovskiy I., Tereikovska L., Mussiraliyeva S., Bagitova K. Deep Neural Network Model for Recognition of Speaker's Emotion. Conference Paper. 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020 - Proceedingsthis link is disabled, 2021, crp. 172–176, 9468017.

15. Tereikovskiy I., Subach I., Tereikovskiy O., Tereikovska L., Toliupa S., & Nakonechnyi, V. (2020). Parameter Definition for Multilayer Perceptron Intended for Speaker Identification (pp. 227–231). Institute of Electrical and Electronics Engineers (IEEE). Scopus.

<https://doi.org/10.1109/atit49449.2019.9030504>.

16. Toliupa S., Tereikovska L., Korystin O., Chernyshev D., & Tereikovskiy I. (2020). Low-Resource Convolution Neural Network for Keyboard Recognition of the User (pp. 222–226). Institute of Electrical and Electronics Engineers (IEEE). Scopus.  
<https://doi.org/10.1109/atit49449.2019.9030437>.

17. Pliushch O., Vyshnivskiy V., Toliupa S., Rybydajlo A. (2020). Utilization of Clipper Circuits to Improve Efficiency of the Gradient Signal Processing Algorithm for Adaptive Antenna Arrays (pp. 191–194). Institute of Electrical and Electronics Engineers (IEEE). Scopus.  
<https://doi.org/10.1109/atit49449.2019.9030529>.

18. Toliupa S., Nakonechnyi V., Kotov M., Solodovnyk V. RF signals encryption with AES in WDID. CEUR Workshop Proceedings, 2021, 2845, стр. 96–105.

19. Toliupa S., Korchenko O., Tereikovskiy I., Tereikovskiy O. Determination of signs of information and psychological influence in the tone of sound sequences. ATIT 2020 - Proceedings: 2020 2nd IEEE International Conference on Advanced Trends in Information Theory, 2020, стр. 276–280, 9349302.

20. Oleksandr Pliushch, Serhii Toliupa, Viktor Vyshnivskiy, Anatolii Rybydajlo. Studying of Useful Signal Impact on Convergence Parameters of the Gradient Signal Processing Algorithm for Adaptive Antenna Arrays that Obviates Reference Signal Presence. Spinger. Chapter 11. 2021. - C. 234-245.

21. Nakonechnyi V., Toliupa S., Saiko V., Ghno G.S.N., Hussain A.K. Blockchain Implementation in the

						<p>Protection System of Banking System During Online Banking Operations. Conference of Open Innovation Association, FRUCT, 2024, страницы 492–500.</p> <p>22. Alnuaimy A.N.H., Jawad A.M., Abdulkareem S.A., Ivanchenko S., Toliupa S. BM3D Denoising Algorithms for Medical Image. Conference of Open Innovation Association, FRUCT, 2024, страницы 135–141.</p> <p>23. Zhurakovskiy B., Poltorak V., Toliupa S., Pliushch O., Platonenko A. Processing and Analyzing Images based on a Neural Network. CEUR Workshop Proceedings Эта ссылка отключена., 2024, 3654, страницы 125–136</p> <p>24. Koriakov I., Pliushch O., Toliupa S. Performing Data Cipherring with the Help of Digital Filters. CEUR Workshop Proceedings, 2024, 3654, страницы 491–496</p>
--	--	--	--	--	--	---

**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
<p><i>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.</i></p>	☒	ОК7.Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК12.Переддипломна практика	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК13.Кваліфікаційна робота	пошуковий метод, метод проблемного виконання, дослідницький метод,	Захист кваліфікаційної роботи

			продуктивно-практичний метод	
<p><i>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.</i></p>	☒	ОК5.Методи побудови та аналізу криптосистем	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК6.Моделювання та оптимізація безпекових процесів авіаційної галузі	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК7.Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		ОК8.Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК9.Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК10Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи
		ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК12.Переддипломна практика	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК13.Кваліфікаційна робота	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
<p><i>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.</i></p>	☒	ОК13.Кваліфікаційна робота	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
		ОК12.Переддипломна практика	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК10Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи
		ОК9.Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен

		ОК6.Моделювання та оптимізація безпекових процесів авіаційної галузі	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
<i>ПРН 21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.</i>	☒	ОК5.Методи побудови та аналізу криптосистем	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК6.Моделювання та оптимізація безпекових процесів авіаційної галузі	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК7.Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		ОК8.Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК9.Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК10.Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи
		ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК12.Переддипломна практика	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК13.Кваліфікаційна робота	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
<i>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.</i>	☒	ОК3.Методологія прикладних досліджень у сфері кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		ОК4.Курсовий проєкт з дисципліни Методологія прикладних досліджень у сфері кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсового проєкту
		ОК6.Моделювання та оптимізація безпекових процесів авіаційної галузі	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК7.Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики

		систем		
		ОК12.Переддипломна практика	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК13.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.	☒	ОК6.Моделювання та оптимізація безпекових процесів авіаційної галузі	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК9.Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК12.Переддипломна практика	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК13.Кваліфікаційна робота	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
		ОК10Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи
ПРН 18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та/або кібербезпеки.	☒	ОК7.Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		ОК8.Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК9.Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК10Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи
		ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК12.Переддипломна практика	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний	Захист звіту з практики

		ОК13.Кваліфікаційна робота	метод пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
<i>ПРН 17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.</i>	☒	ОК3.Методологія прикладних досліджень у сфері кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		ОК4.Курсовий проєкт з дисципліни Методологія прикладних досліджень у сфері кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсового проєкту
		ОК5.Методи побудови та аналізу криптосистем	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК6.Моделювання та оптимізація безпекових процесів авіаційної галузі	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК7.Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		ОК8.Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК9.Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК10.Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи
		ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК13.Кваліфікаційна робота	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
		ОК2.Наукові комунікації у фаховій діяльності	практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		ОК12.Переддипломна практика	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК1.Ділова іноземна мова	практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
<i>ПРН 16. Приймати обґрунтовані рішення з організаційно-</i>	☒	ОК11.Науково-дослідна практика у сфері безпеки інформаційних і	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний	Захист звіту з практики

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.		комунікаційних систем	метод	
		ОК12.Переддипломна практика	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК6.Моделювання та оптимізація безпекових процесів авіаційної галузі	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК9.Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК10Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи
		ОК13.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.	☒	ОК2.Наукові комунікації у фаховій діяльності	практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		ОК5.Методи побудови та аналізу криптосистем	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК6.Моделювання та оптимізація безпекових процесів авіаційної галузі	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК7.Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		ОК8.Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК9.Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК10Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи
		ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК12.Переддипломна практика	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК13.Кваліфікаційна робота	пошуковий метод, метод проблемного виконання,	Захист кваліфікаційної роботи



			дослідницький метод, продуктивно-практичний метод	
<p><i>ПРН 25. Вміння:</i>  - здійснювати організацію функціонування інформаційно-комунікаційної систем;  формуванню 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;  - проектувати захищені (з урахуванням загроз) інформаційні мережі з використанням сучасних методів та технологій забезпечення інформаційної безпеки та/або кібербезпеки.</p>	<input type="checkbox"/>	ОК8.Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК9.Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК10.Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи
		ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК12.Переддипломна практика	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК13.Кваліфікаційна робота	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
<p><i>ПРН 24. Вміння:</i>  - проектувати перспективні криптосистеми та застосовувати сучасні технології криптографічного захисту інформації в системах інформаційної 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-</p>	<input type="checkbox"/>	ОК5.Методи побудови та аналізу криптосистем	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК12.Переддипломна практика	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК13.Кваліфікаційна робота	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи

<p>телекомунікаційних системах; - розробляти та впроваджувати криптографічні системи і використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.</p>				
<p>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.</p>	☒	<p>ОК13.Кваліфікаційна робота</p>	<p>пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод</p>	<p>Захист кваліфікаційної роботи</p>
		<p>ОК12.Переддипломна практика</p>	<p>пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод</p>	<p>Захист звіту з практики</p>
		<p>ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем</p>	<p>пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод</p>	<p>Захист звіту з практики</p>
		<p>ОК5.Методи побудови та аналізу криптосистем</p>	<p>лекції, лабораторні заняття, самостійна робота</p>	<p>Тестування, усне опитування, письмовий контроль, екзамен</p>
<p>ПРН 11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегій і політики інформаційної безпеки та/або кібербезпеки організації.</p>	☒	<p>ОК9.Технології створення та застосування систем захисту кіберпростору</p>	<p>лекції, лабораторні заняття, самостійна робота</p>	<p>Тестування, усне опитування, письмовий контроль, екзамен</p>
		<p>ОК10Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору</p>	<p>лекції, лабораторні заняття, самостійна робота</p>	<p>Тестування, усне опитування, письмовий контроль, захист курсової роботи</p>
		<p>ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем</p>	<p>пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод</p>	<p>Захист звіту з практики</p>
		<p>ОК12.Переддипломна практика</p>	<p>пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод</p>	<p>Захист звіту з практики</p>
		<p>ОК13.Кваліфікаційна робота</p>	<p>пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод</p>	<p>Захист кваліфікаційної роботи</p>
		<p>ОК8.Захист комунікаційних мереж засобами Cisco</p>	<p>лекції, лабораторні заняття, самостійна робота</p>	<p>Тестування, усне опитування, письмовий контроль, екзамен</p>
<p>ПРН 12. Досліджувати, розробляти та впроваджувати методи і заходи</p>	☒	<p>ОК13.Кваліфікаційна робота</p>	<p>пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод</p>	<p>Захист кваліфікаційної роботи</p>

<p><i>протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.</i></p>		ОК7.Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК12.Переддипломна практика	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
<p><i>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.</i></p>	<input checked="" type="checkbox"/>	ОК1.Ділова іноземна мова	практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК2.Наукові комунікації у фаховій діяльності	практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		ОК3.Методологія прикладних досліджень у сфері кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		ОК4.Курсовий проєкт з дисципліни Методологія прикладних досліджень у сфері кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсового проєкту
		ОК5.Методи побудови та аналізу криптосистем	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК6.Моделювання та оптимізація безпекових процесів авіаційної галузі	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК7.Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК8.Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК9.Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК10Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи
		ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК12.Переддипломна практика	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики

		ОК13.Кваліфікаційна робота	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
<i>ПРН 2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.</i>	☒	ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК12.Переддипломна практика	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК13.Кваліфікаційна робота	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
		ОК9.Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК10Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи
		ОК8.Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК7.Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		ОК1.Ділова іноземна мова	практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК2.Наукові комунікації у фаховій діяльності	практичні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК3.Методологія прикладних досліджень у сфері кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		ОК4.Курсовий проєкт з дисципліни Методологія прикладних досліджень у сфері кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсового проєкту
ОК5.Методи побудови та аналізу криптосистем	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен		
ОК6.Моделювання та оптимізація безпекових процесів авіаційної галузі	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен		
<i>ПРН 3. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або</i>	☒	ОК3.Методологія прикладних досліджень у сфері кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		ОК4.Курсовий проєкт	лекції, лабораторні заняття,	Тестування, усне

кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.		з дисципліни Методологія прикладних досліджень у сфері кібербезпеки	самостійна робота	опитування, письмовий контроль, захист курсового проекту
		ОК5.Методи побудови та аналізу криптосистем	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК12.Переддипломна практика	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК13.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.	☒	ОК6.Моделювання та оптимізація безпекових процесів авіаційної галузі	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК8.Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК9.Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК10.Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи
		ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК12.Переддипломна практика	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК13.Кваліфікаційна робота	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
		ОК5.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 міждисциплінарно	☒	ОК5.Методи побудови та аналізу криптосистем	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК6.Моделювання та оптимізація безпекових процесів авіаційної галузі	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен

<p>му рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.</p>		ОК7.Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		ОК9.Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК10Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи
		ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК12.Переддипломна практика	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК13.Кваліфікаційна робота	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
		ОК8.Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
<p>ПРН 6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технологій створення та використання спеціалізованого програмного забезпечення.</p>	☒	ОК6.Моделювання та оптимізація безпекових процесів авіаційної галузі	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК7.Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		ОК8.Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК9.Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК10Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи
		ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК12.Переддипломна практика	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК13.Кваліфікаційна робота	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний	Захист кваліфікаційної роботи

			метод	
<p><i>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.</i></p>	☒	ОК7.Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК12.Переддипломна практика	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК13.Кваліфікаційна робота	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
<p><i>ПРН 8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.</i></p>	☒	ОК13.Кваліфікаційна робота	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
		ОК12.Переддипломна практика	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК10.Курсова робота з дисципліни Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, захист курсової роботи
		ОК9.Технології створення та застосування систем захисту кіберпростору	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК6.Моделювання та оптимізація безпекових процесів авіаційної галузі	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
		ОК7.Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		ОК8.Захист комунікаційних мереж засобами Cisco	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, екзамен
<p><i>ПРН 9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі</i></p>	☒	ОК7.Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики

<i>стратегії і політики інформаційної безпеки.</i>		систем		
		ОК12.Переддипломна практика	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК13.Кваліфікаційна робота	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи
<i>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.</i>	☒	ОК7.Моніторинг та аудит кібербезпеки	лекції, лабораторні заняття, самостійна робота	Тестування, усне опитування, письмовий контроль, диференційований залік
		ОК11.Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК12.Переддипломна практика	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист звіту з практики
		ОК13.Кваліфікаційна робота	пошуковий метод, метод проблемного виконання, дослідницький метод, продуктивно-практичний метод	Захист кваліфікаційної роботи