НАЦІОНАЛЬНЕ АГЕНТСТВО ІЗ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	**Державний університет інформаційно-комунікаційних технологій**
Освітня програма	**71156 Технічні системи інформаційного та кібернетичного захисту**
Рівень вищої освіти	**Магістр**
Спеціальність	**F5 Кібербезпека та захист інформації**

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

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

Використані скорочення:

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

Загальні відомості

1. Інформація про ЗВО (ВСП ЗВО)

Реєстраційний номер ЗВО у ЄДЕБО	**82**
Повна назва ЗВО	**Державний університет інформаційно-комунікаційних технологій**
Ідентифікаційний код ЗВО	**38855349**
ПІБ керівника ЗВО	**Шульга Володимир Петрович**
Посилання на офіційний веб-сайт ЗВО	**http://www.duikt.edu.ua**

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

https://registry.edbo.gov.ua/university/82

3. Загальна інформація про ОП, яка подається на акредитацію

ID освітньої програми в ЄДЕБО	**71156**
Назва ОП	**Технічні системи інформаційного та кібернетичного захисту**
Галузь знань	**F Інформаційні технології**
Спеціальність	**F5 Кібербезпека та захист інформації**
Спеціалізація (за наявності)	*відсутня*
Рівень вищої освіти	**Магістр**
Тип освітньої програми	**Освітньо-професійна**
Вступ на освітню програму здійснюється на основі ступеня (рівня)	**Бакалавр, Магістр (ОКР «спеціаліст»)**
Структурний підрозділ (кафедра або інший підрозділ), відповідальний за реалізацію ОП	**Навчально-науковий інститут кібербезпеки та захисту інформації: кафедра Технічних систем кіберзахисту**
Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП	**Навчально-науковий інститут Телекомунікацій, кафедра Української мови; Навчально-науковий інститут Інформаційних технологій, Кафедра Англійської мови та комп'ютерних лінгвотехнологій кафежра**
Місце (адреса) провадження освітньої діяльності за ОП	**03110, Україна, м. Київ, вулиця Солом'янська, буд. 7**
Освітня програма передбачає присвоєння професійної кваліфікації	*не передбачає*
Професійна кваліфікація, яка присвоюється за ОП (за наявності)	***відсутня***
Мова (мови) викладання	**Українська**
ID гаранта ОП у ЄДЕБО	**455594**
ПІБ гаранта ОП	**Туровський Олександр Леонідович**
Посада гаранта ОП	**Завідувач кафедри**
Корпоративна електронна адреса гаранта ОП	**o.turovskyi@duikt.edu.ua**
Контактний телефон гаранта ОП	**+38(068)-408-18-69**
Додатковий телефон гаранта ОП	*відсутній*

Форми здобуття освіти на ОП	Термін навчання
очна денна	1 р. 5 міс.

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

Зміст ОПП «Технічні системи інформаційного та кібернетичного захисту» сформовано з урахуванням потреб ринку праці, сучасного розвитку технологій кібербезпеки і технічного захисту інформації, вимог роботодавців та досвіду Університету. Програму започатковано у 2017 році, тоді ж здійснено перший набір здобувачів. У 2018 році ОПП пройшла акредитацію (сертифікат від 10.07.2018 №11007045), термін дії якої надалі було продовжено до 2026 року. ОПП передбачає підготовку за напрямами створення і застосування комплексів захисту інформації з обмеженим доступом, охорони об'єктів інформаційної діяльності, теорії захисту інформаційних ресурсів, радіомоніторингу і радіопротидії, організації та проведення спеціальних досліджень. Практична підготовка реалізується через науково-дослідну, науково-педагогічну та переддипломну практики.
Під час розвитку ОПП використано результати проєкту ЄС Tempus №544455-TEMPUS-1-2013-1-SE-TEMPUS-JPCR, що сприяло врахуванню європейського досвіду підготовки фахівців у сфері кібербезпеки.
Чинну редакцію ОПП оновлено у 2025 році відповідно до Стандарту вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації» для другого (магістерського) рівня, затвердженого наказом МОН України від 18.03.2021 №332, а також з урахуванням рекомендацій акредитаційних комісій, роботодавців, здобувачів та інших стейкголдерів. ОПП реалізується за спеціальністю F5 «Кібербезпека та захист інформації» галузі знань F «Інформаційні технології».
Для оновлення програми сформовано робочу групу, до якої увійшли науково-педагогічні працівники кафедри, представник роботодавців і здобувач. Члени робочої групи провели детальний аналіз ринку праці, визначивши вимоги роботодавців до компетентностей фахівців у сфері кібербезпеки.
Оновлену ОПП схвалено кафедрою (протокол №11 від 06.03.2025), затверджено Вченою радою ДУІКТ (протокол №5 від 18.03.2025) та введено в дію наказом ректора №99 від 21.03.2025 з 01.09.2025. Реалізацію програми забезпечує кафедра Технічних систем кіберзахисту ННІ кібербезпеки та захисту інформації ДУІКТ. Подальше оновлення ОПП здійснюється з урахуванням змін нормативної бази, технологій, рекомендацій роботодавців, академічної спільноти та пропозицій здобувачів.

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

Рік навчання	Навчальний рік, у якому відбувся набір здобувачів відповідного року навчання	Обсяг набору на ОП у відповідному навчальному році	Контингент студентів на відповідному році навчання станом на 1 жовтня поточного навчального року	У тому числі іноземців
			ОД	*ОД*
1 курс	2026 - 2027	60	14	0
2 курс	2025 - 2026	60	28	0

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

6. Інформація про інші ОП ЗВО за відповідною спеціальністю

Рівень вищої освіти	Інформація про освітні програми
початковий рівень (короткий цикл)	*програми відсутні*
перший (бакалаврський) рівень	*програми відсутні*
другий (магістерський) рівень	**71152 Інформаційна та кібернетична безпека** **71156 Технічні системи інформаційного та кібернетичного захисту** **71163 Управління інформаційною та кібернетичною безпекою**
третій (освітньо-науковий/освітньо-творчий) рівень	*програми відсутні*

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

	Загальна площа	Навчальна площа
Усі приміщення ЗВО	16518	7032

Власні приміщення ЗВО (на праві власності, господарського відання або оперативного управління)	16518	7032
Приміщення, які використовуються на іншому праві, аніж право власності, господарського відання або оперативного управління (оренда, безоплатне користування тощо)	0	0
Приміщення, здані в оренду	0	0

Примітка. Для ЗВО із ВСП інформація зазначається:
- щодо ОП, яка реалізується у базовому ЗВО – без урахування приміщень ВСП;
- щодо ОП, яка реалізується у ВСП – лише щодо приміщень даного ВСП.

8. Документи щодо ОП

Документ	Назва файла	Хеш файла
Освітня програма	*ОПП_Магістри_ТСІКЗ_2025.pdf*	KBYHdcAe8ei85Aa7kEVzVE78HNlSMscWupTTUCAV42A=
Освітня програма	*ОПП_Магістри_ТСІКЗ_2026.pdf*	QXFjNRzA11JG86ykYeKOvxEvqDoyaK4IvXa45nFI9u0=
Навчальний план за ОП	*Навч.план_Магістри_Каф.ТСКБ_2026-27 н.р..pdf*	M+2Kjw7140iy0KV22hZJT9Mx2nux2jLO3lOzDoh+1VU=
Навчальний план за ОП	*Навч.план_Магістри_Каф.ТСКБ_2025-26 н.р..pdf*	+iIRKauQ6C863TQflxPPt7KdccYoTdFdVRrvS6XHgrM=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Рецензія ЗНУ_на_ОПП_ТСІКЗ_Магістри_2025.pdf*	hiaczav9ZmK7qywpUOJozlh6kqkC7A1LKui2g/F5iZs=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Рецензія_ЛУЧ_на_ОП_ТСІКЗ_Магістри_2025.pdf*	4KNgyuwTrN5d3O/XeUuCPXGDkbTNM7fr2mieqwwt5eU=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Рецензія_ДержНДІ КБЗІ_на_ОПП_ТСІКЗ_Магістри_2026.pdf*	vkIsnUvFIvKe90GNu++ICp0xW/5QOqUXjQ0/FtbCC9A=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Рецензія Каф.кібербезпеки ЗНУ_ОП_ТСІКЗ_Магістри_2026 р..pdf*	VC/UzMKhgJ2z5A7AVwI/H0E14a8GvVp7UxXMYAIzdUU=

1. Проєктування освітньої програми

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

Нормативний зміст освітньо-професійної програми «Технічні системи інформаційного та кібернетичного захисту» другого (магістерського) рівня за спеціальністю F5 «Кібербезпека та захист інформації» відповідає компетентностям і програмним результатам навчання, визначеним Стандартом вищої освіти за спеціальністю 125 «Кібербезпека та

захист інформації» для другого (магістерського) рівня, затвердженим наказом МОН України від 18.03.2021 № 332. Відповідно до цього Стандарту ОПП була переглянута та оновлена у 2025 році.
Для співвіднесення компетентностей, освітніх компонентів і програмних результатів навчання в ОПП використано структурно-логічну схему підготовки, матрицю відповідності програмних компетентностей компонентам ОПП та матрицю забезпечення програмних результатів навчання. Це дає змогу простежити взаємозв'язок між змістом освітніх компонентів, загальними і фаховими компетентностями та результатами навчання. Фахові компетентності охоплюють застосування нормативних документів і стандартів, дослідження та супроводження методів кіберзахисту, управління доступом, протидію кіберінцидентам, технічний і криптографічний захист, аудит та моніторинг інформаційних систем.
Наприклад, компетентності КФ2, КФ3, КФ6, КФ11 реалізуються, зокрема, через ОК10 «Організація і проведення спеціальних досліджень на об'єкті інформаційної діяльності», яка забезпечує досягнення РН7, РН8, РН10, РН11, РН12, РН14, РН15, РН16, РН18, РН20, РН28. Це підтверджує безпосередній зв'язок між фаховими компетентностями, змістом магістерської підготовки та програмними результатами навчання.
Програмні результати ОПП відповідають сьомому рівню Національної рамки кваліфікацій: НРК України — 7 рівень, QF-EHEA — другий цикл, EQF-LLL — 7 рівень. Вони співвідносяться з дескрипторами НРК за складовими: знання та розуміння — РН2, РН5–РН11; уміння та навички — РН3, РН4, РН6–РН14, РН19–РН28; комунікація — РН1, РН15, РН18; відповідальність і автономія — РН16–РН18, РН24, РН27. Програма передбачає здатність здійснювати дослідницьку та інноваційну діяльність, розробляти й упроваджувати системи кіберзахисту, використовувати сучасні стандарти, проводити моделювання і дослідження та приймати обґрунтовані рішення у складних умовах.
Таким чином, ОПП забезпечує досягнення визначених Стандартом компетентностей і програмних результатів навчання та відповідає вимогам 7 рівня НРК. Її структурно-логічна побудова і матриці відповідності забезпечують послідовне формування компетентностей, необхідних для розв'язання складних професійних, дослідницьких та інноваційних завдань у сфері кібербезпеки та захисту інформації.

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

Зміст програми ОПП «Технічні системи інформаційного та кібернетичного захисту» другого (магістерського) рівня за спеціальністю F5 «Кібербезпека та захист інформації», орієнтовано на компетентності, що відповідають кваліфікаційним вимогам професій у сфері інформаційної безпеки, кібербезпеки та технічного захисту інформації.
В ОПП визначено можливість професійної діяльності за ДК 003:2010, зокрема: 2149.2 «Професіонал із організації захисту інформації з обмеженим доступом», 2310.2 «Викладач закладу вищої освіти», 2149.2 «Професіонал із організації інформаційної безпеки», 3439 «Фахівець із організації захисту інформації з обмеженим доступом».
Професійну підготовку забезпечують ОК5–ОК10, які формують здатність застосовувати нормативні документи, оцінювати захищеність систем, організовувати технічний і кібернетичний захист інформації та проводити спеціальні дослідження. ОК10 забезпечує РН7, РН8, РН10–РН12, РН14–РН16, РН18, РН20.
Дослідницькі компетентності формують ОК3 та ОК12, що забезпечують планування досліджень, моделювання, аналіз та інтерпретацію результатів; ОК12 формує РН3–РН5, РН8, РН11–РН13, РН17, РН19–РН23.
Педагогічні компетентності забезпечують ОК2 та ОК11, орієнтовані на організацію освітнього процесу і науково-педагогічну діяльність; ОК11 формує РН1, РН2, РН15, РН17, РН18.
Таким чином, ОПП забезпечує підготовку до професійної, дослідницької та науково-педагогічної діяльності відповідно до кваліфікаційних вимог ДК 003:2010.

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

Мета ОПП полягає у підготовці висококваліфікованих фахівців-магістрів, здатних проводити наукові дослідження, здійснювати професійну діяльність у системі державних і комерційних підприємств, пов'язану з наданням послуг щодо захисту інформації на об'єктах інформаційної діяльності.
Інтереси здобувачів вищої освіти враховуються під час моніторингу, перегляду та оновлення змісту ОПП і її освітніх компонентів: https://duikt.edu.ua/ua/3134-opituvannya-zdobuvachiv-diyalnist-kafedri. На ній розміщено результати опитувань здобувачів другого (магістерського) рівня вищої освіти за 2023–2024 та 2024–2025 навчальні роки.
Крім анкетування, здобувачі магістерського рівня безпосередньо залучаються до обговорення структури та змісту освітньо-професійної програми: https://duikt.edu.ua/ua/news-1-9-15131-studenti-magistri-doluchilisya-do-obgovorennya-onovlennya-osvitno-profesiynih-program-kafedri-tehnichnih-sistem-kiberzahistu.
Проводяться зустрічі здобувачів з представниками ІТ компаній в галузі кібербезпеки: https://duikt.edu.ua/ua/news-1-569-14541-studenti-magistri-doluchilisya-do-seminaru-kafedri-tehnichnih-sistem-kiberzahistu--i-tov-defendiko-schodo-vprovadzhennya-zakonodavchih-novaciy-u-sferi-kiberbezpeki_kafedra-cistem-tehnichnogo-zahistu-informacii.

- роботодавці

Представники роботодавців брали участь у зовнішній експертизі ОП як на етапі її формування, так і на етапі її оновлення: Вимоги компаній-партнерів враховуються також при організації змісту навчання. На робочих зустрічах та під час проведення семінарів обговорюються питання поєднання теоретичної і практичної роботи з використанням сучасного обладнання, програмного забезпечення та програмно-апаратних комплексів: https://duikt.edu.ua/ua/news-1-569-14076-kafedra-tehnichnih-sistem-kiberbezpeki-provela-robochu-zustrich-z-predstavnikami-policii-ohoroni_kafedra-cistem-tehnichnogo-zahistu-informacii, https://duikt.edu.ua/ua/news-1-569-14129-vzaemodiya-zi-steykholderami-magistranti-kafedri-tehnichnih-sistem-kiberzahistu-na-zustrichi-z-policieyu-ohoroni_kafedra-cistem-tehnichnogo-zahistu-informacii, https://duikt.edu.ua/ua/news-1-569-14627-studenti-magistri-doluchilisya-do-seminaru-kafedri-tehnichnih-sistem-kiberzahistu-ta-tov-defendiko-schodo-novaciy-u-sferi-zahistu-

informacii-ta-kiberzahistu_kafedra-cistem-tehnichnogo-zahistu-informacii.
Під час проведення днів кар'єри студенти-магістри безпосередньо спілкувалися з представниками ІТ-сектору, сфери: https://duikt.edu.ua/ua/news-1-525-14327-den-kareri-yarmarok-vakansiy_kafedra-angliyskoi-movi-ta-kompyuternih-lingvotehnologiy, https://www.duikt.edu.ua/ua/news-1-569-15546-den-kareri-u-duikt-zustrich-steykholderiv-kafedri-tehnichnih-sistem-kiberzahistu-zi-studentami-magisterskogo-ta-bakalavrskogo-rivniv-pidgotovki_kafedra-cistem-tehnichnogo-zahistu-informacii,

- академічна спільнота

Академічні інтереси враховуються через роботу профільної кафедри, участь науково-педагогічних працівників у наукових і науково-технічних заходах, використання результатів досліджень у змісті дисциплін та функціонування в Університеті технічного комітету стандартизації ТК 107 «Технічний захист інформації»: https://duikt.edu.ua/ua/119-tehnichniy-komitet-tk-107-tehnichniy-zahist-informacii-nauka.
Рецензентом оновленої ОП у 2025 році є завідувач кафедр кібербезпеки Західноукраїнського національного університету д.т.н., професор Михайло Касянчук.
Також, до обговорення ОП залучалися члени спеціалізованої вченої ради Д 26.861.06 https://duikt.edu.ua/ua/1369-personalniy-sklad-diyalnist-specializovanoi-vchenoi-radi-d2686106 , у якій проводяться захисти дисертацій за спеціальністю 05.13.21 – Системи захисту інформації.
Завдяки рекомендаціям академічної спільноти до програми було удосконалено зміст дисципліни: «Організація проведення наукових досліджень», «Технологія створення та застосування комплексів захисту інформації з обмеженим доступом та охорони об'єктів інформаційної діяльності». Було введено дисципліни вільного вибору «Управління інформаційними інцидентами в системах технічного захисту інформації», «Проектування систем технічного захисту інформації», які було перепрофільовано для вивчення у Навчальній лабораторії засобів технічного захисту інформації.

- інші стейкхолдери

Крім компаній світового рівня (IBM, CISCO, HP, ESET) Університет активно співпрацює з вітчизняними організаціями та установами: Інститутом кібернетики ім. В.М. Глушкова НАН України, ТОВ «Луч», ТОВ «Альфа Безпека», ТОВ «Модуль Сек'юріті», ДП «Безпека», ДП «Українські спеціальні системи», ТОВ « Ajax Systems», Департаментом Кіберполіції. Департаментом поліції охорони Національної поліції України, Департаментом контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України та ін., стосовно змістовного наповнення навчальних програм освітніх компонент https://duikt.edu.ua/ua/2758-partneri-kafedri-kafedra-tehnichnih-sistem-kiberzahistu.
Створений на базі ДУІКТ технічний комітет ТК 107 «Технічний захист інформації», який є суб'єктом національної системи щодо розроблення, розгляду та погодження міжнародних (регіональних) та національних стандартів, дозволяє приймати участь у роботі споріднених ТК міжнародних та регіональних організацій і формувати позиції України щодо нормативних документів та сприяти осучасненню ОП https://duikt.edu.ua/ua/119-tehnichniy-komitettk-107-tehnichniy-zahist-informacii-nauka?lang=ua&id=119&sys_link=tehnichniy-komitet-tk-107-tehnichniy-zahistinformacii-nauka

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

Мета ОПП відповідає Концепції розвитку ДУІКТ на 2024–2026 роки та Стратегії розвитку ДУІКТ на 2025–2029 роки, оприлюдненим у розділі «Публічна інформація»: https://duikt.edu.ua/ua/949-publichna-informaciya-pro-universitet. Відповідно до Концепції (https://duikt.edu.ua/uploads/p_949_80703640.pdf), місією Університету є реалізація суспільної ролі через якісну освіту, наукові дослідження та розвиток творчої особистості.

Реалізація цих завдань забезпечується співпрацею з ІТ-компаніями та державними установами: https://dut.edu.ua/ua/869-partneri-institutunavchalno-naukoviy-institut-zahistu-informacii; орієнтацією навчальних планів на сучасні досягнення ІТ і кібербезпеки; залученням здобувачів до наукової роботи та стажувань: https://duikt.edu.ua/ua/news-1-569-14216-startuvala-reestraciya-na-programu-stazhuvannya-quality-assurance-device-vid-ajax-systems_kafedra-cistem-tehnichnogo-zahistu-informacii; створенням умов для продовження навчання в аспірантурі: https://duikt.edu.ua/ua/news-1-569-13468-doslidzhennya-metodiv-protidii-kiberzagrozam-studenti-duikt-proveli-robotu-poza-mezhami-osnovnoi-programi_kafedra-cistem-tehnichnogo-zahistu-informacii.

ОПП реалізує стратегічний вектор ДУІКТ через поєднання фундаментальної, професійної, дослідницької та практичної підготовки, використання сучасних лабораторій, залучення роботодавців і орієнтацію на актуальні завдання захисту інформаційної та критичної інфраструктури

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

Тенденції розвитку науки і спеціальності враховано у фокусі ОПП, компетентностях, результатах навчання та освітніх компонентах. Програма передбачає використання математичних моделей, сучасних ІТ, спеціалізованого ПЗ, системного аналізу, теорії прийняття рішень, оптимізації, статистики, фізичного й комп'ютерного моделювання. Формуються компетентності з кіберзахисту, технічного і криптографічного захисту, моніторингу, управління доступом, протидії кіберінцидентам, оцінювання ризиків і захисту критичної інфраструктури: https://duikt.edu.ua/ua/news-1-569-14402-navchannya-za-specialnistyu-kiberbezpeka-ta-zahist-informacii-%E2%80%93-pershiy-krok-do-zahistu-maybutnogo_kafedra-cistem-tehnichnogo-zahistu-informacii

Актуальність технічного напряму підтверджується діяльністю кафедри щодо виявлення радіоелектронних, візуально-оптичних, акустичних, віброакустичних каналів витоку, ПЕМВН і закладних пристроїв. Кафедра постійно вивчає нові технології захисту: https://duikt.edu.ua/ua/47-kafedra-cistem-tehnichnogo-zahistu-informacii-kafedri; https://duikt.edu.ua/ua/news-1-569-15210-vikladachi-duikt-vidvidali-zahid-prisvyacheniy-novim-suchasnim-rishennyam-epson_kafedra-cistem-tehnichnogo-zahistu-informacii
До оновлення ОПП залучаються здобувачі та роботодавці. Під час обговорень актуалізовано тематику технічних каналів витоку, моніторингу, кіберризиків, контролю доступу та стійкості ІКС. Це забезпечує оновлення програми відповідно до технологічних змін.

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

Ринок праці враховується через постійну взаємодію кафедри з роботодавцями, їх участь у робочій групі, рецензуванні ОПП, організації практик і кар'єрних заходів: https://duikt.edu.ua/ua/news-1-569-14129-vzaemodiya-zi-steykholderami-magistranti-kafedri-tehnichnih-sistem-kiberzahistu-na-zustrichi-z-policieyu-ohoroni_kafedra-cistem-tehnichnogo-zahistu-informacii; https://duikt.edu.ua/ua/news-1-569-15546-den-kareri-u-duikt-zustrich-steykholderiv-kafedri-tehnichnih-sistem-kiberzahistu-zi-studentami-magisterskogo-ta-bakalavrskogo-rivniv-pidgotovki_kafedra-cistem-tehnichnogo-zahistu-informacii
Професійні траєкторії випускників охоплюють розроблення систем захисту, аналіз загроз, реагування на кіберінциденти, підтримку інфраструктури кіберзахисту та управління безпекою. Вимоги партнерів враховуються у практикоорієнтованому навчанні: https://duikt.edu.ua/ua/47-kafedra-cistem-tehnichnogo-zahistu-informacii-kafedri
Галузевий контекст визначається потребами державного і комерційного секторів у захисті інформаційних ресурсів, критичної інфраструктури та протидії кіберзагрозам. Участь Департаменту поліції охорони НПУ, ТОВ «ЛУЧ» і ТОВ «ДЕФЕНДІКО» в оцінюванні ОПП забезпечує врахування вимог практичної діяльності.
Регіональний контекст пов'язаний із розташуванням ДУІКТ у Києві — центрі концентрації державних органів, ІТ- і телеком-компаній та об'єктів критичної інфраструктури, що сприяє практикам, стажуванням і працевлаштуванню. Водночас компетентності ОПП мають загальнонаціональне застосування.

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

Під час розвитку ОПП враховується досвід підготовки магістрів зі спеціальності «Кібербезпека та захист інформації» у провідних ЗВО України та результати акредитацій суміжних освітніх програм. Порівняльний аналіз засвідчує наявність споріднених магістерських програм технічного спрямування, зокрема ОПП «Системи технічного захисту інформації» НТУУ «КПІ ім. Ігоря Сікорського» (https://osvita.kpi.ua/sites/default/files/oop/f5_oppm_stzi_2025.pdf), програми «Системи технічного захисту інформації та автоматизації її обробки» Харківського національного університету радіоелектроніки (https://nure.ua/en/applicants/specialties-and-specialization/f5-cyber-security-and-information-protection/master-s-degree-f5-cyber-security-and-information-protection/educational-program-system-of-technical-protection-of-information-and-automation-of-its-processing), ОПП ««Системи технічного захисту інформації, автоматизація її обробки» національного університету «Київський авіаційний інститут»: https://www.kzzi.kai.edu.ua/spetsalynsty-125-kberbezpeka/.
Спільними рисами таких програм є підготовка до розв'язання складних завдань кібербезпеки, дослідження технічних каналів витоку інформації, проєктування та експлуатація комплексів технічного захисту, аналіз ефективності заходів безпеки та застосування нормативно-правової бази. Відмінною рисою ОПП «Технічні системи інформаційного та кібернетичного захисту» ДУІКТ є комплексне поєднання систем технічного захисту інформації, захисту інформації з обмеженим доступом, автоматизації її обробки, спеціальних досліджень на об'єктах інформаційної діяльності та суттєвої практичної складової із використанням спеціалізованих лабораторій кафедри.

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

З метою врахування кращих закордонних практик підготовки магістрів за спеціальністю F5 «Кібербезпека та захист інформації» при розвитку ОПП «Технічні системи інформаційного та кібернетичного захисту» використовується досвід іноземних ЗВО.

Blekinge Institute of Technology (Швеція), Master's Programme in Cyber Security, 120 ECTS поєднує теоретичну підготовку з практичною роботою та орієнтується на потреби промисловості й державного сектору. Основні напрями: криптографія, мережева й програмна безпека, захист критичної інфраструктури, penetration testing, аналіз шкідливого ПЗ, DevSecOps, виявлення загроз і машинне навчання. Проєктний і проблемно-орієнтований підходи корелюють з РН3, РН5, РН6, РН8, РН12, РН19–РН22, РН24 ОПП ДУІКТ.

Tallinn University of Technology — TalTech (Естонія), MSc Cybersecurity, 120 ECTS реалізує англомовну магістерську програму, орієнтовану на міжнародність, практичні завдання та формування компетентностей із захисту інформаційних систем. Це відповідає підходу ОПП ДУІКТ щодо поєднання фундаментальної, професійної та практичної підготовки.

Важливим джерелом є проєкт ENGENSEC — Educating the Next Generation Experts in Cyber Security програми TEMPUS. Він був спрямований на створення сучасної магістерської програми з ІТ-безпеки з використанням ECTS, академічної мобільності, взаємного визнання результатів та практикоорієнтованого навчання. У межах проєкту розроблено модулі Advanced Network & Cloud Security, Wireless & Mobile Security, Secure Software Development,

Malware Analysis, Penetration Testing and Ethical Hacking, Digital Forensics.
Досвід ENGENSEC безпосередньо корелює зі змістом ОПП ДУІКТ, що охоплює захист інформації з обмеженим доступом, створення комплексів захисту, моніторинг, спеціальні дослідження, технічний і криптографічний захист, моделювання та оцінювання захищеності. В ОПП 2025 року зазначено використання результатів проєкту ЄС Tempus №544455-TEMPUS-1-2013-1-SE-TEMPUS-JPCR.
Відмінністю ОПП ДУІКТ є виражена спеціалізація на технічному захисті інформації на об'єктах інформаційної діяльності, виявленні та блокуванні технічних каналів витоку, спеціальних дослідженнях і використанні спеціалізованого обладнання. Водночас програма інтегрує європейські підходи до практикоорієнтованого, проєктного та дослідницького навчання, що підвищує її конкурентоспроможність.

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)?

65

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

25

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

Компоненти ОПП «Технічні системи інформаційного та кібернетичного захисту» другого (магістерського) рівня відповідають предметній області спеціальності F5 «Кібербезпека та захист інформації» та забезпечують реалізацію її мети. Зміст програми спрямований на формування здатності розв'язувати складні професійні, дослідницькі й інноваційні завдання у сфері інформаційної безпеки, кібербезпеки, технічного та криптографічного захисту, проєктувати, впроваджувати й супроводжувати системи захисту інформації на об'єктах інформаційної діяльності.

Загальну, дослідницьку та соціально-професійну підготовку забезпечують ОК1–ОК4: «Корпоративна та професійна етика в кібербезпеці», «Організація проведення наукових досліджень», «Педагогіка та психологія у вищій школі», «Науково-технічний переклад». Вони формують професійну етику, дослідницькі, педагогічні, комунікативні та іншомовні компетентності.

Професійне ядро формують ОК5–ОК10: ліцензування, атестація і сертифікація; стандарти кібербезпеки; створення комплексів захисту інформації; теорія захисту інформаційних ресурсів; радіомоніторинг і радіопротидія; спеціальні дослідження на ОІД. Їх зміст охоплює нормативне забезпечення, захист інформації з обмеженим доступом, технічні канали витоку, моніторинг, спеціальні дослідження та оцінювання захищеності.

Практикоорієнтованість ОПП забезпечується використанням спеціалізованих лабораторій, програмно-апаратних комплексів, засобів контролю доступу, біометричних терміналів, систем відеоспостереження та обладнання лабораторії ТЗІ «PIAC» для дослідження акустичних, віброакустичних і електромагнітних каналів витоку інформації.

Вибіркові компоненти поглиблюють підготовку за напрямами: виявлення вразливостей і протидія шкідливому ПЗ; системи контролю доступу; захист електронних засобів від потужних полів; захист конфіденційної інформації; автоматизація обробки інформації з обмеженим доступом; управління інцидентами; проєктування систем ТЗІ; аналіз ефективності кіберзахисту.

Таким чином, обов'язкові та вибіркові компоненти утворюють логічну взаємопов'язану систему, що забезпечує загальнонаукову, дослідницьку, мовну, професійну та практичну підготовку і повністю відповідає предметній області спеціальності F5 «Кібербезпека та захист інформації» та фокусу ОПП на технічних системах інформаційного і кібернетичного захисту.

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

Компоненти ОПП «Технічні системи інформаційного та кібернетичного захисту» другого (магістерського) рівня відповідають предметній області спеціальності F5 «Кібербезпека та захист інформації» та забезпечують реалізацію її мети. Програма формує здатність розв'язувати професійні, дослідницькі й інноваційні завдання у сфері інформаційної безпеки, кібербезпеки, технічного та криптографічного захисту, проєктувати й супроводжувати системи захисту інформації.

Загальну та дослідницьку підготовку забезпечують ОК1–ОК4, що формують етичні, наукові, педагогічні, комунікативні та іншомовні компетентності. Професійне ядро становлять ОК5–ОК10, зміст яких охоплює ліцензування і сертифікацію, стандарти кібербезпеки, створення комплексів захисту, захист інформації з обмеженим доступом, радіомоніторинг, радіопротидію, спеціальні дослідження та оцінювання захищеності ОІД.

Практикоорієнтованість забезпечується використанням спеціалізованих лабораторій, програмно-апаратних комплексів, засобів контролю доступу та обладнання лабораторії ТЗІ «PIAC».

Вибіркові компоненти поглиблюють підготовку з аналізу вразливостей, контролю доступу, захисту конфіденційної інформації, управління інцидентами, проєктування систем ТЗІ та оцінювання ефективності кіберзахисту.

Таким чином, обов'язкові й вибіркові компоненти утворюють взаємопов'язану систему та повністю відповідають предметній області спеціальності F5 і фокусу ОПП на технічних системах інформаційного та кібернетичного захисту.

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

Вибір навчальних дисциплін у ДУІКТ регламентується Положенням про формування індивідуальних освітніх траєкторій (https://duikt.edu.ua/uploads/p_447_22834975.pdf), яке визначає реалізацію права здобувачів на вільний вибір дисциплін відповідно до ст. 62 Закону України «Про вищу освіту».

Для здобувачів ОПП «Технічні системи інформаційного та кібернетичного захисту» другого (магістерського) рівня за спеціальністю F5 «Кібербезпека та захист інформації» процедура реалізується поетапно.

Перший крок: до початку відповідного навчального періоду здобувачі ознайомлюються з дисциплінами, представленими у Каталозі освітніх компонентів вільного вибору студентами ДУІКТ (https://duikt.edu.ua/ua/2080-katalog-osvitnih-komponentiv-vilnogo-viboru-studentami-navchannya), їх силабусами, змістом, результатами навчання, формами занять і контролю.

Другий крок: здобувач самостійно обирає дисципліни відповідно до індивідуальної освітньої траєкторії. За потреби він може отримати консультацію гаранта ОПП, завідувача кафедри, куратора або викладачів щодо змісту компонентів та їх відповідності професійним інтересам і тематиці кваліфікаційної роботи.

Третій крок: навчальний підрозділ ННІ кібербезпеки та захисту інформації узагальнює результати вибору, формує академічні групи та включає відповідні компоненти до розкладу.

Четвертий крок: обрані дисципліни вносяться до індивідуального навчального плану здобувача і стають обов'язковими для опанування.

Загальний обсяг ОПП становить 90 кредитів ЄКТС, з яких 25 кредитів (27,8 %) відведено на вибіркові компоненти. Передбачено п'ять позицій ВК1–ВК5 по 5 кредитів ЄКТС, що перевищує нормативну мінімальну частку 25 %.

Вибіркова складова дозволяє поглибити підготовку у сферах технічного захисту інформації, кібербезпеки, контролю доступу, виявлення вразливостей, протидії шкідливому ПЗ, захисту конфіденційної інформації, управління інцидентами, проєктування систем ТЗІ та оцінювання ефективності кіберзахисту.

Здобувачі також можуть обирати компоненти інших кафедр та освітніх програм ДУІКТ відповідно до встановленої процедури. Такий механізм забезпечує академічну свободу, індивідуалізацію магістерської підготовки та адаптацію її змісту до особистих професійних і освітніх потреб здобувача.

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

За ОПП «Технічні системи інформаційного та кібернетичного захисту» передбачено системну практичну підготовку, що поєднує практичні й лабораторні заняття з науково-педагогічною, науково-дослідною та переддипломною практиками. ОК11 і ОК12 мають по 6 кредитів ЄКТС, ОК13 — 9 кредитів; загальний обсяг практик становить 21 кредит ЄКТС (23,3 % ОПП).

Практики регламентуються Положенням про проведення практик у ДУІКТ: https://duikt.edu.ua/uploads/p_447_23214805.pdf. ОК11 формує педагогічні й комунікаційні компетентності та забезпечує РН1, РН2, РН15, РН17, РН18. ОК12 спрямована на проведення наукових і прикладних досліджень, моделювання, аналіз та інтерпретацію результатів і забезпечує РН3–РН5, РН8, РН11–РН13, РН17, РН19–РН23. ОК13 забезпечує комплексне застосування знань при розв'язанні професійних і дослідницьких завдань перед виконанням кваліфікаційної роботи. Практична підготовка реалізується також у межах ОК5–ОК10 через виконання завдань із ліцензування, стандартів кібербезпеки, створення комплексів захисту, радіомоніторингу та спеціальних досліджень. Практичні й лабораторні заняття проводяться на спеціалізованій базі кафедри: https://duikt.edu.ua/ua/258-materialna-baza-kafedra-cistem-tehnichnogo-zahistu-informacii, що забезпечує набуття практичних навичок з виявлення каналів витоку, контролю доступу та оцінювання засобів захисту: https://duikt.edu.ua/ua/257-robota-iz-studentami-kafedra-cistem-tehnichnogo-zahistu-informacii.

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

ОПП «Технічні системи інформаційного та кібернетичного захисту» забезпечує системне формування soft skills через загальні компетентності КЗ1–КЗ11 та відповідні освітні компоненти. Здобувачі набувають навичок професійної комунікації, командної роботи, критичного й аналітичного мислення, прийняття рішень, самоорганізації, відповідальності та адаптації до змін.
ОК1 «Корпоративна та професійна етика в кібербезпеці» формує професійну етику, відповідальність і культуру взаємодії (КЗ1, КЗ4–КЗ6; РН2, РН17). ОК2 «Педагогіка та психологія у вищій школі» розвиває комунікаційні та організаційні навички, здатність працювати з персоналом (КФ10; РН2, РН17, РН18). ОК3 «Організація проведення наукових досліджень» формує критичне мислення, здатність розв'язувати проблеми, планувати діяльність і презентувати результати (РН3, РН17, РН19–РН21, РН24). ОК4 «Науково-технічний переклад» забезпечує іншомовну професійну комунікацію (РН1, РН2, РН17, РН20, РН23).
Розвиток soft skills продовжується під час ОК11–ОК13, де формуються навички публічного представлення результатів, автономності, відповідальності, аргументації та роботи в умовах невизначеності. Особливе значення мають РН15–РН17, що передбачають професійну комунікацію, прийняття рішень та самостійне навчання.
Таким чином, ОПП забезпечує послідовне формування soft skills, необхідних конкурентоспроможному магістру за спеціальністю F5 «Кібербезпека та захист інформації».

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

Зміст ОПП «Технічні системи інформаційного та кібернетичного захисту» другого (магістерського) рівня за спеціальністю F5 «Кібербезпека та захист інформації» має чітку структуру та охоплює: загальнокультурну й етичну підготовку; дослідницькі та аналітичні компетентності; іншомовну професійну комунікацію; спеціальну підготовку з кібербезпеки і технічного захисту інформації; практичну, науково-дослідну та кваліфікаційну підготовку; формування індивідуальної освітньої траєкторії.
До загальної підготовки належать ОК1–ОК4: «Корпоративна та професійна етика в кібербезпеці», «Педагогіка та психологія у вищій школі», «Організація проведення наукових досліджень», «Науково-технічний переклад». Вони формують етичні, комунікативні, дослідницькі, аналітичні та іншомовні компетентності, здатність приймати обґрунтовані рішення, працювати з інформацією, взаємодіяти з професійними групами та аналізувати суспільні аспекти кібербезпеки.
Професійний блок утворюють ОК5–ОК10: ліцензування, атестація і сертифікація; стандарти кібербезпеки; створення комплексів захисту; теорія захисту інформаційних ресурсів; радіомоніторинг і радіопротидія; спеціальні дослідження на ОІД. Логіка побудови полягає у переході від нормативно-стандартизаційної підготовки до проєктування, застосування й оцінювання засобів захисту, виявлення загроз і вразливостей та проведення спеціальних досліджень.
Взаємозв'язок компонентів, компетентностей і результатів навчання підтверджується матрицями відповідності ОПП. Наприклад, ОК7 забезпечує РН1–РН8, РН10–РН13, РН15, РН19, РН21, РН22, РН26–РН28.
Завершальний етап включає ОК11 «Науково-педагогічна практика», ОК12 «Науково-дослідна практика», ОК13 «Переддипломна практика» та ОК14 «Підготовка кваліфікаційної роботи, підсумкова атестація», що забезпечують практичну апробацію компетентностей та самостійне розв'язання професійних і дослідницьких завдань.
Самостійність і аналітичне мислення підтримуються, зокрема, РН15–РН18.

Вибіркова складова становить 25 кредитів ЄКТС із 90 (27,8 %) і дозволяє поглиблювати підготовку з актуальних напрямів кібербезпеки та технічного захисту інформації.
Таким чином, ОПП є логічною взаємопов'язаною системою, що забезпечує послідовний перехід від загальної та дослідницької підготовки до професійної, практичної й кваліфікаційної та дає змогу досягти заявленої мети і програмних результатів навчання.

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

Підхід до співвіднесення обсягу освітніх компонентів ОПП передбачає, щоб установлені кредити ЄКТС, результати навчання та навантаження з урахуванням самостійної роботи були досяжними й адекватними.
Відповідно до Положення про організацію освітнього процесу ДУІКТ (https://duikt.edu.ua/uploads/p_447_49109699.pdf) тривалість теоретичного навчання, семестрового контролю та самостійної роботи становить 40 тижнів на рік.
Загальний обсяг ОПП становить 90 кредитів ЄКТС (2700 годин), з яких аудиторна робота — 808 годин (29,9 %), самостійна — 1892 години (70,1 %). Обов'язкові компоненти становлять 65 кредитів ЄКТС (1950 годин), вибіркові — 25 кредитів ЄКТС (750 годин), або 27,8 % програми.
Обсяг семестрових завдань, проєктів та інших видів роботи не перевищує часу, передбаченого навчальним планом для самостійної підготовки. Вона забезпечується підручниками, посібниками, методичними матеріалами, курсами лекцій, практикумами та лабораторним обладнанням.
Навчально-методичні матеріали розміщуються в Google Workspace Education: https://classroom.google.com/.
Додаткові ресурси доступні в Електронній бібліотеці ДУІКТ: https://duikt.edu.ua/ua/lib/1/category/2122.

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

ОПП «Технічні системи інформаційного та кібернетичного захисту» має практикоорієнтований характер і поєднує теоретичну підготовку, практичні та лабораторні заняття, науково-дослідну роботу і три види практики. Професійні компетентності формуються в межах ОК5–ОК10, що охоплюють ліцензування і сертифікацію, стандарти кібербезпеки, створення комплексів захисту, захист інформаційних ресурсів, радіомоніторинг, радіопротидію та спеціальні дослідження.

Практична підготовка включає ОК11 «Науково-педагогічна практика» — 6 кредитів ЄКТС, ОК12 «Науково-дослідна практика» — 6 кредитів, ОК13 «Переддипломна практика» — 9 кредитів. Загальний обсяг практик становить 21 кредит ЄКТС. Вони забезпечують набуття дослідницьких, педагогічних і професійних навичок та комплексне застосування компетентностей під час підготовки кваліфікаційної роботи.

Практикоорієнтованість посилюється використанням спеціалізованих лабораторій, програмно-апаратних комплексів, засобів контролю доступу та обладнання лабораторії ТЗІ «PIAC».

Навчання за дуальною формою регламентується Положенням про дуальну форму здобуття вищої освіти у ДУІКТ: https://duikt.edu.ua/uploads/p_447_91663915.pdf. Водночас в ОПП 2025 року не зафіксовано фактичної реалізації дуальної форми, тому практична підготовка здійснюється переважно через лабораторні заняття, практики, співпрацю з роботодавцями та використання матеріально-технічної бази кафедри.

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

ОПП «Технічні системи інформаційного та кібернетичного захисту» за спеціальністю F5 «Кібербезпека та захист інформації» забезпечує формування компетентностей, пов'язаних із реалізацією Цілей сталого розвитку до 2030 року, визначених резолюцією ГА ООН №70/1 та Указом Президента України №722/2019.
Зміст ОПП орієнтований на підготовку фахівців, здатних розв'язувати дослідницькі й інноваційні завдання, розробляти сучасні ІТ, моделі та засоби кіберзахисту, аналізувати ризики, протидіяти кіберінцидентам і забезпечувати технічний та криптографічний захист.
ОПП сприяє досягненню Цілі 4 «Якісна освіта» через розвиток автономного навчання, дослідницьких і педагогічних компетентностей (РН17, РН18; ОК2–ОК4, ОК11); Цілі 8 «Гідна праця та економічне зростання» — через підготовку фахівців для державного, ІТ- та інфраструктурного секторів і формування здатності управляти кіберризиками та безперервністю процесів (РН10); Цілі 9 «Промисловість, інновації та інфраструктура» — через розроблення, моделювання та впровадження систем кіберзахисту (РН19–РН24); Цілі 16 «Мир, справедливість та сильні інституції» — через протидію кіберінцидентам, аудит, моніторинг і захист критичної інфраструктури.
Ціль 17 «Партнерство заради сталого розвитку» реалізується через співпрацю з роботодавцями та державними структурами, зокрема Департаментом поліції охорони НПУ, ТОВ «ЛУЧ» і ТОВ «ДЕФЕНДІКО». Отже, ОПП сприяє цифровій стійкості, інноваціям, якісній освіті та підвищенню рівня національної кібербезпеки.

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

Правила прийому на навчання до Державного університету інформаційно-комунікаційних технологій та вимоги до вступників оприлюднені на офіційному вебсайті ДУІКТ у розділі «Вступ 2026 – Правила прийому». https://duikt.edu.ua/ua/108-pravila-priyomu-priymalna-komisiya?id=108&lang=ua&sys_link=pravila-priyomu-priymalna-komisiya На сторінці розміщено чинні Правила прийому до ДУІКТ у 2026 році та додатки до них із переліком спеціальностей, освітніх програм, конкурсних пропозицій і вимог до вступу. Для спеціальності F5 «Кібербезпека та захист інформації» у переліку магістерських програм зазначена ОПП «Технічні системи інформаційного та кібернетичного захисту».

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

Правила прийому до ДУІКТ та вимоги до вступників на ОПП «Технічні системи інформаційного та кібернетичного захисту» другого (магістерського) рівня за спеціальністю F5 «Кібербезпека та захист інформації» враховують складність і професійну спрямованість програми через вимоги до попереднього рівня освіти та конкурсного відбору. До вступу допускаються особи зі ступенем бакалавра або магістра, що відповідає 7 рівню НРК та змісту ОПП, орієнтованої на розв'язання складних професійних, дослідницьких та інноваційних завдань у сфері кібербезпеки, технічного і криптографічного захисту інформації.
Конкурсний відбір дає можливість оцінити академічну підготовленість вступника та його готовність до магістерського навчання, що передбачає дослідницьку діяльність, роботу з нормативно-технічною документацією, математичними і системними методами, спеціалізованим програмним та апаратним забезпеченням.

Правила прийому не обмежують вступ випускниками однієї спеціальності, що відповідає міждисциплінарному характеру кібербезпеки. Поєднання вимог до попередньої освіти, конкурсного відбору та відкритості для вступників із суміжною підготовкою забезпечує належний рівень готовності до опанування ОПП.

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?

Питання визнання результатів навчання, отриманих в інших ЗВО, у тому числі в межах академічної мобільності, для здобувачів ОПП «Технічні системи інформаційного та кібернетичного захисту» регулюються нормативними документами ДУІКТ: Положенням про академічну мобільність (https://duikt.edu.ua/uploads/p_447_36289291.pdf), Положенням про організацію освітнього процесу (https://duikt.edu.ua/uploads/p_447_49109699.pdf) та Положенням про неформальну та інформальну освіту (https://duikt.edu.ua/uploads/p_447_35048489.pdf). Документи визначають порядок участі у внутрішній і міжнародній мобільності, погодження індивідуальної освітньої траєкторії, перезарахування освітніх компонентів і кредитів ЄКТС та визнання результатів навчання, здобутих в інших ЗВО. Визнання здійснюється шляхом зіставлення змісту компонентів, кількості кредитів, компетентностей і програмних результатів. За їх відповідності вимогам ОПП результати можуть бути зараховані без повторного вивчення дисципліни.
Інформація про партнерство та можливості академічної мобільності оприлюднюється на сайті ДУІКТ: https://duikt.edu.ua/ua/233-spivrobitnictvo-mizhnarodna-diyalnist.
Такий механізм забезпечує гнучкість індивідуальної освітньої траєкторії та розширює можливості набуття професійного й дослідницького досвіду.

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

Застосування практики визнання результатів навчання, отриманих у інших освітніх програмах для здобувачів вищої освіти ОПП «Технічні системи інформаційного та кібернетичного захисту» протягом звітного періоду не відбувалось.

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?

Визнання результатів навчання, отриманих здобувачами ОПП «Технічні системи інформаційного та кібернетичного захисту» у неформальній та/або інформальній освіті, регулюється Положенням про неформальну та інформальну освіту у ДУІКТ: https://duikt.edu.ua/uploads/p_447_35048489.pdf та Положенням про порядок перезарахування результатів навчання: https://duikt.edu.ua/uploads/p_949_73284553.pdf.

Документи визначають порядок подання заяви, перелік підтвердних документів, оцінювання та співвіднесення набутих результатів із компетентностями і програмними результатами відповідного освітнього компонента, а також процедуру їх визнання і перезарахування.

Для ОПП така процедура актуальна, оскільки професійні компетентності можуть додатково формуватися під час сертифікованих курсів, тренінгів і програм підвищення кваліфікації з кібербезпеки, технічного захисту інформації, контролю доступу, управління інцидентами та мережевої безпеки. Результати визнаються за умови їх відповідності результатам навчання ОПП.

Доступність процедури забезпечується оприлюдненням нормативних документів на сайті ДУІКТ: https://duikt.edu.ua/ua/447-polozhennya-normativni-dokumenti, а також інформуванням здобувачів гарантом ОПП, кафедрою та навчальним підрозділом. Це забезпечує можливість інтегрувати додатково набуті компетентності в індивідуальну освітню траєкторію.

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

Застосування практики визнання результатів навчання, отриманих у неформальній освіті, для здобувачів вищої освіти другого (магістерського) рівня по ОП Технічні системи інформаційного та кібернетичного захисту» протягом 2024 –2026 навчальних років не було.

4. Навчання і викладання за освітньою програмою

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

Освітній процес за ОП «Технічні системи інформаційного та кібернетичного захисту» другого (магістерського) рівня за спеціальністю F5 «Кібербезпека та захист інформації» організовано відповідно до Закону України «Про вищу

освіту», який визначає основні форми освітнього процесу: навчальні заняття, самостійну роботу, практичну підготовку та контрольні заходи.
Підготовка магістрів у ДУІКТ регламентується Положенням про організацію освітнього процесу: https://duikt.edu.ua/uploads/p_447_49109699.pdf, розробленим відповідно до законодавства України. Положення визначає порядок планування освітнього процесу, форми і види занять, самостійну та практичну підготовку, контрольні заходи й атестацію. Навчання здійснюється також відповідно до затверджених ОПП та навчального плану.
Досягнення мети та програмних результатів забезпечується поєднанням лекційних, практичних і лабораторних занять, самостійної та науково-дослідної роботи, практик, консультацій і контролю.
ОПП та інформація про освітні компоненти розміщені на сайті: https://duikt.edu.ua/ua/1823-osvitno-profesiyni-programi-kafedra-sistem-informaciynogo-ta-kibernetichnogo-zahistu.
Силабуси дисциплін доступні за посиланням: https://duikt.edu.ua/ua/253-navchalni-disciplini-kafedra-cistem-tehnichnogo-zahistu-informacii.

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?

Здобувачам другого (магістерського) рівня за ОПП «Технічні системи інформаційного та кібернетичного захисту» забезпечено доступ до силабусів, навчально-методичних матеріалів, завдань, електронної бібліотеки та цифрових ресурсів ДУІКТ. Методи навчання охоплюють лекційні, практичні, лабораторні, дослідницькі та інтерактивні форми.

Студентоцентрований підхід реалізується через вибір індивідуальних завдань, тематики дослідницької й кваліфікаційної роботи та формування індивідуальної освітньої траєкторії. Вибіркові компоненти становлять 25 із 90 кредитів ЄКТС (27,8 %). Каталог вибору: https://duikt.edu.ua/ua/2080-katalog-osvitnih-komponentiv-vilnogo-viboru-studentami-navchannya

Застосовуються аналіз професійних ситуацій, групові й індивідуальні завдання, лабораторні роботи, презентації, спеціалізоване ПЗ і технічні засоби. Зворотний зв'язок забезпечується консультаціями, спілкуванням із викладачами та гарантом ОПП, електронними засобами й опитуваннями.

Результати опитувань оприлюднюються: https://duikt.edu.ua/ua/1352-rezultati-opituvan-vnutrishnya-sistema-zabezpechennya--yakosti-vischoi-osviti-ta-osvitnoi-diyalnosti та https://duikt.edu.ua/ua/3134-opituvannya-zdobuvachiv-diyalnist-kafedri. Здобувачі також залучаються до оновлення ОПП: https://duikt.edu.ua/ua/news-1-9-15131-studenti-magistri-doluchilisya-do-obgovorennya-onovlennya-osvitno-profesiynih-program-kafedri-tehnichnih-sistem-kiberzahistu. Загалом здобувачі позитивно оцінюють методи й організацію навчання.

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

Відповідно до Положення про організацію освітнього процесу у ДУІКТ науково-педагогічні працівники мають право на академічну свободу, що передбачає самостійний вибір форм, методів, засобів і технологій навчання для досягнення програмних результатів та забезпечення якості освітнього процесу: https://duikt.edu.ua/uploads/p_447_49109699.pdf.
На ОПП «Технічні системи інформаційного та кібернетичного захисту» академічна свобода реалізується під час розроблення силабусів і робочих програм, визначення змісту лекційних, практичних і лабораторних занять, добору наукових і нормативних джерел, організації самостійної роботи та форм контролю. Викладачі адаптують методи навчання до специфіки компонентів, рівня підготовки здобувачів і сучасних тенденцій кібербезпеки.
Для здобувачів академічна свобода забезпечується через індивідуальну освітню траєкторію, вибір дисциплін, тематики досліджень, практик і кваліфікаційної роботи. Вибіркові компоненти становлять 25 із 90 кредитів ЄКТС (27,8 %). Каталог: https://duikt.edu.ua/ua/2080-katalog-osvitnih-komponentiv-vilnogo-viboru-studentami-navchannya.
Отже, академічна свобода поєднує автономію викладачів і здобувачів із відповідальністю за досягнення результатів навчання та якість підготовки.

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

Основними інформаційними ресурсами ДУІКТ для здобувачів ОП «Технічні системи інформаційного та кібернетичного захисту» є офіційний сайт , сторінка кафедри; https://duikt.edu.ua/ua/47-kafedra-cistem-tehnichnogo-zahistu-informacii-kafedri, електронне освітнє середовище та електронна бібліотека. У відкритому доступі розміщуються ОПП, силабуси, навчально-методичні матеріали та інша інформація щодо організації навчання.
В електронному середовищі доступні презентації, конспекти лекцій, завдання до практичних і лабораторних занять, матеріали для самостійної роботи, контрольні завдання та методичні рекомендації. Інформація про е-навчання: https://duikt.edu.ua/ua/149-e-navchannya-navchannya. Для дистанційної роботи використовуються Google Classroom і Google Meet.
У силабусах визначаються цілі, зміст, компетентності, програмні результати навчання, форми занять, види контролю та критерії оцінювання. Вони доступні до початку або на початку вивчення дисципліни. На першому занятті викладач додатково роз'яснює мету, структуру компонента, форми контролю, порядок нарахування балів та критерії оцінювання.

Додаткові ресурси доступні в електронній бібліотеці ДУІКТ: https://duikt.edu.ua/ua/lib/1/category/2122.
Отже, необхідна інформація надається завчасно, уточнюється на початку вивчення компонента та залишається доступною протягом семестру, що забезпечує прозорість освітнього процесу.

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

Під час реалізації ОП Кібербезпека викладання теорії поєднується з різноманітними елементами досліджень. Заняття за ОП проводяться у спеціалізованих навчальних лабораторіях: Мережевої безпеки; Реагування на кіберінциденти; Захисту кінцевих точок; Засобів контролю доступу; Технічного захисту інформації; Security Operation Center; Систем безпеки та телекомунікаційного обладнання із штучним інтелектом, та ін: https://duikt.edu.ua/ua/news-1-569-14627-studenti-magistri-doluchilisya-do-seminaru-kafedri-tehnichnih-sistem-kiberzahistu-ta-tov-defendiko-schodo-novaciy-u-sferi-zahistu-informacii-ta-kiberzahistu_kafedra-cistem-tehnichnogo-zahistu-informacii, https://duikt.edu.ua/ua/news-1-569-14052-na-kafedri-tehnichnih-sistem-kiberzahistu-vidbuvsya-naukovo-praktichniy-seminar-vid-kompanii-ajax-systems_kafedra-cistem-tehnichnogo-zahistu-informacii.
Поєднання навчання і досліджень за ОП підкріплюється спільними публікаціями викладачів та здобувачів вищої освіти другого (магістерського) рівня.
Студенти мають можливість публікувати результати своїх досліджень у наукових виданнях ДУІКТ: «Телекомунікаційні та інформаційні технології», «Зв'язок», «Сучасний захист інформації», «Наукові записки Державного університету інформаційно-комунікаційних технологій» (https://duikt.edu.ua/ua/123-periodichnividannya. Результати досліджень доповідаються на конференціях, семінарах та засіданнях круглих столів: https://duikt.edu.ua/uploads/p_2779_72486260.pdf, https://duikt.edu.ua/uploads/p_2661_93669247.pdf

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

Зміст освітніх компонентів за потреби оновлюється НПП напередодні навчального року. Порядок і підстави внесення змін визначено Положенням про запровадження та оновлення освітніх програм у ДУІКТ: https://duikt.edu.ua/uploads/p_447_73345463.pdf.
Оновлення здійснюється з урахуванням наукових досягнень і сучасних практик у тісній співпраці зі стейкхолдерами та на основі їх досвіду впровадження технологій технічного захисту інформації у державному і корпоративному секторах: https://duikt.edu.ua/ua/news-1-569-14627-studenti-magistri-doluchilisya-do-seminaru-kafedri-tehnichnih-sistem-kiberzahistu-ta-tov-defendiko-schodo-novaciy-u-sferi-zahistu-informacii-ta-kiberzahistu_kafedra-cistem-tehnichnogo-zahistu-informacii; https://duikt.edu.ua/ua/news-1-569-14541-studenti-magistri-doluchilisya-do-seminaru-kafedri-tehnichnih-sistem-kiberzahistu--i-tov-defendiko-schodo-vprovadzhennya-zakonodavchih-novaciy-u-sferi-kiberbezpeki_kafedra-cistem-tehnichnogo-zahistu-informacii.

Важливим чинником оновлення ОПП є результати НДР кафедри: «Шляхи підвищення ефективності захисту командно-телеметричної інформації безпілотних літальних апаратів» (0120U100244, керівник О. Туровський); «Розроблення алгоритмів для забезпечення функціональної стійкості інтелектуальних систем при прийнятті рішень» (0125U000865, Ю. Пепа); «Розробка методу оцінки завадостійкості когерентного прийому дискретного сигналу з багатопозиційною фазовою маніпуляцією в умовах нефлуктаційних завад» (0126U001466, О. Туровський); «Розробка засобів зниження впливу імпульсних нефлуктуаційних перешкод на завадостійкість прийому сигналів управління безпілотними системами» (0126U001544, О. Туровський).
У 2026 р. подано заявку на прикладне дослідження «Розроблення інтелектуальної системи оцінювання стану кіберзахисту об'єктів інформаційної інфраструктури на основі аналізу аномалій мережевого трафіку» (протокол Вченої ради ДУІКТ №21 від 15.07.2026, керівник М. Рижаков), яка перебуває на розгляді МОН України. Результати досліджень відображаються у силабусах ОК «Організація проведення наукових досліджень», «Радіомоніторинг і радіопротидія на об'єктах ІД», «Технологія створення та застосування комплексів засобів захисту інформації…», «Ліцензування, атестація та сертифікація у сфері безпеки ОІД». Практичним результатом стала «Методика виявлення закладних пристроїв», на підставі якої Університет отримав ліцензію Держспецзв'язку: https://cip.gov.ua/ua/news/nakaz-pro-vidachu-licenziyi-drzhavnomu-universitetu-telekomunikacii.

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

Міжнародна діяльність ДУІКТ здійснюється на основі договорів з іноземними ЗВО, науковими установами та міжнародними організаціями: https://duikt.edu.ua/ua/233-spivrobitnictvo-mizhnarodna-diyalnist. Інтернаціоналізація безпосередньо закладена в ОПП «Технічні системи інформаційного та кібернетичного захисту»: передбачено викладання українською та англійською мовами, а ОК4 «Науково-технічний переклад» формує іншомовну професійну комунікацію.
ОПП орієнтована на використання кращих світових практик і міжнародних стандартів; це закріплено у КФ2, КФ4 та РН7. Важливим елементом є використання результатів міжнародного проєкту ЄС TEMPUS ENGENSEC №544455-TEMPUS-1-2013-1-SE-TEMPUS-JPCR, спрямованого на підготовку нового покоління експертів з кібербезпеки.
Наукова складова ОПП передбачає застосування світового досвіду, самостійну науково-дослідну роботу, участь у міжнародних конференціях, публікаціях і спільних дослідженнях. Програмою також передбачено міжнародну кредитну мобільність, участь у програмах подвійних дипломів і можливість навчання іноземних громадян.
Отже, інтернаціоналізація ОПП реалізується через міжнародну мобільність, англомовну підготовку, світові стандарти, проєкт ENGENSEC та міжнародне наукове співробітництво.

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?

Процедура проведення контрольних заходів за ОПП «Технічні системи інформаційного та кібернетичного захисту» регламентується Положенням про організацію освітнього процесу у ДУІКТ: https://duikt.edu.ua/uploads/p_447_49109699.pdf. В освітньому процесі застосовуються вхідний, поточний, рубіжний (модульний, тематичний) та підсумковий контроль. Оцінювання сформованих компетентностей здійснюється під час контрольних заходів, передбачених ОПП і навчальним планом.
Форми контролю для кожного освітнього компонента визначаються його змістом, компетентностями та програмними результатами навчання і конкретизуються у силабусах. Застосовуються тестування, усне й письмове опитування, виконання практичних і лабораторних робіт, ситуаційних та індивідуальних завдань, презентації, звіти за практиками, заліки та іспити. ОПП передбачає лекційні, практичні, лабораторні заняття, розв'язання ситуаційних завдань, тестування, презентації, кейси партнерів кафедри та три види практики.
Такий комплексний підхід дозволяє оцінити не лише засвоєння теоретичних знань, а й здатність застосовувати їх у професійних ситуаціях. Наприклад, контроль за ОК7–ОК10 дозволяє перевірити досягнення результатів щодо аналізу захищеності, застосування стандартів, управління доступом, технічного захисту, радіомоніторингу та спеціальних досліджень. У межах програми РН8–РН13 передбачають здатність розробляти й супроводжувати системи захисту, оцінювати ризики, забезпечувати управління доступом, протидіяти кіберінцидентам та використовувати засоби технічного і криптографічного захисту.
Результати практичної підготовки контролюються шляхом оцінювання виконаних завдань і звітів за науково-педагогічною, науково-дослідною та переддипломною практиками. Досягнення результатів навчання за ОПП у цілому завершується підготовкою та публічним захистом кваліфікаційної роботи, що дозволяє комплексно оцінити здатність магістранта самостійно розв'язувати професійні, дослідницькі та інноваційні завдання.
Згідно з практикою ДУІКТ, реалізація контролю ґрунтується на системному оцінюванні вимірюваних результатів навчання та комплексному використанні різних форм контролю. Результати оцінюються за 100-бальною шкалою, національною шкалою та шкалою ECTS: для іспитів — A, B, C, D, E, FX, F; для заліків — «зараховано/не зараховано» з відповідним переведенням у шкалу ECTS.
Таким чином, поєднання поточного, рубіжного та підсумкового контролю, різних форм перевірки теоретичних і практичних результатів, чітких критеріїв оцінювання та підсумкового захисту кваліфікаційної роботи дозволяє об'єктивно встановити рівень досягнення результатів навчання як за кожним окремим освітнім компонентом, так і за ОПП у цілому, а також своєчасно коригувати освітній процес.

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

Чіткість та зрозумілість форм контрольних заходів і критеріїв оцінювання за ОПП «Технічні системи інформаційного та кібернетичного захисту» забезпечуються вимогами Положення про організацію освітнього процесу у ДУІКТ: https://duikt.edu.ua/uploads/p_447_49109699.pdf та їх конкретизацією у силабусах освітніх компонентів. ОПП передбачає вхідний, поточний, рубіжний (модульний, тематичний) та підсумковий контроль. Оцінювання сформованих компетентностей здійснюється через контрольні заходи, визначені ОПП і навчальним планом. Для кожної дисципліни у силабусі зазначаються форми контролю, види навчальної роботи, максимальна кількість балів, умови допуску до підсумкового контролю та критерії відповідності результатів певному рівню компетентності. Застосовується 100-бальна шкала з переведенням у національну шкалу та шкалу ЄКТС. Приклади силабусів ДУІКТ підтверджують деталізацію балів за практичні роботи, опитування, презентації, модульні завдання, залік або іспит. На початку вивчення дисципліни викладач доводить до здобувачів форми контролю, порядок нарахування балів і критерії оцінювання. Силабуси доступні на сайті кафедри: https://duikt.edu.ua/ua/253-navchalni-disciplini-kafedra-cistem-tehnichnogo-zahistu-informacii. Це забезпечує прозорість, передбачуваність та однакове розуміння вимог усіма здобувачами.

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

Інформація про форми контрольних заходів та критерії оцінювання за ОПП «Технічні системи інформаційного та кібернетичного захисту» доводиться до здобувачів завчасно та системно. В ОПП передбачено вхідний, поточний, рубіжний (модульний, тематичний) і підсумковий контроль, а оцінювання сформованих компетентностей здійснюється відповідно до навчального плану та силабусів освітніх компонентів. На початку кожного семестру, на першому занятті, викладач ознайомлює здобувачів зі структурою дисципліни, формами контролю, видами завдань, порядком нарахування балів і критеріями оцінювання. Надалі перед проведенням конкретного контрольного заходу додатково уточнюються вимоги до його виконання.
Форми контролю та критерії оцінювання наведені у силабусах освітніх компонентів, доступних на сторінці кафедри: https://duikt.edu.ua/ua/253-navchalni-disciplini-kafedra-cistem-tehnichnogo-zahistu-informacii. Навчально-методичні матеріали також доступні через Google Classroom, що передбачено інформаційним забезпеченням ОПП. Строки семестрового контролю визначаються навчальним планом і розкладом освітнього процесу. Отже, здобувачі отримують інформацію про форми та критерії оцінювання до початку або на початку вивчення освітнього компонента, а вона залишається доступною протягом усього семестру.

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

Атестація здобувачів за ОПП «Технічні системи інформаційного та кібернетичного захисту» другого (магістерського) рівня відповідає Стандарту вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації», затвердженому наказом МОН України від 18.03.2021 №332. В ОПП атестація визначена у формі публічного захисту кваліфікаційної роботи.
Кваліфікаційна робота має передбачати розв'язання складної задачі інформаційної та/або кібербезпеки, проведення досліджень та/або здійснення інновацій, не містити академічного плагіату, фабрикації чи фальсифікації. Атестація проводиться відкрито і гласно. ОК14 «Підготовка кваліфікаційної роботи, підсумкова атестація» має обсяг 9 кредитів ЄКТС і забезпечує комплексну перевірку РН3–РН5, РН8, РН10–РН13, РН17, РН19–РН23.
Відповідно до чинного переліку спеціальностей, затвердженого постановою КМУ №497, для F5 «Кібербезпека та захист інформації» ЄДКІ передбачений на першому (бакалаврському), а не на другому (магістерському) рівні. Тому для цієї магістерської ОПП підтвердження результатів навчання через ЄДКІ не застосовується; підсумкова атестація здійснюється шляхом публічного захисту кваліфікаційної роботи.

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

Процедура проведення контрольних заходів за ОПП «Технічні системи інформаційного та кібернетичного захисту» регламентується Положенням про організацію освітнього процесу у ДУІКТ: https://duikt.edu.ua/uploads/p_447_49109699.pdf. Контрольні заходи є елементом зворотного зв'язку та дають змогу встановити відповідність набутих здобувачами знань, умінь і навичок вимогам освітньої програми. Перелік екзаменів і заліків визначається навчальним планом. В ОПП передбачено вхідний, поточний, рубіжний (модульний, тематичний) та підсумковий контроль, а оцінювання сформованих компетентностей здійснюється під час контрольних заходів, визначених ОПП і навчальним планом. Доступність процедури для учасників освітнього процесу забезпечується оприлюдненням нормативних документів на офіційному сайті ДУІКТ та конкретизацією форм контролю і критеріїв оцінювання у силабусах кожного освітнього компонента. Силабуси ОПП доступні на сторінці кафедри: https://duikt.edu.ua/ua/253-navchalni-disciplini-kafedra-cistem-tehnichnogo-zahistu-informacii. Додатково здобувачам доступні графік освітнього процесу, розклади занять і атестації на сайті ДУІКТ: https://duikt.edu.ua/ua/136-navchalniy-proces-navchannya. На початку семестру викладачі ознайомлюють здобувачів із формами контрольних заходів, порядком їх проведення та критеріями оцінювання.

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

Об'єктивність екзаменаторів за ОПП «Технічні системи інформаційного та кібернетичного захисту» забезпечується єдиними вимогами до контрольних заходів, визначеними Положенням про організацію освітнього процесу, навчальним планом і силабусами. Форми контролю та критерії оцінювання доводяться до здобувачів завчасно, що мінімізує суб'єктивність оцінювання. В ОПП передбачено вхідний, поточний, рубіжний і підсумковий контроль.
Запобігання та врегулювання конфлікту інтересів регламентує Положення про вирішення конфліктних ситуацій у ДУІКТ: https://duikt.edu.ua/uploads/p_447_88699516.pdf. Воно визначає порядок подання й розгляду звернень та процедури врегулювання конфліктів. Додатковими механізмами є Кодекс академічної доброчесності https://duikt.edu.ua/uploads/p_447_96297052.pdf та Положення про систему внутрішнього забезпечення якості https://duikt.edu.ua/uploads/p_447_18879118.pdf. Повідомити про можливі порушення можна через керівництво Університету, уповноважену особу з питань запобігання корупції або скриньку довіри vps@duikt.edu.ua: https://duikt.edu.ua/ua/1471-protidii-korupcii-pro-universitet. За доступними матеріалами ДУІКТ, задокументованих випадків оскарження об'єктивності екзаменаторів або конфлікту інтересів саме на цій ОПП не виявлено; отже, наводити вигаданий приклад застосування процедури недоцільно.

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

Порядок повторного проходження контрольних заходів за ОПП «Технічні системи інформаційного та кібернетичного захисту» регламентується Положенням про організацію освітнього процесу у ДУІКТ: https://duikt.edu.ua/uploads/p_447_49109699.pdf. ОПП передбачає поточний, рубіжний та підсумковий контроль, а форми підсумкового контролю визначаються навчальним планом і силабусами. У разі отримання незадовільної оцінки здобувач має право на перескладання екзамену (заліку) не більше двох разів з кожного освітнього компонента: перше перескладання проводить викладач, друге — комісія, створена директором інституту. Оцінка комісії є остаточною. Якщо здобувач, допущений до семестрового контролю, без поважної причини не з'явився, це вважається використанням першої спроби. За документально підтверджених поважних причин може встановлюватися індивідуальний графік. Здобувачам, які мають академічну заборгованість у межах, установлених Положенням, надається можливість ліквідувати її у визначені строки, як правило, до початку наступного семестру.

На ОП ці правила застосовуються до передбачених навчальним планом іспитів і заліків. Документально підтверджених випадків другого перескладання перед комісією саме за цією ОПП у доступних матеріалах ДУІКТ не виявлено, тому фактичні приклади без підтвердження не наводяться.

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

Порядок оскарження процедури та результатів контрольних заходів у ДУІКТ регламентується Положенням про організацію освітнього процесу https://duikt.edu.ua/uploads/p_447_49109699.pdf та Положенням про вирішення конфліктних ситуацій https://duikt.edu.ua/uploads/p_447_88699516.pdf. Здобувач має право оскаржити оцінку, яку вважає необ'єктивною, шляхом подання відповідного звернення або скарги. Для розгляду питань, що виникли під час підсумкового семестрового контролю, розпорядженням директора ННІ не пізніше наступного робочого дня після звернення створюється апеляційна комісія. До її складу, залежно від ситуації, можуть входити директор або заступник директора ННІ, завідувач кафедри, куратор групи та голова студентської ради. Комісія розглядає звернення не пізніше п'яти робочих днів, після чого рішення повідомляється здобувачу та оформлюється протоколом, який зберігається в навчальній частині ННІ. За ОПП «Технічні системи інформаційного та кібернетичного захисту» форми контролю визначаються навчальним планом і силабусами; ОПП передбачає вхідний, поточний, рубіжний та підсумковий контроль. У доступних матеріалах ДУІКТ випадків оскарження результатів контрольних заходів саме на цій ОПП не зафіксовано, тому фактичні приклади застосування апеляційної процедури відсутні.

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

Політика, стандарти і процедури дотримання академічної доброчесності прописані в Кодексі академічної доброчесності https://duikt.edu.ua/uploads/p_447_96297052.pdf; Положенні про систему внутрішнього забезпечення якості вищої освіти https://duikt.edu.ua/uploads/p_447_18879118.pdf; Положенні про систему запобігання та виявлення академічного плагіату в ДУІКТ https://duikt.edu.ua/uploads/p_447_61575036.pdf
Також, в Університеті створено Комісію з питань академічної доброчесності ДУІКТ
https://duikt.edu.ua/uploads/p_2704_50494310.pdf
Повноваженнями щодо впровадження політики академічної доброчесності та дотримання її процедури наділені: Гарант ОНП, Комісія з питань академічної доброчесності, директори інститутів, завідувачі кафедр, члени групи забезпечення спеціальності.

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

В якості інструментів щодо запобігання проявам академічної недоброчесності використовуються: інформування здобувачів вищої освіти про неприпустимість наявності плагіату у кваліфікаційних роботах, перевірка наукових та кваліфікаційних робіт на плагіат з використанням комп'ютерної програми для внутрішньої перевірки текстів на наявність академічного плагіату StrikePlagiarism.com https://panel.strikeplagiarism.com/#/ . Процедура інформування НПП щодо потреби запобігати академічній недоброчесності при вивченні освітніх компонентів в Університеті закріплена обов'язковим підписанням НПП відповідної декларації.
Крім того, всі навчальні аудиторії, в яких ведеться підготовка здобувачів за ОПП, обладнані відеокамерами, що унеможливлює використання під час екзамену матеріалів, не передбачених програмою іспиту.
Кваліфікаційні роботи здобувачів вищої освіти ОП знаходяться в вільному доступі та розміщені в репозитарії на сайті університету: https://duikt.edu.ua/ua/reposit?
path=%D0%9A%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B0+%D0%A2%D0%B5%D1%85%D0%BD%D1%96%D1%87%D0%BD%D0%B8%D1%85+%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC+%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83%2F2026

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

Популяризація академічної доброчесності серед здобувачів освіти здійснюється шляхом: формування умов довіри й поваги між учасниками освітнього процесу; інформування учасників освітнього процесу про необхідність дотримання правил академічної доброчесності; комп'ютерної перевірки текстів на наявність академічного плагіату; запровадження викладання у рамках освітніх компонент тем з основ академічного письма та дослідницької роботи з особливою увагою до принципів самостійної роботи, коректного застосування інформації; ознайомлення усіх учасників освітнього процесу з Кодексом академічної доброчесності
https://duikt.edu.ua/uploads/p_447_96297052.pdf , підписання кожним учасником освітнього процесу Декларації про академічну доброчесність. Питання дотримання правил академічної доброчесності обговорюються також на засіданнях кафедри.

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

Порушення академічної доброчесності з боку здобувачів передбачає повторне проходження оцінювання; повторне проходження відповідного освітнього компонента освітньої програми; позбавлення академічної стипендії; позбавлення наданих закладом освіти пільг з оплати за навчання, або відрахування із ДУІКТ.
Порушення академічної доброчесності науково-педагогічними, педагогічними працівниками передбачає з боку ЗВО відмову у присудженні наукового ступеня чи присвоєнні вченого звання; позбавленні права брати участь у роботі визначених законом органів чи займати визначені законом посади.
За час реалізації ОПП «Технічні системи інформаційного та кібернетичного захисту» випадків виявлення порушень академічної доброчесності з боку науково-педагогічних працівників та здобувачів вищої освіти другого рівня 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

Кваліфікація викладачів, залучених до реалізації ОПП, підтверджується профільною освітою, науковими ступенями, публікаціями у фахових виданнях, навчально-методичними працями та підвищенням кваліфікації.
Туровський О.Л., д.т.н., професор, викладає ОК «Корпоративна та професійна етика в кібербезпеці» та «Організація проведення наукових досліджень». Має фахову дисертацію. Праці з професійних стандартів, моделювання, кіберзахисту телекомунікаційних мереж та посібники з етики й основ наукових досліджень відповідають змісту ОК.

Котенко А.М., к.т.н., доцент, викладає ОК «Технологія створення та застосування комплексів засобів захисту інформації з обмеженим доступом та охорони ОІД» і «Теорія захисту інформаційних ресурсів обмеженого доступу». Має фахову дисертацію. Профільність підтверджують праці з моделювання систем захисту, оцінювання захищеності корпоративних мереж, навчальний посібник та стажування в ТОВ «ЛУЧ» і ТОВ «ДЕФЕНДІКО».

Іванченко І.С., к.т.н., доцент, професор кафедри, викладає ОК «Організація і проведення спеціальних досліджень на ОІД». Має фахову дисертацію. Праці з оцінювання кіберзахищеності, захисту мовної інформації, виявлення DDoS-атак та аномалій відповідають змісту ОК.

Пепа Ю.В., к.т.н., доцент, професор кафедри, викладає ОК «Радіомоніторинг і радіопротидія на ОІД». Має фахову дисертацію, освіту з радіоелектронних систем і кібербезпеки. Наукові роботи з радіотехнічних систем, обробки сигналів та кіберзагроз, а також профільні стажування забезпечують відповідність ОК.

Рижаков М.М., доктор філософії, старший викладач, викладає ОК «Ліцензування, атестація та сертифікація у сфері безпеки ОІД». Має фахову дисертацію. Публікації з аналізу ризиків, загроз, вразливостей та аномалій мережевого трафіку формують науково-практичну основу ОК.

Поночовний П.М., доктор філософії, доцент, викладає ОК «Стандарти кібербезпеки та захисту конфіденційної інформації». Має фахову дисертацію. Праці з протидії DDoS-атакам, кібербезпеки хмарного середовища та мережевих вторгнень, експертна діяльність і підвищення кваліфікації відповідають змісту ОК.

Колісниченко А.В., к.філол.н., доцент, викладає ОК «Англійська мова для ділової комунікації». Має фахову дисертацію. Відповідність забезпечують філологічна підготовка, закордонне стажування та підвищення кваліфікації з методики викладання й академічної доброчесності.

Кондратенко Н.Ю., к.пед.н., доцент, викладає ОК «Педагогіка і психологія у вищій школі». Має фахову дисертацію. Дослідження комунікативної компетентності та підвищення кваліфікації з педагогіки й академічної доброчесності підтверджують відповідність ОК.

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

Формування колективу для забезпечення освітньої діяльності за ОПП, здійснюється відповідно до чинних нормативно-правових вимог, Ліцензійних умов провадження освітньої діяльності, Статуту та нормативних документів Університету. Відповідальність щодо визначення відповідності кваліфікації працівника та його рівня професійної та наукової активності покладається на завідувача кафедри або керівника групи забезпечення спеціальності на підставі Ліцензійних умов. Процедури проведення конкурсу на заміщення вакантних посад та порядок перевиборів здійснюються відповідно до нормативних документів Університету, це: Положення про порядок проведення конкурсу на заміщення вакантних посад НПП https://duikt.edu.ua/uploads/p_447_91164126.pdf , Положення про щорічну рейтингову оцінку діяльності НПП https://duikt.edu.ua/uploads/p_447_89539392.pdf Кандидатури на заміщення посад НПП попередньо обговорюються на кафедрі в їх присутності. Претендент проводить відкрите заняття після цього здійснюється обговорення рівня його професійної майстерності. НПП по закінченню терміну контракту подає документи до Конкурсної комісії у повному обсязі на рівних умовах. Для оцінки рівня відповідності НПП долучається рейтингова картка. Рішення конкурсної комісії затверджується Вченою радою Університету. Рейтинг НПП Університету щорічно висвітлюється на офіційному сайті https://duikt.edu.ua/uploads/p_2703_19984749.pdf

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

ДУІКТ системно залучає роботодавців, професіоналів-практиків та експертів галузі до реалізації ОПП «Технічні системи інформаційного та кібернетичного захисту». Представник роботодавців — заступник директора ТОВ «ЛУЧ» Герман Шуклін — входить до робочої групи ОПП, що забезпечує врахування вимог галузі при її перегляді. ОПП передбачає практичну складову за участю компаній-партнерів, використання професійних кейсів та залучення фахівців до занять. Конкретним прикладом є науково-практичний семінар Ajax Systems, присвячений сучасним охоронним технологіям і системам безпеки: https://duikt.edu.ua/ua/news/1/category/569/view/14052. Фахівці Поліції

охорони під час робочої зустрічі ознайомили кафедру з практикою захисту важливих об'єктів інформаційної діяльності та сучасними технологіями захисту: https://duikt.edu.ua/ua/news/1/category/569/view/14076. До оновлення професійного змісту підготовки залучається ТОВ «ДЕФЕНДІКО» через спільні семінари щодо законодавчих новацій у сфері кібербезпеки: https://duikt.edu.ua/ua/news-1-569-14627-vikladachi-kafedri-tehnichnih-sistem-kiberzahistu-proveli-seminar-z-tov-defendiko-schodo-zmin-u-zakonodavstvi-pro-kiberbezpeku. Роботодавці також беруть участь у Днях кар'єри та ярмарках вакансій, де знайомлять здобувачів із вимогами ринку, реальними проєктами, вакансіями та можливостями працевлаштування.

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

ДУІКТ сприяє викладачам ОП у проходженні підвищення кваліфікації відповідно до Положення про підвищення кваліфікації науково-педагогічних працівників https://duikt.edu.ua/uploads/p_447_82499307.pdf .
Кількість заходів професійного розвитку викладачів становлять:
Туровський О.Л.: 2025 р. – підвищення кваліфікації у ТОВ «ДЕФЕНДІКО» за програмою «Захист державних інформаційних ресурсів»; 2026 р. – онлайн-курс Prometheus «Академічна доброчесність».
Котенко А.М.: 2025 р. – підвищення кваліфікації у ТОВ «ДЕФЕНДІКО» за програмою «Захист державних інформаційних ресурсів».
Іванченко І.С.: 2024 р. – стажування у ДВНЗ «Ужгородський національний університет».
Пепа Ю.В.:2026 р. – міжнародне стажування в European Institute for Innovation Development за програмою «Implementation of Innovations in Technologies and Engineering: Experience of the Czech Republic», м. Острава (Чеська Республіка);
Рижаков М.М.: 2026 р. – онлайн-курс Prometheus «Академічна доброчесність».
Поночовний П.М.: 2025 – підвищення кваліфікації у ТОВ «ЛУЧ» за програмою «Організація захисту інформації під час введення в експлуатацію інфокомунікаційних систем».
Колісниченко А.В.: 2025 р. – курси підвищення кваліфікації ENAI «Educational Materials on Academic Integrity» за програмою «Дослідницька доброчесність»;
Кондратенко Н.Ю.: 2024 р. – курс Prometheus для викладачів «Академічна доброчесність».
Всі викладачі ОП мають встановлений вимогами законодавства об'єм стажувань та підвищення кваліфікації в 6 кредитів ECTS за 5 років.

Наведіть конкретні приклади заохочення розвитку викладацької майстерності

У ДУІКТ розвиток викладацької майстерності НПП забезпечується системою професійного розвитку, рейтингового оцінювання та морального і матеріального заохочення. Нормативну основу становлять Положення про підвищення кваліфікації НПП, Положення про щорічну рейтингову оцінку діяльності НПП та інші документи, оприлюднені на сайті Університету. Нормативні документи ДУІКТ
Заохочується участь викладачів у підвищенні кваліфікації, стажуваннях, конференціях, професійних заходах, науковій роботі та здобутті наукових ступенів. Конкретним прикладом професійного зростання є здобуття викладачами кафедри Технічних систем кіберзахисту Петром Поночовним (2025 р.) та Миколою Рижаковим (2026 р.) ступеня доктора філософії зі спеціальності 125 «Кібербезпека». Застосовуються й моральні заохочення. У травні 2026 р. професора кафедри Ігоря Іванченка нагороджено грамотою МОН України за багаторічну сумлінну працю, внесок у підготовку фахівців і науково-педагогічну діяльність. Старшого викладача Миколу Рижакова відзначено грамотою Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ» за плідну співпрацю. Крім того, відповідно до Положення про порядок заохочення осіб, які працюють, навчаються в ДУІКТ https://duikt.edu.ua/uploads/p_447_90869904.pdf застосовується також щомісячне заохочення керівництва ННІКБЗІ, завідувачів кафедр та викладачів грошовими преміями.
Такі механізми стимулюють НПП до постійного професійного розвитку, удосконалення методик викладання та впровадження сучасних наукових і практичних результатів в освітній процес.

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

Основними джерелами фінансування діяльності Університету є: кошти державного бюджету; доходи від надання платних освітніх послуг; доходи від господарської діяльності; виконання науково-дослідних робіт. Університет має у своєму складі: навчальні приміщення, комп'ютерні та спеціалізовані лабораторії, редакційний відділ, бібліотеку, стадіон, спортивний майданчик, тренажерну залу, їдальню, актову залу, студентський центр, гуртожиток, медичний пункт, доступ до WiFi, що сприяє забезпеченню досягнення цілей та ПРН. Перелік комп'ютерних класів, спеціалізованих лабораторій та їх обладнання наведені на сайті: duikt.edu.ua/360tours/3d_tour2/.
Загальний фонд бібліотеки становить більше 160000 примірників: https://duikt.edu.ua/ua/lib/1/category/2122
Дисципліни забезпечені навчально-методичними посібниками, рекомендаціями, що постійно оновлюються: https://duikt.edu.ua/ua/lib/1/category/2360/view/2401.
Заняття за ОП проводяться у спеціалізованих навчальних лабораторіях безпосередньо кафедри технічних систем кіберзахисту: https://duikt.edu.ua/ua/258-materialna-baza-kafedra-cistem-tehnichnogo-zahistu-informacii. Також використовуються навчальні лабораторії інших кафедр навчально-наукового інституту кібербезпеки та інших університету. Перелік лабораторій, програмних засобів та обладнання, яке застосовується під час навчання за ОП,

наведено на сайті: https://duikt.edu.ua/ua/2698-materialna-baza-navchalno-naukoviy-institut-zahistu-informacii

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

З метою координації організаційного та науково-методичного забезпечення роботи з обдарованою молоддю, створення сприятливих умов для розвитку та реалізації творчих здібностей здобувачів освіти в ДУІКТ діє Науково-методична рада https://duikt.edu.ua/uploads/p_447_88907135.pdf та Рада молодих вчених https://duikt.edu.ua/ua/896-rada-molodih-vchenih-nauka, яка включена до реєстру рад молодих вчених при МОН України.
Передбачена участь науковців грантових програмах та міжнародних стажуваннях https://duikt.edu.ua/ua/1271-informaciya-pro-grantovi-programi-stipendii-ta-mizhnarodni-stazhuvannya-rada-molodih-vchenih?lang=ua&id=1271&sys_link=informaciya-pro-grantovi-programi-stipendii-ta-mizhnarodni-stazhuvannya-rada-molodihvchenih. Крім того, в Університеті функціонує Наукове товариство студентів, аспірантів, докторантів і молодих вчених ДУІКТ: https://duikt.edu.ua/uploads/p_947_67705004.pdf? та низка студентських наукових гуртків https://duikt.edu.ua/uploads/p_947_38259199.pdf. Здобувачі освіти мають змогу брати участь у різноманітних конкурсах та олімпіадах https://duikt.edu.ua/ua/2110- vseukrainski-konkursi-studentskih-naukovih-robit-nauka. Для задоволення інтересів здобувачів вищої освіти у
позанавчальний час діють: студентський центр, тренажерна зала та фітнес центр, стадіон, їдальня, Центр культури та мистецтва. Також, фінансуються численні соціальні ініціативи – матеріальна допомога, соціальні стипендії, поліпшення умов проживання у гуртожитках та ін.

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

В ДУІКТ значна увага приділяється забезпеченню безпечності освітнього середовища. Перед початком навчального року з усіма здобувачами вищої освіти проводиться вступний інструктаж, щодо: видів та джерел небезпеки у навчальних приміщеннях, загальних правил поведінки під час освітнього процесу, ознайомлення з Правилами пожежної безпеки для навчальних закладів та установ системи освіти України.
Визначено обов'язки посадових осіб щодо забезпечення пожежної безпеки окремих будівель, споруд, приміщень, інженерного обладнання, а також за утримання та експлуатацію засобів протипожежного захисту. Розроблено і затверджено плани евакуації студентів і працівників у разі виникнення пожежі та порядок оповіщення учасників освітнього процесу. Усі приміщення та умови для навчання студентів відповідають діючим санітарним вимогам.
В умовах воєнного стану в Університеті забезпечено належний рівень оповіщення про ракетну небезпеку, Створено групи з надання першої допомоги, які забезпечені усіма необхідними засобами. Розроблено план розміщення студентів в укриттях, проведено тренування щодо безпечного переміщення навчальних груп під керівництвом відповідальних кураторів груп до укриття відповідно до затвердженого плану.

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.

ДУІКТ забезпечує комплексну освітню, організаційну, інформаційну, консультативну та соціальну підтримку здобувачів ОПП «Технічні системи інформаційного та кібернетичного захисту». Освітня підтримка здійснюється через лекційні, практичні, лабораторні та індивідуальні заняття, консультації, практики, самостійну роботу й доступ до навчально-методичних матеріалів. В ОПП передбачено використання електронної бібліотеки, Google Classroom і Google Meet.
Організаційну й консультативну підтримку забезпечують гарант ОПП, викладачі, завідувач кафедри, дирекція ННІ кібербезпеки та захисту інформації і структурні підрозділи Університету. Здобувачі отримують консультації щодо навчання, вибору дисциплін, практик, академічної мобільності, підготовки кваліфікаційної роботи та працевлаштування. Інформаційна підтримка здійснюється через офіційний сайт, сторінку кафедри, силабуси, електронні ресурси та бібліотеку: https://duikt.edu.ua/ua/149-e-navchannya-navchannya; https://duikt.edu.ua/ua/lib/1/category/2122.
Соціальну підтримку координує Відділ по роботі зі студентами, який опікується соціальними та навчальними питаннями: https://duikt.edu.ua/ua/2150-socialna-robota-viddil-z-pitan-socialnih-ta-navchalnih-problem-studentiv.
Передбачена підтримка здобувачів пільгових категорій, зокрема соціальні стипендії та пільги щодо проживання в гуртожитку. Важливу роль відіграє студентське самоврядування: https://duikt.edu.ua/ua/929-zagalna-informaciya-studentska-rada.
Здобувачі можуть подавати пропозиції, звернення та повідомлення через систему внутрішнього забезпечення якості й Скриньку довіри vps@duikt.edu.ua: https://duikt.edu.ua/ua/519-vnutrishnya-sistema-zabezpechennya--yakosti-vischoi-osviti-ta-osvitnoi-diyalnosti-sistema-zabezpechennya--yakosti-vischoi-osviti-ta-osvitnoi-diyalnosti.
Підтримка ментального здоров'я реалізується через зустрічі та тренінги з психологами. У 2026 р. проведено лекцію-тренінг щодо регуляції тривожних і депресивних станів, панічних атак, порушень сну та емоційного виснаження, а також зустріч із психологинею Центру сім'ї Солом'янської РДА щодо розвитку стресостійкості.
Підтримка фізичного здоров'я забезпечується через спортивні секції, заняття з фізичного виховання, спортивну інфраструктуру та оздоровчі заходи; у 2026 р. для студентів організовано регулярні тренування з боксу. https://duikt.edu.ua/ua/758-zagalna-informaciya-kafedra-bezpeki-zhittediyalnosti-ta-fizichnogo-vihovannya.
Таким чином, система підтримки ДУІКТ охоплює всі основні потреби здобувачів і сприяє успішному навчанню, соціальній адаптації, професійному розвитку та збереженню фізичного й ментального здоров'я.

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)

ДУІКТ створює інклюзивне освітнє середовище для спільного навчання, виховання та розвитку здобувачів освіти з урахуванням їхніх потреб та можливостей. Згідно ч. 2 ст.30 Закону України «Про освіту» пункту про умови доступності закладу освіти для навчання осіб з особливими освітніми потребами в ЗВО проведено обстеження будівель та прилеглої до них території з метою визначення доступності навчальних приміщень для осіб з особливими освітніми потребами та інших маломобільних груп населення. Враховуючи вимоги та нормативи Державних будівельних норм України; ДСТУ-Н В.2.2-31-2011 в Університеті розроблено Положення про інклюзивне навчання в ДУІКТ https://duikt.edu.ua/uploads/p_447_39062918.pdf та Порядок супроводу (надання допомоги) осіб з інвалідністю та інших маломобільних груп населення в Університеті https://duikt.edu.ua/uploads/p_1846_89231492.pdf , наказом ректора закріплена відповідальна особа за супровід, створені умови для вільного пересування осіб з особливими освітніми потребами, встановлені підйомні платформи для інвалідів і таблички, надруковані шрифтом Брайля. Для осіб з особливими освітніми потребами, під час вступу в Університеті створюються пільгові умови вступу. Порядок їх участі у конкурсному відборі передбачена Правилами прийому ЗВО. Випадків вступу осіб з особливими освітніми потребами на ОП Технічні системи інформаційного та кібернетичного захисту спеціальності F5 Кібербезпека та захист інформації 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 ЗВО побудована на принципах дотримання цінностей свободи, справедливості, рівності прав і можливостей, інклюзивності, толерантності, недискримінації; відкритості та прозорості. В Університеті діє Положення про вирішення конфліктних ситуацій https://duikt.edu.ua/uploads/p_447_88699516.pdf , яке визначає порядок врегулювання ситуацій у разі конфлікту інтересів, дотримання прав людини, гендерної дискримінації, конфліктів в освітньому процесі, сексуальних домагань та булінгу.
Також, функціонує Відділ по роботі зі студентами https://duikt.edu.ua/ua/2146-zagalna-informaciya-viddil-z-pitansocialnih-ta-navchalnih-problem-studentiv Затверджено Положення про вирішення конфліктних ситуацій https://duikt.edu.ua/uploads/p_447_88699516.pdf У разі необхідності, вступники можуть звернутись до Апеляційної комісії https://duikt.edu.ua/uploads/p_447_93714477.pdf У здобувачів ОП є можливість скористатися електронною скринькою довіри https://duikt.edu.ua/ua/519-vnutrishnya-sistema-zabezpechennya--yakosti-vischoi-osviti-ta-osvitnoi-diyalnosti-sistema-zabezpechennya--yakostivischoi-osviti-ta-osvitnoi-diyalnosti для письмового звернення щодо вирішення конфліктної ситуації (у тому числі пов'язаної із сексуальними домаганнями, корупцією, дискримінацією). У разі потреби створюється тимчасова комісія, яка перевіряє факти, після чого приймається рішення відповідно до чинного законодавства.
Врегулювання конфліктних ситуацій, пов'язаних з корупцією, здійснюється відповідно до Закону України «Про запобігання корупції». В Університеті призначено уповноважену особу з питань запобігання і протидії корупції та затверджено Положення про уповноважену особу з питань запобігання та виявлення корупції у ДУІКТ https://duikt.edu.ua/uploads/p_1471_85184024.pdf. Всі аудиторії та інші приміщення Університету обладнані системою цілодобового відеоспостереження, яка, у разі необхідності, дозволяє вирішувати спірні ситуації.
Розгляд звернень, скарг і заяв, що надходять до ЗВО, відбувається відповідно до Закону України «Про доступ до публічної інформації», Закону України «Про звернення громадян». Врегулювання скарг та звернень у ЗВО відбувається шляхом особистого прийому громадян адміністрацією ДУІКТ. Про результати розгляду скарг і звернень громадянину повідомляється письмово або усно, за його бажанням.
За період реалізації ОП випадків звернень щодо вирішення конфліктної ситуації (у тому числі пов'язані із сексуальними домаганнями, корупцією, дискримінацією) зафіксовано 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

Розробка, затвердження, моніторинг і оновлення ОПП реалізуються згідно з Положенням про систему внутрішнього забезпечення якості освіти ДУІКТ https://duikt.edu.ua/uploads/p_447_18879118.pdf , та Положенням про запровадження та оновлення освітніх програм в ДУІКТ https://duikt.edu.ua/uploads/p_447_73345463.pdf Ці положення уніфікують процедури щодо ОП для всіх спеціальностей Університету, що забезпечує єдиний підхід до контролю якості за реалізацією процедур, а також механізми вдосконалення.
Для розроблення освітньої програми відповідного рівня підготовки здобувачів вищої освіти та спеціальності, утворюється проектна група з числа НПП, які за рівнем своєї кваліфікації, рівнем наукової та професійної активності та наявністю відповідного науково-педагогічного стажу можуть входити до складу таких проєктних груп. До розробки проєктів освітніх програм залучаються роботодавці, здобувачі та провідні фахівці з відповідної спеціальності. За якість реалізації ОПП відповідає група забезпечення ОП. Процедура перегляду і оновлення ОП описана у Положенні про запровадження та оновлення освітніх програм в ДУІКТ https://duikt.edu.ua/uploads/p_447_73345463.pdf. З метою оцінювання ОП щороку здійснюється моніторинг на

предмет її відповідності стандарту, спроможності ЗВО забезпечити досягнення здобувачами вищої освіти програмних результатів, рівня задоволеності роботодавців та здобувачів. З метою врахування змін законодавства та інноваційного розвитку у галузі інформаційних технологій та сфері захисту інформації вносяться зміни як до ОП так і до силабусів освітніх компонент.
Зважаючи на світовий прогрес у розвитку комп'ютерних систем, технологій штучного інтелекту, хмарних технологій та у зв'язку зі зростаючою динамікою появи нових загроз щодо цілісності, доступності та конфіденційності інформації існує необхідність у підготовці таких фахівців, які займуть своє місце саме в цій галузі. Дані тенденції і були враховані в оновленій ОП Технічні системи інформаційного та кібернетичного захисту.

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

Перегляд і оновлення ОПП «Технічні системи інформаційного та кібернетичного захисту» здійснюється відповідно до Положення про запровадження та оновлення освітніх програм у ДУІКТ: https://duikt.edu.ua/uploads/p_447_73345463.pdf. Положення визначає процедури розроблення, затвердження, моніторингу та перегляду ОП. Моніторинг проводиться щороку з урахуванням відповідності стандарту вищої освіти, досягнення програмних результатів навчання, розвитку спеціальності, змін нормативної бази, результатів опитувань та пропозицій здобувачів, роботодавців і академічної спільноти.
Остання завершена редакція поданої ОПП затверджена кафедрою Технічних систем кіберзахисту 06.03.2025 (протокол №11), введена в дію наказом ректора №99 від 21.03.2025 та застосовується з 01.09.2025. Підставами оновлення визначено Стандарт вищої освіти за спеціальністю 125 другого (магістерського) рівня, рекомендації акредитаційних комісій суміжних ОП, роботодавців, здобувачів та інших стейкхолдерів. До робочої групи безпосередньо включено представника роботодавців — заступника директора ТОВ «ЛУЧ» Г. Шукліна, представника ДержНДІ технологій кібербезпеки Володимира Кошарського та звідувача кафедри Кібербезпеки ЗНУ Михайла Касянчука, здобувача А. Довгополого. https://duikt.edu.ua/ua/news-1-569-13824-zahodi-zaluchennya-studentiv-magistriv-do-obgovorennya-ta-onovlennya-osvitnih-program-kafedri-tehnichnih-sistem-kiberzahistu_kafedra-cistem-tehnichnogo-zahistu-informacii
За результатами перегляду актуалізовано профіль і зміст професійної підготовки, зокрема закріплено галузь F «Інформаційні технології», спеціальність F5 «Кібербезпека та захист інформації», уточнено компетентності та програмні результати навчання. У структурі ОПП сформовано тематику та зміст навчальних занять ОК, що спрямовані на актуальні завдання галузі: ОК5 «Ліцензування, атестація та сертифікація у сфері безпеки об'єктів інформаційної діяльності», ОК6 «Стандарти кібербезпеки та захисту конфіденційної інформації», ОК7 «Технологія створення та застосування комплексів засобів захисту інформаці», ОК10 «Організація і проведення спеціальних досліджень на об'єкті інформаційної діяльності». Посилено практичну й дослідницьку підготовку через науково-педагогічну, науково-дослідну та переддипломну практики (21 кредит ЄКТС) і підготовку кваліфікаційної роботи (9 кредитів).
Оновлення обґрунтовано необхідністю посилення підготовки з технічного захисту інформації, нормативного забезпечення, контролю захищеності ОІД, радіомоніторингу та практичного застосування сучасних засобів кіберзахисту. Моніторинг продовжується: у лютому 2026 р. залучені до обговорення здобувачі другого освітного рівні - магістри запропонували посилити лабораторно-практичну складову, тематику аналізу технічних каналів витоку, кіберризиків, контролю доступу та захисту мережевої інфраструктури; ці пропозиції враховуються при наступному оновленні ОП у редакції 2026 року.

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

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
Пропозиції від здобувачів одержуються в особистому спілкуванні, на засіданнях кафедр, Вченої ради інституту та під час опитувань https://duikt.edu.ua/uploads/p_1352_28154611.pdf . Узагальнені результати опитувань розміщені на сайті https://duikt.edu.ua/ua/1352-rezultati-opituvan-vnutrishnya-sistema-zabezpechennya--yakosti-vischoi-osviti-taosvitnoi-diyalnosti. Здобувачі можуть надавати свої пропозиції через форму зворотного зв'язку та скриньку довіри.
Також, ефективним засобом моніторингу ОП є залучення здобувачів вищої освіти до їх обговорення: https://duikt.edu.ua/ua/news-1-569-13824-zahodi-zaluchennya-studentiv-magistriv-do-obgovorennya-ta-onovlennya-osvitnih-program-kafedri-tehnichnih-sistem-kiberzahistu_kafedra-cistem-tehnichnogo-zahistu-informacii; https://duikt.edu.ua/ua/news-1-9-15131-studenti-magistri-doluchilisya-do-obgovorennya-onovlennya-osvitno-profesiynih-program-kafedri-tehnichnih-sistem-kiberzahistu.
Найбільш актуальні зміни, запропоновані здобувачами знайшли своє відображення в зміні тематики навчальних занять ражу освітніх компонентів ОП.

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

Представники студентського самоврядування є членами Вченої ради університету, яка задіяна в процесах забезпечення якості ОП. Важливим моментом є співпраця студентства з іншими організаціями та залучення з їхньої пропозиції різноманітних спікерів, які проводять доповіді з різних напрямів роботи. Студенти також беруть участь в організації ярмарку вакансій, студентських конференцій та тематичних опитуваннях. В ДУІКТ створена та функціонує Рада молодих вчених https://duikt.edu.ua/ua/896-rada-molodih-vchenih-nauka до роботи якої залучаються найбільш активні студенти-здобувачі вищої освти другого рівня. Здобувачі вищої освіти мають право: подавати пропозиції до

вченої ради інституту, університету з питань удосконалення стратегії університету щодо контролю освітнього процесу; брати участь у вирішенні спірних ситуацій, що можуть виникнути між здобувачами вищої освіти та представниками адміністрації/науково-педагогічними працівниками; подавати пропозиції щодо змісту навчальних планів та освітніх програм.

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

Роботодавці системно залучаються до перегляду та забезпечення якості ОПП через участь у робочій групі, зовнішнє рецензування, публічне обговорення, професійні зустрічі, семінари, практичну підготовку здобувачів та оцінювання актуальності змісту освітніх компонентів. Механізмом відкритого залучення є сторінка «Публічне обговорення освітніх програм», де розміщується проєкт магістерської ОПП та форма для подання пропозицій безпосередньо завідувачу кафедри: https://duikt.edu.ua/ua/3036-publichne-obgovorennya-osvitnih-program-osvitni-programi. Це дає роботодавцям можливість надавати зауваження не лише під час офіційного рецензування, а й упродовж процедури громадського обговорення. Конкретним прикладом врахування потреб ринку праці є взаємодія кафедри з Поліцією охорони: https://duikt.edu.ua/ua/news/1/category/569/view/14076. Додатковим каналом зворотного зв'язку є регулярні зустрічі студентів і кафедри з компаніями-партнерами: https://duikt.edu.ua/ua/251-zagalna-informaciya-kafedra-cistem-tehnichnogo-zahistu-informacii. Та Дні кар'єри, наприклад 2026 рік: https://www.duikt.edu.ua/ua/news-1-569-15546-den-kareri-u-duikt-zustrich-steykholderiv-kafedri-tehnichnih-sistem-kiberzahistu-zi-studentami-magisterskogo-ta-bakalavrskogo-rivniv-pidgotovki. Участь роботодавців має не формальний, а постійний характер: їхні пропозиції використовуються під час щорічного моніторингу ОПП, оновлення змісту ОК, організації практичної підготовки та оцінювання відповідності програми сучасним потребам сфери кібербезпеки.

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

Інформація щодо кар'єрного шляху випускників ОПП «Технічні системи інформаційного та кібернетичного захисту» збирається кафедрою через постійну комунікацію з випускниками, роботодавцями та компаніями-партнерами, під час практик, професійних зустрічей, Днів кар'єри й ярмарків вакансій.

На сторінці кафедри «Відгуки студентів та роботодавців» наведені конкретні кар'єрні траєкторії. Так, Валерій Цесарський ще під час навчання працевлаштувався в компанії «ВОЛЯ», а Максим Вовк поєднував магістратуру з роботою DevOps-інженером. У компанії «Українські спеціальні системи» працює випускник Антон Загіней, у DEPS — Сергій Зозуля, а в Epos інженерами з технічного захисту інформації працюють Георгій Чупрін та Єгор Шарай, які співпрацювали з компанією ще під час практики: https://duikt.edu.ua/ua/news-1-569-12300-kompaniya-epos-%E2%80%93-osnovna-baza-oznayomchoi-praktiki-studentiv-2-kursu-kafedri-sistem-informaciynogo-ta-kibernetichnogo-zahistu_kafedra-cistem-tehnichnogo-zahistu-informacii

Інформація від випускників і роботодавців аналізується під час моніторингу та перегляду ОПП і використовується для оновлення змісту освітніх компонентів, посилення практичної підготовки, розвитку партнерств, організації практик і стажувань та забезпечення відповідності підготовки актуальним потребам ринку праці у сфері кібербезпеки й технічного захисту інформації.

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

У ДУІКТ діє багаторівнева система внутрішнього забезпечення якості реалізації ОП: на рівні кафедри здійснюється контроль діяльності НПП та обговорення результатів на засіданнях; на рівні ННІ – контроль роботи кафедр і розгляд питань Вченою радою інституту; на рівні Університету – моніторинг виконання прийнятих рішень навчально-методичним відділом.

Результати опитувань здобувачів регулярно оприлюднюються на сайті ДУІКТ: https://duikt.edu.ua/ua/1352-rezultati-opituvan-vnutrishnya-sistema-zabezpechennya--yakosti-vischoi-osviti-ta-osvitnoi-diyalnosti.

За результатами внутрішнього моніторингу у 2025 р. розширено можливості формування індивідуальної освітньої траєкторії: здобувачі можуть обирати дисципліни з Каталогу компонентів вільного вибору, у тому числі з інших спеціальностей і рівнів підготовки: https://duikt.edu.ua/ua/2080-katalog-osvitnih-komponentiv-vilnogo-viboru-studentami-navchannya. До каталогу додано дисципліни «Аналіз ефективності систем кібернетичного захисту» та «Управління інформаційними інцидентами в системах технічного захисту інформації», що зумовлено зростанням складності кіберзагроз та потребою в підготовці фахівців з виявлення, аналізу й локалізації інцидентів. Також у 2025 р. оновлено зміст силабусів відповідно до розвитку технологій кібербезпеки, розширено використання сервісів Google в освітньому процесі та можливості участі здобувачів у наукових конференціях і семінарах

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

Результати зовнішнього забезпечення якості системно враховуються під час перегляду ОПП «Технічні системи інформаційного та кібернетичного захисту». На сайті ДУІКТ оприлюднено висновки акредитаційних експертиз,

зокрема попередньої акредитації магістерської ОПП за спеціальністю 125 «Кібербезпека». Експертна комісія МОН у 2018 р. визнала підготовку за програмою такою, що здійснюється на належному рівні; виявлені під час експертизи недоліки Університетом були усунені.
Безпосередній зв'язок зовнішнього оцінювання з удосконаленням програми зафіксований у редакції ОПП 2025 р.: серед підстав її оновлення прямо визначено рекомендації акредитаційних комісій суміжних освітніх програм, поряд із рекомендаціями роботодавців, здобувачів та інших стейкхолдерів. Оновлена ОПП затверджена кафедрою 06.03.2025 та введена в дію наказом ректора №99 від 21.03.2025.
З урахуванням досвіду акредитацій інших ОП у програмі посилено структурованість та доказовість досягнення результатів навчання: для кожного ОК визначено відповідність компетентностям і РН; професійний блок сформовано з ОК5–ОК10, що охоплюють ліцензування й сертифікацію, стандарти кібербезпеки, комплексні засоби захисту, захист інформаційних ресурсів, радіомоніторинг та спеціальні дослідження на ОІД. Посилено практичну складову — передбачено науково-педагогічну, науково-дослідну та переддипломну практики загальним обсягом 21 кредит ЄКТС, а на кваліфікаційну роботу й атестацію відведено 9 кредитів. Вибіркова складова становить 25 із 90 кредитів ЄКТС, що розширює індивідуальну освітню траєкторію.
Удосконалено також процедури залучення стейкхолдерів. До робочої групи ОПП включено представника роботодавця — заступника директора ТОВ «ЛУЧ» Г. Шукліна та здобувача А. Довгополого. Проєкти ОПП проходять публічне обговорення, де роботодавці, здобувачі та академічна спільнота можуть подавати пропозиції: https://duikt.edu.ua/ua/3036-publichne-obgovorennya-osvitnih-program-osvitni-programi.
Таким чином, зовнішнє оцінювання використовується не формально, а як джерело для оновлення структури ОПП, матриць компетентностей і РН, практичної підготовки, вибіркової складової, кадрового та стейкхолдерського забезпечення. Водночас у самій ОПП 2025 р. не наведено покрокового зіставлення «конкретна рекомендація акредитації — конкретна зміна», тому таке співвіднесення доцільно не деталізувати понад наявні документальні підтвердження.

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

Відповідно до Положення про систему внутрішнього забезпечення якості вищої освіти ДУІКТ академічна спільнота залучається до моніторингу, перегляду та вдосконалення ОП, оцінювання діяльності кафедр і обговорення результатів навчання. Питання якості розглядаються на засіданнях кафедри, Вченої ради ННІ кібербезпеки та захисту інформації та Вченої ради ДУІКТ: https://duikt.edu.ua/uploads/p_447_18879118.pdf.

В ОПП 2026 р. зазначено, що її оновлення здійснювалося з урахуванням пропозицій НПП та досвіду аналогічних вітчизняних і зарубіжних програм. До робочої групи входять д.т.н., професор Туровський О.Л., к.т.н., доцент Іванченко І.С., к.т.н., доцент Пепа Ю.В., які безпосередньо беруть участь у формуванні та перегляді змісту ОПП.

Зовнішня академічна спільнота залучається через рецензування та експертне оцінювання. У погодженні ОПП 2026 р. представлені кафедра кібербезпеки Західноукраїнського національного університету (д.т.н., професор М. Касянчук) та ДержНДІ технологій кібербезпеки (PhD В. Кошарський). Їх рекомендації враховуються щодо компетентностей, РН та змісту ОК.

Отже, академічна спільнота залучена до розроблення, експертизи, моніторингу, обговорення та оновлення ОПП.

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

Культура якості освіти у ДУІКТ у 2026 році підтримується через системне оновлення освітніх програм, внутрішній моніторинг, залучення здобувачів, НПП, роботодавців і випускників до процедур забезпечення якості. Актуальність такого підходу підтверджується стабільно високим інтересом вступників до ІТ- та кіберспеціальностей Університету. За проміжними результатами вступної кампанії 2026 року ДУІКТ увійшов до числа лідерів серед столичних і національних ЗВО за кількістю поданих заяв: за спеціальністю F5 «Кібербезпека та захист інформації» — 5 місце, за F2 «Інженерія програмного забезпечення» — 4 місце.
Високий попит на підготовку фахівців з кібербезпеки корелює зі спрямованістю ОПП «Технічні системи інформаційного та кібернетичного захисту», яка орієнтована на потреби ринку праці, інноваційні технології та практичну підготовку у сфері технічного захисту інформації. В редакції ОПП 2026 року прямо зазначено, що її оновлення здійснено з урахуванням пропозицій здобувачів, НПП, випускників, роботодавців, громадських організацій, тенденцій розвитку спеціальності, ринку праці та досвіду вітчизняних і зарубіжних програм. Показником результативності системи якості є й те, що у 2026 році ДУІКТ продовжує активно розвивати вступну кампанію, професійні партнерства, кар'єрні заходи та практикоорієнтоване навчання. Загальноукраїнський інтерес до ІТ-освіти також залишається високим.

9. Прозорість і публічність

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

Права та обов'язки усіх учасників освітнього процесу ДУІКТ регулюються Статутом ДУІКТ, ухваленим загальними зборами трудового колективу ДУІКТ та затвердженим наказом МОН України від 13.06.2023 р. № 728 https://duikt.edu.ua/uploads/p_949_13841785.pdf ; Концепцією розвитку ДУІКТ на 2024-2026 роки

https://duikt.edu.ua/uploads/p_949_80703640.pdf ; Положенням про організацію освітнього процесу в ДУІКТ https://duikt.edu.ua/uploads/p_447_49109699.pdf , Колективним договором ДУІКТ https://duikt.edu.ua/uploads/p_1462_63527482.pdf , Кодексом академічної доброчесності ДУІКТ https://duikt.edu.ua/uploads/p_447_96297052.pdf , договором про навчання у закладі вищої освіти та надання платної освітньої послуги між ЗВО та фізичною (юридичною) особою, контрактами з науково-педагогічними працівниками, посадовими інструкціями.
Зазначені документи разом з іншими нормативно-правовими актами доступні на офіційному сайті Університету https://duikt.edu.ua/ua/949-publichna-informaciya-pro-universitet

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

https://duikt.edu.ua/ua/3036-publichne-obgovorennya-osvitnih-program-osvitni-programi

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

Освітньо-наукова програма:
https://duikt.edu.ua/uploads/p_1822_98423007.pdf
https://duikt.edu.ua/uploads/p_1823_29391024.pdf

Навчальні плани:
https://duikt.edu.ua/uploads/p_1823_13391943.pdf
https://duikt.edu.ua/uploads/p_1823_56137909.pdf

Силабуси навчальних дисциплін (Цикл обов'язкових компонент):
https://duikt.edu.ua/ua/253-navchalni-disciplini-kafedra-cistem-tehnichnogo-zahistu-informacii

Силабуси навчальних дисциплін (Цикл вибіркових компонент):
https://duikt.edu.ua/ua/2994-katalog-osvitnih-komponentiv-vilnogo-viboru

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП?

До сильних сторін ОПП «Технічні системи інформаційного та кібернетичного захисту» належить її виразна професійна спрямованість на технічний захист інформації та потреби ринку праці. Програма базується на компетентнісному підході, містить чітко визначені результати навчання, передбачає студентоцентроване навчання, практичні кейси від партнерів, науково-педагогічну, науково-дослідну та переддипломну практики. Важливою перевагою є потужна матеріально-технічна база: лабораторії контролю доступу та технічного захисту інформації «PIAC» оснащені біометричними терміналами, мережевими контролерами, HikVision, Ajax, DigiSkan EX, PROTEKT, сканувальними приймачами та локаторами нелінійностей. Кафедра співпрацює з роботодавцями та залучає їх до практичної підготовки і працевлаштування здобувачів.
Сильною стороною є також кадрове забезпечення: НПП мають підтверджену наукову й професійну активність, а склад групи забезпечення відповідає ліцензійним вимогам.
До напрямів подальшого вдосконалення ОПП доцільно віднести розширення міжнародної академічної мобільності, посилення участі іноземних фахівців, подальше оновлення вибіркових компонентів відповідно до нових кіберзагроз та ширше залучення здобувачів до міжнародних проєктів і сертифікаційних програм. Загалом ОПП має достатнє кадрове, методичне та матеріально-технічне забезпечення і відповідає сучасним вимогам підготовки магістрів у сфері кібербезпеки.

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

Перспективи розвитку ОПП «Технічні системи інформаційного та кібернетичного захисту» упродовж найближчих трьох років пов'язані з подальшим підвищенням якості підготовки магістрів, оновленням змісту відповідно до розвитку кіберзагроз, технічного захисту інформації та потреб ринку праці. ОПП має прикладну спрямованість, орієнтована на інноваційні методи ТЗІ та передбачає використання сучасного світового досвіду.
Пріоритетними напрямами визначено:
• щорічне оновлення обов'язкових і вибіркових ОК з урахуванням нових технологій, стандартів і рекомендацій роботодавців;
• модернізацію лабораторій контролю доступу та ТЗІ «PIAC», розширення використання сучасних програмно-апаратних комплексів;
• розширення співпраці з Epos, Altex, PIAC, DEPS та іншими партнерами щодо практик, стажувань, кейсів і

працевлаштування;
• посилення академічної мобільності здобувачів і НПП, міжнародних стажувань та участі в освітніх і наукових проєктах;
• залучення до викладання фахівців-практиків і зарубіжних експертів;
• розширення участі студентів у конференціях, професійних сертифікаційних програмах та прикладних дослідженнях.
Реалізації цих перспектив сприятиме міжнародна діяльність ДУІКТ, зокрема членство в ITU, що створює можливості академічної мобільності, спільних досліджень і залучення до міжнародних стандартів у сфері кібербезпеки.

Запевнення

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

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

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

Додатки:

Таблиця 1. Інформація про обов'язкові освітні компоненти ОП

Таблиця 2. Зведена інформація про викладачів ОП

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

***

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

Документ підписаний кваліфікованим електронним підписом/кваліфікованою електронною печаткою.

Інформація про КЕП

ПІБ: ШУЛЬГА ВОЛОДИМИР ПЕТРОВИЧ

Дата: 07.09.2026 р.

Таблиця 1. Інформація про освітні компоненти ОП

Назва освітнього компонента	Вид освітнього компонента	Силабус або інші навчально-методичні матеріали		Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього*
		Назва файла	Хеш файла	
Преддипломна практика	практика	*Силабус_ОК-13_Переддипломна_практика_Магістри.pdf*	guu7wK4l1cSMxtR1n61AGQQEjZxyxy+BzsmN0CRMgtA=	*Матеріально-технічне забезпечення та програмне забезпечення відповідно бази проходження практики у лабораторіях:* *1. Навчальна лабораторія мережевої безпеки.* *2. Навчальна лабораторія реагування на кіберінциденти.* *3. Навчальна лабораторія захисту кінцевих точок.* *4. Навчальна лабораторія засобів контролю доступу.* *5. Навчальна лабораторія технічного захисту інформації.* *6. Навчальна лабораторія Security Operation Center.*
Науково-дослідна практика	практика	*Силабус_ОК-12_НД-практика_Магістри.pdf*	c1toAyRCWeksYU6lM2QHQ2ZKpks9IOM3PxtJw3WGevc=	*Матеріально-технічне забезпечення та програмне забезпечення відповідно бази проходження практики у лабораторіях:* *1. Навчальна лабораторія мережевої безпеки.* *2. Навчальна лабораторія реагування на кіберінциденти.* *3. Навчальна лабораторія захисту кінцевих точок.* *4. Навчальна лабораторія засобів контролю доступу.* *5. Навчальна лабораторія технічного захисту інформації.* *6. Навчальна лабораторія Security Operation Center.*
Корпоративна та професійна етика в кібербезпеці	навчальна дисципліна	*Силабус_ОК-1_Корпоративна_та_професійна_етика_Магістри.pdf*	LCyNHTFzkw4Rmi8f9G/O1HUtjn8ixFCuYEOJTJPcrrw=	*Спеціального матеріально-технічного забезпечення не потребує. Мультимедійна система - 1 к-т.*
Педагогіка та психологія у вищій школі	навчальна дисципліна	*Сілабус_ОК-3_ПП_Магістри.pdf*	9zKjt/qaLlfR6J/TYhQ9nVFMsddFmVsfmIICiLsi2m8=	*Спеціального матеріально-технічного забезпечення не потребує. Мультимедійна система - 1 к-т.*
Науково-технічний переклад	навчальна дисципліна	*Силабус_ОК-4_НТП_Магістри.pdf*	iPz1aMI9exwq6fWYFc8zUNTpPcSWBECXobxsrRVBSgI=	*Спеціального матеріально-технічного забезпечення не потребує. Мультимедійна система - 1 к-т.*
Англійська мова для ділової комунікації	навчальна дисципліна	*Силабус_ОК-4_Англійська ДК_Магістри_2026.pdf*	4UNWxbHLwFI2a1WpBTkrupTuFbkjnhpgjpxj9FduE64=	*Спеціального матеріально-технічного забезпечення не потребує. Мультимедійна система - 1 к-т.*
Науково-педагогічна практика	практика	*Силабус_ОК-11_НП-практика_Магістри.pdf*	F2m5KsonZgb2X30V72UMeQ1QVOlMTm5IBm7/PpYUfc4=	*Матеріально-технічне забезпечення та програмне забезпечення відповідно бази проходження практики у лабораторіях:* *1. Навчальна лабораторія засобів контролю доступу.* *2. Навчальна лабораторія технічного захисту інформації.*
Теорія захисту інформаційних	навчальна дисципліна	*Сілабус_ОК-8_ТЗІРОД_Магіст*	s8CeMQdDb8lQQOJFyBNKmmejaCR5xF	*Навчальна лабораторія засобів контролю доступу:*

ресурсів обмеженого доступу		*pu.docx.pdf*	UGAEnkiNW1r+w=	*1. Відеокамери: DS-2CD2420F-1, DS-2CD1021-1, DS-2CD4A26FWDIZS, DS-2CD1331-1, DS-2CD2125F1, DS-7608NI-E2/8P.* *2. Мінівідеокамера Osculus S970.* *3. Контрольний пристрій ST-03-TEST.* *Навчальна лабораторія технічного захисту інформації:* *1. Генератор акустичного шуму PIAC-2ГС.* *2. Пошуковий комплекс DigiScan EX.* *3. Детектор поля Protect 1210.* *4. Індикатор поля Protect 1206і.* *5. Скануючий приймач IC-R2500.* *6. Скануючий приймач IC-R20. Скануючі приймачі AOR 8000 та AOR 8200K.* *7. Локатор нелінійностей NR 900.* *8. Багатофункціональний пошуковий прилад ST-032.*
Радіомоніторинг і радіопротидія на об'єктах ІД	навчальна дисципліна	*Сілабус_ОК-9_РМ_і_РП_Магістри.pdf*	225QGOHZzRMAEeuHLqPyNHS2q/LdVlQI39v78iW9eSU=	*Навчальна лабораторія засобів контролю доступу:* *1. Відеокамери: DS-2CD2420F-1, DS-2CD1021-1, DS-2CD4A26FWDIZS, DS-2CD1331-1, DS-2CD2125F1, DS-7608NI-E2/8P.* *2. Мінівідеокамера Osculus S970.* *3. Контрольний пристрій ST-03-TEST.* *Навчальна лабораторія технічного захисту інформації:* *1. Генератор акустичного шуму PIAC-2ГС.* *2. Пошуковий комплекс DigiScan EX.* *3. Детектор поля Protect 1210.* *4. Індикатор поля Protect 1206і.* *5. Скануючий приймач IC-R2500.* *6. Скануючий приймач IC-R20. Скануючі приймачі AOR 8000 та AOR 8200K.* *7. Локатор нелінійностей NR 900.* *8. Багатофункціональний пошуковий прилад ST-032.*
Організація і проведення спеціальних досліджень на обєкті інформаційної діяльності	навчальна дисципліна	*Сілабус_ОК-10_ОПСД_Магістри.pdf*	QM9poycLroBr9shjwMo98K8QJ5pnqfaoSvk+8bSdavs=	*Навчальна лабораторія засобів контролю доступу:* *1. Відеокамери: DS-2CD2420F-1, DS-2CD1021-1, DS-2CD4A26FWDIZS, DS-2CD1331-1, DS-2CD2125F1, DS-7608NI-E2/8P.* *2. Мінівідеокамера Osculus S970.* *3. Контрольний пристрій ST-03-TEST.* *Навчальна лабораторія технічного захисту інформації:* *1. Генератор акустичного шуму PIAC-2ГС.* *2. Пошуковий комплекс DigiScan EX.* *3. Детектор поля Protect 1210.* *4. Індикатор поля Protect 1206і.* *5. Скануючий приймач IC-R2500.* *6. Скануючий приймач IC-R20. Скануючі приймачі AOR 8000 та AOR 8200K.* *7. Локатор нелінійностей NR 900.* *8. Багатофункціональний пошуковий прилад ST-032.*
Технологія створення та застосування	навчальна дисципліна	*Сілабус_ОК-7_ТСЗКЗЗІОД на*	iBqlR5Bokiy1dzBHOEIzP/lYhoJNtbz5KPl	*Навчальна лабораторія засобів контролю доступу:*

комплексів засобів захисту інформації з обмеженим доступом та охорони ОІД		*ОІД_Магістри.pdf*	w2TJYA+c=	*1. Відеокамери: DS-2CD2420F-1, DS-2CD1021-1, DS-2CD4A26FWDIZS, DS-2CD1331-1, DS-2CD2125F1, DS-7608NI-E2/8P.* *2. Мінівідеокамера Osculus S970.* *3. Контрольний пристрій ST-03-TEST.* *Навчальна лабораторія технічного захисту інформації:* *1. Генератор акустичного шуму PIAC-2ГС.* *2. Пошуковий комплекс DigiScan EX.* *3. Детектор поля Protect 1210.* *4. Індикатор поля Protect 1206і.* *5. Скануючий приймач IC-R2500.* *6. Скануючий приймач IC-R20. Скануючі приймачі AOR 8000 та AOR 8200K.* *7. Локатор нелінійностей NR 900.* *8. Багатофункціональний пошуковий прилад ST-032.*
Стандарти кібербезпеки та захисту інформації	навчальна дисципліна	*Сілабус_ОК-6_СКЗКІ_Магістри.pdf*	c1nN6WWaGLz6aLBvwCKqxRrwM21AKpBKAFkq+2kcpkw=	*Спеціального матеріально-технічного забезпечення не потребує. Мультимедійна система - 1 к-т.*
Ліцензування, атестація та сертифікація у сфері безпеки об'єктів інформаційної діяльності	навчальна дисципліна	*Сілабус_ОК-5_ЛАССОІД_Магістри.pdf*	by7g21YpEyF1ttBFg1ozAGq3XRNvE+L3j9mVaMH7aBE=	*Спеціального матеріально-технічного забезпечення не потребує. Мультимедійна система - 1 к-т.*
Організація проведення наукових досліджень	навчальна дисципліна	*Сілабус_ОК-2_ОПНД_Магістри.pdf*	Ocg0192mbceZ4mjLdSWWVe/gVWb3erIqzeEqTQuLmFE=	*Спеціального матеріально-технічного забезпечення не потребує. Мультимедійна система - 1 к-т.*

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

Таблиця 2. Зведена інформація про відповідність НПП освітнім компонентам

ID викладача	ПІБ	Посада	Структурний підрозділ	Кваліфікація викладача	Стаж	Навчальні дисципліни, що їх викладає викладач на ОП	Обґрунтування відповідності освітньому компоненту (кваліфікація, професійний досвід, наукові публікації)
408025	Пепа Юрій Володимирович	Професор, Основне місце роботи	Навчально-науковий інститут Кібербезпеки та захисту інформації	Диплом спеціаліста, Київський міжнародний університет цивільної авіації, рік закінчення: 2000, спеціальність: 090702 Радіоелектронні пристрої, системи та комплекси, Диплом магістра, Харківський національний університет	22	Радіомоніторинг і радіопротидія на об'єктах ІД	Кандидат технічних наук зі спеціальності 05.22.13 – навігація та управління повітряним рухом. Тема дисертації: «Прогнозування точнісних характеристик радіотехнічних систем посадки повітряних суден з урахуванням дифракції радіохвиль на об’єктах циліндричної форми». Диплом ДК № 021116 від 11.05.2005 року. Вчене звання: доцент кафедри засобів

				радіоелектроніки, рік закінчення: 2020, спеціальність: 125 Кібербезпека, Диплом кандидата наук ДК 029116, виданий 11.05.2005, Атестат доцента 12ДЦ 021590, виданий 23.12.2008			захисту інформації. Атестат 12ДЦ № 021590 від 23.12.2008 року Підвищення кваліфікації: 1. ТОВ «ЛУЧ» «Технічні засоби охорони об'єктів інформаційної діяльності» (2 кредити ECTS), 16-27.01.2023 р. (Сертифікат № ТЗОО 21595641/SUT-1 від 27.01.2023 р.) 2. ТОВ «ЛУЧ» «Датчики, сенсорні системи та системи розпізнавання образів» (2 кредити ECTS), 10-21.02.2023 р. (Сертифікат № ДССРО 21595641/SUT-1 від 21.02.2023 р.) 3. ТОВ «ЛУЧ» «Біометричні системи контролю доступу» (2 кредити ECTS), 6-17.03.2023 р. (Сертифікат № БСКД 21595641/SUT-1 від 17.03.2023 р.) 4. ГО «Українське відділення всесвітньої інтернет спільноти» ISOC UKRAINE CHAPTER «Управління Інтернет» (0,2 кредити ECTS), 10-12.12.2023 р. (Сертифікат № 033 від 12.12.2023 р.) 5. PROMETEUS «Інженер БПЛА. Базовий курс» (0,3 кредити ECTS), 23.12.2023 р. (Сертифікат №280a403ec36e4f849c6b8a69a0d6409c від 23.12.2023 р.) 6. Національне агентство кваліфікацій «Розроблення професійних стандартів (експерт)» (1,5 кредити ECTS), 30.05.2024 р. (Сертифікат № 1411 від 30.05.2024 р.) 7. Волинський національний університет імені Лесі Українки «Актуальні проблеми освітніх і наукових досліджень: перспективи, інновації, розвиток» (2 кредити ECTS), 30.04.2024 р. (Сертифікат № АС 2024-5636 від 30.04.2024 р.) 8. Український державний університет імені Михайла Драгоманова

							«Актуальні проблеми та перспективи розвитку фундаментальних, прикладних, загальнотехнічних та безпекових наук» (0,2 кредити ECTS), 27.06.2024 р. (Сертифікат № А 270624N112 від 27.06.2024 р.) 9. Асоціація інноваційної та цифрової освіти «Штучний Інтелект в освіті» (0,5 кредитів ECTS), 24.07.2024 р. (Сертифікат № 77407814 від 24.07.2024 р.) 10. European Institute for Innovation Development «Implementation of Innovations in Technologies and Engineering: Experience of the Czech Republic» (6 кредитів ECTS), June 16, 2026 – July 24, 2026. (Certificat № tec-2026-20), Ostrava, Czech Republic. Види і результати професійної діяльності за спеціальністю відповідно до п.38 Ліцензійних умов провадження освітньої діяльності: (п.п. 1, 3, 4, 6, 7, 8, 9, 12, 19). Підпункт 1 - наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection: 1. Pepa Y. Devising a Procedure to Determine the Level of Informational Space Security in Social Networks Considering Interrelations Among Users / V. Akhramovych, G. Shuklin, Y. Pepa, T. Muzhanova, S. Zozulia // Eastern-European Journal of Enterprise Technologies (Scopus Indexed), February 2022, Vol. 1/9(115). – pp. 63-74. 2. Pepa Y. Methodology for Calculating the Index of Protection of a Social Media from its Centrality / V.

							Akhramovych, G. Shuklin, Y. Pepa, S. Lehominova, T. Muzhanova, T. Dzyuba, Y. Yakymenko // International Journal of Emerging Technology and Advanced Engineering (Scopus Indexed), April 2023, Vol. 13, Issue 04. – pp. 17-25. 3. Pepa Y. Calculating the Information Security Indicator in Social Media with Consideration of the Path Duration Between Clients / V. Akhramovych, Y. Pepa, A. Zahynei, T. Dzyuba, I. Danylov // Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska (Scopus Indexed), 2024, 14(1). – pp. 71-77. 4. Pepa Y. Determination of the Possibility of the Synthesis of Zn-AL layered Double Hydroxides, Intercalated with Peroxyanions, as a Perspective Solid Disinfectant / V. Kovalenko, A. Borysenko, V. Kotok, V. Verbitskiy, V. Medianyk, V. Stoliarenko, Y. Pepa, S. Simchenko, V. Ved, Sheikh Ahmad Izaddin Sheikh Mohd Ghazali // Eastern-European Journal of Enterprise Technologies (Scopus Indexed), 2024, 2(6(128)). – pp. 49-55. 5. Pepa Y. Prediction Of Quality Software Quality Indicators With Applied Modifications of Integrated Gradiates Methods / A. Shantyr, O. Zinchenko, K. Storchak, A. Bondarchuk, Y. Pepa // Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska (Scopus Indexed), 2025, 15(2). – pp. 139-146. 6. Pepa Y. Detection Confidential Information by Large Language Models / O. Deineka, O. Harasymchuk, A. Partyka, Y. Dreis, Y. Khokhlachova, Y. Pepa // Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska (Scopus Indexed), 2025, 15(3).

							– pp. 91-99. 7. Pepa Y. Analysis of Modern Tools, Methods of Audit and Monitoring of Database Security / K. Mykhailyshyn, O. Harasymchuk, O. Deineka, Y. Dreis, V. Shulha, Y. Pepa // Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska (Scopus Indexed), 2025, 15(4). – pp. 124-129. Підпункт 3 - наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора: 1. Пепа Ю.В. Спеціалізовані програмні засоби наукових досліджень [Навч. посіб.] / М.М. Браіловський, В.Д. Козюра, В.В. Кузавков, Ю.В. Пепа, Ю.М. Ткач, В.О. Хорошко, Ю.Є. Хохлачова. – К.: ФОП Ямчинський О.В., 2022. – 202 с. [ISBN 978-617-8184-14-8] 2. Пепа Ю.В. Комп'ютерні технології [Навч. посіб.] / М.М. Браіловський, Н.С. Вишневська, В.Д. Козюра, Ю.В. Пепа, В.О. Хорошко, Ю.Є. Хохлачова. – К.: ТОВ ЦП Компринт, 2023. – 199 с. [ISBN 978-617-8269-41-8] 3. Пепа Ю.В. Офісні програмні системи [Навч. посіб.] / М.М. Браіловський, С.В. Зибін, В.Д. Козюра, Л.І. Моржова, Ю.В. Пепа, В.О. Хорошко, Ю.Є. Хохлачова. – К.: ФОП Ямчинський О.В., 2024. – 332 с. [ISBN 978-617-8171-11-7] 4. Пепа Ю.В., Герасимчук В.С. Інтеграція AI в процес управління телекомунікаційними послугами на прикладі VoIP. Прикладні системи управління та робототехніка [Кол. моногр.] / За заг. ред.

							С.О. Довгого. – Київ, ІПСУ НАН України, 2026. – С. 185-187. [ISBN 978-617-8261-54-2] 5. Пепа Ю.В. Компонентна база засобів кібербезпеки та захисту інформації [Навч. посіб.] / А.М. Котенко, О.Л. Туровський, Г.В. Шуклін, Ю.В. Пепа, І.С. Іванченко, І.М. Аверічев. – К.: «Компринт», 2026 – 233 с. [ISBN 978-617-8830-56-4] Підпункт 4 - наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування; 1. Пепа Ю.В., Петренко А.Б., Сорокун А.Д. Теорія кіл і сигналів в інформаційному та кіберпросторах: Лабораторний практикум. – К.: ДУІКТ, 2026. – 80 с. 2. Пепа Ю.В., Петренко А.Б., Мелешко Т.В., Трейтяк В.В. Теорія кіл і сигналів в інформаційному та кіберпросторах: Практикум. – К.: ДУІКТ, 2026. – 77 с. Підпункт 6 - Наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня: 1. Захист дисертації аспіранта Поночовний Петро Михайлович. Дисертація на здобуття наукового ступеня PhD за спеціальністю 125 – Кібербезпека. Назва дисертації «Система протидії упередження низькошвидкісних HTTP DDOS-атак на веб-ресурси». Диплом доктора філософії Н25

							№ 002938 від 10.09.2025 р. 2. Захист дисертації аспіранта Герасимчук Владислав Сергійович. Дисертація на здобуття наукового ступеня PhD за спеціальністю 172 – Телекомунікації та радіотехніка. Назва дисертації «Методи підвищення ефективності управління в телекомунікаційних мережах при наданні послуг кінцевому користувачеві». Диплом доктора філософії Н26 № 002250 від 18.06.2026 р. Підпункт 7 - Участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад; 1. Член разової спеціалізованої ради при Державному університету інформаційно-комунікаційних технологій при захисті дисертації Рижакова Миколи Миколайовича на тему «Методи та моделі виявлення аномалій мережевого трафіку на об'єктах критичних інформаційних інфраструктур», подану на здобуття ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека», 2026. 2. Член разової спеціалізованої ради при Державному університету інформаційно-комунікаційних технологій при захисті дисертації Хворостяного Родіона Віталійовича на тему «Моделі та методи управління кібербезпекою транспортної телекомунікаційної мережі на основі мультиагентних технологій», подану на здобуття ступеня доктора філософії з галузі знань 12

							«Інформаційні технології» за спеціальністю 125 «Кібербезпека», 2026. 3. Член разової спеціалізованої ради при Державному університету інформаційно-комунікаційних технологій при захисті дисертації Яковця Всеволода Петровича на тему «Метод підвищення якості функціонування телекомунікаційних мереж за допомогою повітряних безпілотних платформ в умовах невизначеності», подану на здобуття ступеня доктора філософії з галузі знань 17 «Електроніка та телекомунікації» за спеціальністю 172 «Телекомунікації та радіотехніка», 2026. Підпункт 8 - Виконання функцій наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії наукового видання, включеного до переліку наукових фахових видань України, або іноземного рецензованого наукового видання, що індексується в бібліографічних базах: 1. Відповідальний виконавець НДР «Шляхи підвищення ефективності захисту командно-телеметричної інформації безпілотних літальних апаратів» (ДР № 0120U100244), 2020 – 2024 рр. 2. Науковий керівник НДР «Розроблення алгоритмів для забезпечення функціональної стійкості інтелектуальних систем при прийнятті рішень» (ДР № 0125U000865), 2025 – 2026 рр. 3. Науковий керівник НДР «Архітектура і реалізація оптичних технологій в кіберпросторі» (ДР № 0125U002689), 2025 – 2030 рр.

							Підпункт 9 - робота у складі експертної ради з питань проведення експертизи дисертацій МОН або у складі галузевої експертної ради як експерта Національного агентства із забезпечення якості вищої освіти, або у складі Акредитаційної комісії, або міжгалузевої експертної ради з вищої освіти Акредитаційної комісії, або трьох експертних комісій МОН/зазначеного Агентства, або Науково-методичної ради/науково-методичних комісій (підкомісій) з вищої або фахової передвищої освіти МОН, наукових/науково-методичних/експертних рад органів державної влади та органів місцевого самоврядування, або у складі комісій Державної служби якості освіти із здійснення планових (позапланових) заходів державного нагляду (контролю): Експерт Акредитаційної комісії Національної Агенції Кваліфікацій МОН України з акредитації кваліфікаційних центрів підвищення кваліфікацій фахової передвищої освіти МОН України з «Кібербезпеки» та «Інформаційних технологій» з 07.03.2024 р. по цей час. Підпункт 12 - Наявність науково-популярних та/або консультаційних (дорадчих) та/або дискусійних публікацій з наукової або професійної тематики загальною кількістю не менше п’яти публікацій: 1. Пепа Ю.В. Засоби проникнення в автоматизовану систему та раннє їх виявлення / Ю.В. Пепа // Збірник матеріалів міжвідомчого круглого столу «Шкідливі програми

							як загроза об'єктам критичної інфраструктури в умовах кібервійни», Київ, 21 лютого 2023 р. – Київ: ІСТЕ СБУ, 2023. – С. 100-109. 2. Pepa Y. Methods of Detection and Analysis of Malicious Software / Y. Pepa, M. Yurchenko, I. Mykhalchuk // Матеріали Всеукр. наук.-практ. конф. «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу», Київ, 23 лютого 2023 р. – Київ: 2023. – С. 106-107. 3. Пепа Ю. Блокчейн-мости: переваги та ризики / Юрій Пепа, Валерія Назаренко // IV Міжнар. наук.-практ. конф. «Новітні технологічні тенденції інтелектуальної індустрії та Інтернету речей «TTSIIT-2025»», Україна-Ірак-Польща, 30-31 січня 2025 р. – К.: КНУБА. – С. 59-64. 4. Yuriy Pepa. Security of IoT Systems Using Blockchain / Yuriy Pepa, Andrii Petrenko, Valentyna Teliushchenko // IV Міжнар. наук.-практ. конф. «Новітні технологічні тенденції інтелектуальної індустрії та Інтернету речей «TTSIIT-2025»», Україна-Ірак-Польща, 30-31 січня 2025 р. – К.: КНУБА. – С. 65-69. 5. Пепа Ю. Антена протидії роботі радіомережі в діапазоні 2,4 ГГц / Ю. Пепа, В. Бичков // Матеріали XIII Міжнар. наук.-техн. конф. «ITSec: Безпека інформаційних технологій», Львів, 9-11 травня 2024 р. – Л.: ЛНУ ім. І. Франка, 2024. – С. 163-164. 6. Пепа Ю.В. Інтегральне оцінювання стійкості систем управління / Ю.В. Пепа, П.М. Поночовний // Наук.-практ. конф. «Перспективи та проблематика інтелектуальних систем», Київ, 31 травня 2024 року. – К.: ДУІКТ, 2024. – С. 3-4. 7. Пепа Ю.В.

							Удосконалення системи передачі даних бездротовими каналами на об'єкті інформаційної діяльності / В.О. Авраменко, І.Д. Данилов, Ю.В. Пепа // Всеукр. наук.-практ. конф. «Актуальні проблеми безпеки інформаційно-телекомунікаційних систем», Київ, 3 - 5 листопада 2024 р. – К: РВЦ ДУІКТ. – 2024. – С. 48-49. 8. Пепа Ю.В. Виявлення несанкціонованих випромінювань в шумових сигналах / І.Д. Данилов, Ю.В. Пепа // Всеукр. наук.-практ. конф. «Актуальні проблеми безпеки інформаційно-комунікаційних систем», Київ, 5 листопада 2025 р. – К: РВЦ ДУІКТ, 2025. – С. 50-51. 9. Yuriy Pepa. Zero-Trust for SMBs in Cloud / Yuriy Pepa, Tetiana Nimchenko, Viktoria Korsunenko / International Scientific and Practical Conference Digital Transformation: Strengthening the Cybersecurity Capacities in the Modern World, Krakow (Poland), November 4-5, 2025. – pp. 63-64. 10. Pepa Yuriy. Balancing Security and Civil Liberties: a Mixed-Methods Analysis of Constitutional Frameworks and Proportionality in Governance / Wasan Maki Mohammed, Saud Suwaid Armoosh, Omar Ahmed Hassan Khamees, Noor Sabah Abd-Al Latif Jasim, Baker Mohammed Khalil, Mark Belkin, Yuriy Pepa / International Conference on Optimization and Data Science in Industrial Engineering «ODSIE-2025» (Scopus Indexed), Istanbul (Turkey), November 20-22, 2025. – pp. 191. 11. Mohammed, W.M. et al. (2026). Balancing Security and Civil Liberties: A Mixed-Methods Analysis of Constitutional Frameworks and

							Proportionality in Governance. In: Molamohamadi, Z., Babaee Tirkolaee, E., Mirzazadeh, A., Weber, GW. (eds) Optimization and Data Science in Industrial Engineering. «ODSIE-2025». Communications in Computer and Information Science, Vol. 2854. Springer. pp. 685-701. 12. Yuriy Pepa. Integrated Security Framework for the Smart Home IoT Ecosystem / Andrii Petrenko, Yuriy Pepa // The V International Conference on Emerging «Technology Trends on the Smart Industry and the Internet of Things «TTSIIT-2026»», Ukraine-Iraq-Poland (Kyiv, Ukraine), January 29 - 30, 2026. – К.: KNUCA. – pp. 31-34. 13. Yuriy Pepa. An Intelligent Neuro-Adaptive Framework for Functional Stability of Information Systems / Yuliya Olimpiyeva, Yuriy Pepa // The V International Conference on Emerging «Technology Trends on the Smart Industry and the Internet of Things «TTSIIT-2026»», Ukraine-Iraq-Poland (Kyiv, Ukraine), January 29 - 30, 2026. – К.: KNUCA. – pp. 35-38. 14. Yuriy Pepa. Algorithm for Synthesizing Background Network Traffic / Vladyslav Herasymchuk, Yuriy Pepa // The V International Conference on Emerging «Technology Trends on the Smart Industry and the Internet of Things «TTSIIT-2026»», Ukraine-Iraq-Poland (Kyiv, Ukraine), January 29 - 30, 2026. – К.: KNUCA. – pp. 37-40. Підпункт 19 - діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях: 1. Дійсний член професійної «Міжнародної

							асоціації інженерів та технологів» з 08.02.2026 р. по теперішній час. 2. Дійсний член ГО «Асоціація спеціалістів з кібербезпеки» з 26.03.2026 р. по теперішній час.
455594	Туровський Олександр Леонідович	Завідувач кафедри, Основне місце роботи	Навчально-науковий інститут Кібербезпеки та захисту інформації	Диплом спеціаліста, Військово-повітряна інженерна ордена Леніна та Жовтневої революції Червонопрапорна академія імені професор М. Є. Жуковського, рік закінчення: 1992, спеціальність: Обладнання літальних апаратів, Диплом магістра, Національна академія оборони України, рік закінчення: 2008, спеціальність: Організація бойового та оперативного забезпечення військ (за видами та родами військ і сил), Диплом доктора наук ДД 011829, виданий 29.06.2021, Диплом кандидата наук ДК 021196, виданий 10.12.2003, Атестат доцента 12ДЦ 017169, виданий 21.06.2007, Атестат професора АП 004855, виданий 20.02.2023	17	Корпоративна та професійна етика в кібербезпеці	Науковий ступінь: доктор технічних наук, диплом ДД №011829 від 29.06.2021 р. спеціальності 172 – електроні комунікації та радіоелектроніка (05.12.13 – радіотехнічні пристрої та засоби телекомунікацій). Вчене звання: професор за кафедрою засобів захисту інформації, атестат АП № 004855 від 20.02.2023 р. Підвищення кваліфікації: 1. Akademia Techniczno-Humanistyczna, Department of Computer Science and Automatics. м. Бєльсько-Бяла (Республіка Польща). Сертифікат від 30 вересня 2022 року. Термін стажування з 01.08.2022 по 29.09.2022, 180 годин. Програма стажування: «Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту інформації». 2. ТОВ «ЛУЧ», Сертифікат № 000135-2025/S9, Програма стажування: «Організація захисту інформації під час введення в експлуатацію ІКС», 20.01.2025 р., 90 годин (3 кредити ECTS); 3. ТОВ «ДЕФЕНДІКО», Сертифікат № 000112-2025/S4, «Захист державних інформаційних ресурсів», 07.03.2025 р., 90 годин (3 кредити ECTS). 4. «PROMETHEUS» Сертифікат «Академічна дорочесність», 15.03.2026, 60 годин (2 кредити ECTS). Види і результати професійної

							діяльності за спеціальністю відповідно до п.38 Ліцензійних умов провадження освітньої діяльності: (п. 1, 2, 3, 4, 6, 7, 8, 12,) 1.наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection; 1. Makarenko, A., Qasim, N., Turovsky, O., Rudenko, N., Polonskyi, K., Govorun, O. Reducing the impact of interchannel interference on the efficiency of signal transmission in telecommunication systems of data transmission based on the OFDM signal. Eastern-European Journal of Enterprise Technologies, 1(9(121)), 2023, pp. 82–93. https://doi.org/10.15587/1729-4061.2023.274501. (Scopus). 2. Oksana Zghurska, Oleksandr Turovsky, Olena Shevchenko, Inna Zelisko, Ruslan Dymenko, Yuriy Safonov. Improvement of methodological principles of brand protection in cyberspace. Financial and Credit Activity Problems of Theory and Practice, 4(51), 2023, 539–552. https://doi.org/10.55643/fcaptp.4.51.2023.4108. (Scopus) 3. Туровський О. Л. Правдивий А. М. Моделювання сигналів засобів негласного отримання інформації за допомогою Сплайн-функцій. Сучасний захист інформації. №1, 2024, С. 22-27.DOI: 10.31673/2409-7292.2024.010003 4. Turovsky, O., Blazhennyi, N., Vozniak, R., Horbachova, Y., Horbachov, K., & Rudenko, N. (2025). Development of a model for calculating the dilution of precision coefficients of the global navigation

							system at a given point in space. Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska, 15(1), 79–87. https://doi.org/10.35784/iapgos.6401 (Scopus) 5. Конотопець, М., Туровський, О., Самойлов, І., & Комонюк, Є. (2025). Перспективи засосування тепловізорів для виявлення радіоелектронних засобів негласного отримання інформації на обєктах інформаційної діяльності. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (1),1015, 59–69. https://doi.org/10.31891/2219-9365-2025-81-8 6. Конотопець М. М., Сторчак А. С., Голь В. Д., Туровський О. Л. Вплив інформаційних технологій і світових практик на стандартизацію професій. Сучасний захист інформації. №1(61), 2025, С. 165-173. https://doi.org/: 10.31673/2409-7292.2025.015125 7. Іванченко Є. В. , Тарасенко Я. В., Туровський О. Л., Кихтенко Є. М., Трухан Д. В. (2025). Методи кіберзахисту мережі інтернету речей у сфері передачі даних лабораторних досліджень. Наукові записки Державного університету інформаційно-комунікаційних технологій, 1 (2025), 15-25. DOI: 10.31673/2786-8362.2025.011058 8. Хворостяний Р. В., Туровський О. Л. Метод взаємодії агентів в мультиагентній системі управління кібербезпекою транспортної телекомунікаційної мережі під час діагностування кібератак. Телекомунікаційні та інформаційні технології. 2026. No 1 (90). 38–49. https://doi.org/10.31673/2412-4338.2026.019005

							9. Туровський О.Л.,, Іванченко Є.В., Рижаков М.М. Методика побудови системи безпеки об’єкта інформаційної діяльності для роботи з інформацією з обмеженим доступом. Measuring and computing devices in technological processes, (3), 2026, Подано на публікацію 2.наявність одного патенту на винахід або п’яти деклараційних патентів на винахід чи корисну модель, включаючи секретні, або наявність не менше п’яти свідоцтв про реєстрацію авторського права на твір; 1. Пат. 150761 UA. МПК G01N23/02 G02F1/157.; - № u 202106129; заявл. 01.11.2021; опубл. 13.04.2022, бюл. № 15. С. 4.13-4.14. 2. Пат. 158391. МПК G01S5/10 - № u 202403422; заявл. 01.07.2024; опубл. 29.01.2025, бюл. № 5/2025. С.4.13. 3.наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора); 1. Туровський О.Л, Аверічев І.М, Копоративна та професійна єтика в кібербезпеці. Навчальний посібник. — К.: ДУІКТ, 2026. — 128 с. Поданий до друку 2. Туровський О.Л., Іванченко Є.В., Лозова І.Л. Основи наукових досліджень в кібербезпеці. Навчальний посібник. — К.: ДУІКТ, 2026. — 184 с. Поданий до друку 3. Луцький М. Г., О. Ю. Пузиренко, Туровський О. Л., Жарова О. В. Методи обробки мультимедійної інформації. Навчальний посібник. — К.: НАУ, 2023. — 268 с.

							4.наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування; 1. Туровський О.Л., А.М. Котенко. «Технології створення та застосування комплексів засобів захисту інформації з обмеженим доступом та охорони об'єктів інформаційної діяльності». Конспект лекцій. — К.: ДУІКТ, 2026. — 94 с. 2. С.В. Лазаренко, В.О. Темников, О.Л. Туровський, Ю.В. Баланюк. Кібербезпека систем технічного захисту інформації, автоматизація їх обробки. Методичні рекомендації. – К.:НАУ, 2022. –68 с. 3. В.В. Козловський, О.Л. Туровський , С.В. Лазаренко, О.Ю. Пузиренко. Спеціальні вимірювання. Лабораторний практикум. –К.:НАУ, 2022. –62 с. 6.наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня; 1. Доктор філософії (PhD), Спеціальність 125 – кібербезпека та захист інформації, Хворостяний Родіон Віталійович, 2026 р. «Моделі та методи управління кібербезпекою транспортної телекомунікаційної мережі на основі мультиагентних технологій» 2. Доктор філософії (PhD), Спеціальність 172 – електронні комунікації та радіотехніка, Невгод Максим Юрійович,

							2023 р. «Методика підвищення точності роботи системи фазової синхронізації когерентних демодуляторів супутникових телекомунікацій в перехідних режимах стеження за несучою частотою» 7.участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад; 1. Член спеціалізованої вченої ради Д 26.861.01 при ДУІКТ з правом прийняття до розгляду та проведення захисту дисертацій на здобуття наукового ступеня доктора (кандидата) технічних наук за спеціальністю 05.12.13 – радіотехнічні пристрої та засоби телекомунікацій. 2. Член разової спеціалізованої ради при КНУ ім. Т.Шевченка при захисті дисертації Корчака Олександра Володимировича на тему: «Методологія вдосконалення терабітних телекомунікаційних систем засобами ВКР фотоніки», поданої на здобуття ступеня доктора філософії з спеціальності 172 Телекомунікації та радіотехніка (2022). 3. Член разової спеціалізованої ради при Державному університету інформаційно-комунікаційних технологій при захисті дисертації Шапрана Олександра Олександровича на тему “Методика підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України”, подану на здобуття ступеня доктора філософії з галузі знань 12 “Інформаційні технології” за спеціальністю 125 “Кібербезпека” (2024). 4. Член разової спеціалізованої ради

							при Державному університету інформаційно-комунікаційних технологій при захисті дисертації Цмоканича Івана Володимировича на тему: «Методи та алгоритми захисту інформації від високочастотного нав'язування» подану на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 – Кібербезпека (2024). 5. Член разової спеціалізованої ради при Державному університету інформаційно-комунікаційних технологій при захисті дисертації Запорожченко М.М. «Методи прогнозування соціоінженерних атак на корпоративні інформаційні системи на основі профілю захищеності користувача» подану на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 – Кібербезпека (2025). 6. Член разової спеціалізованої ради при Державному університету інформаційно-комунікаційних технологій при захисті дисертації Магомедової Марії Сергіївни на тему: «Метод створення антенно-фідерного тракту мобільної цифрової тропосферноіоносферної станції» подану на здобуття ступеня доктора філософії з галузі знань 17 Електроніка та телекомунікації за спеціальністю 172 – Телекомунікації та радіотехніка (2024). 6. Член разової спеціалізованої ради при Державному університету інформаційно-комунікаційних технологій при захисті дисертації Треньової Катерини Олександрівни Методика оперативного аналізу характеристик

							трафіку для автоматизованого управління якістю послуг у мультисервісних інформаційних системахподану на здобуття ступеня доктора філософії з галузі знань 17 Електроніка та телекомунікації за спеціальністю 172 – Телекомунікації та радіотехніка (2024) 8.виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах; 1. Член редколегії наукового журналу «Вимірювальна та очислювальна техніка в технологічних процесах» (Measuring and computing devices in technological processes) включеного до переліку наукових фахових видань України. 2. Член редколегії наукового журналу «Штучний інтелект"-"Artificial intelligence» включеного до переліку наукових фахових видань України. 12.наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п'яти публікацій; 1. O. Golubenko, A. Onysko, A. Lemeshko, A. Zelnytskyi, O. Zabolotnyi, A. Zakharzhevskyi, O. Turovsky, "Assessment of Possibility of Modernization of Hierarchy Code Structure of Multidimensional

							Signal to Increase the Efficiency of Functioning of Educational and Training Telecommunication Systems", Emerging Technology Trends on the Smart Industry and the Internet of Thing Conference (TTSIIT - 2022). The 1st International Conference CEUR Workshop Proceedings, Kyiv, Ukraine, January 19, 2022, P. 154-162. http://ceur-ws.org/Vol-3149/short6.pdf. (Scopus). 2. O. Turovsky, H. M. Jawad, M. J. Abu-AlShaeer, S. Yevseiev, V. Kornienko. Improvement of the Methodology of Building a System of Phase Synchronization of Coherent Demodulators in Telecommunication Control Systems and Distance Learning. "2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)", 6th International Symposium on Multidisciplinary Studies and Innovative Technologies. October 20-22, 2022, Ankara, Turkey 2022, pp. 1013-1016. doi: 10.1109/ISMSIT56059.2022.9932844. (Конференція) (Scopus). 3. Nahlah M.A.M Najm, Nada Adnan Taher, Oleksandr Valchenko, Oleksandr Turovsky. Improvement of the methodology for evaluating the carrier frequency of the signal during data transmission in telecommunication control and distance learning systems. The III international scientific – practical conference – modern information, measurement, and control systems: problems, applications and perspectives 2022 (MIMCS' - 2022). November 04-05, 2022 Antalya, Türkiye. Pp. 60-61. https://doi.org/10.36962/piretc24032023-56 4. Nahlah M.A.M Najm, Nada Adnan Taher, Oleksandr Valchenko,

							Oleksandr Turovsky. Improvement of the methodology for evaluating the carrier frequency of the signal during data transmission in telecommunication control and distance learning systems. Namig Isazade, Piretc - Proceedings of the international research, education & training center. Zenodo, 2023. https://doi.org/10.5281/zenodo.17932401 5. Mustafa F.M., Jasim M.A., Mejbel B.G., Abdullah S.B., Gati K.H., Noga H., Turovsky O. Using Emergency Drones to Speed Up Hospital Alerts and Ambulance Dispatch. (2024) Conference of Open Innovation Association, FRUCT, pp. 409 - 422. DOI: 10.23919/FRUCT64283.2024.10749864. (Scopus);
269011	Котенко Андрій Миколайович	Доцент, Основне місце роботи	Навчально-науковий інститут Кібербезпеки та захисту інформації	Диплом молодшого спеціаліста, Керченский судомеханический техникум, рік закінчення: 1988, спеціальність: , Диплом спеціаліста, Київське вище ін-женерне радіо-технічне училище протиповітряної оборони ім. О.І. Покришкіна, рік закінчення: 1993, спеціальність: радіотехнічні засоби, кваліфікація - радіоінженер, Диплом кандидата наук ДК 049262, виданий 12.11.2008, Атестат доцента АД 003527, виданий 16.12.2019	23	Технологія створення та застосування комплексів засобів захисту інформації з обмеженим доступом та охорони ОІД	Кандидат технічних наук зі спеціальності 05.13.06 – інформаційні технології. Тема дисертації: «Методика обґрунтування характеристик неортогональних широкосмугових сигналів у телекомунікаційній мережі системи дистанційного спостереження та охорони воєнних об'єктів». Диплом ДК №049262 від 12.11.2008 року. Вчене звання: доцент кафедри Систем інформаційного та кібернетичного захисту АД № 003527 від 16.12.2019 року. Підвищення кваліфікації: 1. ТОВ «ЛУЧ», Сертифікат № 000136-2025/S9, Програма стажування: «Організація захисту інформації під час введення в експлуатацію ІКС», 20.01.2025 р., 90 годин (3 кредити ECTS); 2. ТОВ «ДЕФЕНДІКО», Сертифікат № 000113-2025/S4, «Захист державних інформаційних ресурсів», 07.03.2025

							р., 90 годин (3 кредити ECTS). Види і результати професійної діяльності за спеціальністю відповідно до п.38 Ліцензійних умов провадження освітньої діяльності: (п. 1, 3,5, 8, 11, 14, 19) 1.наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, WebofScienceCoreCollection; 1. Laptiev O., Savchenko V., Kotenko A., et. al. Method of Determining Trust and Protection of Personal Data in Social Networks. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 13, No. 1, pp.15-21. 2021 april, 2021.https://doi.org/10.17762/ijcnis.v13i1.4882 2. TalalTaha R., MuhanadM.Salih M., Raheem Mohammed Al-Ani A., Mahmood Jawad H., Waleed Abdulah N., Kotenko A., Mahmoud Al-Jawher W. Method Integrating IMS with Blockchain: A New Frontier in Secure Communication Networks.ISSN 2305-7254, PROCEEDING OF THE 36TH CONFERENCE OF FRUCT ASSOCIATION, 2024. pp.778-786. https://fruct.org/publications/volume-36/fruct36/files/Tal.pdf 3.ІгорКозубцов, НаталіяЗінченко, Андрій Котенко, ІгорАверічев.Проблемизабезпеченняінформаційноїбезпекисуб'єктамиосвітньоїдіяльності в цифровому освітньо-науковомусередовищізакладівосвіти.SMART TECHNOLOGIES. Київ. КНУБА, 2024, № 2(15), с. 56 – 65. https://doi.org/10.32347/uwt.2024.15 4. Чабан Б. В., Котенко А. М. Модель системи захисту інформації від витоку матеріально-речовим каналом на

							базі ланцюгів Маркова / ДУІКТ: Сучасний захист інформації 2024 № 4(60) с. 46-53. https://journals.dut.edu.ua/index.php/dataprotect/article/view/3058/2948 3.наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора); А.М. Котенко, О.Л. Туровський, Г.В.Шуклін, Ю.В. Пепа, І.С. Іванченко, І.М. Аверічев. Компонентна база засобів кібербезпеки та захисту інформації Навчальний посібник. - К.: ДУІКТ. – 236 с. https://duikt.edu.ua/ua/lib/1/category/2351/view/2376 (9,6 авт. арк) 4.наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування; Котенко А.М., Хлапонін Ю.І. Конспект лекцій “Цифрова обробка сигналів“ для студентів спеціальності 123 “Комп’ютерна інженерія“ з дисципліни “Цифрова обробка сигналів“. - К.: КНУБА, 2023. – 99 с. (6 друк. аркуш) https://repositary.knuba.edu.ua/handle/123456789/13418 Котенко А.М., Хлапонін Ю.І. Методичні вказівки до виконання

							лабораторних робіт для студентів з галузі знань 12 “Інформаційні технології“ за спеціальністю 123 “Комп’ютерна інженерія“ з дисципліни “Цифрова обробка зображень“. - К.: КНУБА, 2022. – 36 с. (1 друк. аркуш) https://repositary.knuba.edu.ua/items/63eef550-cd51-4248-9210-45bf47165e09 Котенко А.М. Конспект лекцій для студентів зі спеціальності 125 «Кібербезпека та захист інформації» з дисципліни «Системи контролю та управління доступом на об’єкти інформаційної діяльності». –К, ДУІКТ, 2024. – 79 с. https://duikt.edu.ua/ua/lib/1/category/1014/view/1372 Конспект лекцій для студентів з галузі знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека та захист інформації» з дисципліни «Програмно-апаратні засоби захисту»/ Уклад. А.М. Котенко, Ю.І. Хлапонін, В.М. Трофимчук – К.:КНУБА, 2025. – 154 с. – у процесі викладки на сайт 9.робота у складі експертної ради з питань проведення експертизи дисертацій МОН або у складі галузевої експертної ради як експерта Національного агентства із забезпечення якості вищої освіти, або у складі Акредитаційної комісії, або міжгалузевої експертної ради з вищої освіти Акредитаційної комісії, або трьох експертних комісій МОН/зазначеного Агентства, або Науково-методичної ради/науково-методичних комісій (підкомісій) з вищої або фахової передвищої освіти МОН, наукових/науково-

							методичних/експертних рад органів державної влади та органів місцевого самоврядування, або у складі комісій Державної служби якості освіти із здійснення планових (позапланових) заходів державного нагляду (контролю); Член редакційної колегії/експерт видання:Proceedingsof FRUCT'35Tampere, Finland, 24-26 April 2024 FRUCTOy, Finland, ISSN 2305-7254, ISBN 978-952-65246-1-0 https://www.fruct.org/conferences/FRUCT36_Program.pdf 12.наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п’яти публікацій; Котенко А.М., Гребенніков А.Б.Підвищення ефективності захисту кібернетичної безпеки об’єкту інформаційної діяльності. Теза доповіді XII Всеукраїнська науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави» - Київ: - Національна академія Служби Безпеки України, Науково-дослідний інститут інформатики і права Національної академії правових наук України. 26 березня 2021 року. С. 190 – 192. https://nasbu.edu.ua/uploads/p_57_53218641.pdf Котенко А.М., Каліш В,В. Порівняння криптографічних алгоритми хешуваннясha-3 та sha-256// Всеукраїнська конференція «Актуальні проблеми безпеки інформаційно-телекомунікаційних систем», 5 листопада 2024 р. Державний

							університет інформаційно-комунікаційних технологій - Київ: 2024 р. С.. 12-13 https://duikt.edu.ua/uploads/p_2661_93669247.pdf А.М. Котенко, Б.В. Чабан Математична модель матеріально-речового каналу витоку інформації// Всеукраїнська конференція «Актуальні проблеми безпеки інформаційно-телекомунікаційних систем», 5 листопада 2024 р. Державний університет інформаційно-комунікаційних технологій - Київ: 2024р. С. 72-73https://duikt.edu.ua/uploads/p_2661_93669247.pdf
455594	Туровський Олександр Леонідович	Завідувач кафедри, Основне місце роботи	Навчально-науковий інститут Кібербезпеки та захисту інформації	Диплом спеціаліста, Військово-повітряна інженерна ордена Леніна та Жовтневої революції Червонопрапорна академія імені професор М. Є. Жуковського, рік закінчення: 1992, спеціальність: Обладнання літальних апаратів, Диплом магістра, Національна академія оборони України, рік закінчення: 2008, спеціальність: Організація бойового та оперативного забезпечення військ (за видами та родами військ і сил), Диплом доктора наук ДД 011829, виданий 29.06.2021, Диплом кандидата наук ДК 021196, виданий 10.12.2003, Атестат доцента 12ДЦ 017169, виданий 21.06.2007, Атестат	17	Організація проведення наукових досліджень	Науковий ступінь: доктор технічних наук, диплом ДД №011829 від 29.06.2021 р. спеціальності 172 – електроні комунікації та радіоелектроніка (05.12.13 – радіотехнічні пристрої та засоби телекомунікацій). Вчене звання: професор за кафедрою засобів захисту інформації, атестат АП № 004855 від 20.02.2023 р. Підвищення кваліфікації: 1. Akademia Techniczno-Humanistyczna, Department of Computer Science and Automatics. м. Бєльсько-Бяла (Республіка Польща). Сертифікат від 30 вересня 2022 року. Термін стажування з 01.08.2022 по 29.09.2022, 180 годин. Програма стажування: «Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту інформації». 2. ТОВ «ЛУЧ», Сертифікат № 000135-2025/S9, Програма стажування: «Організація захисту інформації під час введення в експлуатацію ІКС»,

				професора АП 004855, виданий 20.02.2023			20.01.2025 р., 90 годин (3 кредити ECTS); 3. ТОВ «ДЕФЕНДІКО» , Сертифікат № 000112-2025/S4, «Захист державних інформаційних ресурсів», 07.03.2025 р., 90 годин (3 кредити ECTS). 4. «PROMETHEUS» Сертифікат «Академічна дорочесність», 15.03.2026, 60 годин (2 кредити ECTS). Види і результати професійної діяльності за спеціальністю відповідно до п.38 Ліцензійних умов провадження освітньої діяльності: (п. 1, 2, 3, 4, 6, 7, 8, 12,) 1.наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection; 1. Makarenko, A., Qasim, N., Turovsky, O., Rudenko, N., Polonskyi, K., Govorun, O. Reducing the impact of interchannel interference on the efficiency of signal transmission in telecommunication systems of data transmission based on the OFDM signal. Eastern-European Journal of Enterprise Technologies, 1(9(121)), 2023, pp. 82–93. https://doi.org/10.15587/1729-4061.2023.274501. (Scopus). 2. Oksana Zghurska, Oleksandr Turovsky, Olena Shevchenko, Inna Zelisko, Ruslan Dymenko, Yuriy Safonov. Improvement of methodological principles of brand protection in cyberspace. Financial and Credit Activity Problems of Theory and Practice, 4(51), 2023, 539–552. https://doi.org/10.55643/fcaptp.4.51.2023.4108. (Scopus) 3. Туровський О. Л. Правдивий А. М. Моделювання сигналів засобів

							негласного отримання інформації за допомогою Сплайн-функцій. Сучасний захист інформації. №1, 2024, С. 22-27.DOI: 10.31673/2409-7292.2024.010003 4. Turovsky, O., Blazhennyi, N., Vozniak, R., Horbachova, Y., Horbachov, K., & Rudenko, N. (2025). Development of a model for calculating the dilution of precision coefficients of the global navigation system at a given point in space. Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska, 15(1), 79–87. https://doi.org/10.35784/iapgos.6401 (Scopus) 5. Конотопець, М., Туровський, О., Самойлов, І., & Комонюк, Є. (2025). Перспективи засосування тепловізорів для виявлення радіоелектронних засобів негласного отримання інформації на обєктах інформаційної діяльності. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (1),1015, 59–69. https://doi.org/10.31891/2219-9365-2025-81-8 6. Конотопець М. М., Сторчак А. С., Голь В. Д., Туровський О. Л. Вплив інформаційних технологій і світових практик на стандартизацію професій. Сучасний захист інформації. №1(61), 2025, С. 165-173. https://doi.org/: 10.31673/2409-7292.2025.015125 7. Іванченко Є. В. , Тарасенко Я. В., Туровський О. Л., Кихтенко Є. М., Трухан Д. В. (2025). Методи кіберзахисту мережі інтернету речей у сфері передачі даних лабораторних досліджень. Наукові записки Державного університету інформаційно-комунікаційних технологій, 1 (2025), 15-25. DOI: 10.31673/2786-

							8362.2025.011058 8. Хворостяний Р. В., Туровський О. Л. Метод взаємодії агентів в мультиагентній системі управління кібербезпекою транспортної телекомунікаційної мережі під час діагностування кібератак. Телекомунікаційні та інформаційні технології. 2026. No 1 (90). 38–49. https://doi.org/10.31673/2412-4338.2026.019005 9. Туровський О.Л.,, Іванченко Є.В., Рижаков М.М. Методика побудови системи безпеки об'єкта інформаційної діяльності для роботи з інформацією з обмеженим доступом. Measuring and computing devices in technological processes, (3), 2026, Подано на публікацію 2.наявність одного патенту на винахід або п'яти деклараційних патентів на винахід чи корисну модель, включаючи секретні, або наявність не менше п'яти свідоцтв про реєстрацію авторського права на твір; 1. Пат. 150761 UA. МПК G01N23/02 G02F1/157.; - № u 202106129; заявл. 01.11.2021; опубл. 13.04.2022, бюл. № 15. С. 4.13-4.14. 2. Пат. 158391. МПК G01S5/10 - № u 202403422; заявл. 01.07.2024; опубл. 29.01.2025, бюл. № 5/2025. С.4.13. 3.наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора); 1. Туровський О.Л, Аверічев І.М, Копоративна та професійна єтика в кібербезпеці. Навчальний посібник. — К.: ДУІКТ, 2026. —

							128 с. Поданий до друку 2. Туровський О.Л., Іванченко Є.В., Лозова І.Л. Основи наукових досліджень в кібербезпеці. Навчальний посібник. — К.: ДУІКТ, 2026. — 184 с. Поданий до друку 3. Луцький М. Г., О. Ю. Пузиренко, Туровський О. Л., Жарова О. В. Методи обробки мультимедійної інформації. Навчальний посібник. — К.: НАУ, 2023. — 268 с. 4.наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування; 1. Туровський О.Л., А.М. Котенко. «Технології створення та застосування комплексів засобів захисту інформації з обмеженим доступом та охорони об'єктів інформаційної діяльності». Конспект лекцій. — К.: ДУІКТ, 2026. — 94 с. 2. С.В. Лазаренко, В.О. Темников, О.Л. Туровський, Ю.В. Баланюк. Кібербезпека систем технічного захисту інформації, автоматизація їх обробки. Методичні рекомендації. – К.:НАУ, 2022. –68 с. 3. В.В. Козловський, О.Л. Туровський , С.В. Лазаренко, О.Ю. Пузиренко. Спеціальні вимірювання. Лабораторний практикум. –К.:НАУ, 2022. –62 с. 6.наукове керівництво (консультування) здобувача, який одержав документ про

							присудження наукового ступеня; 1. Доктор філософії (PhD), Спеціальність 125 – кібербезпека та захист інформації, Хворостяний Родіон Віталійович, 2026 р. «Моделі та методи управління кібербезпекою транспортної телекомунікаційної мережі на основі мультиагентних технологій» 2. Доктор філософії (PhD), Спеціальність 172 – електронні комунікації та радіотехніка, Невгод Максим Юрійович, 2023 р. «Методика підвищення точності роботи системи фазової синхронізації когерентних демодуляторів супутникових телекомунікацій в перехідних режимах стеження за несучою частотою» 7.участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад; 1. Член спеціалізованої вченої ради Д 26.861.01 при ДУІКТ з правом прийняття до розгляду та проведення захисту дисертацій на здобуття наукового ступеня доктора (кандидата) технічних наук за спеціальністю 05.12.13 – радіотехнічні пристрої та засоби телекомунікацій. 2. Член разової спеціалізованої ради при КНУ ім. Т.Шевченка при захисті дисертації Корчака Олександра Володимировича на тему: «Методологія вдосконалення терабітних телекомунікаційних систем засобами ВКР фотоніки», поданої на здобуття ступеня доктора філософії з спеціальності 172 Телекомунікації та радіотехніка (2022). 3. Член разової спеціалізованої ради

							при Державному університету інформаційно-комунікаційних технологій при захисті дисертації Шапрана Олександра Олександровича на тему “Методика підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України”, подану на здобуття ступеня доктора філософії з галузі знань 12 “Інформаційні технології” за спеціальністю 125 “Кібербезпека” (2024). 4. Член разової спеціалізованої ради при Державному університету інформаційно-комунікаційних технологій при захисті дисертації Цмоканича Івана Володимировича на тему: «Методи та алгоритми захисту інформації від високочастотного нав’язування» подану на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 – Кібербезпека (2024). 5. Член разової спеціалізованої ради при Державному університету інформаційно-комунікаційних технологій при захисті дисертації Запорожченко М.М. «Методи прогнозування соціоінженерних атак на корпоративні інформаційні системи на основі профілю захищеності користувача» подану на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 – Кібербезпека (2025). 6. Член разової спеціалізованої ради при Державному університету інформаційно-комунікаційних технологій при захисті дисертації Магомедової Марії Сергіївни на тему: «Метод створення антенно-фідерного

							тракту мобільної цифрової тропосферноіоносферної станції» подану на здобуття ступеня доктора філософії з галузі знань 17 Електроніка та телекомунікації за спеціальністю 172 – Телекомунікації та радіотехніка (2024). 6. Член разової спеціалізованої ради при Державному університету інформаційно-комунікаційних технологій при захисті дисертації Треньової Катерини Олександрівни Методика оперативного аналізу характеристик трафіку для автоматизованого управління якістю послуг у мультисервісних інформаційних системахподану на здобуття ступеня доктора філософії з галузі знань 17 Електроніка та телекомунікації за спеціальністю 172 – Телекомунікації та радіотехніка (2024) 8.виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах; 1. Член редколегії наукового журналу «Вимірювальна та очислювальна техніка в технологічних процесах» (Measuring and computing devices in technological processes) включеного до переліку наукових фахових видань України. 2. Член редколегії наукового журналу «Штучний інтелект"-"Artificial intelligence» включеного до переліку наукових

							фахових видань України. 12.наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п’яти публікацій; 1. O. Golubenko, A. Onysko, A. Lemeshko, A. Zelnytskyi, O. Zabolotnyi, A. Zakharzhevskyi, O. Turovsky, "Assessment of Possibility of Modernization of Hierarchy Code Structure of Multidimensional Signal to Increase the Efficiency of Functioning of Educational and Training Telecommunication Systems", Emerging Technology Trends on the Smart Industry and the Internet of Thing Conference (TTSIIT - 2022). The 1st International Conference CEUR Workshop Proceedings, Kyiv, Ukraine, January 19, 2022, P. 154-162. http://ceur-ws.org/Vol-3149/short6.pdf. (Scopus). 2. O. Turovsky, H. M. Jawad, M. J. Abu-AlShaeer, S. Yevseiev, V. Kornienko. Improvement of the Methodology of Building a System of Phase Synchronization of Coherent Demodulators in Telecommunication Control Systems and Distance Learning. "2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)”, 6th International Symposium on Multidisciplinary Studies and Innovative Technologies. October 20-22, 2022, Ankara, Turkey 2022, pp. 1013-1016. doi: 10.1109/ISMSIT56059.2022.9932844. (Конференція) (Scopus). 3. Nahlah M.A.M Najm, Nada Adnan Taher, Oleksandr Valchenko, Oleksandr Turovsky.

							Improvement of the methodology for evaluating the carrier frequency of the signal during data transmission in telecommunication control and distance learning systems. The III international scientific – practical conference – modern information, measurement, and control systems: problems, applications and perspectives 2022 (MIMCS' - 2022). November 04-05, 2022 Antalya, Türkiye. Pp. 60-61. https://doi.org/10.36962/piretc24032023-564. Nahlah M.A.M Najm, Nada Adnan Taher, Oleksandr Valchenko, Oleksandr Turovsky. Improvement of the methodology for evaluating the carrier frequency of the signal during data transmission in telecommunication control and distance learning systems. Namig Isazade, Piretc - Proceedings of the international research, education & training center. Zenodo, 2023. https://doi.org/10.5281/zenodo.17932401 5. Mustafa F.M., Jasim M.A., Mejbel B.G., Abdullah S.B., Gati K.H., Noga H., Turovsky O. Using Emergency Drones to Speed Up Hospital Alerts and Ambulance Dispatch. (2024) Conference of Open Innovation Association, FRUCT, pp. 409 - 422. DOI: 10.23919/FRUCT64283.2024.10749864. (Scopus);
356622	Кондратенко Наталія Юріївна	Доцент, Основне місце роботи	Навчально-науковий інститут Телекомунікацій	Диплом спеціаліста, Київський університет імені Тараса Шевченка, рік закінчення: 1998, спеціальність: Українська мова та література, Диплом кандидата наук ДК 050257, виданий 18.12.2018, Атестат доцента АД 010895, виданий	13	Педагогіка та психологія у вищій школі	Кандидат педагогічних наук. Наукова спеціальність: 13.00.02 теорія та методика навчання (українська мова), тема дисертації: «Методика формування комунікативної компетентності майбутніх журналістів на засадах лінгвокультурології» (ДК №050257, 2018 р., виданий МОН України); Доцент кафедри української мови Атестат доцента Від

				09.08.2022			09.08.22 АД №010895 Підвищення кваліфікації: 1. Теоретико-практичний курс «Освіта як індикатор суспільного розвитку», Центр українсько-європейського наукового співробітництва, 02.10.2023-12.11.2023, Свідоцтво № ADV-021012-PSI від 12.11.2023, 180 годин /6 кредитів. 2. Prometheus. Онлайн-курс для викладачів: Академічна доброчесність. 60 годин (2 кредити). Сертифікат від15.11.2024. Ідентифікаційний номер сертифікату fc474956fb5b4a8ca92957188a69eb48 https://certs.prometheus.org.ua/cert/fc474956fb5b4a8ca92957188a69eb48 Види і результати професійної діяльності за спеціальністю відповідно до п.38 Ліцензійних умов провадження освітньої діяльності: (п.п. 1, 3, 12, 19) Підпункт 1 - наявність не менше п’яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection: 1. Stezhko S., Kondratenko N., Zabolotnia R., 1. Стежко С.О., Кондратенко Н.Ю., Ситник Л.І. Психологічні та лінгвістичні чинники ефективності професійно орієнтованого мовного навчання у вищій школі // Соціальна педагогіка: теорія та практика № 4, Полтава, 2025 С. 190-197. URL: DOI https://doi.org/10.12958/1817-3764-2025-4-190-197 http://socped.luguniv.edu.ua/index.php/socped/issue/view/10 2. Стежко С.О., Кондратенко Н.Ю., Заболотня Р.В.

							Формування професійної мовної особистості студента: психолінгвістичний, педагогічний і психологічний виміри, Збірника наукових праць Педагогіка формування творчої особистості у вищій і загальноосвітній школах, Журнал включено до міжнародної наукометричної бази Index Copernicus International (Республіка Польща). № 102, Запоріжжя, 2025, С. 58-63, DOI https://doi.org/10.32782/1992-5786.2025.102.10 .https://pedagogy-journal.kpu.zp.ua/102-2025. 3. Кондратенко Н., Кравченко В., Воропай І., Цифрова комунікація і штучний інтелект: методичний потенціал формування мовнокомунікативної компетентності Multidisciplinární mezinárodní vědecký magazín “Věda a perspektivy” je registrován v České republice. Státní registrační číslo u Ministerstva kultury ČR: E 24142. № 5(60) 2026, c. 95-107 DOI:10.52058/2708-7530-2026-5(60)-95-107. https://perspectives.pp.ua/index.php/vp/issue/archive 4. Стежко С.О., Колісниченко А.В., Кондратенко Н.Ю., Павлов В.О. Методика формування академічної мовної компетентності українською та англійською мовами засобами цифрових освітніх платформ. «Вісник науки та освіти»: журнал. 2026. № 3(45) 2026. С.1354-1368 .DOI: https://doi.org/10.52058/2786-6165-2026-3(45) .https://perspectives.pp.ua/index.php/vno/issue/view/461/564 5. Стежко С.О., Зозуля Н.Ю., Кондратенко Н.Ю. Переконувальне мовлення як результат взаємодії риторики та психолінгвістики. «Наукові інновації та

							передові технології» Державне управління, економіка, право, педагогіка, психологія: журнал. 2026. № 3(55) 2026, С. 1941-1953. https://doi.org/10.52058/2786-5274-2026-4(56)-1941-1953. https://perspectives.pp.ua/index.php/nauka/issue/view/463/566 . 6. Стежко С.О., Кондратенко Н.Ю., Аташкаде Р. В., Волкотруб Г. Й., Мелешко Т.В. Активізація критичного мислення студентів засобами інтерактивної мовної взаємодії у навчальному процесі ЗВО. «Вісник науки та освіти»: журнал. 2026. № 4(46) 2026. С 2122-2135. https://doi.org/10.52058/2786-6165-2026-4(46)-2122-2135 .https://perspectives.pp.ua/index.php/vno/issue/view/475/578 . 7. Стежко С. О., Зозуля Н. Ю., Павлов В. О., Кондратенко Н. Ю., Професійний дискурс майбутнього фахівця: порівняльний аналіз мовних засобів юридичної та іт-комунікації, «Вісник науки та освіти»: журнал. 2026. № 6(48) 2026. С. 796-809. DOI:10.52058/2786-6165-2026-6(48)-796-809. https://perspectives.pp.ua/index.php/vno/issue/archive 8. Stezhko Svitlana, Kondratenko Natalia, Zabolotnia Ruslana, Zabolotnii Bohdan, TEAMBUILDING AS A TOOL FOR EFFECTIVE IT-COMPANY MANAGEMENT // Danish scientific journal Published September 26, 2024 № 88. С.15-17. https://zenodo.org/records/13884 Підпункт 3 - наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві

							(обсягом не менше 1,5 авторського аркуша на кожного співавтора: Стежко.С.О., Кондратенко Н.Ю., Заїка В.Ф. Сучасні методи викладання у вищій школі. Навчальний посібник. - Київ: ДУІКТ., 2025, 100с. https://duikt.edu.ua/ua/lib/1/category/516/view/2385
							Підпункт 12 - Наявність науково-популярних та/або консультаційних (дорадчих) та/або дискусійних публікацій з наукової або професійної тематики загальною кількістю не менше п'яти публікацій: 1. Стежко С.О, Кондратенко Н.Ю., Волкотруб Г.Й., Заболотня Р.В. Сучасний стан та перспективи розвитку штучного інтелекту у вищій школі./ Освіта як індикатор суспільного розвитку: теоретикопрактичний курс: матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, 2 жовтня – 12 листопада 2023 року. – Львів – Торунь: Liha-Pres, 2023. – С.37-41. 2. Стежко С.О., Кондратенко Н.Ю. Теоретичні аспекти формування комунікативної компетентності майбутніх юристів// «Часопис Київського університету права» №3, 2024, С.40-44 https://kup.edu.ua/vyyshov-drukom-iii-y-nomer-2024-roku-iurydychnoho-naukovo-teoretychnoho-shchokvartalnyka-chasopys-kyivskoho-universytetu-prava 3. Стежко С.О., Кондратенко Н.Ю., Волкотруб Г.Й., Заболотня Р.В. Лінгвоцид української мови як головної ознаки етносу. Збірник тез XVI Міжнародна конференція 5-6 травня 2025 р. Нові перспективи

							національної ідентичності в культурі, мові, мистецтві та літературі, С.213-219. https://duikt.edu.ua/ua/2779-konferencii-2025-roku-konferencii-ta-seminari 4. Стежко С.О., Кравченко В.І., Кондратенко Н.Ю., Ситник Л.І. Розвиток культури українського професійного мовлення у фаховій підготовці студентів. «Sciences of Europe» (Praha, Czech Republic)№179, 2025, с.76-795 https://duikt.edu.ua/ua/1712-naukova-robota-kafedra-ukrainskoi-movi 5. Стежко С.О., Кондратенко Н.Ю. Мовна етика електронного спілкування в умовах захисту персональних даних III Міжнародна науково-практична конференція «Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії», 4–6 грудня 2025 року, https://duikt.edu.ua/ua/2779-konferencii-2025-roku-konferencii-ta-seminari 6. Стежко С.О., Кондратенко Н.Ю. Мовна освіта в системі підготовки майбутніх педагогів: інтеграційний підхід. Матеріали конференції «Сучасні досягнення компанії Hewlett Packard Enterprise в галузі іт та нові можливості їх вивчення і застосування», 11 грудня 2025 року, https://duikt.edu.ua/ua/2779-konferencii-2025-roku-konferencii-ta-seminari 7. Стежко С.О., Кондратенко Н.Ю., Заболотня Р.В., Використання цифрових технологій у формуванні професійного мовлення студентів, «Проблеми ефективності професійної мовної комунікації в умовах інформаційної агресії»: матеріали II Всеукраїнської науково-практичної конференції з

							міжнародною участю (м. Київ, 28 листопада 2025 року) Київ: Київського інституту Національної гвардії України, 2025 С.240-243 https://kingu.edu.ua/naukovi-zahodi/ Підпункт 14. 8.14). Керівництво студентом, який зайняв призове місце на І або ІІ етапі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт), або робота у складі організаційного комітету / журі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт), або керівництво постійно діючим студентським науковим гуртком / проблемною групою; керівництво студентом, який став призером або лауреатом Міжнародних, Всеукраїнських мистецьких конкурсів, фестивалів та проектів, робота у складі організаційного комітету або у складі журі міжнародних, всеукраїнських мистецьких конкурсів, інших культурно-мистецьких проектів (для забезпечення провадження освітньої діяльності на третьому (освітньо-творчому) рівні); керівництво здобувачем, який став призером або лауреатом міжнародних мистецьких конкурсів, фестивалів, віднесених до Європейської або Всесвітньої (Світової) асоціації мистецьких конкурсів, фестивалів, робота у складі організаційного комітету або у складі журі зазначених мистецьких конкурсів, фестивалів); керівництво студентом, який брав участь в Олімпійських, Паралімпійських іграх, Всесвітній та Всеукраїнській Універсіаді,

							чемпіонаті світу, Європи, Європейських іграх, етапах Кубка світу та Європи, чемпіонаті України; виконання обов'язків тренера, помічника тренера національної збірної команди України з видів спорту; виконання обов'язків головного секретаря, головного судді, судді міжнародних та всеукраїнських змагань; керівництво спортивною делегацією; робота у складі організаційного комітету, суддівського корпусу 1. Керівництво постійно діючим студентським науковим гуртком «25 кроків до мовної впевненості» з 2022 р. по теперешній час. Підпункт 19 Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях; 1. Член громадської організації «Міжнародна асоціація сучасної освіти, науки та культури» (код ЄДРПОУ 44094570) №СЧ-360.12.23
455594	Туровський Олександр Леонідович	Завідувач кафедри, Основне місце роботи	Навчально-науковий інститут Кібербезпеки та захисту інформації	Диплом спеціаліста, Військово-повітряна інженерна ордена Леніна та Жовтневої революції Червонопрапорна академія імені професор М. Є. Жуковського, рік закінчення: 1992, спеціальність: Обладнання літальних апаратів, Диплом магістра, Національна академія оборони України, рік закінчення: 2008, спеціальність: Організація бойового та оперативного	17	Науково-технічний переклад	Спеціального матеріально-технічного забезпечення не потребує. Мультимедійна система - 1 к-т.

				забезпечення військ (за видами та родами військ і сил), Диплом доктора наук ДД 011829, виданий 29.06.2021, Диплом кандидата наук ДК 021196, виданий 10.12.2003, Атестат доцента 12ДЦ 017169, виданий 21.06.2007, Атестат професора АП 004855, виданий 20.02.2023			
436190	Поночовний Петро Михайлович	Старший викладач, Основне місце роботи	Навчально-науковий інститут Кібербезпеки та захисту інформації	Диплом молодшого спеціаліста, Київський професійно-педагогічний коледж імені Антона Макаренка, рік закінчення: 2012, спеціальність: Професійна освіта (Будівництво), Диплом бакалавра, Національний педагогічний університет імені М.П. Драгоманова, рік закінчення: 2014, спеціальність: Технологічна освіта, Диплом магістра, Національний педагогічний університет імені М.П. Драгоманова, рік закінчення: 2016, спеціальність: 8.01010301 технологічна освіта, Диплом доктора філософії Н25 002938, виданий 10.09.2025	3	Стандарти кібербезпеки та захисту інформації	Доктор філософії (PhD) спеціальність 125-Кібербезпека, галузь знань 12-Інформаційні технології. Тема дисертації: «Система протидії упередження низькошвидкісних HTTP DDOS-атак на веб-ресурси». Диплом ДФ № 021116 від 28.08.2025 року. Підвищення кваліфікації: 1. Національна академія педагогічних наук України ДЗВО «Університет менеджменту освіти» Центральний інститут післядипломної освіти. За освітньо-професійною програмою «Методисти закладів професійної (професійно-технічної) освіти» (5 кредитів ECTS) – 2022 рік. СП 35830447/1709-22 2. Сумський державний університет свідоцтво про підвищення кваліфікації «STEM освіта online: 3D моделювання та 3D друк» 30 годин (1 кредит ECTS) - 2023 рік.; 3. Підвищення кваліфікації в Товаристві з обмеженою відповідальності «Дефендіко» за темою «Захист державних інформаційних ресурсів» з 11 листопада по 17 січня 2025 (90 ак. годин – 3 кредити ECTS); 4. Підвищення кваліфікації в Товаристві з

							обмеженою відповідальністю «Луч» за темою: «Організація захисту інформації під час введення в експлуатацію інфо-комунікаційних систем» з 20 січня по 07 березня 2025 (90 ак. годин – 3 кредити ECTS) Види і результати професійної діяльності за спеціальністю відповідно до п.38 Ліцензійних умов провадження освітньої діяльності: (пп. 1, 4, 5, 9, 12). 1. наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection; 1. Abraheem, A. S. A., Ahmed, D. K. I., & Ponochovnyi, P. (2025). AI and machine learning in environmental monitoring: Enhancing legal compliance and public trust. Environment and Social Psychology, 10(11). https://doi.org/10.18063/esp.v10i11.3977541082. Рижаков М., Поночоаний П. Модель трансформації на основі штучного інтелекту з елементами захисту від DDoS-атак // Прикладні проблеми комп'ютерних наук, безпеки та математики – 2025. № 4. С. 14-32. покликання на матеріал: https://apcssm.vnu.edu.ua/index.php/Journalone/article/view/1283. ПОНОЧОВНИЙ П., ПЕПА Ю. РЕАЛІЗАЦІЯ СИСТЕМИ ЗАХИСТУ СЕРВЕРІВ З УРАХУВАННЯМ АНОМАЛІЙ В ПАКЕТАХ. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES. 2025. № 1. С. 44–51. URL: https://doi.org/10.31891/2219-9365-2025-81-6

4. Поночовний П. М., Іванченко І. С. Метод раннього виявлення та захисту від мінливих DDoS атак на основі аналізу обробки пакетних груп // Наукові записки ДУІКТ – 2024. No2. – С.153-164 покликання на матеріал: https://journals.dut.edu.ua/index.php/sciencenotes/article/view/3100

5. Поночовний П. М. Модель упередження низькошвидкісних HTTP DDoS атак на кінцевого користувача // Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». Київ: Київський столичний університет імені Бориса Грінченка, 2024. Том 2 № 26. – С.291-304 покликання на матеріал: https://csecurity.kubg.edu.ua/index.php/journal/article/view/695
6. Савченко В.А., Поночовний П.М., Аверічев І.М. Виявлення DDOS-атаки на високошвидкісну мережу: опитування. // Прикладні проблеми комп`ютерних наук, безпеки та математики. Луцьк: Волинський національний університет імені Лесі Українки, №3 2024.. – С. 71-76, покликання на матеріал: https://apcssm.vnu.edu.ua/index.php/Journalone/article/view/127
7. Прокопенко А.Г., Лаврінець К.Г., Поночовний П.М., Оцінка якості системи моніторингу технічного стану телекомунікаційних мереж спеціального призначення // Зв'язок № 4 (69) 2024. – С. 19-23, покликання на матеріал: https://con.dut.edu.ua/index.php/communication/article/view/2787
8. Опанасенко М. І., Поночовний П. М., Технологія забезпечення кібербезпеки хмарного середовища на базі рішення Cisco Cloudlock // Сучасний захист інформації № 1 (78) 2023. – С. 72-78,

							покликання на матеріал: http://journals.dut.edu.ua/index.php/dataprotect/article/view/2746 9. Лук'яненко Т. Ю., Поночовний П. М., Легомінова С. В., Методика виявлення мережевих вторгнень і ознак комп'ютерних атак на основі емпіричного підходу // Сучасний захист інформації № 2 (65) 2022. – С. 15-21 покликання на матеріал: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2634 4. наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування; 1. Пепа Ю.В., Аверічев І.М., Поночовний П.М. Методичні рекомендації для проведення практичних занять з дисципліни Теорія кіл в інформаційному та кібер просторах. – К.: ДУІКТ, 2024. – 48 с. 2. Пепа Ю.В., Аверічев І.М., Поночовний П.М. Методичні рекомендації щодо виконання курсової роботи. – К.: ДУІКТ, 2024. – 25 с. 3. Пепа Ю.В., Аверічев І.М., Поночовний П.М. Теорія кіл в інформаційному та кібер просторах. Лабораторний практикум. – К.: ДУІКТ, 2024. – 38 с. 5. захист дисертації на здобуття наукового ступеня; 2025 рік, тема дисертаційної роботи: «Система протидії упередження низькошвидкісних HTTP DDoS-атак на веб ресурси»

							9. робота у складі експертної ради з питань проведення експертизи дисертацій МОН або у складі галузевої експертної ради як експерта Національного агентства із забезпечення якості вищої освіти, або у складі Акредитаційної комісії, або міжгалузевої експертної ради з вищої освіти Акредитаційної комісії, або трьох експертних комісій МОН/зазначеного Агентства, або Науково-методичної ради/науково-методичних комісій (підкомісій) з вищої або фахової передвищої освіти МОН, наукових/науково-методичних/експертних рад органів державної влади та органів місцевого самоврядування, або у складі комісій Державної служби якості освіти із здійснення планових (позапланових) заходів державного нагляду (контролю); Експерт у сфері професійної діяльності - освіта (інформаційні системи, кібернетика та інформатика), від 09.05.2024 № 13 протокол засідання НАК № 18 (158) 12. наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п’яти публікацій; 1. Шкурченко О.А., Аверічев І.М., Поночовний П.М. (2026) Метод детектування мультивекторних apt-атак із використанням ансамблів алгоритмів машинного навчання. «ПЕРСПЕКТИВНІ НАПРЯМИ ЗАХИСТУ ІНФОРМАЦІЇ» (Advanced Trends in Information Security) VIII Міжнар. наук.-пр. конф. (м. Одеса, 26–28 серпня 2026 р.).

							Одеса-Київ: ДУІТЗ-ДУІКТ, 2026 С. 67 Режим доступу: https://drive.google.com/drive/folders/16VZDrtNNNMsgDk7ANr49yT7jwkXf1mqgDsaHG6_JF2QMjNMODezgFqKQhkJR8Pt6vXVLeodx 2. Поночовний, П. М., & Аверічев, І. М. (2026). Візуальне моделювання кібератак за допомогою Adobe Illustrator як інструмент підвищення ефективності кіберзахисту критичної інфраструктури. В Improvement of all branches of science: digitalization, challenges, interdisciplinary integration: Abstracts of XXIII International Scientific and Practical Conference (Sofia, Bulgaria, June 08–10, 2026) (с. 60–63). European Conference. https://drive.google.com/file/d/12IciXPsUQA49k3R3QT7Bkrh6qSKYyxOs/view?usp=sharing 3. Аверічев І., Поночовний П. Упередження повільних DDoS-атак на хмарні сервіси. ITSec: Безпека інформаційних технологій: матеріали XV Міжнар. наук.-техн. конф. (м. Тернопіль, 27–29 трав. 2026 р.). Тернопіль–Київ: ТНТУ-ДУІКТ, 2026. С. 108 - 111. Режим доступу: https://drive.google.com/drive/folders/1f_WDoOIyqDmVMa5eJZDJ-ABFERbSdEWG 4. Yuriy PEPA, Petro PONOCHOVNYI, Oleksandr LEVKUSHA METHOD FOR DETERMINING VULNERABILITIES TO DDOS ATTACKS ON CONTENT MANAGEMENT SYSTEMS // The IV International Conference on Emerging Technology Trends on the Smart Industry and the Internet of Things “TTSIIT - 2025”, KYIV NATIONAL UNIVERSITY OF CONSTRUCTION AND ARCHITECTURE -30-31 січня 2025, Ukraine-Iraq-Poland С.

							– 95-100. Режим доступу: https://drive.google.com/file/d/145aOtud0A7zl4N9RKXiFyt9iMLKYsMt_/view 5. Поночовний П. М., Іванченко І. С. Експериментальне дослідження системи реалізації захисту серверів з урахуванням аномалій в пакетах // II міжнародна науково-практична конференція «Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії», 2024, м. Київ – С. 173 – 177 покликання на матеріал: https://duikt.edu.ua/uploads/p_2661_99635945.pdf 6. Є.О. Куліш, П.М. Поночовний, Ю.В. Пепа ОЦІНКА ЕФЕКТИВНОСТІ СИСТЕМ РАННЬОГО ВИЯВЛЕННЯ DDOS-АТАК // Всеукраїнська науково-практична конференція «Актуальні проблеми безпеки інформаційно-телекомунікаційних систем», 2024, м. Київ – с.17 – 20 покликання на матеріал: https://duikt.edu.ua/uploads/p_2661_93669247.pdf 7. Поночовний П. М."Кіберзагрози в епоху цифровізації: моделювання та захист від DDoS-атак" // Всеукраїнська науково-практична конференція «Актуальні проблеми безпеки інформаційно-телекомунікаційних систем», 2024, м. Київ – с.85 – 86 покликання на матеріал: https://duikt.edu.ua/uploads/p_2661_93669247.pdf 8. Поночовний П. М., Пепа Ю. В., "Принципи захисту освітнього сервера від мінливих DDoS-атак" // IV Всеукраїнська науково-практична конференція пам’яті академіка Академії наук вищої освіти, професора Анатолія Володимировича

							Касперського «Актуальні проблеми та перспективи розвитку фундаментальних, прикладних, загальнотехнічних та безпекових наук», 2024, м. Київ – с.159 – 162, покликання на матеріал: https://drive.google.com/file/d/1zYSEg2O2x88H3_NHh27EFyTwjRg7mGt6/view 9. Пепа Ю. В., Поночовний П. М., Інтегральне оцінювання стійкості систем управління // Науково-практична конференція «перспективи та проблематика Інтелектуальних систем», 2024, м. Київ – с.3-4, покликання на матеріал: https://duikt.edu.ua/uploads/p_2661_35995256.pdf 10. Петро Поночовний (Ponochovnyy P. M.), Ігор Аверічев (Avierichev I.M.), Критерії виявлення повільних DDoS-атак // XIII Міжнародна науково-технічна ITSec-2024 Безпека інформаційних технологій, 2024, м. Львів – с.175-176, покликання на матеріал: https://drive.google.com/file/d/1N1orbCGW37_pIRTzbHWuEgO3M8lw9B6r/view?usp=drive_link 11. Пепа Ю. В., Поночовний П. М., Вплив сторонніх факторів на обробку сигналів // XIII міжнародна науково-практична конференція «Математика. Інформаційні технології. Освіта, 2024, м. Луцьк – с.157-159, покликання на матеріал: https://drive.google.com/file/d/16GSq2WkNNsnEs6KRBkfCGdcYCKwi1bwO/view 12. П. Поночовний Використання штучного інтелекту в освіті // IV Всеукраїнська науково-практична конференція «Модернізація змісту професійної освіти в умовах євроінтеграції України – 2024», 2024, м. Київ – С.437-439 покликання на

							матеріал: https://drive.google.com/file/d/18Jhvyz_tMhtotu7wjcuRpeXN86R3ony4/view 13. П. Поночовний. Впровадження систем штучного інтелекту у сфери безпеки і оборони, науки і освіти, економіки, медицини // С34 Системи та засоби штучного інтелекту: тези доповідей Міжнародної наукової молодіжної школи. – Київ: ІПШІ «Наука і освіта», 2023. – С. 30-33, покликання на матеріал: https://www.ipai.net.ua/docs/AIIS-2023-school.pdf
473520	Рижаков Микола Миколайович	Старший викладач, Основне місце роботи	Навчально-науковий інститут Кібербезпеки та захисту інформації	Диплом молодшого спеціаліста, Коледж морського і річкового флоту Київської державної академії водного транспорту імені гетьмана Петра Конашевича-Сагайдачного, рік закінчення: 2015, спеціальність: 5.05010301 розробка програмного забезпечення, Диплом бакалавра, Київська державна академія водного транспорту імені гетьмана Петра Конашевича-Сагайдачного, рік закінчення: 2017, спеціальність: 6.050103 програмна інженерія, Диплом магістра, Державний університет телекомунікацій, рік закінчення: 2019, спеціальність: 172 Телекомунікації та радіотехніка, Диплом доктора філософії Н26	7	Ліцензування, атестація та сертифікація у сфері безпеки об'єктів інформаційної діяльності	Доктор філософії (PhD) спеціальність 125-Кібербезпека, галузь знань 12-Інформаційні технології Тема дисертації: «Методи та моделі виявлення аномалій мережевого трафіку на об’єктах критичних інформаційних інфраструктур». Диплом ДФ № 021116 від 21.02.2026 року. Підвищення кваліфікації: 1.☐ ☐ТОВ «ЛУЧ», Сертифікат № 000135-2025/S9, Програма стажування: «Організація захисту інформації під час введення в експлуатацію ІКС», 20.01.2025 р., 90 годин (3 кредити ECTS); 2.☐ ☐ТОВ «ДЕФЕНДІКО» , Сертифікат № 000112-2025/S1, «Захист державних інформаційних ресурсів», 07.03.2025 р., 90 годин (3 кредити ECTS). 3. «PROMETHEUS» Сертифікат «Академічна дорочесність», 15.03.2026, 60 годин (2 кредити ECTS). Виконання умов пункту 38 Ліцензійних вимог (пп. 1,5,12) 5.захист дисертації на здобуття наукового ступеня; Доктор філософії (Диплом № Н26 000391 від

				000391, виданий 10.03.2026			10.03.2026р.) Спеціальність 125 – Кібербезпека та захист інформації Тема докторської дисертації: «Методи та моделі виявлення аномалій мережевого трафіку на об’єктах критичних інформаційних інфраструктур», 2026р. 12.наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п’яти публікацій; 1. M. Ryzhakov, D. Solskyi, “Інтелектуальна модель самопідтримки мережевих функцій у середовищі SDN/NFV з елементами захисту від DDoS-атак”, ITSec: Безпека інформаційних технологій: матеріали XIV Міжнародної науково-технічної конференції, Ternopil, Ukraine, May 22–24, 2025, P. 238–239. 2. Ye. Ivanchenko, M. Ryzhakov, Ye. Kykhtenko, A. Rozhenko, “Використання автоенкодерів для виявлення кібербезпекових аномалій в інформаційно-телекомунікаційних мережах”, ITSec: Безпека інформаційних технологій: матеріали XV Міжнародної науково-технічної конференції, Ternopil, Ukraine, May 27–29, 2026, P. 243–247. 3. R. Khvorostianyi, M. Ryzhakov, “Prospective Structure of a Multi-Agent Cyber Defense Management System for the Transport Information and Communication Network”, International Scientific and Practical Conference “Digital Transformation: Strengthening the Cybersecurity Capacities in the Modern World”, Krakow, Poland, November 4–5, 2025. 4. M. Ryzhakov,

							“Розвиток новітніх методів і технологій для забезпечення кібербезпеки та захисту критичної інформаційної інфраструктури України в умовах сучасних глобальних загроз та військового конфлікту”, Актуальні питання забезпечення кібербезпеки та захисту інформації: матеріали XI Міжнародної науково-практичної конференції, Kyiv, Ukraine, April 24, 2025. 1.наявність не менше п’яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection; 1. Шикула О. М., Рижаков М. М., Білоусова С. В., Литвинець В. В. Розробка сайту автосервісу з можливістю виклику евакуатора за даними геопозиціювання. Наукові записки Державного університету інформаційно-комунікаційних технологій. № 1–2, с. 54–62, 2022. DOI:10.31673/2518767 8.2022.025462. 2. Рижаков М., Поночовний П. Модель трансформації на основі ШІ з елементами захисту від DDoS-атак. Прикладні проблеми комп’ютерних наук, безпеки та математики, 4, с. 14–32, 2025. 3. Іванченко Є., Аверічев І., Рижаков М. Узагальнена модель прогнозування та виявлення кібербезпекових аномалій на основі ШІ. Кібербезпека: освіта, наука, техніка, 4(28), 529–546, 2025. https://doi.org/10.2892 5/2663-4023.2025.28.823 4. Шульга В., Іванченко Є., Аверічев І., Рижаков М. Методи інтелектуального виявлення аномалій і

							критичних ситуацій у кіберсистемах на основі глибокого навчання. Information Technology: Computer Science, Software Engineering and Cyber Security, № 2, с. 204–215, 2025. DOI:10.32782/IT/2025-2-21. 5. Туровський О., Рижаков М. Методичний підхід до комплексної ідентифікації та аналізу кіберзагроз трафіку в мережах 5G/IMT-2020 на основі технологій ШІ. Вимірювальна та обчислювальна техніка в технологічних процесах, (1), 267–277, 2025. https://doi.org/10.31891/2219-9365-2025-81-33 6. Шульга В., Іванченко І., Рижаков М. Узагальнена модель інтелектуальної системи прогнозування та виявлення аномалій у кіберінфраструктурі на основі глибокого навчання. Measuring and Computing Device, (3), 217–225, 2025. https://doi.org/10.31891/2219-9365-2025-83-28 7. Шульга В.П., Іванченко І.С., Рижаков М.М.. Математична модель семантичної атрибуції кіберінцидентів у системах виявлення аномалій на основі глибокого навчання, Сучасний захист інформації, 2025, No 3(63), ст. 186 – 198, https://doi.org/10.31673/2409-7292.2025.032076. 8. Туровський О.Л.,, Іванченко Є.В., Рижаков М.М. Методика побудови системи безпеки об'єкта інформаційної діяльності для роботи з інформацією з обмеженим доступом. Measuring and computing devices in technological processes, (3), 2026, Подано на публікацію. 9. Рижаков М. М., Котенко А. М., Іванченко І. С., Пепа Ю. В., Щербак Т. Л. Методика формування профілю безпеки та авторизації

							систем, у яких обробляється інформація з обмеженим доступом. : ДУІКТ: Сучасний захист інформації 2026 №, Подано на публікацію. 10. Ivanchenko Y., Karpinski M., Ryzhakov M., Ivanchenko I., Mazurek P., Sawicki P. An Agent-Based Model of a Controlled Detonation System for Sandbox Analysis of Suspicious Software. Electronics, 15(11), 2348, 2026. https://doi.org/10.3390/electronics15112348
269011	Котенко Андрій Миколайович	Доцент, Основне місце роботи	Навчально-науковий інститут Кібербезпеки та захисту інформації	Диплом молодшого спеціаліста, Керченский судомеханический техникум, рік закінчення: 1988, спеціальність: , Диплом спеціаліста, Київське вище ін-женерне радіо-технічне училище протиповітряної оборони ім. О.І. Покришкіна, рік закінчення: 1993, спеціальність: радіотехнічні засоби, кваліфікація - радіоінженер, Диплом кандидата наук ДК 049262, виданий 12.11.2008, Атестат доцента АД 003527, виданий 16.12.2019	23	Теорія захисту інформаційних ресурсів обмеженого доступу	Кандидат технічних наук зі спеціальності 05.13.06 – інформаційні технології. Тема дисертації: «Методика обґрунтування характеристик неортогональних широкосмугових сигналів у телекомунікаційній мережі системи дистанційного спостереження та охорони воєнних об'єктів». Диплом ДК №049262 від 12.11.2008 року. Вчене звання: доцент кафедри Систем інформаційного та кібернетичного захисту АД № 003527 від 16.12.2019 року. Підвищення кваліфікації: 1. ТОВ «ЛУЧ», Сертифікат № 000136-2025/S9, Програма стажування: «Організація захисту інформації під час введення в експлуатацію ІКС», 20.01.2025 р., 90 годин (3 кредити ECTS); 2. ТОВ «ДЕФЕНДІКО», Сертифікат № 000113-2025/S4, «Захист державних інформаційних ресурсів», 07.03.2025 р., 90 годин (3 кредити ECTS). Види і результати професійної діяльності за спеціальністю відповідно до п.38 Ліцензійних умов провадження освітньої діяльності: (п. 1, 3,5, 8, 11, 14, 19)

							1.наявність не менше п’яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, WebofScienceCoreCollection; 1. Laptiev O., Savchenko V., Kotenko A., et. al. Method of Determining Trust and Protection of Personal Data in Social Networks. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 13, No. 1, pp.15-21. 2021 april, 2021.https://doi.org/10.17762/ijcnis.v13i1.4882 2. TalalTaha R., MuhanadM.Salih M., Raheem Mohammed Al-Ani A., Mahmood Jawad H., Waleed Abdulah N., Kotenko A., Mahmoud Al-Jawher W. Method Integrating IMS with Blockchain: A New Frontier in Secure Communication Networks.ISSN 2305-7254, PROCEEDING OF THE 36TH CONFERENCE OF FRUCT ASSOCIATION, 2024. pp.778-786. https://fruct.org/publications/volume-36/fruct36/files/Tal.pdf 3.ІгорКозубцов, НаталіяЗінченко, Андрій Котенко, ІгорАверічев.Проблемизабезпеченняінформаційноїбезпекисуб'єктамиосвітньоїдіяльності в цифровому освітньо-науковомусередовищізакладівосвіти.SMART TECHNOLOGIES. Київ. КНУБА, 2024, № 2(15), с. 56 – 65. https://doi.org/10.32347/uwt.2024.15 4. Чабан Б. В., Котенко А. М. Модель системи захисту інформації від витоку матеріально-речовим каналом на базі ланцюгів Маркова / ДУІКТ: Сучасний захист інформації 2024 № 4(60) с. 46-53. https://journals.dut.edu.ua/index.php/dataprotect/article/view/3058/2948 3.наявність виданого підручника чи навчального

							посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора); А.М. Котенко, О.Л. Туровський, Г.В.Шуклін, Ю.В. Пепа, І.С. Іванченко, І.М. Аверічев. Компонентна база засобів кібербезпеки та захисту інформації Навчальний посібник. - К.: ДУІКТ. – 236 с. https://duikt.edu.ua/ua/lib/1/category/2351/view/2376 (9,6 авт. арк) 4.наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування; Котенко А.М., Хлапонін Ю.І. Конспект лекцій “Цифрова обробка сигналів“ для студентів спеціальності 123 “Комп’ютерна інженерія“ з дисципліни “Цифрова обробка сигналів“. - К.: КНУБА, 2023. – 99 с. (6 друк. аркуш) https://repositary.knuba.edu.ua/handle/123456789/13418 Котенко А.М., Хлапонін Ю.І. Методичні вказівки до виконання лабораторних робіт для студентів з галузі знань 12 “Інформаційні технології“ за спеціальністю 123 “Комп’ютерна інженерія“ з дисципліни “Цифрова обробка зображень“. - К.: КНУБА, 2022. – 36 с. (1 друк. аркуш)

							https://repositary.knuba.edu.ua/items/63eef550-cd51-4248-9210-45bf47165e09 Котенко А.М. Конспект лекцій для студентів зі спеціальності 125 «Кібербезпека та захист інформації» з дисципліни «Системи контролю та управління доступом на об'єкти інформаційної діяльності». –К, ДУІКТ, 2024. – 79 с. https://duikt.edu.ua/ua/lib/1/category/1014/view/1372 Конспект лекцій для студентів з галузі знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека та захист інформації» з дисципліни «Програмно-апаратні засоби захисту»/ Уклад. А.М. Котенко, Ю.І. Хлапонін, В.М. Трофимчук – К.:КНУБА, 2025. – 154 с. – у процесі викладки на сайт 9.робота у складі експертної ради з питань проведення експертизи дисертацій МОН або у складі галузевої експертної ради як експерта Національного агентства із забезпечення якості вищої освіти, або у складі Акредитаційної комісії, або міжгалузевої експертної ради з вищої освіти Акредитаційної комісії, або трьох експертних комісій МОН/зазначеного Агентства, або Науково-методичної ради/науково-методичних комісій (підкомісій) з вищої або фахової передвищої освіти МОН, наукових/науково-методичних/експертних рад органів державної влади та органів місцевого самоврядування, або у складі комісій Державної служби якості освіти із здійснення планових (позапланових) заходів державного нагляду (контролю);

							Член редакційної колегії/експерт видання:Proceedingsof FRUCT'35Tampere, Finland, 24-26 April 2024 FRUCTOy, Finland, ISSN 2305-7254, ISBN 978-952-65246-1-0 https://www.fruct.org/conferences/FRUCT36_Program.pdf 12.наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п'яти публікацій; Котенко А.М., Гребенніков А.Б.Підвищення ефективності захисту кібернетичної безпеки об'єкту інформаційної діяльності. Теза доповіді XII Всеукраїнська науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави» - Київ: - Національна академія Служби Безпеки України, Науково-дослідний інститут інформатики і права Національної академії правових наук України. 26 березня 2021 року. С. 190 – 192. https://nasbu.edu.ua/uploads/p_57_53218641.pdf Котенко А.М., Каліш В,В. Порівняння криптографічних алгоритми хешуваннясha-3 та sha-256// Всеукраїнська конференція «Актуальні проблеми безпеки інформаційно-телекомунікаційних систем», 5 листопада 2024 р. Державний університет інформаційно-комунікаційних технологій - Київ: 2024 р. С.. 12-13 https://duikt.edu.ua/uploads/p_2661_93669247.pdf А.М. Котенко, Б.В. Чабан Математична модель матеріально-

							речового каналу витоку інформації// Всеукраїнська конференція «Актуальні проблеми безпеки інформаційно-телекомунікаційних систем», 5 листопада 2024 р. Державний університет інформаційно-комунікаційних технологій - Київ: 2024р. С. 72-73https://duikt.edu.ua/uploads/p_2661_93669247.pdf А.М. Котенко, Д.В. Трухан Методи та моделі оцінки захищеності систем захисту інформації в корпоративній мережі з урахуванням ступеня перекриття загроз. // Всеукраїнська конференція «Актуальні проблеми безпеки інформаційно-телекомунікаційних систем», 5 листопада 2024 р. Державний університет інформаційно-комунікаційних технологій - Київ: 2024р. С. 120https://duikt.edu.ua/uploads/p_2661_93669247.pdf А.М. Котенко, Д.В. Бойко Актуальні проблеми безпеки інформаційно-телекомунікаційних систем та методи захисту WI-FI мереж Всеукраїнська конференція «Актуальні проблеми безпеки інформаційно-телекомунікаційних систем», 5 листопада 2024 р. Державний університет інформаційно-комунікаційних технологій - Київ: 2024р. С. 6-8 https://duikt.edu.ua/uploads/p_2661_93669247.pdf А.М. Котенко Вплив чинника акустичної інформації на економічну безпеку підприємсваВсеукраїнської науково-практичної конференції 27 лютого 2025 року«Стратегії кіберстійкості: управління ризиками та безперервність бізнесу»27 лютого 2025. Державний університет

							інформаційно-комунікаційних технологій - Київ: 2025р. С. 62-66. https://duikt.edu.ua/uploads/p_2779_46212583.pdf 19.діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях; Учасник громадського об'єднання (для науково-педагогічнихпрацівників) "Університет лідерства та інновацій". https://drive.google.com/file/d/1PL5_rqbe73hQQ3HX5ICgefcTr1mNK1HV/view?usp=sharing
487740	Колісниченко Анна Віталіївна	Завідувач кафедри, Основне місце роботи	Навчально-науковий інститут Інформаційних технологій	Диплом спеціаліста, Ніжинський державний університет імені Миколи Гоголя, рік закінчення: 2006, спеціальність: 010103 Педагогіка і методика середньої освіти. Українська мова і література та мова і література (англійська), Диплом кандидата наук ДК 044200, виданий 11.10.2017, Атестат доцента АД 015082, виданий 24.04.2024	18	Англійська мова для ділової комунікації	Ніжинський державний університет імені Миколи Гоголя, 2006 р., спеціальність «Педагогіка і методика середньої освіти. Українська мова і література та мова і література (англійська)», кваліфікація – «Учитель української мови і літератури та мови (англійської) і зарубіжної літератури» (ЕН 30323893, 2006 рік) Підвищення кваліфікації: 1. У грудні 2023-січні 2024 років пройшла закордонне стажування на тему «Similarities and differences in teaching philological disciplines in Ukraine and Latvia» («Схожість і відмінність у викладанні філологічних дисциплін в Україні та в Латвійській Республіці» зі спеціальності «Філологія» (обсяг професійної підготовки – 180 години / 6 кредитів ECTS) у Вищій школі менеджменту інформаційних систем (ISMA) у м. Рига (Латвійська Республіка) та отримала сертифікат № FSI-041405-ISMA від 14. 01. 24 р. 2. Із 03.07.2023 по 13.08.2023 р. пройшла всеукраїнське

							науково-педагогічне підвищення кваліфікації на тему «Формування резильєнтних компетенцій здобувача освіти в період трансформацій, сучасних викликів та кризових станів суспільства» (обсяг професійної підготовки – 180 години / 6 кредитів ECTS) у Навчально-реабілітаційному закладі вищої освіти «Кам'янець-Подільський державний інститут» і Центрі українсько-європейського наукового співробітництва й школі менеджменту інформаційних систем у м. Кам'янець-Подільський та отримала сертифікат №ADV-030735-KPSI від 13. 08. 2023. Із 01.07.2024 по 11.08.2024 р. 1. Пройшла всеукраїнське науково-педагогічне підвищення кваліфікації на тему «Дизайн-мислення в освітній діяльності» (обсяг професійної підготовки – 180 години / 6 кредитів ECTS) у Полтавському державному аграрному університеті та Центрі українсько-європейського наукового співробітництва й школі менеджменту інформаційних систем у м. Полтава та отримала сертифікат №ADV-010706-PSAU від 11. 08. 2024. Із 10.03.2025 по 10.05.2025 пройшла курси підвищення кваліфікації ENAI «Educational Materials on Academic Integrity»; з програми «Дослідницька доброчесність» (обсяг професійної підготовки – 90 годин / 3 кредити) від комітету з питань етики Національного агентства із забезпечення якості вищої освіти. 1) публікації у наукових виданнях, включених до переліку наукових фахових видань України:

							1.Anna Kolisnychenko, Svitlana Kharytska. Indian myths as the basis of Hart Crane's mythmaking. Alfred Nobel University Journal of Philology. – Vol. 2 (26/1) – Dnipro, 2023. – P. 89-104. (Scopus) https://doi.org/10.32342/2523-4463-2023-2-26/1-7 2. Харицька, С. В., Колісниченко, А. В. (2025). Інтеграція професійної англійської мови в підготовку ІТ-фахівців. Наукові записки. Серія «Психолого-педагогічні науки» (Ніжинський державний університет імені Миколи Гоголя), (4), 218–225. https://doi.org/10.31654/2663-4902-2025-PP-4-218-225 3. Колісниченко А. В., Харицька С. В. Художня ретрансляція етноментальних констант та сучасної соціально-історичної конкретики в імагінативному просторі ліричної творчості Анни Малігон. Рідне слово в етнокультурному вимірі». № 10. Дрогобич, 2025. С. 45-51 4. Харицька С.В., Колісниченко А.В., Конопляник Л.М. Національна складова стандартизації перекладних словників у процесі формування національної термінології і галузевих наукових тезаурусів. Науковий вісник Вінницької академії безперервної освіти. Серія «Педагогіка. Психологія». Вип. 7. Вінниця, 2025. С. 246-253. 5. Харицька С. В., Колісниченко А. В. Search-informational competence of future biomedical engineers and economists as an important component of adjustment of safety professional activity standards. Перспективи та інновації науки. Серія «Педагогіка». Серія «Психологія». Серія «Медицина». №

							15(33). Київ, 2023. С. 38-54. https://doi.org/10.52058/2786-4952-2023-15(33)-38-54 6. Харицька С. В., Колісниченко А. В. Інтенсифікація концепції інклюзії в сучасних соціально-педагогічних доктринах та літературних студіях дизабіліті. Актуальні питання гуманітарних наук. – Випуск 47. Том 1– Дрогобич, 2022. – С. 207-213. https://doi.org/10.24919/2308-4863/47-1-31 7. Харицька С. В., Колісниченко А. В. Проблема адаптації форм виховних заходів до сучасних вимог дистанційного навчання. Перспективи та інновації науки. Серія: Педагогіка. Психологія. Медицина. – Випуск №8 (13), 2022. – С. 306-315. https://doi.org/10.52058/2786-4952-2022-8(13)-306-315 8. Колісниченко. А. В. Конфлікт культур крізь призму індійської національної свідомості у оповіданні Порошурама «Сватання». Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Філологія. Журналістика. – Том 32 (71). – №2, 2021. – С. 178-182. https://doi.org/10.32838/2710-4656/2021.2-2/31 9. Харицька С. В, Колісниченко А. В. Інтеграція професійної англійської мови в підготовку ІТ фахівців. Психолого-педагогічні науки. № 4. Ніжин, 2025. С. 218-225. Стежко С. О., Колісниченко А. В., Кондратенко Н. Ю., Павлов В. О. Методика формування академічної мовної компетентності українською та англійською мовами

							засобами цифрових освітніх платформ. Вісник науки та освіти: журнал. 2026. № 3(45) 2026. С. 1354-1368. 3) наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора); 1. Professional English. Information Technology: навч. посібник / О.В. Ковтун, Л. М. Конопляник, Ю. Ю. Пришупа, А. В. Колісниченко, С. В. Харицька. – Київ: ДУ «КАІ», 2025. 160 с. (20%). 2. Харицька С. В., Колісниченко А. В. The metaspace of the functioning of the concept of academic integrity as a factor in the formation of the identity of moral and ethical patterns. MODERNÍ ASPEKTY VĚDY. Svazek XL mezinárodní kolektivní monografie (Modern aspects of science. 40-th volume of the international collective monograph). Česká republika, 2024. – С. 166-180. 3. Харицька С. В., Колісниченко А. В. Патріотичне татуювання як виразник національної самоідентифікації. MODERNÍ ASPEKTY VĚDY. Svazek XXI mezinárodní kolektivní monografie (Modern aspects of science. 21-th volume of the international collective monograph). Česká republika, 2022. – С. 150-158. 4) наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів,

							конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування; 1. А. В. Колісниченко, С. В. Харицька. English for academis purposes. Методичні рекомендації для самостійної роботи здобувачів наукового ступеня доктора філософії з дисципліни «Англійська мова наукового спрямування» . – Київ: ДУІКТ, 2026. 30 с. 2.Professional English. Information Technology: навч. посібник / О.В. Ковтун, Л. М. Конопляник, Ю. Ю. Пришупа, А. В. Колісниченко, С. В. Харицька. – Київ: ДУ «КАІ», 2025. 160 с. (20%). 3. Колісниченко А. В. Professional English. Biomedical engineering: практикум з англійської мови / А. В. Колісниченко. – К.:НАУ, 2021. – 53 с. 4. Колісниченко А. В. Professional English. Ecology: практикум з англійської мови / А. В. Колісниченко. – К.:НАУ, 2021. – 53 с. 8) виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах; «Експлікація концептосфери національної ідентичності у мета дискурсі сучасних соціальних комунікацій» (реєстраційний номер: 44 – 2020 /

							12.01.04) – держбюджетна (кафедральна) науково-дослідна робота (2020-2022), відповідальний виконавець «Культурна мультимодальність як визначник національної ідентичності у світовій літературно-художній спадщині» (реєстраційний номер: 45-2022/12.01.04) – держбюджетна (кафедральна) науково-дослідна робота (2022-2025), науковий керівник «Методи та засоби оптимізації параметрів та ресурсів електронних комунікаційних мереж та ІКС із застосуванням ШІ» (2025-2026 р.) , виконавець 10) участь у міжнародних наукових та / або освітніх проєктах, залучення до міжнародної експертизи, наявність звання «суддя міжнародної категорії»; Міжнародна науково-практична конференція «Національна ідентичність в мові і культурі», член оргкомітету, відповідальна за секцію «Інтерпретація творів зарубіжної літератури» (2021-2025 р.) 3. VII Всеукраїнська студентська науково-практична конференція «Мова і світ: мовознавчі, літературознавчі і перекладознавчі аспекти взаємодії», член оргкомітету (2026). 12) наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п’яти публікацій; 1. Харицька С. В., Колісниченко А. В. Лінгвокультурні

							аспекти перекладу кулінаронімів. Проблеми ефективності професійної мовної комунікації в умовах інформаційної агресії: матеріали II Всеукр. наук.-практ. конф. з міжнародною участю (м. Київ, 28 листопада 2025 року). Київ : Київський інститут Національної гвардії України, 2025. С. 302-305. 2. Харицька С. В., Колісниченко А. В. Екстраполяція національної ідентичності в кулінарні патерни України. Нові перспективи національної ідентичності мові, мистецтві та літературі: збірник наукових праць. К., 2025. С. 145-150. 3. Романчук В. Ю., Колісниченко А. В. Revolutionizing creativity: the impact of AI on modern creative industries. Проблеми ефективності професійної мовної комунікації в умовах інформаційної агресії: матеріали II Всеукр. наук.-практ. конф. з міжнародною участю (м. Київ, 28 листопада 2025 року). Київ : Київський інститут Національної гвардії України, 2025. С. 223-225. 4.Колісниченко А. В., Харицька С. В. Мультимодальність інкорпорування STEM-освіти у процес формування Soft Skills та професійних компетентностей. Importance of Soft Skills for Life and Scientific Success: Proceedings of the 4th International Scientific and Practical Internet Conference, March 6-7, 2025. FOP Marenichenko V.V., Dnipro, Ukraine, 2025. С. 108-109. 5. Харицька С. В., Колісниченко А. В. Транслітерація фольклорних жанрів як засіб популяризації української культурної спадщини: кейс vesnianky. Global trends in science and education. Proceedings of XI International Scientific and Practical Conference. Kyiv,

							Ukraine, 2025. С. 915-919 6. Kharytska S., Kolisnychenko A. English texts reading strategies across professionally oriented training. Similarities and differences in teaching philological disciplines in Ukraine and Latvia. Proceedings of the scientific and pedagogical internship, December 4 – January 14, 2024. Riga, the Republic of Latvia, 2024. P. 41-45. 7. Kolisnychenko A., Kharytska S. Fake vs critical consumption of information. Interaction of the experience of post-Yugoslav and Ukrainian areas: cultural, linguistic, literary, artistic, historical, and journalistic aspects (February 23–24, 2024. Ljubljana, Slovenia). Riga, Latvia: Baltija Publishing, 2024. P. 10-1 8. Kharytska S., Kolisnychenko A. Inappropriate technologies of business administration of the Ukrainian aviation industry in the 21st century. Proceedings of the 11th World Congress «Aviation in the XXI-st century». September 25-25, 2024. P. 433-437. 9. Колісниченко А. В. Застосування дизайн-мислення при створенні мистецької студії як креативного студентського простору. Дизайн-мислення в освітній діяльності : матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, 1 липня – 11 серпня 2024 року. Львів – Торунь: Liha-Pres, 2024. С. 16-17. 10. Колісниченко А. В., Харицька С. В. Роль асистента вчителя в системі національної освіти України. Integration of Education, Science and Business in Modern Environment: Summer Debates: Proceedings of the 6th International Scientific and Practical Internet Conference, August 1-2, 2024. FOP Marenichenko V.V., Dnipro, Ukraine, C. 155-157.

							11. Колісниченко А. В. Особливості трансформації позитивного мислення: від поліаннізму до синдрома Поліанни (за романом Елеонор Портнр «Поліанна»). Proceedings of I International Scientific and Practical Conference «Scientific Acheievements of Contemporary Society», 15-17 August 2024. London, United Kingdom, 2024. С. 315-318. 12. Харицька С. В., Колісниченко А. В. Дотримання принципів академічної доброчесності як чинник формування морально-етичної ідентичності студентів-спеціалістів у сфері захисту інформації: матеріали V Міжнародного науково-практичного форуму «Ефективне врядування та виховання доброчесності в секторі безпеки та оборони» (11 грудня 2024 р.). Київ, 2024. С. 59-50. 13. А. Колісниченко. Концепт «Фастівської культури» у творах Гарта Крейна. Національна ідентичність в мові і культурі: збірник наукових праць / за заг. ред. О. Г. Шостак. К.: Талком, 2023. С. 83-85. 14. А. Колісниченко, С. Харицька. Фейк як одиниця медіаманіпуляції соціальною думкою. Подолання мовних та комунікативних бар'єрів: освіта, наука, культура: збірник наукових праць / за заг. ред.. О. В. Ковтун. К.: НАУ, 2023. С. 159-162. 15. Харицька С. В., Колісниченко А. В. Виховна функція роботи гуртка під час кризової трансформації національної самосвідомості. Формування резильєнтних компетентностей здобувача освіти в період трансформацій, сучасних викликів та

							кризових станів суспільства: матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, 3 липня – 13 серпня 2023 року. Одеса: Видавничий дім «Гельветика», 2023. С. 155-159. 16. A. Kolisnychenko, S. Kharytska. Localization of video games as the important component of national / cultural patterns expressing. Національна ідентичність в мові і культурі: збірник наукових праць / за заг. ред. О. Г. Шостак. К.: Талком, 2021. С. 169-172. 17. Kharytska S., Kolisnychenko A. Features of foreign language competence of future aviation industry engineers. Modern problems in science: Proceedings of the XIX International Scientific and Practical Conference. Vancouver, Canada. 2022. Pp. 456-459. 18. Колісниченко А. В., Харицька С. В. Жанрова парадигма лірики Гарта Крейна. Філологічні науки: сучасні тенденції та фактори розвитку: Міжнародна науково-практична конференція, м. Одеса, 28–29 січня 2022 року. Одеса: Південноукраїнська організація «Центр філологічних досліджень», 2022. С. 68-70. 19. С. Харицька, А. Колісниченко. Проблеми адаптації студентів ВЗО до навчання у період воєнного стану. Подолання мовних та комунікативних бар'єрів: освіта, наука, культура: збірник наукових праць / за заг. ред.. О. В. Ковтун. К.: НАУ, 2022. С. 249-253. 20. Колісниченко А. В. Концепт «гендер» як базис гендерних студій. Мова та література у полікультурному просторі: Міжнародна науково-практична конференція, м. Львів 11–12 лютого 2022 року. Львів: Наукова філологічна організація «Логос», 2022. С. 7-8.

							21. С. Харицька, А. Колісниченко. Інтегрування засад національної ідентичності у виховний процес у закладах вищої освіти. Інновації в сучасній освіті: український та світовий контекст: матеріали V Міжнар. наук.-практ. Інтернет-конф. (Умань, 20 жовтня 2022 р.) / МОН України, Уманський держ. пед. ун-т імені Павла Тичини [та ін.]; [редкол.: О. І. Безлюдний, Т. Л. Годованюк, І. С. Постоленко [та ін.]; відпов. за вип. І. Ю. Гурський]. Умань: Візаві, 2022. С. 198-201. 22. Колісниченко А. В. Національні традиції Емілі Дікінсон та Волта Вітмена vs модерністські новації Езри Паунда й Томаса Стірнза Еліота в формуванні оригінальності письма Гарта Крейна. Fundamental and applied research in the modern world. Abstracts of the 6th International scientific and practical conference. BoScience Publisher, Boston, USA. 2021. Pp. 580-587. 23. Романчук В. Ю., Колісниченко А. В. Revolutionizing creativity: the impact of AI on modern creative industries. Проблеми ефективності професійної мовної комунікації в умовах інформаційної агресії: матеріали ІІ Всеукр. наук.-практ. конф. з міжнародною участю (м. Київ, 28 листопада 2025 року). Київ : Київський інститут Національної гвардії України, 2025. С. 223-225. 24. 1. Харицька С. В., Колісниченко А. В. Розвиток навичок критичного аналізу англомовних джерел як складова професійної підготовки студентів ІТ. Лінгвістичні та методологічні аспекти викладання іноземних мов професійного спрямування: матеріали VII Міжнародної науково-

							практичної конференції 26–27 березня 2026 р. / За заг. ред. О. М. Акмалдінової. К.: НУ «КАІ». 2026. С. 64-65. 14) керівництво студентом, який зайняв призове місце на І або ІІ етапі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт), або робота у складі організаційного комітету / журі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт), або керівництво постійно діючим студентським науковим гуртком / проблемною групою; керівництво студентом, який став призером або лауреатом Міжнародних, Всеукраїнських мистецьких конкурсів, фестивалів та проектів, робота у складі організаційного комітету або у складі журі міжнародних, всеукраїнських мистецьких конкурсів, інших культурно-мистецьких проектів (для забезпечення провадження освітньої діяльності на третьому (освітньо-творчому) рівні); керівництво здобувачем, який став призером або лауреатом міжнародних мистецьких конкурсів, фестивалів, віднесених до Європейської або Всесвітньої (Світової) асоціації мистецьких конкурсів, фестивалів, робота у складі організаційного комітету або у складі журі зазначених мистецьких конкурсів, фестивалів); керівництво студентом, який брав участь в Олімпійських, Параолімпійських іграх, Всесвітній та Всеукраїнській Універсіаді, чемпіонаті світу, Європи, Європейських іграх, етапах Кубка світу та Європи,

							чемпіонаті України; виконання обов'язків тренера, помічника тренера національної збірної команди України з видів спорту; виконання обов'язків головного секретаря, головного судді, судді міжнародних та всеукраїнських змагань; керівництво спортивною делегацією; робота у складі організаційного комітету, суддівського корпусу; Студентський науковий гурток «Літературознавчі та мистецькі студії», керівник (2020-2024). Студентський науковий гурток «Scientific Hub», керівник (2024-2026 р.). Робота у складі журі Всеукраїнського конкурсу студентських наукових робіт з галузей знань і спеціальностей (Галузь: гуманітарні науки; Спеціальність: 023 Соціолінгвістика) (2024). Робота в складі оргкомітету Всеукраїнської олімпіади з англійської мови (2025-2026). Робота у складі журі Міжнародного конкурсу з української мови імені Петра Яцика (2024-2026 р.). Керівництво студентами, які зайняли 2 та 3 місця у І етапі Всеукраїнської олімпіади з англійської мови (2026 р.). 19) діяльність за спеціальністю у формі участі у професійних та / або громадських об'єднаннях; Член Української асоціації дослідників освіти.
521859	Іванченко Ігор Сергійович	Професор, Основне місце роботи	Навчально-науковий інститут Кібербезпеки та захисту інформації	Диплом спеціаліста, Національний авіаційний університет, рік закінчення: 2009, спеціальність: Захист інформації з обмеженим доступом та автоматизація	13	Організація і проведення спеціальних досліджень на обєкті інформаційної діяльності	Кандидат технічних наук зі спеціальності 05.13.21 – системи захисту інформації. Тема дисертації: « Моделі мультирівневого розмежування доступу для підтримки цілісності інформаційних ресурсів». Диплом Кандидата

				ії обробки, Диплом магістра, Національний авіаційний університет, рік закінчення: 2011, спеціальність: Захист інформації з обмеженим доступом та автоматизація її обробки, Диплом кандидата наук ДК 047943, виданий 05.07.2018, Атестат доцента АД 006211, виданий 09.02.2021			технічних наук - ДК №047943, від 2018-07-05, виданий: Національний авіаційний університет, науковий ступінь кандидат технічних наук, шифр та найменування наукової спеціальності (05.13.21) Системи захисту інформації. Атестат доцента - АД 3006211, від 2021-02-09, виданий: Атестаційна колегія Міністерства освіти і науки України, вчене звання доцент, за якою кафедрою (спеціальністю) присвоєно: кафедра безпеки інформаційних технологій. Підвищення кваліфікації: Державний вищий навчальний заклад "Ужгородський національний університет", 01.12.2033-01.04.2024, за програмою 180 годин (6 кредитів ЄКТС) на кафедрі твердотільної електроніки та інформаційної безпеки. Види і результати професійної діяльності за спеціальністю відповідно до п.38 Ліцензійних умов провадження освітньої діяльності: (п. 1, 5 6, 7, 8, 10, 19) 1. наявність не менше п’яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection; 1. Pedchenko Y., Ivanchenko Y., Ivanchenko I., Lozova I., Jancarczyk D., Sawicki P. Analysis of modern cloud services to ensure cybersecurity. Procedia Computer Science. 2022. Vol. 207. P. 110-117. Mode of access: https://www.sciencedirect.com/science/article/pii/S1877050922009164 . DOI : https://doi.org/10.1016/j.procs.2022.09.043 . 2. Педченко Є.М., Іванченко І.С. Структурна модель системи оцінювання

							кібербезпеки хмарних сервісів об’єктів інформаційної інфраструктури. Кібербезпека: освіта, наука, техніка. 2024. Том 1, № 25. С. 505-515. URL: https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/667. DOI : https://doi.org/10.28925/2663-4023.2024.25.505515 3. Педченко Є.М., Іванченко І.С. Метод оцінювання кіберзахищеності хмарних сервісів об’єктів інформаційної інфраструктури. Сучасний захист інформації. 2024. Том. 59, №3. С. 75-84. URL: https://doi.org/10.31673/2409-7292.2024.030008 4. Педченко Є.М., Іванченко І.С. Аналіз моделей та методів оцінювання стану кіберзахищеності хмарних сервісів об’єктів інформаційної інфраструктури. Безпека інформації. 2024. Том. 30, №2. С. 279-287. URL: https://doi.org/10.18372/2225-5036.30.19240 5. Tolkachov, M., Dzheniuk, N., Yevseiev, S., Lysetskyi, Y., Shulha, V., Grod, I., Faraon, S., Ivanchenko, I., Pasko, I., & Balagura, D. (2024). Development of a method for protecting information resources in a corporate network by segmenting traffic . Eastern-European Journal of Enterprise Technologies, 5(9 (131), 63–78. https://doi.org/10.15587/1729-4061.2024.313158 6. Поночовний П. М., Іванченко І.С. Метод раннього виявлення та захисту від мінливих ddos атак на основі аналізу обробки пакетних груп. Наукові записки ДУІКТ, № 2 (6) (2024), С. 153-164 DOI: 10.31673/2786-8362.2024.027035 7. Юрх Н.Г., Петченко М.В., Іванченко І.С. Аналіз методів захисту системи передавання мовноїіінформації. Сучасний захист інформації. № 2 (62) (2025) С. 107-113. DOI:

							10.31673/2409-7292.2025.026026 8. Володимир Шульга, Микола Рижаков, Ігор Іванченко. Узагальнена модель інтелектуально системи прогнозування та виявлення аномалій у кіберінфраструктурі на основі глибокого навчання. Міжнародний науково-технічний журнали«Вимірювальна та обчислювальна техніка в технологічних процесах» № 3, 2025, С. 217-225. DOI: 10.31891/2219-9365-2025-83-28 9. Ivanchenko, Y., Karpinski, M., Ryzhakov, M., Ivanchenko, I., Mazurek, P., & Sawicki, P. (2026). An Agent-Based Model of a Controlled Detonation System for Sandbox Analysis of Suspicious Software. Electronics, 15(11), 2348. https://doi.org/10.3390/electronics15112348. 6.наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня; 2025 р. Педченко Євген Максимович, PhD 2025 р. Поночовний Петро Михайлович, PhD 2026 р. Рижаков Микола Миколайович, PhD 7.участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад; 1. "Рецензент дисертаційної роботи Аясраха Ахмада Расмі Алі на тему «Моделі оцінювання стану кіберзахищеності інформаційних систем» наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека», 2023 р. "8.виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або

							головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах; Виконавець науково-дослідної роботи «Розробка системи імітації зоряного неба для тестування навігаційних сенсорів робототехнічних платформ» (державний реєстраційний номер 0126U002656, 2026 р.) 10. Участь у міжнародних наукових проектах, залучення до міжнародної експертизи, наявність звання “суддя міжнародної категорії: Swedish grant recipient: Hogskolan i Halmstad SI project registration number: 0028512025 Project title : AI-Driven cybersecurity: opportunities and challenges Project period: 2025-10-01 - 2027-03-31 19.діяльність за спеціальністю у формі участі у професійних та/або громадських об’єднаннях; Учасник Громадської організації «Асоціація спеціалістів кібербезпеки».

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**
РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а	☒	Науково-педагогічна практика	Презентації; дискусії; пояснення технічних рішень різним аудиторіям; взаємне рецензування; практичні вправи з професійної комунікації.	Поточне та рубіжне оцінювання: Оцінювання презентації, зрозумілості висновків, аргументації та відповідей на запитання. Підсумковий контроль: Іспит: ОК1, ОК8, ОК9, ОК10.

також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.				Залік: ОК11.
		Організація і проведення спеціальних досліджень на обєкті інформаційної діяльності	Презентації; дискусії; пояснення технічних рішень різним аудиторіям; взаємне рецензування; практичні вправи з професійної комунікації.	Поточне та рубіжне оцінювання: Оцінювання презентації, зрозумілості висновків, аргументації та відповідей на запитання. Підсумковий контроль: Іспит: ОК1, ОК8, ОК9, ОК10. Залік: ОК11.
		Радіомоніторинг і радіопротидія на об'єктах ІД	Презентації; дискусії; пояснення технічних рішень різним аудиторіям; взаємне рецензування; практичні вправи з професійної комунікації.	Поточне та рубіжне оцінювання: Оцінювання презентації, зрозумілості висновків, аргументації та відповідей на запитання. Підсумковий контроль: Іспит: ОК1, ОК8, ОК9, ОК10. Залік: ОК11.
		Теорія захисту інформаційних ресурсів обмеженого доступу	Презентації; дискусії; пояснення технічних рішень різним аудиторіям; взаємне рецензування; практичні вправи з професійної комунікації.	Поточне та рубіжне оцінювання: Оцінювання презентації, зрозумілості висновків, аргументації та відповідей на запитання. Підсумковий контроль: Іспит: ОК1, ОК8, ОК9, ОК10. Залік: ОК11.
		Корпоративна та професійна етика в кібербезпеці	Презентації; дискусії; пояснення технічних рішень різним аудиторіям; взаємне рецензування; практичні вправи з професійної комунікації.	Поточне та рубіжне оцінювання: Оцінювання презентації, зрозумілості висновків, аргументації та відповідей на запитання. Підсумковий контроль: Іспит: ОК1, ОК8, ОК9, ОК10. Залік: ОК11.
РН26. Створювати систему допуску учасників інформаційної діяльності з обмеженим допуском у відповідності з поточною політикою інформаційного та кібернетичного захисту і з урахуванням чинного законодавства.	☒	Технологія створення та застосування комплексів засобів захисту інформації з обмеженим доступом та охорони ОІД	Практичні кейси допуску; моделювання ролей і повноважень; проєктування порядку допуску; аналіз відповідності політиці захисту.	Поточне та рубіжне оцінювання: Оцінювання проєкту порядку допуску та його відповідності політиці захисту; усний захист. Підсумковий контроль: Іспит: ОК5, ОК7.
РН25. Розділяти складові, які відносяться до інформаційної безпеки та захисту інформації на об'єктах інформаційної діяльності.	☒	Радіомоніторинг і радіопротидія на об'єктах ІД	Пояснювальні лекції; класифікація складових захисту; порівняльний аналіз загроз і каналів витоку; практичні завдання з радіомоніторингу.	Поточне та рубіжне оцінювання: Тематичне тестування; оцінювання класифікації складових захисту та аналізу каналів витоку. Підсумковий контроль: Іспит: ОК8, ОК9.
		Теорія захисту інформаційних ресурсів обмеженого доступу	Пояснювальні лекції; класифікація складових захисту; порівняльний аналіз загроз і каналів витоку; практичні завдання з радіомоніторингу.	Поточне та рубіжне оцінювання: Тематичне тестування; оцінювання класифікації складових захисту та аналізу каналів витоку. Підсумковий контроль: Іспит: ОК8, ОК9.
РН24. Планувати та виконувати наукові та прикладні дослідження у сфері інформаційної безпеки та/або кібербезпеки із	☒	Педагогіка та психологія у вищій школі	Проблемні лекції; дослідницькі завдання; системний аналіз; моделювання та оптимізація; застосування статистичних методів і теорії прийняття рішень	Поточне та рубіжне оцінювання: Оцінювання дослідницького завдання, вибору методів, розрахунків та інтерпретації результатів. Підсумковий контроль: Іспит: ОК5. Залік: ОК3

застосуванням сучасних технологій, експериментальних і теоретичних методів і моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики.				
РН23. 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.	☒	Преддипломна практика	Порівняльний аналіз програмного забезпечення й обладнання; робота з технічною документацією; практичні кейси вибору засобів; консультації	Поточне та рубіжне оцінювання: Оцінювання порівняльного аналізу засобів, технічних обмежень і аргументованості вибору. Підсумковий контроль: Залік: ОК12, ОК13. ОК4: залік, іспит. ОК14: публічний захист кваліфікаційної роботи.
		Науково-дослідна практика	Порівняльний аналіз програмного забезпечення й обладнання; робота з технічною документацією; практичні кейси вибору засобів; консультації	Поточне та рубіжне оцінювання: Оцінювання порівняльного аналізу засобів, технічних обмежень і аргументованості вибору. Підсумковий контроль: Залік: ОК12, ОК13. ОК4: залік, іспит. ОК14: публічний захист кваліфікаційної роботи.
		Англійська мова для ділової комунікації	Порівняльний аналіз програмного забезпечення й обладнання; робота з технічною документацією; практичні кейси вибору засобів; консультації	Поточне та рубіжне оцінювання: Оцінювання порівняльного аналізу засобів, технічних обмежень і аргументованості вибору. Підсумковий контроль: Залік: ОК12, ОК13. ОК4: залік, іспит. ОК14: публічний захист кваліфікаційної роботи.
		Науково-технічний переклад	Порівняльний аналіз програмного забезпечення й обладнання; робота з технічною документацією; практичні кейси вибору засобів; консультації	Поточне та рубіжне оцінювання: Оцінювання порівняльного аналізу засобів, технічних обмежень і аргументованості вибору. Підсумковий контроль: Залік: ОК12, ОК13. ОК4: залік, іспит. ОК14: публічний захист кваліфікаційної роботи.
РН28. Виявляти пристрої несанкціонованого зняття інформації на об'єктах інформаційної діяльності.	☒	Технологія створення та застосування комплексів засобів захисту інформації з обмеженим доступом та охорони ОІД	Демонстрація пошукової апаратури; лабораторний пошук і локалізація закладних пристроїв; практичне складання програми спеціального обстеження.	Поточне та рубіжне оцінювання: Захист лабораторної роботи; оцінювання протоколу пошуку, локалізації та висновків обстеження. Підсумковий контроль: Іспит: ОК5, ОК7, ОК10
		Організація і проведення спеціальних досліджень на обєкті інформаційної діяльності	Демонстрація пошукової апаратури; лабораторний пошук і локалізація закладних пристроїв; практичне складання програми спеціального обстеження.	Поточне та рубіжне оцінювання: Захист лабораторної роботи; оцінювання протоколу пошуку, локалізації та висновків обстеження. Підсумковий контроль: Іспит: ОК5, ОК7, ОК10
РН21. Використовувати методи натурного, фізичного і комп'ютерного	☐	Науково-дослідна практика	Натурне, фізичне та комп'ютерне моделювання; лабораторні експерименти; зіставлення результатів моделей; самостійна	Поточне та рубіжне оцінювання: Захист моделей; оцінювання адекватності моделювання та зіставлення з

моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.			дослідницька робота.	експериментом. Підсумковий контроль: Іспит: ОК7. Залік: ОК3, ОК12. ОК14: публічний захист кваліфікаційної роботи.
		Технологія створення та застосування комплексів засобів захисту інформації з обмеженим доступом та охорони ОІД	Натурне, фізичне та комп'ютерне моделювання; лабораторні експерименти; зіставлення результатів моделей; самостійна дослідницька робота.	Поточне та рубіжне оцінювання: Захист моделей; оцінювання адекватності моделювання та зіставлення з експериментом. Підсумковий контроль: Іспит: ОК7. Залік: ОК3, ОК12. ОК14: публічний захист кваліфікаційної роботи.
		Педагогіка та психологія у вищій школі	Натурне, фізичне та комп'ютерне моделювання; лабораторні експерименти; зіставлення результатів моделей; самостійна дослідницька робота.	Поточне та рубіжне оцінювання: Захист моделей; оцінювання адекватності моделювання та зіставлення з експериментом. Підсумковий контроль: Іспит: ОК7. Залік: ОК3, ОК12. ОК14: публічний захист кваліфікаційної роботи.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.	☒	Педагогіка та психологія у вищій школі	Проблемні лекції; розв'язання інженерних задач; аналіз стандартів і фахових джерел; дослідницький проєкт; індивідуальні консультації	Поточне та рубіжне оцінювання: Оцінювання розв'язання інженерної задачі та відповідності рішення стандартам; усний захист. Підсумковий контроль: Іспит: ОК5, ОК8, ОК10. Залік: ОК3, ОК12, ОК13. ОК4: залік, іспит. ОК14: публічний захист кваліфікаційної роботи.
		Науково-технічний переклад	Проблемні лекції; розв'язання інженерних задач; аналіз стандартів і фахових джерел; дослідницький проєкт; індивідуальні консультації	Поточне та рубіжне оцінювання: Оцінювання розв'язання інженерної задачі та відповідності рішення стандартам; усний захист. Підсумковий контроль: Іспит: ОК5, ОК8, ОК10. Залік: ОК3, ОК12, ОК13. ОК4: залік, іспит. ОК14: публічний захист кваліфікаційної роботи.
		Теорія захисту інформаційних ресурсів обмеженого доступу	Проблемні лекції; розв'язання інженерних задач; аналіз стандартів і фахових джерел; дослідницький проєкт; індивідуальні консультації	Поточне та рубіжне оцінювання: Оцінювання розв'язання інженерної задачі та відповідності рішення стандартам; усний захист. Підсумковий контроль: Іспит: ОК5, ОК8, ОК10. Залік: ОК3, ОК12, ОК13. ОК4: залік, іспит. ОК14: публічний захист кваліфікаційної роботи.
		Англійська мова для ділової комунікації	Проблемні лекції; розв'язання інженерних задач; аналіз стандартів і фахових джерел; дослідницький проєкт; індивідуальні консультації	Поточне та рубіжне оцінювання: Оцінювання розв'язання інженерної задачі та відповідності рішення стандартам; усний захист. Підсумковий контроль: Іспит: ОК5, ОК8, ОК10. Залік: ОК3, ОК12, ОК13. ОК4: залік, іспит. ОК14:

				публічний захист кваліфікаційної роботи.
		Преддипломна практика	Проблемні лекції; розв'язання інженерних задач; аналіз стандартів і фахових джерел; дослідницький проєкт; індивідуальні консультації	Поточне та рубіжне оцінювання: Оцінювання розв'язання інженерної задачі та відповідності рішення стандартам; усний захист. Підсумковий контроль: Іспит: ОК5, ОК8, ОК10. Залік: ОК3, ОК12, ОК13. ОК4: залік, іспит. ОК14: публічний захист кваліфікаційної роботи.
		Науково-дослідна практика	Проблемні лекції; розв'язання інженерних задач; аналіз стандартів і фахових джерел; дослідницький проєкт; індивідуальні консультації	Поточне та рубіжне оцінювання: Оцінювання розв'язання інженерної задачі та відповідності рішення стандартам; усний захист. Підсумковий контроль: Іспит: ОК5, ОК8, ОК10. Залік: ОК3, ОК12, ОК13. ОК4: залік, іспит. ОК14: публічний захист кваліфікаційної роботи.
		Організація і проведення спеціальних досліджень на обєкті інформаційної діяльності	Проблемні лекції; розв'язання інженерних задач; аналіз стандартів і фахових джерел; дослідницький проєкт; індивідуальні консультації	Поточне та рубіжне оцінювання: Оцінювання розв'язання інженерної задачі та відповідності рішення стандартам; усний захист. Підсумковий контроль: Іспит: ОК5, ОК8, ОК10. Залік: ОК3, ОК12, ОК13. ОК4: залік, іспит. ОК14: публічний захист кваліфікаційної роботи.
РН19. 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.	☒	Преддипломна практика	Проєктне та дослідницьке навчання; порівняння аналітичних і експериментальних методів; розроблення плану проєкту; аналіз інтелектуальної власності.	Поточне та рубіжне оцінювання: Оцінювання плану проєкту, вибору методів і заходів захисту інтелектуальної власності. Підсумковий контроль: Іспит: ОК5. Залік: ОК3, ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Науково-дослідна практика	Проєктне та дослідницьке навчання; порівняння аналітичних і експериментальних методів; розроблення плану проєкту; аналіз інтелектуальної власності.	Поточне та рубіжне оцінювання: Оцінювання плану проєкту, вибору методів і заходів захисту інтелектуальної власності. Підсумковий контроль: Іспит: ОК5. Залік: ОК3, ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Педагогіка та психологія у вищій школі	Проєктне та дослідницьке навчання; порівняння аналітичних і експериментальних методів; розроблення плану проєкту; аналіз інтелектуальної власності.	Поточне та рубіжне оцінювання: Оцінювання плану проєкту, вибору методів і заходів захисту інтелектуальної власності. Підсумковий контроль: Іспит: ОК5. Залік: ОК3, ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму	☒	Науково-педагогічна практика	Практичне планування навчання персоналу; педагогічні кейси; моделювання інструктажу; проведення навчальних занять; аналіз зворотного зв'язку	Поточне та рубіжне оцінювання: Оцінювання плану заняття, навчальних матеріалів, проведення інструктажу та аналізу результатів. Підсумковий контроль:

інформаційної безпеки та/або кібербезпеки.				Іспит: ОК1, ОК9, ОК10. Залік: ОК2, ОК11.
		Організація і проведення спеціальних досліджень на обєкті інформаційної діяльності	Практичне планування навчання персоналу; педагогічні кейси; моделювання інструктажу; проведення навчальних занять; аналіз зворотного зв'язку	Поточне та рубіжне оцінювання: Оцінювання плану заняття, навчальних матеріалів, проведення інструктажу та аналізу результатів. Підсумковий контроль: Іспит: ОК1, ОК9, ОК10. Залік: ОК2, ОК11.
		Радіомоніторинг і радіопротидія на об'єктах ІД	Практичне планування навчання персоналу; педагогічні кейси; моделювання інструктажу; проведення навчальних занять; аналіз зворотного зв'язку	Поточне та рубіжне оцінювання: Оцінювання плану заняття, навчальних матеріалів, проведення інструктажу та аналізу результатів. Підсумковий контроль: Іспит: ОК1, ОК9, ОК10. Залік: ОК2, ОК11.
		Корпоративна та професійна етика в кібербезпеці	Практичне планування навчання персоналу; педагогічні кейси; моделювання інструктажу; проведення навчальних занять; аналіз зворотного зв'язку	Поточне та рубіжне оцінювання: Оцінювання плану заняття, навчальних матеріалів, проведення інструктажу та аналізу результатів. Підсумковий контроль: Іспит: ОК1, ОК9, ОК10. Залік: ОК2, ОК11.
РН17. 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.	☒	Преддипломна практика	Самостійне навчання за індивідуальним планом; пошук і критичне опрацювання джерел; консультації; рефлексія та самооцінювання.	Поточне та рубіжне оцінювання: Оцінювання індивідуальних завдань, портфоліо результатів та самоаналізу навчального поступу. Підсумковий контроль: Іспит: ОК1. Залік: ОК2, ОК3, ОК11, ОК12, ОК13. ОК4: залік, іспит. ОК14: публічний захист кваліфікаційної роботи.
		Науково-дослідна практика	Самостійне навчання за індивідуальним планом; пошук і критичне опрацювання джерел; консультації; рефлексія та самооцінювання.	Поточне та рубіжне оцінювання: Оцінювання індивідуальних завдань, портфоліо результатів та самоаналізу навчального поступу. Підсумковий контроль: Іспит: ОК1. Залік: ОК2, ОК3, ОК11, ОК12, ОК13. ОК4: залік, іспит. ОК14: публічний захист кваліфікаційної роботи.
		Англійська мова для ділової комунікації	Самостійне навчання за індивідуальним планом; пошук і критичне опрацювання джерел; консультації; рефлексія та самооцінювання.	Поточне та рубіжне оцінювання: Оцінювання індивідуальних завдань, портфоліо результатів та самоаналізу навчального поступу. Підсумковий контроль: Іспит: ОК1. Залік: ОК2, ОК3, ОК11, ОК12, ОК13. ОК4: залік, іспит. ОК14: публічний захист кваліфікаційної роботи.
		Науково-технічний переклад	Самостійне навчання за індивідуальним планом; пошук і критичне опрацювання джерел; консультації; рефлексія та самооцінювання.	Поточне та рубіжне оцінювання: Оцінювання індивідуальних завдань, портфоліо результатів та самоаналізу навчального поступу. Підсумковий контроль: Іспит: ОК1. Залік: ОК2, ОК3, ОК11, ОК12, ОК13. ОК4:

				залік, іспит. ОК14: публічний захист кваліфікаційної роботи.
		Педагогіка та психологія у вищій школі	Самостійне навчання за індивідуальним планом; пошук і критичне опрацювання джерел; консультації; рефлексія та самооцінювання.	Поточне та рубіжне оцінювання: Оцінювання індивідуальних завдань, портфоліо результатів та самоаналізу навчального поступу. Підсумковий контроль: Іспит: ОК1. Залік: ОК2, ОК3, ОК11, ОК12, ОК13. ОК4: залік, іспит. ОК14: публічний захист кваліфікаційної роботи.
		Корпоративна та професійна етика в кібербезпеці	Самостійне навчання за індивідуальним планом; пошук і критичне опрацювання джерел; консультації; рефлексія та самооцінювання.	Поточне та рубіжне оцінювання: Оцінювання індивідуальних завдань, портфоліо результатів та самоаналізу навчального поступу. Підсумковий контроль: Іспит: ОК1. Залік: ОК2, ОК3, ОК11, ОК12, ОК13. ОК4: залік, іспит. ОК14: публічний захист кваліфікаційної роботи.
		Науково-педагогічна практика	Самостійне навчання за індивідуальним планом; пошук і критичне опрацювання джерел; консультації; рефлексія та самооцінювання.	Поточне та рубіжне оцінювання: Оцінювання індивідуальних завдань, портфоліо результатів та самоаналізу навчального поступу. Підсумковий контроль: Іспит: ОК1. Залік: ОК2, ОК3, ОК11, ОК12, ОК13. ОК4: залік, іспит. ОК14: публічний захист кваліфікаційної роботи.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.	☒	Організація і проведення спеціальних досліджень на обєкті інформаційної діяльності	Проблемні лекції; ситуаційні завдання в умовах невизначеності; порівняння альтернатив; обґрунтування організаційно-технічних рішень.	Поточне та рубіжне оцінювання: Оцінювання ситуаційного рішення, порівняння альтернатив та обґрунтованості вибору. Підсумковий контроль: Іспит: ОК1, ОК5, ОК10.
		Корпоративна та професійна етика в кібербезпеці	Проблемні лекції; ситуаційні завдання в умовах невизначеності; порівняння альтернатив; обґрунтування організаційно-технічних рішень.	Поточне та рубіжне оцінювання: Оцінювання ситуаційного рішення, порівняння альтернатив та обґрунтованості вибору. Підсумковий контроль: Іспит: ОК1, ОК5, ОК10.
РН27. Організовувати гнучку адаптацію пропускної системи на підприємстві або організації з урахуванням поточних змін, пов'язаних з розвитком інформаційних технологій.	☒	Технологія створення та застосування комплексів засобів захисту інформації з обмеженим доступом та охорони ОІД	Сценарне моделювання змін пропускної системи; практичне проєктування; аналіз нових технологічних вимог; перевірка запропонованих рішень.	Поточне та рубіжне оцінювання: Оцінювання проєкту адаптації пропускної системи та перевірки роботи за змінених умов. Підсумковий контроль: Іспит: ОК7.
РН22. Планувати та виконувати експериментальні і теоретичні дослідження,	☐	Преддипломна практика	Постановка гіпотез; планування експерименту; лабораторні вимірювання; статистична обробка даних; обговорення достовірності	Поточне та рубіжне оцінювання: Оцінювання плану експерименту, статистичної обробки, перевірки гіпотез і

висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.			результатів	достовірності висновків. Підсумковий контроль: Іспит: ОК7, ОК8, ОК9. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Радіомоніторинг і радіопротидія на об'єктах ІД	Постановка гіпотез; планування експерименту; лабораторні вимірювання; статистична обробка даних; обговорення достовірності результатів	Поточне та рубіжне оцінювання: Оцінювання плану експерименту, статистичної обробки, перевірки гіпотез і достовірності висновків. Підсумковий контроль: Іспит: ОК7, ОК8, ОК9. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Теорія захисту інформаційних ресурсів обмеженого доступу	Постановка гіпотез; планування експерименту; лабораторні вимірювання; статистична обробка даних; обговорення достовірності результатів	Поточне та рубіжне оцінювання: Оцінювання плану експерименту, статистичної обробки, перевірки гіпотез і достовірності висновків. Підсумковий контроль: Іспит: ОК7, ОК8, ОК9. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Технологія створення та застосування комплексів засобів захисту інформації з обмеженим доступом та охорони ОІД	Постановка гіпотез; планування експерименту; лабораторні вимірювання; статистична обробка даних; обговорення достовірності результатів	Поточне та рубіжне оцінювання: Оцінювання плану експерименту, статистичної обробки, перевірки гіпотез і достовірності висновків. Підсумковий контроль: Іспит: ОК7, ОК8, ОК9. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Науково-дослідна практика	Постановка гіпотез; планування експерименту; лабораторні вимірювання; статистична обробка даних; обговорення достовірності результатів	Поточне та рубіжне оцінювання: Оцінювання плану експерименту, статистичної обробки, перевірки гіпотез і достовірності висновків. Підсумковий контроль: Іспит: ОК7, ОК8, ОК9. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
РН13. 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.	☒	Преддипломна практика	Лекції з демонстрацією засобів захисту; лабораторні експерименти; розрахунок показників ефективності; порівняння технічних і криптографічних рішень	Поточне та рубіжне оцінювання: Захист лабораторних робіт; перевірка розрахунків ефективності; оцінювання вибору засобів. Підсумковий контроль: Іспит: ОК5, ОК7, ОК8. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Науково-дослідна практика	Лекції з демонстрацією засобів захисту; лабораторні експерименти; розрахунок показників ефективності; порівняння технічних і криптографічних рішень	Поточне та рубіжне оцінювання: Захист лабораторних робіт; перевірка розрахунків ефективності; оцінювання вибору засобів. Підсумковий контроль: Іспит: ОК5, ОК7, ОК8. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Теорія захисту	Лекції з демонстрацією	Поточне та рубіжне

		інформаційних ресурсів обмеженого доступу	засобів захисту; лабораторні експерименти; розрахунок показників ефективності; порівняння технічних і криптографічних рішень	оцінювання: Захист лабораторних робіт; перевірка розрахунків ефективності; оцінювання вибору засобів. Підсумковий контроль: Іспит: ОК5, ОК7, ОК8. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Технологія створення та застосування комплексів засобів захисту інформації з обмеженим доступом та охорони ОІД	Лекції з демонстрацією засобів захисту; лабораторні експерименти; розрахунок показників ефективності; порівняння технічних і криптографічних рішень	Поточне та рубіжне оцінювання: Захист лабораторних робіт; перевірка розрахунків ефективності; оцінювання вибору засобів. Підсумковий контроль: Іспит: ОК5, ОК7, ОК8. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.	☒	Преддипломна практика	Сценарне навчання; аналіз кіберінцидентів; практичне розроблення плану реагування; дослідження та обґрунтування заходів попередження	Поточне та рубіжне оцінювання: Оцінювання плану реагування, аналізу інциденту та профілактичних рекомендацій. Підсумковий контроль: Іспит: ОК10. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Науково-дослідна практика	Сценарне навчання; аналіз кіберінцидентів; практичне розроблення плану реагування; дослідження та обґрунтування заходів попередження	Поточне та рубіжне оцінювання: Оцінювання плану реагування, аналізу інциденту та профілактичних рекомендацій. Підсумковий контроль: Іспит: ОК10. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Організація і проведення спеціальних досліджень на обєкті інформаційної діяльності	Сценарне навчання; аналіз кіберінцидентів; практичне розроблення плану реагування; дослідження та обґрунтування заходів попередження	Поточне та рубіжне оцінювання: Оцінювання плану реагування, аналізу інциденту та профілактичних рекомендацій. Підсумковий контроль: Іспит: ОК10. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
РН14. 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.	☒	Організація і проведення спеціальних досліджень на обєкті інформаційної діяльності	Практичні кейси аудиту; розроблення програми моніторингу; аналіз результатів вимірювань; підготовка рекомендацій з усунення невідповідностей.	Поточне та рубіжне оцінювання: Оцінювання програми аудиту, звіту моніторингу й рекомендацій; тематичне тестування. Підсумковий контроль: Іспит: ОК6, ОК10.
РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для	☐	Науково-педагогічна практика	Практичний переклад фахових текстів; усні доповіді та презентації; обговорення професійних ситуацій державною й	Поточне та рубіжне оцінювання: Оцінювання перекладу, усної доповіді та відповідей на запитання. Підсумковий контроль:

представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес/операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.			іноземною мовами	Іспит: ОК5, ОК6. Залік: ОК11. ОК4: залік, іспит
		Англійська мова для ділової комунікації	Практичний переклад фахових текстів; усні доповіді та презентації; обговорення професійних ситуацій державною й іноземною мовами	Поточне та рубіжне оцінювання: Оцінювання перекладу, усної доповіді та відповідей на запитання. Підсумковий контроль: Іспит: ОК5, ОК6. Залік: ОК11. ОК4: залік, іспит.
		Науково-технічний переклад	Практичний переклад фахових текстів; усні доповіді та презентації; обговорення професійних ситуацій державною й іноземною мовами	Поточне та рубіжне оцінювання: Оцінювання перекладу, усної доповіді та відповідей на запитання. Підсумковий контроль: Іспит: ОК5, ОК6. Залік: ОК11. ОК4: залік, іспит.
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.	☒	Науково-педагогічна практика	Проблемні лекції; міждисциплінарні кейси; дискусії щодо професійних та педагогічних ситуацій; самостійне опрацювання джерел.	Поточне та рубіжне оцінювання: Оцінювання розв'язання комплексного кейсу та аргументації; тематичне тестування. Підсумковий контроль: Іспит: ОК1, ОК6. Залік: ОК2, ОК11. ОК4: залік, іспит
		Англійська мова для ділової комунікації	Проблемні лекції; міждисциплінарні кейси; дискусії щодо професійних та педагогічних ситуацій; самостійне опрацювання джерел	Поточне та рубіжне оцінювання: Оцінювання розв'язання комплексного кейсу та аргументації; тематичне тестування. Підсумковий контроль: Іспит: ОК1, ОК6. Залік: ОК2, ОК11. ОК4: залік, іспит.
		Науково-технічний переклад	Проблемні лекції; міждисциплінарні кейси; дискусії щодо професійних та педагогічних ситуацій; самостійне опрацювання джерел	Поточне та рубіжне оцінювання: Оцінювання розв'язання комплексного кейсу та аргументації; тематичне тестування. Підсумковий контроль: Іспит: ОК1, ОК6. Залік: ОК2, ОК11. ОК4: залік, іспит.
		Педагогіка та психологія у вищій школі	Проблемні лекції; міждисциплінарні кейси; дискусії щодо професійних та педагогічних ситуацій; самостійне опрацювання джерел	Поточне та рубіжне оцінювання: Оцінювання розв'язання комплексного кейсу та аргументації; тематичне тестування. Підсумковий контроль: Іспит: ОК1, ОК6. Залік: ОК2, ОК11. ОК4: залік, іспит.
		Корпоративна та професійна етика в кібербезпеці	Проблемні лекції; міждисциплінарні кейси; дискусії щодо професійних та педагогічних ситуацій; самостійне опрацювання джерел.	Поточне та рубіжне оцінювання: Оцінювання розв'язання комплексного кейсу та аргументації; тематичне тестування. Підсумковий контроль: Іспит: ОК1, ОК6. Залік: ОК2, ОК11. ОК4: залік, іспит.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	☒	Преддипломна практика	Дослідницькі завдання; планування експерименту; лабораторні дослідження; індивідуальні консультації; підготовка наукового проєкту.	Поточне та рубіжне оцінювання: Оцінювання плану дослідження, експериментальних результатів і наукового звіту. Підсумковий контроль: Іспит: ОК5, ОК9. Залік: ОК3, ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Науково-дослідна практика	Дослідницькі завдання; планування експерименту; лабораторні дослідження; індивідуальні консультації; підготовка наукового	Поточне та рубіжне оцінювання: Оцінювання плану дослідження, експериментальних результатів і наукового

			проєкту.	звіту. Підсумковий контроль: Іспит: ОК5, ОК9. Залік: ОК3, ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Радіомоніторинг і радіопротидія на об'єктах ІД	Дослідницькі завдання; планування експерименту; лабораторні дослідження; індивідуальні консультації; підготовка наукового проєкту.	Поточне та рубіжне оцінювання: Оцінювання плану дослідження, експериментальних результатів і наукового звіту. Підсумковий контроль: Іспит: ОК5, ОК9. Залік: ОК3, ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки	☒	Преддипломна практика	Практичні розрахунки; фізичне й математичне моделювання; обробка експериментальних даних; розроблення та перевірка технічних рішень.	Поточне та рубіжне оцінювання: Перевірка розрахунків, моделей та їх валідації; захист практичних результатів. Підсумковий контроль: Іспит: ОК9. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Науково-дослідна практика	Практичні розрахунки; фізичне й математичне моделювання; обробка експериментальних даних; розроблення та перевірка технічних рішень.	Поточне та рубіжне оцінювання: Перевірка розрахунків, моделей та їх валідації; захист практичних результатів. Підсумковий контроль: Іспит: ОК9. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Радіомоніторинг і радіопротидія на об'єктах ІД	Практичні розрахунки; фізичне й математичне моделювання; обробка експериментальних даних; розроблення та перевірка технічних рішень.	Поточне та рубіжне оцінювання: Перевірка розрахунків, моделей та їх валідації; захист практичних результатів. Підсумковий контроль: Іспит: ОК9. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.	☒	Преддипломна практика	Критичний огляд наукових джерел; дослідницькі семінари; зіставлення альтернативних підходів; самостійна робота над проблемою дослідження	Поточне та рубіжне оцінювання: Оцінювання аналітичного огляду, критичного зіставлення підходів та обґрунтування проблеми. Підсумковий контроль: Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Науково-дослідна практика	Критичний огляд наукових джерел; дослідницькі семінари; зіставлення альтернативних підходів; самостійна робота над проблемою дослідження	Поточне та рубіжне оцінювання: Оцінювання аналітичного огляду, критичного зіставлення підходів та обґрунтування проблеми. Підсумковий контроль: Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
РН7. Обґрунтовувати використання, впроваджувати та	☒	Теорія захисту інформаційних ресурсів обмеженого доступу	Проблемні лекції; порівняльний аналіз стандартів; практичні кейси впровадження вимог;	Поточне та рубіжне оцінювання: Тематичне тестування; оцінювання аналізу стандартів та

аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.			підготовка фрагментів технічної документації.	обґрунтування їх застосування. Підсумковий контроль: Іспит: ОК5, ОК6, ОК7, ОК8, ОК9, ОК10.
		Технологія створення та застосування комплексів засобів захисту інформації з обмеженим доступом та охорони ОІД	Проблемні лекції; порівняльний аналіз стандартів; практичні кейси впровадження вимог; підготовка фрагментів технічної документації.	Поточне та рубіжне оцінювання: Тематичне тестування; оцінювання аналізу стандартів та обґрунтування їх застосування. Підсумковий контроль: Іспит: ОК5, ОК6, ОК7, ОК8, ОК9, ОК10.
		Радіомоніторинг і радіопротидія на об'єктах ІД	Проблемні лекції; порівняльний аналіз стандартів; практичні кейси впровадження вимог; підготовка фрагментів технічної документації.	Поточне та рубіжне оцінювання: Тематичне тестування; оцінювання аналізу стандартів та обґрунтування їх застосування. Підсумковий контроль: Іспит: ОК5, ОК6, ОК7, ОК8, ОК9, ОК10.
		Організація і проведення спеціальних досліджень на обєкті інформаційної діяльності	Проблемні лекції; порівняльний аналіз стандартів; практичні кейси впровадження вимог; підготовка фрагментів технічної документації	Поточне та рубіжне оцінювання: Тематичне тестування; оцінювання аналізу стандартів та обґрунтування їх застосування. Підсумковий контроль: Іспит: ОК5, ОК6, ОК7, ОК8, ОК9, ОК10.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	☒	Технологія створення та застосування комплексів засобів захисту інформації з обмеженим доступом та охорони ОІД	Проєктне навчання; лабораторне дослідження засобів захисту; моделювання систем; практичні завдання на супроводження та вдосконалення захисту	Поточне та рубіжне оцінювання: Оцінювання проєкту системи захисту, результатів випробувань і рекомендацій із супроводження. Підсумковий контроль: Іспит: ОК6, ОК7, ОК8, ОК9, ОК10. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Теорія захисту інформаційних ресурсів обмеженого доступу	Проєктне навчання; лабораторне дослідження засобів захисту; моделювання систем; практичні завдання на супроводження та вдосконалення захисту	Поточне та рубіжне оцінювання: Оцінювання проєкту системи захисту, результатів випробувань і рекомендацій із супроводження. Підсумковий контроль: Іспит: ОК6, ОК7, ОК8, ОК9, ОК10. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Преддипломна практика	Проєктне навчання; лабораторне дослідження засобів захисту; моделювання систем; практичні завдання на супроводження та вдосконалення захисту	Поточне та рубіжне оцінювання: Оцінювання проєкту системи захисту, результатів випробувань і рекомендацій із супроводження. Підсумковий контроль: Іспит: ОК6, ОК7, ОК8, ОК9, ОК10. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Науково-дослідна практика	Проєктне навчання; лабораторне дослідження засобів захисту; моделювання систем; практичні завдання на супроводження та вдосконалення захисту	Поточне та рубіжне оцінювання: Оцінювання проєкту системи захисту, результатів випробувань і рекомендацій із супроводження. Підсумковий контроль: Іспит: ОК6, ОК7, ОК8, ОК9, ОК10. Залік: ОК12, ОК13.

				ОК14: публічний захист кваліфікаційної роботи.
		Організація і проведення спеціальних досліджень на обєкті інформаційної діяльності	Проєктне навчання; лабораторне дослідження засобів захисту; моделювання систем; практичні завдання на супроводження та вдосконалення захисту	Поточне та рубіжне оцінювання: Оцінювання проєкту системи захисту, результатів випробувань і рекомендацій із супроводження. Підсумковий контроль: Іспит: ОК6, ОК7, ОК8, ОК9, ОК10. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Радіомоніторинг і радіопротидія на об'єктах ІД	Проєктне навчання; лабораторне дослідження засобів захисту; моделювання систем; практичні завдання на супроводження та вдосконалення захисту	Поточне та рубіжне оцінювання: Оцінювання проєкту системи захисту, результатів випробувань і рекомендацій із супроводження. Підсумковий контроль: Іспит: ОК6, ОК7, ОК8, ОК9, ОК10. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки	☒	Технологія створення та застосування комплексів засобів захисту інформації з обмеженим доступом та охорони ОІД	Проблемна лекція; кейс розроблення політики безпеки; проєктування системи управління; обговорення сценаріїв її супроводження.	Поточне та рубіжне оцінювання: Оцінювання проєкту політики та системи управління безпекою; усний захист рішення. Підсумковий контроль: Іспит: ОК7.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	☒	Преддипломна практика	Ситуаційні завдання з аналізу ризиків; моделювання загроз; практичне виявлення вразливостей; розроблення заходів безперервності процесів	Поточне та рубіжне оцінювання: Оцінювання реєстру ризиків, аналізу вразливостей і плану безперервності процесів. Підсумковий контроль: Іспит: ОК5, ОК8, ОК10. Залік: ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Організація і проведення спеціальних досліджень на обєкті інформаційної діяльності	Ситуаційні завдання з аналізу ризиків; моделювання загроз; практичне виявлення вразливостей; розроблення заходів безперервності процесів	Поточне та рубіжне оцінювання: Оцінювання реєстру ризиків, аналізу вразливостей і плану безперервності процесів. Підсумковий контроль: Іспит: ОК5, ОК8, ОК10. Залік: ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Теорія захисту інформаційних ресурсів обмеженого доступу	Ситуаційні завдання з аналізу ризиків; моделювання загроз; практичне виявлення вразливостей; розроблення заходів безперервності процесів	Поточне та рубіжне оцінювання: Оцінювання реєстру ризиків, аналізу вразливостей і плану безперервності процесів. Підсумковий контроль: Іспит: ОК5, ОК8, ОК10. Залік: ОК13. ОК14: публічний захист кваліфікаційної роботи.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології	☒	Технологія створення та застосування комплексів засобів захисту інформації з обмеженим доступом та охорони ОІД	Лекції з демонстраціями; лабораторне оцінювання захищеності; аналіз вразливостей; практичні кейси вибору комплексу засобів захисту.	Поточне та рубіжне оцінювання: Захист лабораторних робіт; оцінювання звіту про захищеність і запропонованих заходів. Підсумковий контроль:

створення та використання спеціалізованого програмного забезпечення.				Іспит: ОК7.
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації	☒	Преддипломна практика	Лабораторні та практичні роботи із системами доступу; моделювання ролей і повноважень; аналіз політик; перевірка ефективності контролю доступу.	Поточне та рубіжне оцінювання: Захист лабораторних робіт; оцінювання матриці доступу та результатів перевірки політик. Підсумковий контроль: Іспит: ОК7, ОК8, ОК9, ОК10. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Науково-дослідна практика	Лабораторні та практичні роботи із системами доступу; моделювання ролей і повноважень; аналіз політик; перевірка ефективності контролю доступу.	Поточне та рубіжне оцінювання: Захист лабораторних робіт; оцінювання матриці доступу та результатів перевірки політик. Підсумковий контроль: Іспит: ОК7, ОК8, ОК9, ОК10. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Організація і проведення спеціальних досліджень на обєкті інформаційної діяльності	Лабораторні та практичні роботи із системами доступу; моделювання ролей і повноважень; аналіз політик; перевірка ефективності контролю доступу.	Поточне та рубіжне оцінювання: Захист лабораторних робіт; оцінювання матриці доступу та результатів перевірки політик. Підсумковий контроль: Іспит: ОК7, ОК8, ОК9, ОК10. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Радіомоніторинг і радіопротидія на об'єктах ІД	Лабораторні та практичні роботи із системами доступу; моделювання ролей і повноважень; аналіз політик; перевірка ефективності контролю доступу.	Поточне та рубіжне оцінювання: Захист лабораторних робіт; оцінювання матриці доступу та результатів перевірки політик. Підсумковий контроль: Іспит: ОК7, ОК8, ОК9, ОК10. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Технологія створення та застосування комплексів засобів захисту інформації з обмеженим доступом та охорони ОІД	Лабораторні та практичні роботи із системами доступу; моделювання ролей і повноважень; аналіз політик; перевірка ефективності контролю доступу.	Поточне та рубіжне оцінювання: Захист лабораторних робіт; оцінювання матриці доступу та результатів перевірки політик. Підсумковий контроль: Іспит: ОК7, ОК8, ОК9, ОК10. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.
		Теорія захисту інформаційних ресурсів обмеженого доступу	Лабораторні та практичні роботи із системами доступу; моделювання ролей і повноважень; аналіз політик; перевірка ефективності контролю доступу.	Поточне та рубіжне оцінювання: Захист лабораторних робіт; оцінювання матриці доступу та результатів перевірки політик. Підсумковий контроль: Іспит: ОК7, ОК8, ОК9, ОК10. Залік: ОК12, ОК13. ОК14: публічний захист кваліфікаційної роботи.