НАЦІОНАЛЬНЕ АГЕНТСТВО ІЗ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	**Державний університет інформаційно-комунікаційних технологій**
Освітня програма	**58269 Управління інформаційною та кібернетичною безпекою**
Рівень вищої освіти	**Магістр**
Спеціальність	**125 Кібербезпека та захист інформації**

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

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

Використані скорочення:

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

Загальні відомості

1. Інформація про ЗВО (ВСП ЗВО)

Реєстраційний номер ЗВО у ЄДЕБО	**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	**www.dut.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	**58269**
Назва ОП	**Управління інформаційною та кібернетичною безпекою**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека та захист інформації**
Спеціалізація (за наявності)	*відсутня*
Рівень вищої освіти	**Магістр**
Тип освітньої програми	**Освітньо-професійна**
Вступ на освітню програму здійснюється на основі ступеня (рівня)	**Бакалавр, Магістр (ОКР «спеціаліст»)**
Структурний підрозділ (кафедра або інший підрозділ), відповідальний за реалізацію ОП	**кафедра управління інформаційною та кібернетичною безпекою, Навчально-науковий інститут захисту інформації**
Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП	**Навчально-науковий інститут захисту інформації: кафедра інформаційної та кібернетичної безпеки; кафедра систем інформаційного та кібернетичного захисту. Навчально-науковий інститут телекомунікацій: кафедра української мови)**
Місце (адреса) провадження освітньої діяльності за ОП	**Україна, 03110, м. Київ, вул. Солом'янська, 7**
Освітня програма передбачає присвоєння професійної кваліфікації	*передбачає*
Професійна кваліфікація, яка присвоюється за ОП (за наявності)	**Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою**
Мова (мови) викладання	**Українська, Англійська**
ID гаранта ОП у ЄДЕБО	**150389**
ПІБ гаранта ОП	**Легомінова Світлана Володимирівна**
Посада гаранта ОП	**завідувач кафедри**
Корпоративна електронна адреса гаранта ОП	**s.legominova@duikt.edu.ua**
Контактний телефон гаранта ОП	**+38(095)-487-67-05**
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

Освітньо-професійна програма «Управління інформаційною та кібернетичною безпекою» другого (магістерського) рівня вищої освіти й інші нормативні документи Державного університету інформаційно-комунікаційних технологій (ДУІКТ) визначає, мету, цілі та зміст підготовки фахівців за спеціальністю 125 Кібербезпека та захист інформації освітньої кваліфікації магістра з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою (УІКБ).
Потреба в зазначеній ОПП пов'язана з необхідністю:
1) підготовки висококваліфікованих фахівців - магістрів, здатних проводити наукові дослідження у сфері УІКБ, практично впроваджувати інноваційні наукові результати, ефективно вирішувати управлінські й науково-дослідні завдання з УІКБ.
2) формування кадрового резерву викладачів ДУІКТ і фахівців вищої кваліфікації для діяльності в галузі кібербезпеки і захисту інформації.
Стратегія розвитку ДУІКТ https://duikt.edu.ua/uploads/p_949_11377077.pdf акцентує увагу на підготовці конкурентоспроможного людського капіталу для високотехнологічного та інноваційного розвитку держави.
ОПП «Управління інформаційною та кібернетичною безпекою» є логічним продовженням ОПП «Управління інформаційною безпекою», яку було запроваджено в ДУТ з 2016 року. Необхідність запровадження ОП з новою назвою пов'язана з ухваленням Постанови КМ України від 16.12.2022 №1392, якою було введено нову спеціальність «257 Управління інформаційною безпекою» в галузі знань «25 Воєнні науки, національна безпека, безпека державного кордону», та з метою розмежування ОПП та нової спеціальності за назвою.
На момент запровадження ОПП у 2016 р. Державний університет телекомунікацій (ДУТ), який з 2023 року перейменовано на ДУІКТ, здійснював ступеневу освіту зі спеціальності 125 Кібербезпека за освітнім рівнем «бакалавр».
Для розробки оновленої ОПП «Управління інформаційною та кібернетичною безпекою» другого (магістерського) рівня вищої освіти, рішенням Вченої ради ДУІКТ був схвалений склад робочої та проектної групи (протокол № 15 від 26 квітня 2023 р.) і затверджений наказом ректора № 58 від 26 квітня 2023 р.
Члени робочої групи здійснили детальний аналіз ринку праці, вивчили вимоги роботодавців до кваліфікацій і компетентностей фахівців з УІКБ, за результатами якого була розроблена ОПП. Програма базується на положеннях Державного стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти, затвердженого і введеного в дію наказом МОН України від 18.03.2021 р. № 332.
У відповідності з ОПП розроблені навчальний план підготовки та індивідуальні плани здобувачів кваліфікації магістра з кібербезпеки.
Підготовка здобувачів за ОПП здійснюється на базі трьох кафедр Навчально-наукового інституту захисту інформації (управління інформаційною та кібернетичною безпекою, інформаційної та кібернетичної безпеки, систем інформаційного та кібернетичного захисту) та Навчально-наукового інституту телекомунікацій (кафедра української мови).

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	2024 - 2025	90	40	0
2 курс	2023 - 2024	90	37	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	**58820 Інформаційна та кібернетична безпека** **58822 Технічні системи інформаційного та кібернетичного захисту** **58823 Управління інформаційною та кібернетичною безпекою**
другий (магістерський) рівень	**58819 Технічні системи інформаційного та кібернетичного захисту**

	58810 Інформаційна та кібернетична безпека **58269 Управління інформаційною та кібернетичною безпекою**
третій (освітньо-науковий/освітньо-творчий) рівень	**59589 Кібербезпека**

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_2024_ІБ_!.pdf*	3e055jZCyquQUA09uQMYsOfR5fSPyH32+Wtd/xgqcxk=
Навчальний план за ОП	*НП_2024.pdf*	+2NiOIFz8ajXMSIUUP617XXq/W7OMtF71TEsSjJmvAI=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Рецензія IT Сеціаліст.pdf*	zUacwzHksLPIL3IkBYcsysbWC/7btqL9TRrTf/2Xc9w=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Рецензія_Ec Ti.pdf*	Utunsmn90IqOLmL1lLosny2rfiHPpB9VMvtDZZqFOMU=

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 ОПП повністю відповідає програмним результатам навчання (РН), що сформульовані у Стандарті вищої освіти України другого (магістерського) рівня, галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека, затвердженому і введеному в дію наказом МОН України від 18.03.2021 р. № 332. З метою співвіднесення програмних РН і компетентностей, зазначених в ОПП, у процесі її розроблення використані: структуро-логічна схема й матриця відповідності визначених РН та компетентностей компонентам програми (таблиці 4 та 5 ОПП). Зміст ОПП сприяє досягненню програмних РН через вивчення дисциплін, які дозволяють здобувачам набути основні загальні (КЗ) й фахові компетентності (КФ). Так, наприклад, діючий стандарт вищої освіти України визначає як фахову компетентність «КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог». Зазначена компетентність в ОПП забезпечується освітніми компонентами «Системи управління інформаційною безпекою», «Прикладна загальна теорія систем інформаційної та кібербезпеки», «Управління проєктами

інформаційної безпеки». У свою чергу зазначені освітні компоненти забезпечують досягнення програмних результатів РН 9, 16 стосовно КФ4.
Також, для розвитку soft skills (загальних компетентностей) передбачено вивчення таких освітніх компонент програми як «Корпоративна та професійна етика в кібербезпеці» (РН 1, 7, 15, 16, 18), «Організація проведення наукових досліджень» (РН 2, 3, 5, 7, 20, 22), «Науково-технічний переклад» (РН 1, 3, 7, 15).
Таким чином, можна констатувати, що діюча ОПП дає можливість досягти РН, визначених Стандартом вищої освіти України другого (магістерського) рівня, галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека та захист інформації.

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

Затверджені на сьогоднішній день професійні стандарти неодноразово обговорювалися під час перегляду ОПП та бралися до уваги при перегляді змісту освітніх компонент.
https://duikt.edu.ua/ua/news-1-611-11674-obgovorennya-na-kafedri-uikb-dokumentiv-vid-administracii-derzhavnoi-sluzhbi-specialnogo-zvyazku--po-polipshennyu-sistemi-osvitno-profesiynoi-standartizacii-ta-sertifikacii-kadriv-u-sferi-kiberbezpeki_kafedra-upravlinnya-informaciynoyu-ta-kibernetichnoyu-bezpekoyu

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

Інтереси здобувачів вищої освіти враховуються під час обговорення пропозицій щодо покращення змісту й структури ОПП, яке проводилося на засіданнях кафедри, а також під час різноманітних наукових заходів, які проводяться в університеті
https://duikt.edu.ua/ua/news-1-611-11498-naukovo-metodichne-zasidannya-kafedri-uikb_kafedra-upravlinnya-informaciynoyu-ta-kibernetichnoyu-bezpekoyu,
зустрічей студентів-магістрів з представниками ІТ компаній
https://duikt.edu.ua/ua/news-1-611-11500-spivpracya-kafedri-uikb-z-dp-es-end-ti-ukraina_kafedra-upravlinnya-informaciynoyu-ta-kibernetichnoyu-bezpekoyu;
https://duikt.edu.ua/ua/news-1-611-12690-yarmarka-vakansiy-kompanii-partneri-integruyut-studentiv-duikt-v-svit-it-industrii_kafedra-upravlinnya-informaciynoyu-ta-kibernetichnoyu-bezpekoyu
засідань Вченої ради Навчально-наукового інституту захисту інформації, на яких обговорюються питання оновлення ОПП та її освітніх компонентів.
Під час таких зустрічей студенти-магістри неодноразово висловлювали побажання та рекомендації, які в подальшому були враховані та сформовані у вигляді цілей програми і мають своє відображення у програмних РН, зокрема: здійснення процедур оцінювання й розслідування інцидентів безпеки; аналіз, розробка і супровід систем аудиту й моніторингу ефективності функціонування систем УІКБ; розробка, реалізація і супровід проєктів з УІКБ, інноваційної діяльності та захисту інтелектуальної власності.

- роботодавці

Представники роботодавців брали участь у зовнішній експертизі ОПП як на етапі її формування, так і на етапі її оновлення.
Рецензентами оновленої ОПП стали: директор ТОВ «ІТ Спеціаліст» Морозов О.Ю. та директор ДТ «ЕС ЕНД ТІ Україна» Лисецький Ю.М., які відзначили, що оновлена ОПП враховує інноваційні аспекти захисту інформації й відображає зміни у підходах до УІКБ як організаційного, так і технічного характеру. У результаті постійного удосконалення ОПП забезпечує належну підготовку фахівців вищої категорії у відповідності з вимогами роботодавців сучасного ринку праці та підтверджує здатність ДУІКТ якісно готувати висококваліфікованих фахівців у сфері інформаційної та кібербезпеки.
Крім того, ОПП постійно моніториться представниками компанії «ІТ Спеціаліст», з якою підписано договір щодо співпраці з питань удосконалення змісту освітніх програм та освітнього процесу https://duikt.edu.ua/ua/news-1-611-11481-spivpracya-kafedri-uikb-z-kompanieyu-it-specialist_kafedra-upravlinnya-informaciynoyu-ta-kibernetichnoyu-bezpekoyu?lang=ua&act=view&page=1&category=611&id=11481&sys_link=spivpracya-kafedri-uikb-z-kompanieyu-it-specialist_kafedra-upravlinnya-informaciynoyu-ta-kibernetichnoyu-bezpekoyu

- академічна спільнота

При формулюванні фахових компетентностей і програмних РН були враховані інтереси та рекомендації академічної спільноти, зокрема фахівців, які працюють у сфері захисту інформації Київського національного університету ім. Т. Шевченка, Київського столичного університету ім. Б. Грінченка, Національного університету «Львівська політехніка» і наукових установ.
Завдяки рекомендаціям академічної спільноти до оновленої програми було введено ОК: «Управління ризиками інформаційної безпеки». Також було доопрацьовано зміст ОК «Системи управління інформаційною безпекою», «Управління проєктами інформаційної безпеки», а також освітніх компонент вільного вибору студента, зокрема «Управління безпекою інформаційних мереж», з урахуванням розвитку технологій кібербезпеки та захисту інформації.

- інші стейкхолдери

Крім міжнародних компаній (IBM, CISCO, HP, ESET) Університет активно співпрацює з вітчизняними

організаціями та установами: ТОВ «Smart Technologies», ТОВ «ІНФОРМАЦІЙНІ СПЕЦІАЛІЗОВАНІ СИСТЕМИ», Департаментом кіберполіції Національної поліції України щодо оновлення змісту ОК та ОПП https://duikt.edu.ua/ua/855-partneri-kafedri-kafedra-upravlinnya-informaciynoyu-bezpekoyu?lang=ua&id=855&sys_link=partneri-kafedri-kafedra-upravlinnya-informaciynoyu-bezpekoyu; https://duikt.edu.ua/ua/news-1-611-10933-pidtverdzhennya-na-kafedri-uikb-innovaciyniy-pidhid-do-yakisnogo-navchannya-v-dii_kafedra-upravlinnya-informaciynoyu-ta-kibernetichnoyu-bezpekoyu?lang=ua&act=view&page=1&category=611&id=10933&sys_link=pidtverdzhennya-na-kafedri-uikb-innovaciyniy-pidhid-do-yakisnogo-navchannya-v-dii_kafedra-upravlinnya-informaciynoyu-ta-kibernetichnoyu-bezpekoyu.
Створений на базі ДУІКТ ТК 107 «Технічний захист інформації», який є суб'єктом нацсистеми щодо розроблення, розгляду та погодження міжнародних (регіональних) та національних стандартів, що дозволяє формувати позиції України щодо нормативних документів та сприяти осучасненню ОПП https://duikt.edu.ua/ua/119-tehnichniy-komitet-tk-107-tehnichniy-zahist-informacii-nauka?lang=ua&id=119&sys_link=tehnichniy-komitet-tk-107-tehnichniy-zahist-informacii-nauka. Відповідно до наказу ДП «УкрНДНЦ» від 23 березня 2021 р. № 98 головою ТК 107 призначено д. т. н., професора Савченка В. А., заступником голови – к. т. н., доцента Дзюбу Т. М.
https://docs.google.com/document/d/1y45hdWlWUZGNVDoOY-BwC5SpDYh-Ku23/edit?pli=1

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

Відповідно до Стратегії розвитку ДУІКТ https://duikt.edu.ua/uploads/p_949_11377077.pdf, місією Університету є реалізація його суспільної ролі у розбудові держави через якісну освіту, наукові дослідження, розвиток творчої особистості з креативним мисленням, а однією із стратегічних цілей є підготовка конкурентоспроможного людського капіталу для високотехнологічного та інноваційного розвитку держави.
Виконання означених Стратегією завдань забезпечується:
– тісною співпрацею з ІТ-компаніями та державними установами http://surl.li/bulrjk;
– формуванням навчальних планів, які орієнтуються на новітні досягнення у галузі ІТ та кібербезпеки
http://surl.li/mpdvlk;
– відбором талановитої молоді з метою підготовки наукових і науково-педагогічних кадрів
http://surl.li/szwbfb;
http://surl.li/ubfemt.
– підготовкою студентів-магістрів до науково-педагогічної діяльності у ЗВО
http://surl.li/aljajr;
http://surl.li/zagvxx
– проведенням опитувань магістрів з приводу їх побажань щодо введення нових курсів та оцінки якості викладання дисциплін
1 курс https://duikt.edu.ua/uploads/p_1352_55431429.pdf;
2 курс https://duikt.edu.ua/uploads/p_1352_11964173.pdf;
Загально університетські опитування щодо якості освітніх програм і викладання
https://duikt.edu.ua/uploads/p_1352_14356761.pdf
https://duikt.edu.ua/uploads/p_1352_99675417.pdf

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

З метою моніторингу тенденцій розвитку науки і спеціальності викладачі та студенти кафедри беруть активну участь у науково-практичних заходах, організованих кафедрою, університетом, іншими установами й організаціями
http://surl.li/skqlur
http://surl.li/ncgzjl
http://surl.li/pfifei
http://surl.li/nnjufa
http://surl.li/loygud.
До обговорення залучаються колишні випускники ДУІКТ, зокрема К. Андрущенко, В. Самко, М. Ющенко (СвітІТ), М. Костроміна (Сітон), А. Вершигора (Harwind)
http://surl.li/ptobtm
http://surl.li/kwueba.
Крім того, здобувачі ступеня магістра та НПП постійно беруть участь у спеціалізованих заходах, зокрема у різноманітних змаганнях з кібербезпеки http://surl.li/zwgfnx,
Днях кар'єри, ярмарках вакансій http://surl.li/qowxvi
http://surl.li/qfgyoa
та заходах Держспецзв'язку http://surl.li/kpzwyo.
Під час таких заходів обговорювались зміни до ОПП, зокрема: питання захисту інформаційних систем та мережевої інфраструктури - РН 18, 19, 20, 22; створення комплексних автоматизованих систем захисту - РН 11, 14, 16, 17, 21, 23; тенденції розвитку науки у галузі інформаційної та кібербезпеки - РН 3, 5, 7, 8, 9, 12, 20.

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

Участь компаній-партнерів кафедри в освітньому процесі обумовлює набуття здобувачами ступеня магістра з кібербезпеки за ОПП Управління інформаційною та кібернетичною безпекою переліку компетентностей з урахуванням вимог та очікувань потенційних роботодавців. Упродовж навчання за ОПП здобувачі отримують затребувані ринком праці освітні та дослідницькі навички, які відображені у програмних результатах ОПП. Такий результат досягається шляхом співпраці з провідними організаціями галузі (галузевий контекст): Департаментом Кіберполіції Національної поліції України (Меморандум від 18.03.2021 № 21/ННІЗІ/342), ТОВ «ІТ Спеціаліст»

(договір від 23.01.2020 № 34/1294), рекомендації яких щодо підвищеної уваги до захисту об'єктів інформаційної діяльності були враховані при формуванні РН 8, 13, 19.
Регіональний контекст формується на співпраці переважно з комерційними підприємствами та приватними закладами освіти, які провадять професійну дослідницьку діяльність у галузі кібербезпеки та захисту інформації, зокрема Міжнародна Кіберакадемія (договір від 28.10.2019 № 10/2019), у співпраці з якою було сформульовано результати щодо методології наукового дослідження (РН 8, 12, 13, 22).
Наявність зазначених договорів і тісна співпраця з компаніями дозволяє Університету не лише визначати пріоритетні напрями розвитку спеціальності, формувати необхідні компетентності, а й проводити наукові дослідження на базі цих підприємств та організацій.

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

Під час оновлення ОПП було проаналізовано відповідні програми інших ЗВО України, зокрема:
КНУ ім. Тараса Шевченка ОНП Кібербезпека https://kbzi.knu.ua/onp_magistr_2023/
НТУУ «КПІ ім. Сікорського» ОПП Системи, технології та математичні методи кібербезпеки https://osvita.kpi.ua/sites/default/files/opfiles/125_oppm_stmmkb_2024.pdf
НУ «Львівська політехніка» ОПП Управління інформаційною безпекою https://lpnu.ua/sites/default/files/2021/program/15321/125-mag-opp-uib-2023.PDF

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

Чи мета освітньої програми та програмні результати навчання визначаються з урахуванням досвіду аналогічних іноземних освітніх програм? довге поле
З метою запозичення кращих закордонних практик підготовки фахівців з інформаційної та кібербезпеки вивчено досвід реалізації магістерських програм в іноземних ЗВО:
Mississippi State University (США) https://www.cse.msstate.edu/grad/ms-cyso/ – на основі програми The Master of Science in Cyber Security and Operations (MS CYSO) було сформовано РН 2, 16, 23.
Capitol Technology University (США) https://www.captechu.edu/degrees-and-programs/masters-degrees/cybersecurity-ms – курс Master of Science (MS) in Cybersecurity дав підстави для коригування РН 9, 10.
Dakota State University (США) https://dsu.edu/programs/mscd/index.html – з урахуванням змісту й очікуваних результатів програми Cyber Defense Master of Science (MSCD) було вдосконалено дисципліну «Корпоративна та професійна етика в кібербезпеці» (РН 15, 16).
Відмінністю даної ОПП від розглянутих програм є те, що вона базується на поєднанні фундаментальних теоретичних і практичних знань з акцентом на сучасних методах і підходах розв'язання складних управлінських і технічних завдань захисту інформації, вирішення проблем інформаційної та кібербезпеки в правовому полі та з урахуванням етичних аспектів, розробки та створення ефективних технологій запобігання і подолання загроз безпеці інформації, завдяки чому забезпечується конкурентоспроможність програми «Управління інформаційною та кібернетичною безпекою» серед вітчизняних та іноземних аналогів.

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 повністю забезпечують реалізацію поставленої мети та відповідають предметній області спеціальності 125 «Кібербезпека та захист інформації».
Базові компоненти ОПП «Організація проведення наукових досліджень», «Системи управління інформаційною безпекою», «Прикладна загальна теорія систем інформаційної та кібербезпеки» забезпечують теоретичний зміст предметної області та оволодіння основними методами, методиками і технологіями, які застосовуються в галузі інформаційної та кібербезпеки. Процес вивчення цих компонент формує навички та вміння використання системного підходу до вирішення завдань УІКБ.
Компоненти ОПП, спрямовані на поглиблене оволодіння окремими аспектами УІКБ, для їх теоретичного

осмислення та практичного застосування у подальших наукових дослідженнях у розрізі тематики наукових досліджень, обираються студентами в каталозі освітніх компонент вільного вибору: https://duikt.edu.ua/ua/2080-katalog-osvitnih-komponentiv-vilnogo-viboru-studentami-navchannya.
У результаті аналізу ОПП можна зробити висновок, що здобувачі засвоюють знання й навички використання сучасних підходів до УІКБ з метою якісного проведення наукових досліджень, практичного впровадження інноваційних наукових результатів, ефективного вирішення управлінських і науково-дослідних завдань з УІКБ.

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

Основним інструментом формування індивідуальної освітньої траєкторії (ІОТ) є вибіркові дисципліни, частка яких складає 25 кредитів (28% ОПП). Формування ІОТ базується на індивідуальному виборі кожного студента-магістра, що передбачено
Положенням про організацію освітнього процесу в ДУІКТ https://duikt.edu.ua/uploads/p_447_49109699.pdf,
Положенням про порядок організації права на академічну мобільність
https://duikt.edu.ua/uploads/p_447_36289291.pdf,
Положенням про формування індивідуальних освітніх траєкторій здобувачів вищої освіти у Державному університеті інформаційно-комунікаційних технологій
https://duikt.edu.ua/uploads/p_447_22834975.pdf
і регламентується через такі процедури: самостійне обрання вибіркових компонентів навчального плану; створення індивідуального навчального плану студента; участь у програмах академічної мобільності; складання індивідуальних графіків навчання та сесії; отримання права на академічну відпустку, зокрема з причин навчання в інших освітніх установах; визнання результатів навчання, отриманих в інших ЗВО.
Всі студенти ОПП проходять процедуру обрання вибіркових дисциплін з Каталогу освітніх компонент вільного вибору (http://surl.li/cgotwd) та формування індивідуального плану. Студент має право вибору дисциплін не лише за спеціальністю навчання, а, за необхідності, і з інших спеціальностей.

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

Вибір навчальних дисциплін в університеті регламентовано Положенням про формування індивідуальних освітніх траєкторій здобувачів вищої освіти у ДУІКТ https://duikt.edu.ua/uploads/p_447_22834975.pdf.
Положення містить основні вимоги щодо здійснення права вибору відповідно до пункту 15 частини першої статті 62 Закону України «Про вищу освіту» № 1556-VII від 01.07.2014 року. З точки зору студента магістратури ОПП процес вибору навчальних дисциплін виглядає таким чином:
перший крок: на початку навчального року студенти знайомляться на сайті з переліком вибіркових компонентів ОПП (за циклами підготовки для поточного та наступного семестрів) та силабусами цих компонентів, підготовлені кафедрами ННІЗІ та інших інститутів Університету;
другий крок: після ознайомлення із запропонованими матеріалами та відповідно до особисто визначеної освітньої траєкторії, здобувачі мають самостійно сформувати перелік вибіркових компонентів ОПП для свого індивідуального навчального плану (студент може звернутися за консультацією до завідувача кафедри);
третій крок: навчальна частина ННІЗІ організовує роботу з формування списків навчальних груп для вивчення обраних вибіркових компонентів ОПП та формує розклад занять;
четвертий крок: обрані студентом вибіркові компоненти ОПП вносяться до його індивідуального навчального плану.
Перелік дисциплін для вибору здобувачами ОПП (не менше 25 % загальної кількості кредитів ЄКТС від обсягу ОПП) наведено у Каталозі освітніх компонент вільного вибору (https://duikt.edu.ua/ua/2080-katalog-osvitnih-komponentiv-vilnogo-viboru-studentami-navchannya?lang=ua&id=2080&sys_link=katalog-osvitnih-komponentiv-vilnogo-viboru-studentami-navchannya). Здобувачі ОПП мають право обирати дисципліни, які запропоновані іншими кафедрами Університету, за погодженням з директором навчально-наукового інституту.

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

За ОПП передбачено проходження студентами науково-педагогічної практики (6 кредитів), яке регламентується Положенням про проведення практики в ДУІКТ https://duikt.edu.ua/uploads/p_447_23214805.pdf, програмами практики для спеціальності 125 «Кібербезпека та захист інформації» галузі знань 12 «Інформаційні технології» (наведено у таблиці 1 додатку).
Загальні засади організації, проведення, звітування й оцінювання результатів проходження науково-педагогічної (НПП), науково-дослідної (НДП) і переддипломної практики (ПП) студентів магістратури визначені у програмах:
https://duikt.edu.ua/uploads/p_366_55804317.pdf
https://duikt.edu.ua/uploads/p_366_48742927.pdf
https://duikt.edu.ua/uploads/p_366_96359229.pdf
Базою НПП є кафедри ННІЗІ ДУІКТ. НПП проводиться під керівництвом досвідчених викладачів кафедри.
http://surl.li/mkvtgf
http://surl.li/zfqjbe
http://surl.li/hereai
Базою НПП і ПП може бути компанія-партнер кафедри або, в разі самостійного обрання здобувачем місця практики, - підприємства й організації муніципального, державного та корпоративного управління.
http://surl.li/heslau
http://surl.li/hxetnq

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

Окрім професійних навичок, важливим елементом професійного портрету фахівця в сучасному світі є soft skills, тобто певного набору рис і знань, які допомагають йому здійснювати взаємодію й успішно спілкуватися з іншими спеціалістами галузі.
ОПП дозволяє студенту набути навички етичного поводження у професійному середовищі й ефективної комунікації, в т.ч. англійською мовою як мовою міжнародного спілкування (дисципліни «Корпоративна та професійна етика в кібербезпеці» (РН 1, 7, 15, 16), «Науково-технічний переклад» (РН 1, 3), вдосконалити аналітичні навички, здатність навчатися й організовувати свій час під час науково-дослідницької і викладацької діяльності «Організація проведення наукових досліджень» (РН 3, 17, 20, 22) та «Педагогіка та психологія у вищій школі» (РН 1, 2, 17, 18).
Зазначені дисципліни забезпечують набуття soft skills у рамках загальних компетентностей.
Крім того, розвиток soft skills, а саме навички командної роботи й ефективної комунікації в проєктній групі, забезпечується також під час вивчення дисципліни «Управління проєктами інформаційної безпеки» (РН 4, 8, 9, 14, 17, 20), що забезпечують набуття фахових компетентностей. Ці освітні компоненти сприяють розвитку освітньої та професійної складових ОПП і дозволяють випускнику на належному рівні проводити наукові дослідження, реалізувати отримані наукові результати на практиці, ефективно вирішувати управлінські й науково-дослідницькі завдання в галузі інформаційної та кібербезпеки.

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

Відповідно до встановлених вимог ОПП охоплює цикл компонент загальної та професійної підготовки. У рамках першого циклу ОПП забезпечує оволодіння здобувачами практичних умінь і навичок наукової і викладацької діяльності. До освітніх компонентів, які формують комплекс компетентностей загальної підготовки, відносяться «Педагогіка та психологія у вищій школі», «Організація проведення наукових досліджень», «Науково-технічний переклад».
Цикл компонент професійної підготовки спрямований на формування набору фахових компетентностей фахівця з УІКБ, який охоплює глибокі знання засад ефективного впровадження, супроводу й оцінювання систем управління інформаційною безпекою, здатність до аналізу, прогнозування й оцінювання ризиків інформаційній та кібербезпеці, вміння застосовувати методи ризик-орієнтованого і системного підходів, впроваджувати й удосконалювати заходи реагування на інциденти безпеки, реалізувати проєкти в галузі інформаційної та кібербезпеки.

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, який використовувався для співвіднесення обсягу компонентів ОПП, передбачає забезпечення досяжності й адекватності встановлених кредитів і визначених РН і навантаження з урахуванням самостійної роботи.
Відповідно до Положення про організацію освітнього процесу у ДУІКТ https://duikt.edu.ua/uploads/p_447_49109699.pdf тривалість теоретичного навчання, семестрового контролю та самостійної роботи складає 40 тижнів на рік. Загальний бюджет навчального часу складає 90 кредитів ЄКТС (2700 годин), з яких обсяг аудиторних становить 660 годин (24,4%), а обсяг самостійної роботи здобувачів становить 2040 годин (75,6%) https://duikt.edu.ua/uploads/p_1826_85331881.pdf.
Загальний обсяг часу, необхідного на виконання всіх видів семестрових завдань, рефератів, проєктів тощо не перевищує кількості передбачених навчальними планами годин на самостійну роботу студентів. Самостійна робота забезпечується системою навчально-методичних засобів, передбачених для вивчення конкретної навчальної дисципліни чи окремої теми: підручники, навчальні посібники, методичні матеріали, курси лекцій, практикуми, навчально-лабораторне обладнання тощо.
Підручники, навчальні посібники, конспекти лекцій, методичні рекомендації до проведення практичних / лабораторних /семінарських занять знаходяться в е-бібліотеці, яка відкрита для студентів Університету постійно.
Навчально-методичні матеріали з усіх освітніх компонентів ОПП розміщені в Google Class викладачів, і здобувачі мають доступ до них на період навчання.

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

Структура ОПП забезпечує набуття здобувачами практичних умінь і навичок науково-педагогічної діяльності у рамках освітніх компонентів «Педагогіка та психологія у вищій школі», «Організація проведення наукових досліджень», «Науково-технічний переклад» і науково-педагогічна практика. Завдяки цьому забезпечується поповнення викладацького складу кафедри.

У рамках компонентів професійної підготовки ОПП здобувачі удосконалюють набір фахових компетентностей з УІКБ, які передбачають знання засад ефективного впровадження, супроводу й оцінювання СУІБ («Системи управління інформаційною безпекою»), навички аналізу, прогнозування й оцінювання ризиків («Управління ризиками інформаційної безпеки»), вміння застосовувати методи системного підходу в галузі захисту інформації («Прикладна загальна теорія систем інформаційної та кібербезпеки»), реалізувати проєкти з УІКБ («Управління проєктами інформаційної безпеки»).
Навчання за дуальною формою регламентується Положенням про дуальну форму здобуття вищої освіти у ДУІКТ https://duikt.edu.ua/uploads/p_447_91663915.pdf. Підготовка здобувачів за дуальною формою освіти в рамках ОПП не здійснюється, але для підвищення якості освітньої підготовки й подолання розриву між теорією і практикою в ДУІКТ запроваджено практику залучення до освітнього процесу професіоналів-практиків (Д. Рабчун, К. Андрущенко), представників роботодавців (О. Стешенко, М. Ющенко) і працевлаштування випускників ОПП на посадах НПП в Університеті (М. Запорожченко, В. Тищенко).

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 Управління інформаційною та кібернетичною безпекою забезпечує набуття здобувачами низки актуальних і затребуваних навичок та компетентностей, серед яких зокрема не тільки професійні навички, такі як прогнозування й аналіз для запобігання динамічним ризикам і загрозам безпеці, швидке й ефективне реагування на інциденти з метою зменшення потенційних негативних наслідків для організації, але й т. зв. soft skills: уміння ефективно працювати в команді, забезпечувати успішну комунікацію, приймати оптимальні рішення в умовах обмеженого часу й даних тощо.
Володіння переліченими навичками і компетентностями дозволить фахівцям з УІКБ зробити свій вагомий внесок у досягнення глобальних цілей сталого розвитку до 2030 р., серед яких стале економічне зростання, повна і продуктивна зайнятість, створення стійкої інформаційно-комунікаційної інфраструктури, впровадження технологічних інновацій у галузі ІТ та захисту інформації.
Підготовка кваліфікованих фахівців з УІКБ сприятиме підвищенню рівня кваліфікації персоналу у цій сфері і, як наслідок, зростання результативності протидії інформаційним загрозам і підвищення рівня інформаційної та кібербезпеки в Україні. Крім цього впровадження зазначеної ОПП забезпечує надання комплексної та якісної освіти у галузі кібербезпеки та захисту інформації, заохочує здобувачів навчатися упродовж усього життя, підвищувати свій професійний рівень і сприяти зростанню захищеності інформаційних ресурсів та інфраструктури України.

3. Доступ до освітньої програми та визнання результатів навчання

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

Інформація про правила прийому на навчання для здобуття освітнього ступеня магістра містяться за посиланнями:
Правила прийому до ДУІКТ у 2024 році
https://duikt.edu.ua/uploads/p_108_92895538.pdf
строки прийому заяв та документів, конкурсного відбору та зарахування на навчання для здобуття освітнього ступеня магістра; https://duikt.edu.ua/uploads/p_108_96478899.pdf
програма вступних випробувань зі спеціальності 125 Кібербезпека та захист інформації, які проводяться для вступників пільгових категорій https://duikt.edu.ua/uploads/p_2642_53434670.pdf.
Абітурієнти, які закінчили бакалаврат у 2024 році, вступають в магістратуру на загальних підставах за результатами ЄДКІ та ЄВІ. Абітурієнти, які закінчили бакалаврат раніше 2024 року, вступають в магістратуру за результатами ЄВІ та ЄФВВ.
Усі питання, пов'язані зі вступом до Університету, вирішуються Приймальною комісією на її засіданнях. Рішення Приймальної комісії оприлюднюються на офіційному веб-сайті (https://duikt.edu.ua/ua/363-vstup-2024-priymalna-komisiya) в день прийняття або не пізніше наступного дня після прийняття відповідного рішення.

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

Нормативним документом для організації вступної кампанії до ДУІКТ, в т.ч. за даною ОПП є Правила прийому до ДУІКТ у 2024 році https://duikt.edu.ua/ua/108-pravila-priyomu-priymalna-komisiya, які визначають:
перелік освітніх ступенів та спеціальностей за якими оголошується прийом, ліцензовані обсяги та нормативні терміни навчання;
строки прийому заяв та документів, конкурсного відбору та зарахування на навчання;
перелік конкурсних предметів (вступних іспитів) та вагових коефіцієнтів до складових конкурсного балу для вступу на навчання для здобуття освітнього ступеня бакалавра, магістра;
перелік спеціальностей підготовки ДУІКТ, яким надається особлива підтримка;
таблиці переведення тестових балів НМТ, магістерського тесту навчальної компетентності до шкали 100-200;
перелік акредитованих спеціальностей та освітніх програм ДУІКТ, на які здійснюється вступ у 2024 р.;
критерії оцінювання мотиваційних листів вступників до ДУІКТ у 2024 р..
Правила прийому до магістратури передбачають диференційований підхід до різних категорій вступників:
випускники бакалаврату 2024 р. вступають за результатами ЄДКІ та ЄВІ;
абітурієнти, які закінчили бакалаврат раніше 2024 р., вступають за результатами ЄВІ та ЄФВВ;

вступники пільгових категорій вступають за результатами ЄВІ або внутрішнього іспиту з англійської мови та фахового іспиту, які складаються на базі Університету.

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, зокрема під час академічної мобільності, регулюються такими нормативними документами ДУІКТ:
Положенням про організацію освітнього процесу у ДУІКТ https://duikt.edu.ua/uploads/p_447_49109699.pdf;
Положенням про порядок організації права на академічну мобільність учасників освітнього процесу https://duikt.edu.ua/uploads/p_447_36289291.pdf;
Положенням про формування індивідуальних освітніх траєкторій здобувачів вищої освіти (п.8 Порядок зарахування та перезарахування кредитів в ІНП https://duikt.edu.ua/uploads/p_447_22834975.pdf.
Положенням про неформальну та інформальну освіту Державного університету інформаційно-комунікаційних технологій https://duikt.edu.ua/uploads/p_447_35048489.pdf
Поінформованість здобувачів вищої освіти про можливість визнання результатів навчання забезпечується наявністю відповідної нормативної бази у вільному доступі на сайті Університету та ознайомленням з документами під час оформлення договору про навчання (стажування) за програмою академічної мобільності.

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

Протягом терміну дії даної ОПП не виникало прецедентів визнання результатів навчання, які були отримані в інших ЗВО.

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 здобувачем за програмами неформальної освіти, регулюються Положенням про неформальну та інформальну освіту 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?file=p_949_73284553.pdf.
До результатів навчання, які зараховуються при виконанні ОПП, враховуючи особливості спеціальності 125 Кібербезпека та захист інформації в межах галузі 12 Інформаційні технології, відносяться результати отримані, зазвичай, у формальній освіті.
Результати навчання здобувачів освітнього рівня магістра, отриманих у неформальній освіті, визнаються у частині виконання ними професійної складової індивідуального плану здобувача.

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 даної ОПП не було.

4. Навчання і викладання за освітньою програмою

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

Освітній процес на ОПП відповідає вимогам законодавства, зокрема Закону України «Про вищу освіту» https://zakon.rada.gov.ua/laws/show/1556-18#Text у частинах: прийому на навчання до закладів вищої освіти на конкурсній основі; забезпечення права особи здобувати вищу освіту в різних формах або поєднувати їх; організації освітнього процесу у ЗВО за такими формами: навчальні заняття; самостійна робота; практична підготовка; контрольні заходи; проведення таких видів навчальних занять як: лекція; лабораторне, практичне, семінарське, індивідуальне заняття; консультація.
Форми й методи навчання і викладання за ОПП регулюються Положенням про організацію освітнього процесу у ДУІКТ https://duikt.edu.ua/uploads/p_447_49109699.pdf.
Відповідно до нього підготовка магістрів здійснюється за очною (денною) формою навчання. Підготовка в магістратурі Університету здійснюється за рахунок коштів Державного бюджету України або коштів юридичних і фізичних осіб.
Основними видами навчальних занять на ОПП є: лекції; практичні та лабораторні, семінарські й індивідуальні заняття, консультації. Застосовуються традиційні методи і прийоми, а також інтерактивні інноваційні методики, які пояснюються у силабусах за кожним освітнім компонентом відповідно до результатів навчання.
На сайті Університету розміщено ОПП, де представлені назви освітніх компонентів https://duikt.edu.ua/uploads/p_1826_84148070.pdf та

силабуси компонентів ОПП http://surl.li/njsxwj.

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?

Студентам ОПП забезпечено постійний доступ до підручників, навчальних посібників, конспектів лекцій та інших навчально-методичних матеріалів, які розміщені в електронній бібліотеці Університету й кафедри за посиланням https://duikt.edu.ua/ua/lib/1/category/2122. Доступ є відкритим упродовж усього терміну навчання.
Форми і методи навчання й викладання відповідають вимогам студентоцентрованого підходу, який забезпечується вибором індивідуальних завдань з окремих освітніх компонентів, в тому числі вибіркових https://duikt.edu.ua/ua/2080-katalog-osvitnih-komponentiv-vilnogo-viboru-studentami-navchannya.
Зворотний зв'язок зі студентами, який здійснюється систематично шляхом безпосереднього спілкування з викладачами, дозволяє науково-педагогічним працівникам коригувати власну стратегію викладання й обирати оптимальні методи навчання для підвищення рівня засвоєння здобувачами необхідних знань і навичок, а також їх задоволеності якістю і змістом навчання https://duikt.edu.ua/ua/1352-rezultati-opituvan-vnutrishnya-sistema-zabezpechennya--yakosti-vischoi-osviti-ta-osvitnoi-diyalnosti.
Як свідчать опитування рівень задоволеності здобувачів вищої освіти методами навчання і викладання становить від 75,9 до 90%
https://duikt.edu.ua/uploads/p_1352_55431429.pdf
https://duikt.edu.ua/uploads/p_1352_11964173.pdf

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

Науково-педагогічні, наукові та педагогічні працівники Університету мають право на академічну свободу (п. 18. Положення про організацію освітнього процесу в ДУІКТ https://duikt.edu.ua/uploads/p_447_49109699.pdf), що передбачає право обирати методи та засоби навчання, які забезпечують високу якість освітнього процесу. Принцип академічної свободи реалізується викладачами при складанні силабусів освітніх компонентів і безпосередньо у викладацькій роботі.
Відповідність принципам академічної свободи враховує інтереси здобувачів вищої освіти за ОПП, оскільки викладачі використовують індивідуальний підхід у виборі форм, методів і засобів навчання з урахуванням особливостей контингенту студентів, рівня їх підготовки, інтересів, психологічних особливостей тощо.
Принципи академічної свободи здобувачів освітнього рівня магістра полягають у вільному виборі програми підготовки, наукового керівника (керівників), тематики й напряму кваліфікаційного дослідження, а також свободі від впливу на освітній процес політичної, економічної ситуації у країні.

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

Освітніми ресурсами ДУІКТ є офіційний сайт, на якому зосереджена уся інформація стосовно освітньої діяльності Університету, в тому числі й щодо ОПП, що акредитується.
Здобувачі вищої освіти мають доступ до навчально-методичних матеріалів (конспекти лекцій, методичних вказівок до практичних/лабораторних/семінарських занять, тестів) з усіх освітніх компонентів ОПП у Google Class, дистанційні заняття проводяться з використанням Google Meet.
Відповідно, здобувачі вищої освіти мають повний доступ до силабусів освітніх компонентів, навчальних матеріалів, переліків питань для самостійного вивчення, рекомендацій щодо організації практичних занять і самостійної роботи. ОПП також є у вільному доступі для здобувачів вищої освіти на сторінці кафедри управління інформаційною та кібернетичною безпекою: http://surl.li/qenbmz.
В ОПП сформульовані цілі, загальний зміст та очікувані результати навчання. Деталізований зміст освітніх компонентів представлено у силабусах. На початку навчального семестру під час зустрічей зі студентами кожен викладач презентує освітні компоненти і висвітлює цілі, завдання, очікувані результати навчання, форми і методи викладання дисциплін, порядок і критерії оцінювання навчальних досягнень здобувачів.

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

Під час реалізації ОПП використовуються різноманітні елементи досліджень. Зокрема, заняття за ОПП проводяться у спеціалізованих навчальних лабораторіях, обладнаних апаратними та програмними засобами останнього покоління, серед яких: Центр управління інформаційною та кібербезпекою (Security Operation Center), Академічний центр компетенцій IBM «Кіберполігон», Лабораторія безпеки інформаційно-комунікаційних технологій Cisco, Лабораторія криптографічного захисту на базі технологій «АВТОР», Лабораторія технічного захисту інформації «PIAC» та інші лабораторії Університету.
Результати досліджень викладачів та здобувачів оприлюднюються на конференціях, семінарах та засіданнях круглих столів.
IV Всеукраїнська науково-практична конференція «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу», 2024 рік https://duikt.edu.ua/ua/news-1-611-12326-iv-vseukrainska-naukovo-praktichna-konferenciya---strategii-kiberstiykosti-upravlinnya-rizikami-ta-bezperervnist-biznesu_kafedra-upravlinnya-informaciynoyu-ta-kibernetichnoyu-bezpekoyu
Збірник тез https://duikt.edu.ua/uploads/p_2661_62255520.pdf

III Всеукраїнська науково-практична конференція «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу», 2023 рік https://duikt.edu.ua/ua/news-1-592-10709-iii-vseukrainska-naukovo-praktichna-konferenciya-strategii-kiberstiykosti-upravlinnya-rizikami-ta-bezperervnist-biznesu_navchalno-naukoviy-institut-zahistu-informacii-navchalno-naukovi-instituti?lang=ua&act=view&page=1&category=592&id=10709&sys_link=iii-vseukrainska-naukovo-praktichna-konferenciya-strategii-kiberstiykosti-upravlinnya-rizikami-ta-bezperervnist-biznesu_navchalno-naukoviy-institut-zahistu-informacii-navchalno-naukovi-instituti
Збірник тез https://dut.edu.ua/uploads/p_2626_38605375.pdf
II Всеукраїнська науково-практична конференція «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу», 2022 рік https://duikt.edu.ua/ua/news-1-611-10058-ii-vseukrainska-naukovo-praktichna-konferenciya-strategii-kiberstiykosti-upravlinnya-rizikami-ta-bezperervnist-biznesu_kafedra-upravlinnya-informaciynoyu-ta-kibernetichnoyu-bezpekoyu?lang=ua&act=view&page=1&category=611&id=10058&sys_link=ii-vseukrainska-naukovo-praktichna-konferenciya-strategii-kiberstiykosti-upravlinnya-rizikami-ta-bezperervnist-biznesu_kafedra-upravlinnya-informaciynoyu-ta-kibernetichnoyu-bezpekoyu
Збірник тез https://dut.edu.ua/uploads/p_2121_33783557.pdf
Поєднання навчання і досліджень за ОПП підкріплюється спільними публікаціями викладачів і магістрантів. Студенти освітньо-професійної програми мають можливість публікувати результати своїх досліджень у наукових виданнях ДУІКТ: «Сучасний захист інформації», «Зв'язок», «Телекомунікаційні та інформаційні технології», «Наукові записки ДУІКТ» (https://duikt.edu.ua/ua/123-periodichni-vidannya-nauka?lang=ua&id=123&sys_link=periodichni-vidannya-nauka).

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 обговорюється на кафедрі та оновлюється за потребою кожним НПП напередодні навчального року. Одним із чинників необхідності внесення змін до ОПП є отримання нових результатів у процесі досліджень. Так, протягом 2019-2024 рр. на кафедрі виконувалися науково-дослідні роботи:
НДР «Конкурентна розвідка як складова забезпечення інформаційної безпеки підприємства» (0118U100058). Керівник НДР: Легомінова С.В., виконавці: Мужанова Т.М., Якименко Ю.М., Рабчун Д.І.;
НДР «Кадрові технології у забезпеченні інформаційної безпеки підприємства» (0120U105132). Керівник НДР: Легомінова С.В., виконавці: Мужанова Т.М., Якименко Ю.М., Щавінський Ю.В., Рабчун Д.І., Запорожченко М.М.;
НДР «Запобігання і протидія методам соціальної інженерії у забезпеченні інформаційної безпеки підприємства» (0123U100743). Керівник НДР: Легомінова С.В., виконавці: Мужанова Т.М., Дзюба Т.М., Якименко Ю.М., Щавінський Ю.В., Рабчун Д.І., Капелюшна Т.В., Запорожченко М.М., Тищенко В.С.
Отримані результати наукових досліджень знайшли своє відображення у силабусах таких освітніх компонентів ОПП: «Корпоративна та професійна етика в кібербезпеці», «Системи управління інформаційною безпекою», «Управління проєктами інформаційної безпеки», «Управління ризиками інформаційної безпеки».
За результатами НДР кафедри розроблені рекомендації, які використовувалися в рамках консультування НПП кафедри фахівців компаній-партнерів, а саме «IT Спеціаліст», «ЕС ЕНД ТІ Україна», «Smart Technologies».

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

На базі ДУІКТ, який є членом Міжнародного союзу електрозв'язку (МСЕ), щорічно проводяться конференції МСЕ за участю викладачів, аспірантів і студентів http://surl.li/ivihfz.
Здобувачі ступеня магістра отримують постійну інформаційну та консультативну підтримку щодо можливостей участі у міжнародних програмах обміну студентів, зокрема Erasmus+ https://erasmus-plus.ec.europa.eu/opportunities/opportunities-from-outside-the-eu та підтримки наукових досліджень, в тому числі програма ім. Фулбрайта https://fulbright.org.ua/uk/fulbright-visiting-scholar-program/
У 2024 році кафедра УІКБ ДУІКТ взяла участь у поданні заявки на отримання гранту в галузі кібербезпеки (цифрова криміналістика) спільно з Хальмстадським університетом (Швеція), Львівським національним університетом ім. І. Франка і Національним університетом «Львівська політехніка».
Викладачі ОПП беруть участь у міжнародних конференціях і стажуваннях та отримують міжнародні сертифікати http://surl.li/yihztm.
Студенти ОПП постійно беруть участь у заходах з іноземними компаніями (CISCO, ESET, IBM, INTEL, GIGACLOUD) http://surl.li/clsado.
Прикладом міжнародної академічної мобільності є здобувачка ступеня магістра з кібербезпеки А. Батуркіна, яка у 2022 р. виїхала для продовження досліджень за фахом до Великої Британії. Робота у британській компанії «2T Security Ltd» на посаді аналітика відповідності безпеки була зарахована їй як проходження науково-дослідної практики у рамках ОПП.

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?

Механізм підготовки здобувачів ступеня магістра визначено у Положенні про організацію освітнього процесу в ДУІКТ https://duikt.edu.ua/uploads/p_447_49109699.pdf, відповідно до якого всі студенти зобов'язані відвідувати аудиторні заняття, проходити практики та всі форми поточного й підсумкового контролю, що передбачені

індивідуальним навчальним планом магістра й ОПП.
В освітньому процесі Університету контрольні заходи є необхідним елементом зворотного зв'язку. Запроваджені заходи визначають відповідність рівня набутих здобувачем знань, умінь та навичок вимогам ОПП, її програмним результатам і забезпечують своєчасне коригування освітнього процесу.
Реалізація основних завдань контролю знань здобувачів ступеня магістра досягається системним підходом до оцінювання чітко вимірюваних результатів навчання, комплексністю застосування різних видів контролю та формуванням очікуваних компетентностей.
Оцінювання сформованих компетенцій проводиться під час контрольних заходів, які передбачені ОПП та визначені у навчальному плані.
Критерії оцінювання знань, умінь та навичок здобувачів вищої освіти розроблені у відповідності до чинного законодавства та затверджені у Положенні про організацію освітнього процесу в ДУІКТ. Також, з метою отримання додаткових балів в межах дисциплін зараховуються здобуті студентами сертифікати відомих компаній за тематикою дисциплін.
Кожен вид контрольного заходу має чітко визначені форми проведення та критерії оцінювання навчальних досягнень і націлений на визначення здобутого рівня компетентності. Така система контролю дозволяє перевірити досягнення результатів навчання в межах усіх освітніх компонентів ОПП та об'єктивно їх оцінити.
З метою стимулювання планомірної та систематичної навчальної роботи здобувачів згідно з діючою в Університеті системою комплексної діагностики знань результати складання іспитів оцінюються за національною (чотирибальною), уніфікованою семибальною шкалою ECTS - A (відмінно), B,C (добре), D,E (задовільно), FX,F (незадовільно), і рейтинговою 100-бальною шкалою, а заліків – за двобальною, семибальною шкалою A,B,C,D,E (зараховано), FX,F (не зараховано) і 100-бальною шкалою.

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

Забезпечення чіткості та зрозумілості форм контрольних заходів і критеріїв оцінювання навчальних досягнень здобувачів відбувається шляхом ґрунтовного планування заходів контролю кафедрою і викладачем; повного й точного формулювання вимог до проведення заходів контролю, чіткого встановлення критеріїв оцінювання навчальних досягнень студентів; постійної роз'яснювальної роботи зі студентами з питань організації різних видів контролю знань.
Метою проведення контрольних заходів є комплексне оцінювання якості освітньої діяльності в рамках ОПП і досягнення результатів навчання. Оцінювання здобувачів з освітнього компонента відбувається за 100-бальною шкалою з подальшим переведенням в оцінку за національною шкалою та шкалою ЄКТС.
Згідно з ОПП використовуються такі види контролю знань студентів: поточний, рубіжний (модульний, тематичний) та підсумковий контроль.
Поточний контроль проводиться на аудиторних заняттях. Форми оцінювання навчальних досягнень студентів та його критерії визначаються в силабусах. Результати оцінювання доводяться до відома студентів і за потреби роз'яснюються в індивідуальному порядку.
Підсумковий контроль забезпечує оцінку результатів навчання здобувачів на проміжних або заключному етапах навчання і охоплює семестровий контроль і атестацію.
Критерії оцінювання навчальних досягнень здобувачів описано в силабусах з освітніх компонентів ОПП, зокрема наведено кількість балів, які здобувачі можуть отримати за виконання певного виду роботи й чіткі критерії оцінювання.

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

Попереднє ознайомлення з формами контрольних заходів і критеріями оцінювання за кожним освітнім компонентом здійснює викладач на початку кожного семестру на першому занятті, де роз'яснює структуру курсу та процедуру проведення контрольних заходів з зазначенням відповідних форм і критеріїв, за якими буде здійснюватися оцінювання здобутих знань та навичок. У подальшому при застосуванні того чи іншого контрольного заходу викладач доводить до студентів вимоги щодо оцінювання.
Строки контрольних заходів встановлюються на основі графіку навчального процесу в Університеті і розкладом на поточний семестр, що затверджуються ректором ДУІКТ та розміщуються на офіційному сайті ЗВО до початку 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

Підготовка здобувачів ступеня вищої освіти магістра за ОПП здійснюється на основі Державного стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти, затвердженого і введеного в дію наказом МОН України від 18.03.2021 р. № 332.
Засади атестації здобувачів ступеня магістра за ОПП визначаються Положенням про атестацію здобувачів вищої освіти та організацію роботи екзаменаційної комісії у ДУІКТ https://duikt.edu.ua/uploads/p_447_63335719.pdf.
Положення визначає порядок створення й організацію роботи Екзаменаційної комісії (ЕК), регламентує організаційні й методичні засади проведення атестації.
Відповідно до ОПП атестація магістрів здійснюється у формі публічного захисту кваліфікаційної роботи.
Інформація про графік і результати захисту магістерських кваліфікаційних робіт оприлюднюються на сторінці новин кафедри
http://surl.li/ireowy

http://surl.li/qhiqjo
Загальні вимоги до кваліфікаційної роботи, її змісту, обсягу та структури, порядок виконання кваліфікаційних робіт та засади її організаційного супроводу регламентує Положення про кваліфікаційні роботи здобувачів вищої освіти у ДУІКТ https://duikt.edu.ua/uploads/p_447_53363267.pdf
Положення про систему запобігання та виявлення академічного плагіату в ДУІКТ встановлює обов'язок перевірки магістерських робіт на предмет академічного плагіату https://duikt.edu.ua/uploads/p_447_61575036.pdf.
Проведення єдиного державного кваліфікаційного іспиту за результатами ОПП не передбачено.

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

Проведення контрольних заходів регламентується Положенням про організацію освітнього процесу https://duikt.edu.ua/uploads/p_447_49109699.pdf та Положенням про атестацію здобувачів вищої освіти та організацію роботи екзаменаційної комісії у ДУІКТ https://duikt.edu.ua/uploads/p_447_63335719.pdf. Положення встановлює можливість проведення атестації здобувачів вищої освіти із застосуванням дистанційних технологій у випадку, якщо особа не зможе захистити кваліфікаційну роботу в запланований час з поважних причин (форс-мажорні обставини), за умови визначення додаткового резервного дня атестації, завчасного надсилання здобувачем необхідних
документів і проведення захисту в синхронному режимі (відеоконференція). Цифровий запис процесу захисту кваліфікаційних робіт зберігається на кафедрі, яка здійснює набір, протягом одного року. Зазначені документи знаходяться у відкритому доступі на офіційному сайті ДУІКТ https://duikt.edu.ua/ua/447-polozhennya-normativni-dokumenti. Процедура проведення контрольних заходів та форми контролю з кожного
освітнього компонента ОПП прописана в силабусах, які розміщені на сайті кафедри https://duikt.edu.ua/ua/284-navchalni-disciplini-kafedra-upravlinnya-informaciynoyu-bezpekoyu?lang=ua&id=284&sys_link=navchalni-disciplini-kafedra-upravlinnya-informaciynoyu-bezpekoyu.

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

У ДУІКТ діє Положення про вирішення конфліктних ситуацій https://duikt.edu.ua/uploads/p_284_67285736.pdf, яке визначає порядок і процедури врегулювання ситуацій у разі конфлікту інтересів і конфліктів у навчальному процесі.
Положення про систему внутрішнього забезпечення якості вищої освіти
https://duikt.edu.ua/uploads/p_447_18879118.pdf передбачає системне запобігання та виявлення академічної недоброчесності в діяльності НПП і здобувачів вищої освіти.
Процедури виявлення та запобігання плагіату в академічних текстах працівників і здобувачів вищої освіти регулює відповідне Положення https://duikt.edu.ua/uploads/p_447_61575036.pdf, чинний Кодекс академічної доброчесності https://duikt.edu.ua/uploads/p_447_96297052.pdf. Перевірка кваліфікаційних робіт здобувачів вищої освіти здійснюється з використанням ПЗ StrikePlagiarism.com https://panel.strikeplagiarism.com/#/.
Регулярно здійснюється моніторинг на дотримання норм академічної доброчесності
https://duikt.edu.ua/uploads/p_1352_63204979.pdf
В Університеті призначено уповноважену особу з питань запобігання і протидії корупції та проводяться антикорупційні заходи https://duikt.edu.ua/ua/1471-protidii-korupcii-pro-universitet
Усі аудиторії та інші приміщення Університету обладнані системою цілодобового відеоспостереження та реєстрації, яка, за потреби, дозволяє вирішувати спірні ситуації.
За час існування ОПП випадків оскарження об'єктивності екзаменаторів, конфлікту інтересів не було.

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

Порядок повторного проходження контрольних заходів визначається Положенням про організацію освітнього процесу https://duikt.edu.ua/uploads/p_447_49109699.pdf
Здобувачу, який не склав, зазвичай, не більше двох заліків у встановлений термін, директор ННІ, як виняток, може дозволити перескладання заліків після завершення екзаменаційної сесії до початку наступного семестру (у визначений термін ліквідації академічної заборгованості). Здобувач, який до початку екзаменаційної сесії не склав хоча б один залік, права на одержання стипендії не має.
Перескладання екзамену допускається не більше двох разів з кожної дисципліни: один раз – викладачу, другий – комісії, яка створюється директором інституту. Оцінка комісії є остаточною. Якщо здобувач під час складання екзамену комісії отримав незадовільну оцінку (F, FX), то він відраховується з Університету. Здобувачі, які одержали під час заліково-екзаменаційної сесії три і більше незадовільних оцінок (FX), відраховуються з Університету за невиконання індивідуального навчального плану (за академічну неуспішність). Строки ліквідації академічної заборгованості, як правило, не перевищують трьох місяців.

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

У випадках конфліктної ситуації за мотивованою заявою здобувача чи викладача, директором інституту створюється комісія для приймання екзамену (заліку), до якої входять завідувач кафедри і науково-педагогічні, педагогічні працівники відповідної кафедри, представники деканату.
Відповідно до Положення щодо вирішення конфліктних ситуацій https://duikt.edu.ua/uploads/p_447_88699516.pdf створюється апеляційна комісія для розгляду звернень або скарг здобувача вищої освіти щодо проблем, які виникли

під час підсумкового семестрового контролю, відповідно до розпорядження директора інституту не пізніше наступного робочого дня після подання звернення або скарги.
Апеляційна комісія, до складу якої входять відповідно до ситуації: куратор групи, директор та заступник директора інституту, завідувач кафедри, голова студентської ради інституту, розглядає звернення здобувача вищої освіти не пізніше п'яти робочих днів після його подання.
Результати розгляду апеляційного звернення або скарги повідомляють здобувачеві вищої освіти відразу після прийняття рішення, про що здобувач вищої освіти та члени апеляційної комісії підписують відповідний протокол, який реєструється та зберігається в Навчальній частині інституту.
За час навчання за ОПП випадків оскарження результатів проведення контрольних заходів не було.

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

Політика, стандарти і процедури дотримання академічної доброчесності в Університеті визначені 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
https://duikt.edu.ua/uploads/p_447_61575036.pdf
Повноваженнями щодо впровадження політики академічної доброчесності та дотримання її процедури наділені 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 кваліфікаційних робіт, 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 відповідної декларації.
Крім того, всі навчальні аудиторії, в яких ведеться підготовка здобувачів за ОПП, обладнані відеокамерами, що унеможливлює використання під час проведення заходів контролю навчальних досягнень здобувачів недозволених матеріалів.
В Університеті діє репозиторій, що містить кваліфікаційні роботи здобувачів вищої освіти ОПП Управління інформаційною та кібернетичною безпекою https://duikt.edu.ua/repozitorii/uikb/

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

Популяризація академічної доброчесності серед здобувачів вищої освіти здійснюється шляхом: формування умов взаємної довіри й поваги між учасниками освітнього процесу; інформування учасників освітнього процесу про необхідність дотримання правил академічної доброчесності й ознайомлення з Кодексом академічної доброчесності https://duikt.edu.ua/uploads/p_447_96297052.pdf; використання ПЗ для перевірки текстів на наявність академічного плагіату; викладання в освітніх компонентах тем з основ академічного письма та дослідницької роботи з дотриманням принципів самостійності, коректного застосування інформації з інших джерел; підписання кожним учасником освітнього процесу Декларації про академічну доброчесність.
Здобувачі та НПП беруть участь в заходах, спрямованих на популяризацію академічної доброчесності, зокрема успішно пройшли курс «Академічна доброчесність: онлайн курс для викладачів» від Prometheus і отримали сертифікати http://surl.li/epnwgh
Також на кафедрі були проведені обговорення проблем академічної доброчесності з подальшим інформуванням студентів кураторами груп http://surl.li/nzgatf
http://surl.li/fovpdp
Крім цього у рамках курсу «Організація проведення наукових досліджень» студенти ОПП мають можливість вивчити основи академічної культури й етики поведінки здобувача вищої освіти, ознайомитися з проєктами сприяння академічній доброчесності в Україні (SAIUP); вимогами щодо посилань та цитування, оформлення покликань https://duikt.edu.ua/uploads/p_284_67285736.pdf.

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 ОПП; відрахування із Університету; позбавлення академічної стипендії; позбавлення наданих закладом освіти пільг з оплати за навчання.
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 випадків виявлення порушень академічної доброчесності з боку науково-педагогічних працівників і студентів 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

Усі НПП відповідають ліцензійним вимогам, які прописані в Постанові Кабінету Міністрів України від 30 грудня 2015 року № 1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності», зокрема мають:
- профільну вищу освіту (технічний, економічний, управлінський або педагогічний напрям);
- науковий ступінь (доктор / кандидат наук за предметною спеціалізацією освітніх компонентів);
- досвід професійної діяльності за спеціальністю 125 Кібербезпека та захист інформації не менше п'яти років;
- досвід керівництва (консультування) дисертації на здобуття наукового ступеня за спеціальністю, що була захищена в Україні;
- щонайменше п'ять публікацій у наукових виданнях, які включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection, протягом останніх п'яти років.

Освіта і практичний досвід НПП відповідає профілю освітніх компонентів, наявні публікації за тематикою дисциплін.
Легомінова С.В., д.е.н., проф. («Управління проєктами інформаційної безпеки») займалася дослідженнями в галузі управління проєктами і має практичний досвід їх реалізації.
Савченко В.А., д.т.н., проф. («Системи управління інформаційною безпекою») здійснював наукове керівництво/консультування здобувачів ступенів кандидата (доктора філософії) / доктора наук за спеціальністю 125 Кібербезпека та захист інформації.
Гайдур д.т.н, проф. («Прикладна загальна теорія систем інформаційної та кібербезпеки») здійснювала наукове керівництво здобувачів ступенів кандидата (доктора філософії) за спеціальністю 125 Кібербезпека та захист інформації.
Капелюшна Т.В., к.е.н., доц. («Організація проведення наукових досліджень») має значний досвід проведення наукових досліджень, проходила курси підвищення кваліфікації за спеціальністю 125 Кібербезпека та захист інформації.
Рабчун Д.І., к.т.н («Управління ризиками інформаційної безпеки») має досвід практичної діяльності у галузі управління інформаційною та кібербезпекою понад 5 років.
Мужанова Т.М., к.держ.упр., доц. («Науково-технічний переклад») має сертифікат B2 і досвід викладання англійської мови професійного спрямування з УІКБ понад 5 років.
Щавінський Ю.В., к.т.н., доц. («Корпоративна та професійна етика в кібербезпеці») має практичний досвід управлінської роботи, проходив стажування за спеціальністю 125 Кібербезпека та захист інформації на базі компаній – партнерів кафедри.
Кондратенко Н.Ю., к.пед.н. («Педагогіка та психологія у вищій школі») має профільну педагогічну освіту й досвід викладання дисциплін за напрямом.

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 науково-педагогічного колективу для забезпечення освітньої діяльності за ОПП здійснюється відповідно до чинних нормативно-правових вимог, Ліцензійних умов провадження освітньої діяльності, Статуту й нормативних документів Університету.
Відповідальність за визначення відповідності кваліфікації НПП і його рівня професійної та наукової активності, який забезпечує викладання освітніх компонентів, покладається на завідувача кафедри або групи забезпечення спеціальності на підставі Ліцензійних умов.
Процедури проведення конкурсу на заміщення вакантних посад та порядок перевиборів здійснюється відповідно до нормативних документів Університету:
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 ДУІКТ
https://duikt.edu.ua/uploads/p_447_89539392.pdf.
Кандидатури на заміщення посад НПП попередньо обговорюються на кафедрі в їх присутності. Претендент проводить відкриту лекцію або практичне заняття, після чого здійснюється обговорення рівня його професійної майстерності. По закінченню терміну контракту НПП у повному обсязі подає документи до конкурсної комісії на продовження роботи на посаді та бере участь у конкурсі на рівних умовах з іншими претендентами. Для оцінки рівня відповідності НПП долучається рейтингова картка, звіт за попередній рік роботи й перелік наукових публікацій. Рішення конкурсної комісії затверджується Вченою радою Університету.

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 запровадив в освітній процес модель інноваційного змісту навчання з метою підготовки конкурентоспроможних фахівців, яка передбачає: підготовку здобувачів вищої освіти за компетенціями роботодавців; залучення їх до освітнього процесу та атестації випускників; обговорення змін до ОПП з урахуванням сучасних тенденцій розвитку галузі ІТ, інформаційної та кібербезпеки; включення в навчальний процес курсів з

подальшою видачею сертифікатів компанії-партнера; стажування НПП у компаніях-партнерах.
Приклади залучення до навчальних занять представників роботодавців:
Г. Петриченко (IT Спеціаліст) http://surl.li/kinwxr;
В. Рибчак (ЕС ЕНД ТІ Україна) http://surl.li/klwfam.
ДУІКТ активно залучає до проведення окремих лекційних і практичних занять на ОПП фахівців з інформаційної та кібербезпеки провідних вітчизняних і міжнародних компаній:
К. Лосінський (IT Спеціаліст) http://surl.li/bwleez;
І. Чепур (Департамент кіберполіції) http://surl.li/vgiqcv;
А. Кузьменко (IBM Security, IBM Україна) http://surl.li/vtequl;
М. Висотін (ТОВ «Helsi UA») http://surl.li/jnpujo;
М. Невмержицький (департамент муніципальної безпеки виконавчого органу Київської міської ради (Київської міської державної адміністрації) http://surl.li/odseeu.

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

ДУІКТ сприяє викладачам ОПП у проходженні підвищення кваліфікації відповідно до Положення про підвищення кваліфікації науково-педагогічних працівників https://duikt.edu.ua/uploads/p_447_82499307.pdf.
Прикладами такого сприяння є:
проходження НПП кафедри УІКБ курсу підвищення кваліфікації від компанії AWS при участі SoftServe «Налаштування та безпека хмарних середовищ» http://surl.li/dpqntt;
проходження доцентом кафедри Мужановою Т.М. дистанційного курсу, присвяченого впровадженню у навчальний процес інноваційних підходів і методів викладання http://surl.li/igngmu;
проходження доцентами кафедри Мужановою Т.М., Якименком Ю.М. онлайн-курсів «Цифрові інструменти Google для закладів вищої, фахової передвищої освіти» http://surl.li/rfzjlw;
отримання доцентом кафедри Рабчуном Д.І. міжнародного сертифіката етичного хакера CEH http://surl.li/lgmkmr.

Наведіть конкретні приклади заохочення розвитку викладацької майстерності

Система заходів зі стимулювання підвищення фаховості та викладацької майстерності НПП ДУІКТ передбачає матеріальні й моральні заохочення і регламентується
Статутом Університету https://duikt.edu.ua/uploads/p_949_13841785.pdf,
Колективним договором на 2023-2025 р.р. https://duikt.edu.ua/uploads/p_1462_63527482.pdf?file=p_1462_63527482.pdf,
Положенням про підвищення кваліфікації науково-педагогічних та педагогічних працівників https://duikt.edu.ua/uploads/p_447_82499307.pdf,
Положенням про порядок заохочення осіб, які працюють, навчаються в Державному університеті інформаційно-комунікаційних технологій https://duikt.edu.ua/uploads/p_447_90869904.pdf та
Положенням про надання щорічної грошової винагороди педагогічним працівникам за сумлінну працю зразкове виконання службових обовязків https://duikt.edu.ua/uploads/p_447_98149481.pdf.
Прикладом такого заохочення є нагородження Подякою ректора ДУІКТ доцента кафедри управління інформаційною та кібернетичною безпекою к.держ.упр., доц. Мужанової Т.М. з нагоди Всесвітнього дня електрозв'язку та інформаційного суспільства http://surl.li/yhmdcs.
Зокрема, здійснюється матеріальне стимулювання НПП, що мають вагомі успіхи у науково-педагогічній діяльності. Моральні заохочення передбачають нагородження такими видами: оголошення подяки ректора, грамота ректора, а також за поданням керівництва ДУІКТ на відзначення регіональними та відомчими відзнаками.

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 ДУІКТ є: кошти державного бюджету; доходи від надання платних освітніх послуг і господарської діяльності; виконання науково-дослідних робіт.
Університет має у своєму складі розширену інфраструктуру (навчальні приміщення, комп'ютерні та спеціалізовані лабораторії, організаційно-методичний центр новітніх технологій, редакційний відділ, бібліотеку, студентський центр та інші приміщення, доступ до високошвидкісного WiFi (5 Gb/s), що сприяє забезпеченню досягнення цілей і програмних РН.
Перелік комп'ютерних класів і спеціалізованих лабораторій Навчально-наукового інституту захисту інформації наведено на сайті: https://duikt.edu.ua/ua/566-zagalna-informaciya-navchalno-naukoviy-institut-zahistu-informacii
Загальний фонд електронної бібліотеки https://duikt.edu.ua/ua/lib/1/category/2122 становить понад 160 тис. примірників, серед яких навчальні посібники, конспекти лекцій, методичні рекомендації з освітні компонентів ОПП. Інформаційна платформа Google Workspace for Education (GWE) використовується для організації дистанційного навчання і спільної роботи в межах закладу https://duikt.edu.ua/ua/149-e-navchannya-navchannya.
Викладачі, які забезпечують викладання освітніх компонентів ОПП, розмістили необхідні навчально-методичні матеріали на сторінках курсів у GWE. Всі студенти ОПП отримали персональні облікові записи для роботи в системі GWE, а також коди і посилання на сторінки курсів. Дистанційні заняття проходять із використанням GoogleMeet.

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

ДУІКТ забезпечує вільний доступ викладачів і здобувачів вищої освіти до інфраструктури та інформаційних ресурсів, потрібних для навчання, викладацької та/або наукової діяльності в межах ОПП.
Перелік та силабуси освітніх компонентів ОПП розміщені на сторінці кафедри, навчально-методичні матеріали (методичні розробки для проведення практичних/лабораторних/семінарських занять, конспекти лекцій, завдання для підготовки до підсумкових заходів контролю, тести та інші форми оцінювання навчальних досягнень здобувачів тощо) розміщені на сторінках викладачів у Google Class. Діє електронна бібліотека, де у постійному доступі знаходяться навчальні посібники, підручники та конспекти лекцій з усіх дисциплін.
Для проведення занять, самостійної освітньої та наукової дослідницької діяльності здобувачів ОПП використовуються спеціалізовані лабораторії Навчально-наукового інституту захисту інформації, кафедри УІКБ (Академічний центр компетенцій IBM «Кіберполігон», лабораторії криптографічного захисту, засобів контролю доступу й безпеки інформаційно-комунікаційних технологій CISCO, Центр управління інформаційною та кібербезпекою http://surl.li/rstcms.
Науково-педагогічні працівники і здобувачі ступеня магістра мають можливість користуватися високошвидкісним Інтернетом від компанії Lanet (5 Гб/с) для навчання, викладацької та науково-дослідницької діяльності.

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

У ДУІКТ створене сприятливе для здобувачів ОПП освітнє середовище, зокрема для:
розвитку й реалізації творчих здібностей здобувачів освіти https://duikt.edu.ua/ua/896-rada-molodih-vchenih-nauka.
На кафедрі УІКБ функціонують два наукових гуртка за напрямом кафедри http://surl.li/zagvxx,
організації закордонних стажувань, отримання грантів на проведення наукових досліджень http://surl.li/ojkabd,
організації дистанційних занять і віддаленого доступу до навчальних матеріалів (Google Workspace for Education https://duikt.edu.ua/ua/149-e-navchannya-navchannya,
участі в різноманітних конкурсах і змаганнях за фахом http://surl.li/swlycs, http://surl.li/tpxyff.
Для задоволення потреб та інтересів здобувачів вищої освіти у позанавчальний час постійно діють студентський центр, тренажерна зала та фітнес-центр, їдальня, центр культури та мистецтва. Крім того фінансуються численні соціальні ініціативи: надання матеріальної допомоги, виплата соціальних стипендій, поліпшення умов проживання у гуртожитках тощо.
У ДУІКТ значна увага приділяється безпеці освітнього середовища (вступний інструктаж, щодо видів та джерел небезпеки у навчальних приміщеннях, загальних правил поведінки під час освітнього процесу, ознайомлення з Правилами пожежної безпеки і планами евакуації, оповіщення про ракетну небезпеку, наявність плану розміщення студентів в укриттях).

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 створює і забезпечує механізми різнобічної підтримки здобувачів освіти у ході навчання. Надається організаційна та консультативна підтримка з метою реалізації студентами індивідуальної освітньої траєкторії. Завідувач, куратори груп та НПП кафедри спільно з адміністрацією Університету здійснюють підтримку здобувачів ОПП з організаційних питань навчання в університеті.
Студенти отримують сприяння щодо можливостей додаткового навчання, професійного і кар'єрного зростання, працевлаштування за фахом. У ДУІКТ функціонує Рада молодих вчених https://duikt.edu.ua/ua/896-rada-molodih-vchenih-nauka, яка просуває і захищає інтересів науковців-початківців.
У разі конфліктних або складних ситуацій до вирішення питань залучаються завідувачі кафедр, працівники деканату або ректорату. Здобувачі ОПП мають можливість звернутися через електронний ресурс Скринька довіри: info@dut.edu.ua http://surl.li/xpzepq й залишити анонімне звернення, яке буде негайно розглянуте адміністрацією Університету.
Студентам пільгових категорій надається активна підтримка у вигляді соціальних стипендій та інших видів соціальної допомоги. Також передбачено умови для навчання осіб з особливими потребами з метою їх соціалізації та забезпечення доступності й результативності навчання.
Відділ по роботі зі студентами займається вивченням і вирішенням соціальних проблем студентів, надає консультаційну допомогу з метою покращення навчального середовища студентської молоді, за потреби, бере участь у вирішенні конфліктних ситуацій під час навчального процесу https://duikt.edu.ua/ua/2146-zagalna-informaciya-viddil-z-pitan-socialnih-ta-navchalnih-problem-studentiv.
Постійно здійснюється моніторинг психологічного клімату та міжособистісних відносин здобувачів вищої освіти та їх обізнаності щодо вирішення конфліктних ситуацій https://duikt.edu.ua/uploads/p_1352_81183215.pdf
Важливу роль у забезпеченні різнопланової підтримки здобувачів вищої освіти, а також у їх залученні до студентського самоврядування відіграє Студентська рада Університету, яка, серед іншого, реалізує проєкти, спрямовані на формування і вдосконалення професійних вмінь і навичок студентів, сприяє налагодженню конструктивної комунікації між студентами та викладачами, залучає до освітнього процесу провідні компанії галузі IT, консультує студентів з питань соціального захисту, зокрема осіб пільгових категорій https://duikt.edu.ua/ua/929-zagalna-informaciya-studentska-rada.
Крім цього, Студентська рада організовує спортивні змагання й культурно-просвітницькі заходи для і за участі

студентської молоді https://duikt.edu.ua/ua/142-kultura-studentska-rada, забезпечує роботу студентів-кураторів молодших курсів.
Засади та обов'язки Студентської ради Університету регламентує Положення про студентське самоврядування https://duikt.edu.ua/ua/933-polozhennya-pro-studentske-samovryaduvannya-studentska-rada.

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 й інших маломобільних груп населення (МГН).
Враховуючи вимоги та нормативи Державних будівельних норм України; ДСТУ-Н В.2.2-31-2011 було розроблене Положення про порядок організації інклюзивного навчання https://duikt.edu.ua/uploads/p_447_39062918.pdf, яке містить Порядок супроводу (надання допомоги) осіб з інвалідністю та інших маломобільних груп населення.
В Університеті створені умови для вільного пересування осіб з особливими освітніми потребами, встановлені пандуси і підйомні платформи для інвалідів, біля аудиторій та інших приміщень розміщені таблички, надруковані шрифтом Брайля, обладнані спеціальні санвузли для людей з обмеженими можливостями. Відповідно до Правил прийому під час вступу в ДУІКТ створюються пільгові умови вступу для осіб з особливими освітніми потребами. Випадків вступу осіб з особливими освітніми потребами на ОПП 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 ДУІКТ побудована на принципах дотримання цінностей свободи, справедливості, рівності прав і можливостей, інклюзивності, толерантності, недискримінації; відкритості та прозорості.
В Університеті функціонує відділ з питань соціальних та навчальних проблем студентів http://surl.li/mmnmbt, діяльність якого регламентує відповідне Положення https://duikt.edu.ua/uploads/p_2146_65784140.pdf.
Положення про вирішення конфліктних ситуацій https://duikt.edu.ua/uploads/p_447_88699516.pdf визначає порядок і процедури врегулювання ситуацій у разі конфлікту інтересів, порушення прав людини, конфліктів у навчальному та освітньому процесі, міжособистісних стосунках учасників освітнього процесу тощо.
За потреби вступники можуть звернутися до Апеляційної комісії http://surl.li/zacqyl
У здобувачів ОПП є можливість скористатися електронною скринькою довіри http://surl.li/xpzepq 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, та проводяться антикорупційні заходи https://duikt.edu.ua/ua/1471-protidii-korupcii-pro-universitet
Розгляд звернень, скарг і заяв, що надходять до Університету, відбувається відповідно до Законів України «Про доступ до публічної інформації» та «Про звернення громадян». Врегулювання скарг і звернень відбувається шляхом особистого прийому громадян адміністрацією ДУІКТ. Про результати розгляду скарг і звернень громадянину повідомляється письмово або усно, за його бажанням.
За період реалізації ОПП 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 https://duikt.edu.ua/uploads/p_447_18879118.pdf, та Положенням про запровадження та оновлення освітніх програм https://duikt.edu.ua/uploads/p_447_73345463.pdf. Ці положення уніфікують процедури щодо ОПП для всіх спеціальностей Університету, що забезпечує єдиний підхід до контролю якості за реалізацією процедур, а також механізми вдосконалення.
Для розроблення ОПП утворюється робоча група з числа НПП, які за рівнем своєї кваліфікації, наукової та професійної активності та наявністю відповідного науково-педагогічного стажу можуть входити до складу таких груп. Також до процесу розробки залучаються роботодавці, здобувачі та провідні фахівці з відповідної спеціальності. За якість реалізації ОПП відповідає група забезпечення спеціальності.
Процедура перегляду й оновлення ОП описана у Положенні про запровадження й оновлення освітніх програм https://duikt.edu.ua/uploads/p_447_73345463.pdf.
З метою оцінювання ОПП щороку здійснюється моніторинг на предмет її відповідності стандарту, спроможності ЗВО забезпечити досягнення здобувачами вищої освіти програмних РН, рівня задоволеності роботодавців і

здобувачів. Зміни до ОПП та освітніх компонентів вносяться з урахуванням змін законодавства та інноваційного розвитку галузі ІТ та захисту інформації.

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

Процедура перегляду й оновлення ОПП описана в Положенні про запровадження й оновлення освітніх програм https://duikt.edu.ua/uploads/p_447_73345463.pdf. Відповідно до Положення ОПП переглядається в таких випадках: щорічно за результатами моніторингу; по завершенню циклу ОПП.
З метою оновлення ОПП щороку здійснюється моніторинг змін законодавства й тенденцій інноваційного розвитку галузей ІТ, кібербезпеки та захисту інформації.
У 2024 році до ОПП внесено такі зміни: з основного блоку навчального плану вилучено компонент «Управління інцидентами інформаційної безпеки» та введено компонент «Управління ризиками інформаційної безпеки». Пропозиція зазначених змін була внесена компаніями-партнерами кафедри «ІТ Спеціаліст» і «ЕС ЕНД ТІ УКРАЇНА».
У результаті обговорення перспектив актуалізації ОПП з представниками академічної спільноти (Національний університет «Львівська політехніка») та випускниками програми «Управління інформаційною та кібернетичною безпекою», які працюють за фахом, ОПП була оновлена. Так, у частині 4 «Придатність випускників до подальшого працевлаштування та навчання» додано професійну кваліфікацію, визначену професійним стандартом у галузі кібербезпеки та захисту інформації, розробленим Держспецзв'язку України:
2139.2 – Фахівець з планування політики та стратегії кібербезпеки.

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 і під час опитувань http://surl.li/dqxish.
Узагальнені результати опитувань розміщені на сайті http://surl.li/oonjrg
Здобувачі свої пропозиції можуть надавати через форму зворотного зв'язку, розміщену на сторінці публічного обговорення освітньо-професійних програм http://surl.li/tatgga
та скриньку довіри http://surl.li/jrxlax
Також, ефективним засобом моніторингу ОПП є зустрічі з магістрантами щодо поточних питань організації навчального процесу та підготовки до підсумкової атестації, де обговорюються проблемні питання
http://surl.li/ucnoje
http://surl.li/kkxhoc
Найбільш актуальні зміни обговорюються під час зустрічей з представниками компаній-партнерів
ТОВ «ІТ Спеціаліст»
http://surl.li/rjvfuw
ДП «ЕС ЕНД ТІ УКРАЇНА»
http://surl.li/xoodou
http://surl.li/ethbqy

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

Відповідно до Положення про студентське самоврядування https://duikt.edu.ua/ua/933-polozhennya-pro-studentske-samovryaduvannya-studentska-rada студентське самоврядування забезпечує серед іншого участь студентів в обговоренні та вирішенні питань удосконалення освітнього процесу, науково-дослідної роботи в Університеті, а також захист прав та інтересів студентів, в т.ч. щодо належної якості навчання.
Представники студентського самоврядування Університету, представляючи інтереси здобувачів освіти, можуть звертатися з пропозиціями до вчених рад ДУІКТ та ННІЗІ з питань удосконалення стратегії Університету щодо контролю освітнього процесу; брати участь у вирішенні спірних ситуацій, що можуть виникнути між здобувачами вищої освіти і представниками адміністрації/ НПП; подавати пропозиції щодо вдосконалення структури і змісту навчальних планів та освітніх програм.
У контексті оцінювання й удосконалення змісту та якості навчання члени активу студентського самоврядування беруть активну участь у заходах компаній-партнерів і науково-дослідних організацій, присвячених профорієнтації, інформуванню й обговоренню проблем і перспектив розвитку галузі, впровадження нових технологій і підходів до управління інформаційною та кібернетичною безпекою. Студенти також долучаються до організації ярмарку вакансій, студентських конференцій і тематичних опитувань.

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

Оскільки переважна більшість здобувачів ступеня магістра працевлаштовуються саме в компаніях галузі ІТ, кібербезпеки та захисту інформації, то компанії-партнери кафедри, які є потенційними роботодавцями випускників, беруть безпосередню участь у процесі періодичного перегляду програми. Серед них ключову роль відіграють представники ТОВ «ІТ Спеціаліст»
http://surl.li/kmugkx і
ДП «ЕС ЕНД ТІ УКРАЇНА»
http://surl.li/klfoqg.

Обговорення з роботодавцями перспектив розвитку галузі та необхідних змін до програм здійснюється під час конференцій та семінарів, засідань вчених рад і кафедри, особистих зустрічей.

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

Інформація про працевлаштування випускників ОПП постійно і системно збирається й аналізується. Як відзначено вище, переважна більшість здобувачів ступеня магістра з кібербезпеки та захисту інформації працевлаштовуються в компаніях галузі ІТ, кібербезпеки та захисту інформації.
Так, з випускників ОПП 2023 року більшість працевлаштувалися за фахом у компаніях галузі ІТ, зокрема К. Андрущенко займає посаду менеджера систем інформаційної безпеки в компанії CS-Consulting; А. Батуркіна - аналітика відповідності вимогам безпеки в 2T Security Ltd; В. Самко і М. Ющенко працюють менеджерами систем інформаційної безпеки в ТОВ «Svit IT», М. Костроміна – інженером кібербезпеки в Seeton Group LLC, О. Стешенко – інженером в ТОВ «Октава Дефенс». Л. Гарнатко продовжив працювати адміністратором безпеки у державній структурі - СЗР України.
Випускники магістерської програми УІКБ 2024 року також продовжили ці тенденції: Д. Лабяк працює спеціалістом з інформаційної безпеки в компанії «Divoro», О. Марценюк - спеціалістом з операцій кібербезпеки в GSM, М. Харитончук займає посаду головного фахівця відділу інформаційної безпеки Банку «Кліринговий дім», А. Вершигора - директора з інформаційної безпеки ТОВ «Harvin», у компанії GlobalLogic за фахом працюють М. Довірак (провідний інженер з безпеки) і В. Коржик (провідний розробник).

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

Процедури щодо забезпечення якості реалізації, контролю та моніторингу внутрішніх показників освітньої діяльності за ОПП:
на рівні кафедр – у вигляді контролю діяльності НПП, зокрема перевірки завідувача кафедри та проведення відкритих занять, заслуховування, обговорення та прийняття рішень на засіданнях кафедр;
на рівні навчально-наукового інституту – у вигляді контролю діяльності кафедр, заслуховування, відвідування відкритих занять НПП, обговорення питань і прийняття рішень на засіданні Вченої ради інституту щодо затвердження основних нормативних документів з реалізації ОПП;
на рівні ЗВО – моніторинг щодо виконання прийнятих рішень проводить Навчально-методичний центр (НМЦ).
Кафедра щорічно проводить опитування здобувачів освіти за ОПП щодо рівня їх задоволення змістом і якістю освіти https://duikt.edu.ua/ua/1352-rezultati-opituvan-vnutrishnya-sistema-zabezpechennya--yakosti-vischoi-osviti-ta-osvitnoi-diyalnosti?lang=ua&id=1352&sys_link=rezultati-opituvan-vnutrishnya-sistema-zabezpechennya--yakosti-vischoi-osviti-ta-osvitnoi-diyalnosti.
За результатами опитувань здобувачів вносяться пропозиції щодо оновлення змісту та підвищення якості ОПП https://duikt.edu.ua/ua/news-1-611-11498-naukovo-metodichne-zasidannya-kafedri-uikb_kafedra-upravlinnya-informaciynoyu-ta-kibernetichnoyu-bezpekoyu.

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?

У зв'язку із введенням воєнного стану акредитація ОПП, яка була запланована на 2023 рік, була продовжена автоматично. Упродовж останніх років за спеціальністю 125 Кібербезпека та захист інформації в ДУІКТ акредитація не проводилася.
Водночас, під час оновлення програми було розглянуто недоліки і рекомендації щодо їх виправлення за результатами акредитації ОП «Інженерія програмного забезпечення» та «Штучний інтелект» (2024 р.).
У ході оновлення ОПП враховано зауваження експертів до згаданих вище програм, зокрема:
Критерій 3 Доступ до освітньої програми та визнання результатів навчання
На сайті Університету додано інформацію про грантові програми, стипендії та міжнародні стажування, в більшості з яких можуть брати участь здобувачі магістерської ОПП 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-molodih-vchenih
Критерій 6 Людські ресурси
З метою забезпечення практичної спрямованості ОПП до викладання залучено к.т.н. Рабчуна Д. І., який працює за фахом у ТОВ «ІТ Спеціаліст» і ділиться зі здобувачами своїм практичним досвідом. Крім того, викладач постійно підвищує свій професійний рівень, що дозволяє оновлювати зміст освітніх компонент з урахуванням розвитку галузі інформаційної та кібербезпеки https://duikt.edu.ua/ua/news-1-611-13124-vitaemo-docenta-kafedri-uikb-rabchuna-dmitra-z-otrimannyam-prestizhnogo-sertifikatu-z-kiberbezpeki_kafedra-upravlinnya-informaciynoyu-ta-kibernetichnoyu-bezpekoyu.
Критерій 7 Внутрішнє забезпечення якості освітньої програми
На сторінці Університету розміщено репозиторій кваліфікаційних робіт випускників, в тому числі магістерської ОПП «Управління інформаційною та кібернетичною безпекою» https://duikt.edu.ua/repozitorii/uikb/
Критерій 9 Прозорість та публічність
Започатковано висвітлення на сторінці новин кафедри УІКБ інформації про кар'єрні досягнення випускників ОПП https://duikt.edu.ua/ua/news-1-592-12710-hotiv-buti-hakerom-a-stav-menedzherom-z-kiberbezpeki-istoriya-uspihu-vipusknika-duikt_navchalno-naukoviy-institut-zahistu-informacii-navchalno-naukovi-instituti.

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

Відповідно до Положення про систему внутрішнього забезпечення якості вищої освіти (https://duikt.edu.ua/uploads/p_447_18879118.pdf) ДУІКТ всіляко сприяє залученню учасників академічної спільноти до системи внутрішнього забезпечення якості освіти.
Академічна спільнота бере участь: у здійсненні моніторингу та періодичного перегляду освітніх програм; оцінюванні освітньої та науково-технічної діяльності кафедр інституту. Питання якості освіти обговорюються на засіданнях кафедр, вчених рад Інституту й Університету. Щороку проводиться навчально-методичний збір, на якому кожен викладач презентує змістовне наповнення своїх дисциплін, підтверджуючи свою готовність до навчального року.
Протягом 2022-24 років від академічної спільноти з інших ЗВО до перегляду ОПП залучалися: д.т.н., професор Толюпа С.В. професор кафедри кібербезпеки та захисту інформації КНУ ім. Т. Шевченка, доцент кафедри кібербезпеки та захисту інформації КНУ ім. Т. Шевченка, д.т.н., с.н.с. Лаптєв О.А., професор кафедри засобів захисту інформації НАУ, д.т.н. Лазаренко С.В.; заступник директора Інституту телекомунікацій, радіоелектроніки та електронної техніки Національного університету «Львівська політехніка» к.т.н, доцент Кремер І.П.

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

Завдяки активному висвітленню питань якості навчального процесу й оновлення його змісту на рівні Університету, Інституту і кафедри формується культура якості освіти, яка охоплює не тільки систему уявлень, неписаних норм і цінностей, але й правила поведінки, яких дотримуються у спільноті науково-педагогічних працівників і здобувачів освіти.
Проблеми і завдання забезпечення якості освітніх програм знаходяться у центрі уваги на засіданнях кафедри, Вченої ради ННІЗІ, Вченої ради Університету https://duikt.edu.ua/ua/news-1-611-11498-naukovo-metodichne-zasidannya-kafedri-uikb_kafedra-upravlinnya-informaciynoyu-ta-kibernetichnoyu-bezpekoyu. На рівні закладу й кафедри УІКБ постійно проводяться опитування зацікавлених сторін щодо їх оцінки якості навчання та пропозицій щодо покращення освітнього процесу https://duikt.edu.ua/ua/1352-rezultati-opituvan-vnutrishnya-sistema-zabezpechennya--yakosti-vischoi-osviti-ta-osvitnoi-diyalnosti?lang=ua&id=1352&sys_link=rezultati-opituvan-vnutrishnya-sistema-zabezpechennya--yakosti-vischoi-osviti-ta-osvitnoi-diyalnosti,
https://duikt.edu.ua/uploads/p_1352_99675417.pdf.

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 всіх учасників освітнього процесу ДУІКТ регулюються:
Статутом Університету, погодженого загальними зборами трудового колективу й затвердженого наказом МОН України від 20.03.2023 р. № 309 https://duikt.edu.ua/uploads/p_949_13841785.pdf;
Положенням про організацію освітнього процесу у ДУТ https://duikt.edu.ua/uploads/p_447_49109699.pdf,
Колективним договором ДУТ https://duikt.edu.ua/uploads/p_1462_63527482.pdf?file=p_1462_63527482.pdf,
Кодексом академічної доброчесності ДУТ https://duikt.edu.ua/uploads/p_949_78992606.pdf?file=p_949_78992606.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.

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/2695-publichne-obgovorennya-osvitno-profesiynih-program-kafedra-upravlinnya-informaciynoyu-ta-kibernetichnoyu-bezpekoyu

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

ОПП, навчальні плани https://duikt.edu.ua/ua/1826-osvitno-profesiyni-programi-kafedra-upravlinnya-informaciynoyu-ta-kibernetichnoyu-bezpekoyu
силабуси освітніх компонентів, освітні компоненти вільного вибору студента (УІКБ)
https://duikt.edu.ua/ua/284-navchalni-disciplini-kafedra-upravlinnya-informaciynoyu-bezpekoyu
освітні компоненти вільного вибору студента
https://duikt.edu.ua/ua/2080-katalog-osvitnih-komponentiv-vilnogo-viboru-studentami-navchannya

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП?

Існування ОПП Управління інформаційною та кібернетичною безпекою другого (магістерського) рівня за спеціальністю 125 Кібербезпека та захист інформації галузі знань 12 Інформаційні технології в ДУІКТ забезпечує послідовність і узгодженість процесу підготовки фахівців від першого (бакалаврського) до третього (доктор філософії) освітнього рівня. Наведені показники діяльності Державного університету інформаційно-комунікаційних технологій за ОПП відповідають чинним вимогам. Проведений самоаналіз свідчить, що запроваджена ОПП базується на компетентнісному підході, містить чітко визначені програмні результати навчання і узгоджена з вимогами Національної рамки кваліфікацій. Концептуальні засади освітнього процесу реалізовані у навчальному плані стосовно переліку та змісту навчальних дисциплін, розподілу часу у кредитах ЄКТС, форм проведення навчальних занять та їх обсягу. Кадрове забезпечення освітнього процесу за ОПП та якісний склад групи забезпечення відповідає ліцензійним вимогам щодо підготовки фахівців за другим (магістерським) рівнем. Науково-педагогічні працівники мають відповідну кваліфікацію і здійснюють необхідну роботу з методичного забезпечення освітнього процесу, наукової та науково-технічної діяльності, науково-дослідницької роботи. Особливої уваги заслуговує матеріально-технічне забезпечення освітнього процесу ОПП як за спеціальністю 125 Кібербезпека та захист інформації, так і у ДУІКТ взагалі. Наявність профільованих лабораторій, які розгорнуті на технологіях провідних ІТ компаній України та світу, їх укомплектованість комп'ютерною технікою та програмно-апаратними комплексами відповідають кращим практикам підготовки фахівців як в Україні, так і у світі. Також, перевагою реалізації наведеної ОПП є широке залучення до освітнього процесу професіоналів-практиків, які знайомлять здобувачів освіти з передовими технологіями та підходами у сфері захисту інформації та кібербезпеки. Крім того, підходи, запроваджені в ДУІКТ дозволяють повністю реалізувати індивідуальну освітню траєкторію здобувача вищої освіти на основі його безпосередньої участі у плануванні та реалізації освітнього процесу.
На підставі наведеної інформації можна зробити висновок, що освітня діяльність ДУІКТ з підготовки фахівців освітнього рівня магістр за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою спеціальності 125 Кібербезпека та захист інформації галузі знань 12 Інформаційні технології, відповідає вимогам акредитації і забезпечує державну гарантію якості вищої освіти.

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

Кібербезпека дедалі більше перетворюється на загально-світову проблему. Перспективним та важливим для розвитку ОПП вважаємо підвищення її якості та інноваційний розвиток відповідно до світових стандартів, що сприятиме істотному зростанню інтелектуального, культурного, духовного та морального потенціалу кафедри та особистостей здобувачів освіти. Доцільним вважаємо наукове опрацювання теоретичних, нормативних, організаційних, процесуальних засад інтернаціоналізації змісту освіти магістерського рівня в університетах Європи для формування та впровадження спільних програм, що підсилюється наявними суперечностями: між зростаючими вимогами сучасного глобалізованого суспільства до надання молодим фахівцям міжнародного виміру та недостатнім рівнем готовності вітчизняної системи вищої освіти до відповідних змін; між потребою вдосконалення змісту ОПП в умовах інтернаціоналізації ринку праці та традиційними підходами до розробки навчальних програм. Тобто, розвиток ОПП потрібно здійснювати в напрямі її гармонізації із світовими науковими тенденціями, оскільки саме за допомогою спільних освітніх програм молодь України матиме можливість виходити на освітні та наукові ринки інших країн, розшириться набір іноземних здобувачів, підвищиться академічна мобільність здобувачів освіти та буде можливість залучати кращих зарубіжних викладачів з їх авторськими навчальними програмами до освітнього процесу, а НПП ДУІКТ – їздити з лекціями та на стажування в провідні зарубіжні університети.
Для підвищення якості ОПП, її конкурентоспроможності та інтеграції в європейський і світовий освітній і науковий простір, відповідно до сучасних запитів сьогодення плануються наступні заходи:
- підвищення кваліфікації викладачів через навчання і стажування в провідних закордонних університетах;
- постійне удосконалення матеріально-технічного забезпечення освітнього процесу, наукових досліджень;
- формування спільних освітніх програм з провідними європейськими університетами;
- залучення до освітнього процесу кращих зарубіжних науковців з їх авторськими курсами та програмами;
- висвітлення досягнень науковців через публікацію досліджень у провідних світових фахових виданнях із достатнім імпакт-фактором, у виданнях, індексованих у міжнародних наукометричних базах Scopus та Web of Science;
- розширення партнерських зв'язків з бізнесовими структурами щодо імплементації наукових розробок НПП та здобувачів освіти.

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: 24.09.2024 р.

Таблиця 1. Інформація про освітні компоненти ОП

Назва освітнього компонента	**Вид освітнього компонента**	**Силабус або інші навчально-методичні матеріали**		**Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього***
		Назва файла	**Хеш файла**	
Корпоративна та професійна етика в кібербезпеці	навчальна дисципліна	*1_Корпоративна_та_професійна_етика.pdf*	/oneetkM8mjrtbxdJsWiAImJyN/HzDNmDKDijWAIrWc=	*Навчальна лабораторія Центр управління інформаційною та кібербезпекою (Security Operation Center) – 2017 рік.* *Програмно-апаратний комплекс AlienVault SIEM (OSSIM) від компанії-вендора AlienVault:* *- платформа OSSIM для збору, моніторингу, аналізу подій і загроз інформаційної безпеки;* *- SIEM для управління інформацією та подіями безпеки.* *Програмні засоби підтримки етичного прийняття рішень у сфері інформаційної безпеки («Вибір», Mpriority1.0).* *Програмний комплекс для організації дистанційного навчання в комплексному цифровому навчальному середовищі Google Workspace for Education.*
Педагогіка та психологія у вищій школі	навчальна дисципліна	*2_Педагогіка_та_психологія_у_вищій_школі_2024.pdf*	zMjlCpfLSB+ZvjGLrj8hpfT9gxVkdX9Y/I2jUQQL/ik=	*Програмні засоби підтримки прийняття рішень у сфері інформаційної безпеки («Вибір», Mpriority1.0).* *Програмний комплекс для організації дистанційного навчання в комплексному цифровому навчальному середовищі Google Workspace for Education.*
Організація проведення наукових досліджень	навчальна дисципліна	*3_Організація_проведення_наукових_досліджень.pdf*	Uxc509H7DjTTqeS1Lc7JowC02gQJDoykxK+LlXWAE4=	*Навчальна лабораторія Центр управління інформаційною та кібербезпекою (Security Operation Center) – 2017 рік.* *1.Комп'ютери Asus p5gc-mx - 3шт.; (2015 року) ITS 5400 - 7 шт. (2017 року).* *2. Мультимедійна система Acer X113 DLP – 1шт.* *3. Монітор Panasonic TX 32" FR 250K LED HD – 6 шт.* *4. Системний блок Everest Enterprise 7600.* *5. Монітор Aser SA 240 Ydid – 1 шт.* *Програмно-апаратний комплекс AlienVault SIEM (OSSIM) від компанії-вендора AlienVault – 2017 рік.:* *- платформа USM (OSSIM) для збору, моніторингу, аналізу подій і загроз інформаційної безпеки.* *Лабораторія Безпеки інформаційно-комунікаційних технологій CISCO:* *1.Комп'ютери Intel Cougar Point H61 2x, 2700 MGhz на МП H61b-K, 2 Гб ОЗУ DDR3 (2015) – 15 шт.* *2. Мультимедійна система Acer 113 – 1шт.* *3.Маршрутизатор TP–Link ARCHER C60 AC 1350 – 1 шт.;* *4.Маршрутизатор Huawei AR120 – 1шт.;*

				5.Комутатор L2+24ZIXEL -1шт.; 6.Мережеве сховище My Cloud Home – 1шт. *Програмний комплекс для організації дистанційного навчання в комплексному цифровому навчальному середовищі Google Workspace for Education.*
Науково-технічний переклад	навчальна дисципліна	*4. Науково-технічний переклад_р.pdf*	m1zNnImZgR4aRKQHP7LhbINle8TyrOUvGd012t9R810=	*Навчальна лабораторія Центр управління інформаційною та кібербезпекою (Security Operation Center) - 2017 рік.:* *1.Комп'ютери Asus p5gc-mx - 3шт.; (2015 року) ITS 5400 - 7 шт. (2017 року).* *2. Мультимедійна система Acer X113 DLP – 1шт.* *3. Монітор Panasonic TX 32" FR 250K LED HD – 6 шт.* *4. Системний блок Everest Enterprise 7600.* *5. Монітор Aser SA 240 Ydid – 1 шт.* *Програмно-апаратний комплекс USM/SIEM від компанії-вендора AlienVault:* *- платформа USM (OSSIM) для збору, моніторингу, аналізу подій і загроз інформаційної безпеки;* *- SIEM для управління інформацією та подіями безпеки.* *Програмні засоби підтримки прийняття рішень у сфері інформаційної безпеки («Вибір», Mpriority1.0).* *Мультимедійна система - 1 шт.* *Програмний комплекс для організації дистанційного навчання в комплексному цифровому навчальному середовищі Google Workspace for Education.*
Управління ризиками інформаційної безпеки	навчальна дисципліна	*5. Управління ризиками ІБ.pdf*	tIgL6mDYIjp1Q7Dm7ag3yVJeLRKRi+uXZ49A4fHmhAw=	*Навчальна лабораторія Центр управління інформаційною та кібербезпекою (Security Operation Center) - 2017 рік.:* *1.Комп'ютери Asus p5gc-mx - 3шт.; (2015 року) ITS 5400 - 7 шт. (2017 року).* *2. Мультимедійна система Acer X113 DLP – 1шт.* *3. Монітор Panasonic TX 32" FR 250K LED HD – 6 шт.* *4. Системний блок Everest Enterprise 7600.* *5. Монітор Aser SA 240 Ydid – 1 шт.* *Програмно-апаратний комплекс AlienVault SIEM (OSSIM) від компанії-вендора AlienVault - 2017 рік.:* *- платформа USM (OSSIM) для збору, моніторингу, аналізу подій і загроз інформаційної безпеки;* *- SIEM для управління інформацією та подіями безпеки;* *- Nessus Essentials – для виявлення вразливостей у програмному забезпеченні, мережах і пристроях;* *- Kali Linux - для проведення тестів на проникнення, аналізу безпеки та цифрової криміналістики;* *- QRadar Community Edition для аналізу подій безпеки, управління*

				журналами, розслідування інцидентів. *Лабораторія Безпеки інформаційно-комунікаційних технологій CISCO:* *1.Комп'ютери Intel Cougar Point H61 2x, 2700 MGhz на МП H61b-K, 2 Гб ОЗУ DDR3 (2015) – 15 шт.* *2. Мультимедійна система Acer 113 – 1шт.* *3.Маршрутизатор TP–Link ARCHER C60 AC 1350 – 1 шт.;* *4.Маршрутизатор Huawei AR120 – 1шт.;* *5.Комутатор L2+24ZIXEL -1шт.;* *6.Мережеве сховище My Cloud Home – 1шт.* *Програмні засоби підтримки прийняття рішень у сфері інформаційної безпеки («Вибір», Mpriority1.0).* *Програмний комплекс для організації дистанційного навчання в комплексному цифровому навчальному середовищі Google Workspace for Education.*
Системи управління інформаційною безпекою	навчальна дисципліна	*6. Системи управл ІБ_р.pdf*	VbqKQWTZEGcoC8czDlbP+Ng9GQQDtNHbvDtqayNiVz4=	*Навчальна лабораторія Центр управління інформаційною та кібербезпекою (Security Operation Center) - 2017 рік.:* *1.Комп'ютери Asus p5gc-mx - 3шт.; (2015 року) ITS 5400 - 7 шт. (2017 року).* *2. Мультимедійна система Acer X113 DLP – 1шт.* *3. Монітор Panasonic TX 32" FR 250K LED HD – 6 шт.* *4. Системний блок Everest Enterprise 7600.* *5. Монітор Aser SA 240 Ydid – 1 шт.* *Програмно-апаратний комплекс AlienVault SIEM (OSSIM)від компанії-вендора AlienVault:* *- платформа USM (OSSIM) для збору, моніторингу, аналізу подій і загроз інформаційної безпеки;* *- SIEM для управління інформацією та подіями безпеки;* *- Nessus Essentials – для виявлення вразливостей у програмному забезпеченні, мережах і пристроях;* *- Kali Linux - для проведення тестів на проникнення, аналізу безпеки та цифрової криміналістики;* *- QRadar Community Edition для аналізу подій безпеки, управління журналами, розслідування інцидентів.* *Програмні засоби підтримки прийняття рішень у сфері інформаційної безпеки («Вибір», Mpriority1.0).* *Навчальна лабораторія засобів контролю доступу «HIKVISION»:* *1. Відеокамери DS-2CD2420F-1, DS-2CD1021-1, DS-2CD4A26FWD-IZS, DS-2CD1331-1, DS-2CD2125F1, DS-7608NI-E2/8P.* *2. Мінівідеокамера Osculus S970.* *3. Контрольний пристрій ST-03-TEST.* *Лабораторія Безпеки інформаційно-комунікаційних технологій CISCO:*

				1.Комп'ютери Intel Cougar Point H61 2x, 2700 MGhz на МП H61b-K, 2 Гб ОЗУ DDR3 (2015) – 15 шт. *2. Мультимедійна система Acer 113 – 1шт.* *3.Маршрутизатор TP–Link ARCHER C60 AC 1350 – 1 шт.;* *4.Маршрутизатор Huawei AR120 – 1шт.;* *5.Комутатор L2+24ZIXEL -1шт.;* *6.Мережеве сховище My Cloud Home – 1шт.* *Програмний комплекс для організації дистанційного навчання в комплексному цифровому навчальному середовищі Google Workspace for Education.*
Управління проєктами інформаційної безпеки	навчальна дисципліна	*7. Управління проєктами ІБ_р.pdf*	Bg3BoVaCmgVDTJvS9cm995ErjeQ1GnInpCoQakYv2iw=	*Навчальна лабораторія Центр управління інформаційною та кібербезпекою (Security Operation Center) - 2017 рік.:* *1.Комп'ютери Asus p5gc-mx - 3шт.; (2015 року) ITS 5400 - 7 шт. (2017 року).* *2. Мультимедійна система Acer X113 DLP – 1шт.* *3. Монітор Panasonic TX 32" FR 250K LED HD – 6 шт.* *4. Системний блок Everest Enterprise 7600.* *5. Монітор Aser SA 240 Ydid – 1 шт.* *Програмні засоби підтримки прийняття рішень у сфері інформаційної безпеки («Вибір», Mpriority1.0).* *QRadar Community Edition для аналізу подій безпеки, управління журналами, розслідування інцидентів.* *Програмний комплекс для організації дистанційного навчання в комплексному цифровому навчальному середовищі Google Workspace for Education.*
Прикладна загальна теорія систем інформаційної безпеки	навчальна дисципліна	*8_Прикладана_та_загальна_теорія_систем_ІБ_р.pdf*	yPBj+/Li0OUudNMoS9EhgyiYQFKFNKtnTne10lmDU9A=	*Навчальна лабораторія Центр управління інформаційною та кібербезпекою (Security Operation Center) - 2017 рік.:* *1.Комп'ютери Asus p5gc-mx - 3шт.; (2015 року) ITS 5400 - 7 шт. (2017 року).* *2. Мультимедійна система Acer X113 DLP – 1шт.* *3. Монітор Panasonic TX 32" FR 250K LED HD – 6 шт.* *4. Системний блок Everest Enterprise 7600.* *5. Монітор Aser SA 240 Ydid – 1 шт.* *Лабораторія Безпеки інформаційно-комунікаційних технологій CISCO:* *1.Комп'ютери Intel Cougar Point H61 2x, 2700 MGhz на МП H61b-K, 2 Гб ОЗУ DDR3 (2015) – 15 шт.* *2. Мультимедійна система Acer 113 – 1шт.* *3.Маршрутизатор TP–Link ARCHER C60 AC 1350 – 1 шт.;* *4.Маршрутизатор Huawei AR120 – 1шт.;* *5.Комутатор L2+24ZIXEL -1шт.;* *6.Мережеве сховище My Cloud Home – 1шт.* *Програмні засоби підтримки*

				прийняття рішень у сфері інформаційної безпеки («Вибір», Mpriority1.0). *Програмний комплекс для організації дистанційного навчання в комплексному цифровому навчальному середовищі Google Workspace for Education.*
Науково-педагогічна практика	практика	*Науково-педагогічна практика.pdf*	1MIhnH7FoQxTAxvA28SpQK19aGcd2bhdbi1yYYdkSm8=	*Матеріально-технічне забезпечення та програмне забезпечення відповідно бази проходження практики* *1. Лабораторія Безпеки інформаційно-комунікаційних технологій CISCO.* *2. Академічний центр компетенцій IBM «Кіберполігон».* *3. Навчальна лабораторія технічного захисту інформації «PIAC».* *4. Навчальна лабораторія Центр управління інформаційною та кібербезпекою (Security Operation Center).* *Програмний комплекс для організації дистанційного навчання в комплексному цифровому навчальному середовищі Google Workspace for Education.*
Науково-дослідна практика	практика	*Науково-дослідна практика_р (2).pdf*	LQOTnpqyifsuu8xHb2XZPmzEVmbVeIrxx1SIlYfPhBo=	*Матеріально-технічне забезпечення та програмне забезпечення відповідно бази проходження практики у лабораторіях:* *1. Лабораторія Безпеки інформаційно-комунікаційних технологій CISCO.* *2. Академічний центр компетенцій IBM «Кіберполігон».* *3. Лабораторія Криптографічного захисту на базі технологій АВТОР.* *4. Навчальна лабораторія засобів контролю доступу «HIKVISION».* *5. Навчальна лабораторія технічного захисту інформації «PIAC».* *Програмно-апаратний комплекс AlienVault SIEM (OSSIM)від компанії-вендора AlienVault:* *- платформа USM (OSSIM) для збору, моніторингу, аналізу подій і загроз інформаційної безпеки;* *- SIEM для управління інформацією та подіями безпеки;* *- Nessus Essentials – для виявлення вразливостей у програмному забезпеченні, мережах і пристроях;* *- Kali Linux - для проведення тестів на проникнення, аналізу безпеки та цифрової криміналістики;* *- QRadar Community Edition для аналізу подій безпеки, управління журналами, розслідування інцидентів.* *Програмний комплекс для організації дистанційного навчання в комплексному цифровому навчальному середовищі Google Workspace for Education.*
Переддипломна практика	практика	*Передипл практика.pdf*	t042OT6E/cbcAGyqY1gry6WN5cFX/7UXi	*Матеріально-технічне забезпечення та програмне*

			uUhW9vOC7w=	*забезпечення відповідно бази проходження практики у лабораторіях:* *1. Лабораторія Безпеки інформаційно-комунікаційних технологій CISCO.* *2. Академічний центр компетенцій IBM «Кіберполігон».* *3. Лабораторія Криптографічного захисту на базі технологій АВТОР.* *4. Навчальна лабораторія засобів контролю доступу «HIKVISION».* *5. Навчальна лабораторія технічного захисту інформації «PIAC».* *Навчальна лабораторія Центр управління інформаційною та кібербезпекою (Security Operation Center). Програмно-апаратний комплекс AlienVault SIEM (OSSIM)від компанії-вендора AlienVault:* *- платформа USM (OSSIM) для збору, моніторингу, аналізу подій і загроз інформаційної безпеки;* *- SIEM для управління інформацією та подіями безпеки;* *- Nessus Essentials – для виявлення вразливостей у програмному забезпеченні, мережах і пристроях;* *- Kali Linux - для проведення тестів на проникнення, аналізу безпеки та цифрової криміналістики;* *- QRadar Community Edition для аналізу подій безпеки, управління журналами, розслідування інцидентів.* *Програмний комплекс для організації дистанційного навчання в комплексному цифровому навчальному середовищі Google Workspace for Education.*
Кваліфікаційна робота	підсумкова атестація	*Кваліфікаційна робота_2024_p.pdf*	6ZfiL99GYJB37hVFvPcK3sSUXbtI8hUYB4NWe7mtKOs=	*1. Лабораторія Безпеки інформаційно-комунікаційних технологій CISCO.* *2. Академічний центр компетенцій IBM «Кіберполігон».* *3. Лабораторія Криптографічного захисту на базі технологій АВТОР.* *4. Навчальна лабораторія засобів контролю доступу «HIKVISION».* *5. Навчальна лабораторія технічного захисту інформації «PIAC».* *6. Навчальна лабораторія Центр управління інформаційною та кібербезпекою (Security Operation Center).* *Програмний комплекс для організації дистанційного навчання в комплексному цифровому навчальному середовищі Google Workspace for Education.*

* 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 оствітнім 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)
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	13	Педагогіка та психологія у вищій школі	Освіта: Київський національний університет імені Тараса Шевченка, 1998 р., спеціальність: Українська мова та література, кваліфікація: філолог, викладач української мови та літератури Науковий ступінь: 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) п’ять публікацій у наукових виданнях, які включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection, протягом останніх п’яти років. 1. Н. Кондратенко, М. Швардак Н. Божинський Б. Божинський Г. Марченко Особливості прийняття управлінських рішень керівником закладу освіти, їх оцінка в умовах кризи. Journal of Higher Education Theory and Practice, West Palm Beach, Vol. 21 No. 14 (2021). Збірник індексується в міжнародних базах даних: (Scopus) (Web of Science) 2. Стежко С.О., Кондратенко Н.Ю. Марченко Г.В. Теоретичні аспекти формування комунікативної компетентності майбутніх журналістів на засадах

							лінгвокультурології. Імідж сучасного педагога. №4 (193) 2020 р. С. 67-73. 3. Стежко С.О., Кондратенко Н.Ю. Марченко Г.В. Лінгводидактичні основи формування комунікативної компетентності майбутніх журналістів на засадах лінгвокультурології. Інноваційна педагогіка №27 2020 р. С. 86-93. 4. Нікітченко А. Ю., Яковенко Н. Д., Срібна І. М., Кондратенко Н. Ю. Вплив інформаційних технологій на життя людей з особливими потребами. Зв'язок, № 1 (149), 2021 (фахове видання) 5. Кондратенко Н.Ю., Стежко С.О., Марченко Г В Психолого–педагогічні засади формування комунікативної компетентності майбутніх журналістів на засадах лінгвокультурології Науковий вісник Мукачівського державного університету. Т. 7, № 1, 2021 Серія «Педагогіка і психологія». С. 133-122 (фахове видання) 6. Tetiana Miyer, Larysa Holodiuk, Natalia Siranchuk, Natalia Dyka, Nataliya Kondratenko, Lyudmila Romanenko, Kateryna Romanenko. Pedagogical context of attributiveness of reflection in traditional and elearning of future teachers and already working as socially oriented individuals., Ad Alta: Journal of interdisciplinary Research., 7. (2). С. 166-174. (Scopus) https://elibrary.kubg.edu.ua/id/eprint/43204/1/T_MIYER_L_HOLODIUK_N_SIRANCHUK_ta_in_PCARTEFTAWSOI_FPO_2022.pdf 8. Stezhko Svitlana, Kondratenko Natalia, Zabolotnia Ruslana, Stezhko Myroslav, Zabolotnii Bohdan, TEAMBUILDING AS A TOOL FOR EFFECTIVE IT-COMPANY MANAGEMENT. Телекомунікаційніта

							інформаційні технології, № 2 (83) 2024 фахове видання 9. Стежко С.О., Кондратенко Н.Ю., Марченко Г.В. Запровадження принципів академічної доброчесності у Державному університеті телекомунікацій. Збірник наукових есе учасників дистанційного етапу наукового стажування для освітян (Республіка Польща, Варшава, 02.11 – 11.12.2020) / Польсько-українська фундація «Інститут Міжнародної Академічної та Наукової Співпраці», Духовна Академія Університету Кардинала Стефана Вишинського, Фундація ADD. – Варшава, 2020. С. 115-118.
81112	Гайдур Галина Іванівна	завідувач кафедри, Основне місце роботи	Навчально-науковий інститут Захисту інформації	Диплом спеціаліста, Київський інститут зв'язку Української державної академії зв'язку імені О.С. Попова, рік закінчення: 2001, спеціальність: Телекомунікаційні системи та мережі, Диплом доктора наук ДД 008401, виданий 05.03.2019, Диплом кандидата наук ДК 019172, виданий 17.01.2014, Атестат доцента 12ДЦ 043924, виданий 29.09.2015, Атестат професора АП 001534, виданий 26.02.2020	18	Прикладна загальна теорія систем інформаційної безпеки	1. Гайдур Г. І., Шулімова Д. Д., Бойко А. О., Постніков Є. І. Модель забезпечення кібербезпеки інтернету речей Телекомунікаційні та інформаційні технології. № 2 (2024). С 4-13. DOI: 10.31673/2412-4338.2024.020515 2. Гайдур, Г. І., Гахов, С. О., Марченко, В. В., & Гайдур, К. В. (2024). Концептуальна модель виявлення фішингових атак на основі використання методів опорних векторів. Сучасний захист інформації, 2(58), 24–33. https://doi.org/10.31673/2409-7292.2024.020003 3. Гайдур,Г. І., Бригинець,А. А. (2024). Захист конфіденційних даних у снепшотах Amazon Elastic Block Store. Сучасний захист інформації, 1(57), 15–21. https://doi.org/10.31673/2409-7292.2024.010002. 4. Скибун, О. Ж., Гайдур, Г. І., & Гахов С. О. (2024). Аналіз використання концепції BYOD в корпоративних інформаційних системах. Сучасний захист інформації,

							1(57), 50–56. https://doi.org/10.31673/2409-7292.2024.010006 . 5. Легомінова, С.В., Гайдур Г.І. Аналіз сучасних загроз інформаційній безпеці організацій та формування інформаційної платформи протидії їм. Кібербезпека: освіта, наука, техніка. 2023. - №2(22). – С. 56-67. DOI 10.28925/2663-4023.2023.22.5467 6. Ганченко М.І., Гайдур Г.І., Гахов С.О., Дмітрієв В.Є. “Актуальність та перспектива розвитку Privileged Access Management рішень.” Зв’язок. 2022. №1 (2022). С. 3-9. DOI: 10.31673/2412-9070.2022.010310 Доступ: https://con.dut.edu.ua/index.php/communication/article/view/2578 7. Гайдур Г. І., Гахов С. О., Бригинець А. А. Виявлення мережевих аномалій з використанням алгоритмів нейронних мереж. Телекомунікаційні та інформаційні технології. № 1 (2023). С. 61-73. DOI: 10.31673/2412-4338.2023.016173 8. Гайдур Г. І. Гахов С. О, Сич М. В., Дмітрієв В. Є. Аналіз загроз мережевого трафіку рівнів моделі OSI для динамічного розрахунку RTO в контексті боротьби з DDOS атаками. Телекомунікаційні та інформаційні технології. № 3 (2023). С. 12-21. DOI: 10.31673/2412-4338.2023.031221 9. Haidur, H. The Method of Increasing the Efficiency of Signal Processing Due to the Use of Harmonic Operators // Zamrii, I., Haidur, H., Sobchuk, A., Zinchenko, K., Polovinkin, I. // 2022 IEEE 4th International Conference on Advanced Trends in Information Theory, ATIT 2022 - Proceedings, 2022, pp. 138–141.(Scopus) 10. Гайдур Г.І., Гахов С.О., Марченко В.В. Метод побудови динамічної моделі

							логічного об'єкта інформаційної системи та визначення закону його функціонування. Radioelectronic and Computer Systems, 2022, no. 1(101). С. 129-140. doi: 10.32620/reks.2022.1.10 . (Категорія А, Scopus). 11. Кожухівський А. Д., Квантовий алгоритм пошуку в неструктурованій базі даних / А. Д. Кожухівський, Г. І. Гайдур, О. А. Кожухівська // Наукові записки Державного університету телекомунікацій. 2022. - № 1-2 (2022). –с 10-14. 12. Гайдур Г.І., Гахов С.О. Дмітрієв В.Є., Бондаренко Н.В. Виявлення аномалій трафіку в інформаційних системах організацій з використанням методів Machine Learning на основі алгоритмів прогнозування категорійних полів. Телекомунікаційні та інформаційні технології. 2021. № 4 (73). С.41-53. 13. Гайдур Г. І., Гахов С. О. , Дмітрієв В. Є. , Ганченко М. І. Актуальність та перспектива розвитку Privileged Access Management рішень. Зв'язок. № 1 (2022).- С. 3-9. 14. V. Savchenko, H. Haidur, S. Gakhov, S. Lehominova, T. Muzshanova, I. Novikova. Model of Control in a UAV Group for Hidden Transmitters Detection on the Basis of Local Self-Organization. International Journal of Advanced Trends in Computer Science and Engineering. Volume 9, No.4, pp. 6167-6174. July – August 2020. Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse291942020.pdf. https://doi.org/10.30534/ijatcse/2020/291942020 Scopus. 15. .Semon Bohdan , Bondarchuk Andrii , Vyshnivskyi Viktor , Sierykh Serhii , Haidur Halyna, Kalashnyk-Rybalko Myroslava , Safarian Marat The

							electromagnetic waves scattering evaluation on the composite material fractal structure with radioisotope elements 2019. International Journal of Advanced Trends in Computer Science and Engineering. - dvanced Trends in Computer Science and Engineering, 8(5), September - October 2019. - Scopus Indexed - ISSN. 2278-3091, P 2273-2276 Scopus. 16. Laptiev Oleksandr, Shuklin German, Savchenko Vitalii, Barabash Oleg, Musienko Andrii and Haidur Halyna, The Method of Hidden Transmitters Detection based on the Differential Transformation Model. International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) Volume 8 No. 6 (November - December 2019) Scopus Indexed - ISSN 2278 – 3091, P.2840-2846. Режим доступу: www.warse.org/IJATCSE/static/pdf/file/ijatcse26862019.pdf . Scopus. 17. Гайдур Г.І., Гахов С.О. Теоретичний підхід до вирішення проблеми виявлення шкідливих процесів на основі аналізу станів логічного об'єкта інформаційної системи. Телекомунікаційні та інформаційні технології. 2021. № 1 (70). С. 79-87. 18. Борсуковський Ю. В., Гайдур Г.І. Визначення вимог щодо побудови концепції інформаційної безпеки в умовах гібридних загроз. Частина 4 SWorld Journal, September 2021, Issue 9, Part 1, p.36-42. / DOI: 10.30888/2663-5712.2021-09-01-025 / ISSN 2663-5712
115586	Мужанова Тетяна Михайлівна	доцент, Основне місце роботи	Навчально-науковий інститут Захисту інформації	Диплом спеціаліста, Чернівецький державний університет імені Федьковича, рік закінчення: 1996, спеціальність: , Диплом	15	Науково-технічний переклад	Освіта: 1.Чернівецький державний університет ім. Ю. Федьковича, 1996, спеціальність: всесвітня історія, кваліфікація: історик, викладач історії. 2. Українська академія державного

				магістра, УАДУ при Призеленті України, рік закінчення: 2002, спеціальність: , Диплом кандидата наук ДК 053265, виданий 08.07.2009, Атестат доцента АД 006514, виданий 09.02.2021			управління при Президентові України, 2002, спеціальність: державне управління, кваліфікація: магістр державного управління. Науковий ступінь: кандидат наук з державного управління, (ДК № 053265 від 08.07.2009 р.) спеціальність: 25.00.01 – теорія та історія державного управління. Вчене звання: доцент за кафедрою управління інформаційною та кібернетичною безпекою 2021р., (АД № 006514, 2021 р.) п’ять публікацій у наукових виданнях, які включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection, протягом останніх п’яти років 1. Мужанова Т.М., Легомінова С.В., Якименко Ю.М., Щавінський Ю.В., Нестеренко Г.П. Основні підходи й напрями розвитку політики кібербезпеки Європейського Союзу. Кібербезпека: освіта, наука, техніка. 2024. № 4. С. 133-149. DOI: 10.28925/2663-4023.2024.24.133149 2. Lehominova, S., Shchavinsky, Y., Muzhanova, T., Rabchun, D., Zaporozhchenko, M. Application of Sentiment Analysis to Prevent Cyberattacks on Objects of Critical Information Infrastructure. International Journal of Computing, 2023, 22(4), pp. 534–540 URL: https://doi.org/10.47839/ijc.22.4.3362 (SCOPUS) 3. Shchavinsky, Y. V., T. M. Muzhanova, Y. M. Yakymenko, and M. M. Zaporozhchenko. Application of Artificial Intelligence for Improving Situational Training of Cybersecurity Specialists. Information Technologies and

							Learning Tools, vol. 97, no. 5, Oct. 2023, pp. 215-26, https://doi.org/10.33407/itlt.v97i5.5424 (WEB OF SCIENCE) 4. Якименко Ю.М., Рабчун Д.І., Мужанова Т.М., Запорожченко М.М., Щавінський Ю.В. Технічний аудит захищеності інформаційно-телекомунікаційних систем підприємства. Кібербезпека: освіта, наука, техніка. 2023. № 2. С. 45-61. URL: https://doi.org/10.28925/2663-4023.2023.20.4561 5. Lehominova S.V., Shchavinsʹkyy YU.V., Muzhanova T.M., Dzyuba T.M., Rabchun D.I. Legal mechanisms for ensuring information security in Ukraine in the conditions of hybrid war. Телекомунікаційні та інформаційні технології. 2023. № 1. С.100-110. URL: https://doi.org/10.31673/2412-4338.2023.0101111 6. Тищенко В.С., Мужанова Т.М. Дезінформація і фейкові новини: ознаки та методи виявлення в мережі Інтернет. Кібербезпека: освіта, наука, техніка. 2022. № 2(18), С. 175-186. URL: https://csecurity.kubg.edu.ua/index.php/journal/ article/view/413 7. Tetiana M. Muzhanova, Yuriy M. Yakymenko, Mykhailo M. Zaporozhchenko, Vitalij S. Tyshchenko. International Vendor-Neutral Certification for Information Security Professionals. Кібербезпека: освіта, наука, техніка. 2022. № 4 (16). С. 129-141. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/ view/369/306 8. Akhramovych, V., Shuklin, G., Pepa, Y., Muzhanova, T., Zozulia, S. Devising a Procedure to Determine the Level of Informational Space Security in Social Networks Considering Interrelations Among Users. Eastern-European Journal of Enterprise

							Technologies, 2022, 1(9-115), pp. 63–74 URL: https://journals.uran.ua/eejet/article/view/252135 (SCOPUS) 9. Легомінова С.В., Мужанова Т.М., Якименко Ю.М. Системний аналіз технічних систем забезпечення інформаційної безпеки підприємств від компанії Fireeye. Кібербезпека: освіта, наука, техніка. 2021. № 2. С.36-50. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/251/22510. Мужанова Т.М., Легомінова С.В., Якименко Ю.М., Мордас І.В. Технології моніторингу й аналізу діяльності користувачів у запобіганні внутрішнім загрозам інформаційній безпеці організації. Кібербезпека: освіта, наука, техніка. 2021. Том 1. № 13. С.50-62. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/281/24111. В. Зацерковний, Л. Плічко, О. Приліпко, О. Ніколаєнко, Т. Мужанова Обгрунтування доцільності застосування геоінформаційних систем у ландшафтно-екологічному моніторингу. Вісник Київського Національного Університету імені Тараса Шевченка. Геологія. 2020. Випуск 1(88). С. 98-105. (Web of Science) 12. Мордас І.В., Мужанова Т. М. Забезпечення економічної безпеки України в контексті глобалізаційних процесів. Економіка. Менеджмент. Бізнес. 2020. № 1(31). С. 44-48. 13. Мужанова Т.М., Якименко Ю.М. Аналіз стану використання методичних підходів до оцінки рівня економічної безпеки підприємства. Економіка. Менеджмент. Бізнес. 2020. № 1(31). С. 64-69.

435683	Щавінський Юрій Віталійович	доцент, Основне місце роботи	Навчально-науковий інститут Захисту інформації	Диплом спеціаліста, Хмельницьке вище артилерійське командне училище, рік закінчення: 1982, спеціальність: командна, тактична, артилерійське озброєння, Диплом кандидата наук ДК 055434, виданий 16.12.2019	16	Корпоративна та професійна етика в кібербезпеці	Освіта: 1. Хмельницьке вище артилерійське командне училище імені маршала артилерії Яковлєва М.Д. спеціальність - «командна, тактична, артилерійське озброєння», кваліфікація - «Офіцер з вищою військово-спеціальною освітою, інженер по експлуатації артилерійського озброєння», 1982. (Диплом ИВ-1 № 372900) 2.Академія ЗСУ, спеціальність - «8.140103 Частини та з'єднання РВіА», кваліфікація - «Офіцер військового управління оперативно-тактичної рівня». 1996. (Диплом ЛЖ БЕ№011564) Науковий ступінь: Кандидат технічних наук, спеціальності 20.02.14 Озброєння та військова техніка, (ДК № 055434 від 16.12.2019 р.) Вчене звання: доцент за кафедрою Управління інформаційною та кібернетичною безпекою, (АД № 014638 від 21.02. 2024 р.) п'ять публікацій у наукових виданнях, які включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection, протягом останніх п'яти років 1. Легомінова С.В., Щавінський Ю.В., Рабчун Д.І., Запрожченко М.М., Будзинський О.В. Небезпека інструментів OSINT та способи пом'якшення наслідків їх використання для організації. Кібербезпека: освіта, наука, техніка, 2024. Т 1(25). С. 45–61. 2. Легомінова С.В., Мужанова Т.М., Якименко Ю.М., Щавінський Ю.В., Нестеренко Г.П. Розвиток політики кібербезпеки ЄС: підходи та рішення Кібербезпека: освіта,

							наука, техніка. 2024. № 4 (24). С. 77-84. 3. Легомінова С.В., Щавінський Ю.В., Будзинський О.В. Аналіз сучасних підходів до забезпечення кібербезпеки корпоративних баз даних Сучасний захист інформації. 2024. №2(58). С. 84-91. 4. Lehominova, S., Shchavinsky, Y., Muzhanova, T., Rabchun, D., & Zaporozhchenko, M. (2023). Application of Sentiment Analysis to Prevent Cyberattacks on Objects of Critical Information Infrastructure. International Journal of Computing, 22(4), 534-540. URL: https://doi.org/10.47839/ijc.22.4.3362 (Scopus) 5. Shchavinsky Y. V., Muzhanova T. M., Yakymenko Y. M., and Zaporozhchenko M. M.. Application of artificial intelligence for improving situational training of cybersecurity specialists, ITLT, vol. 97, no. 5, pp. 215–226, 2023. URL: https://doi.org/10.33407/itlt.v97i5.5424 (Web of Science) 6. Власенко В.О., Щавінський Ю.В., Запорожченко М.М., Тищенко В.С. Аналіз технологій побудови мережі передавання даних із високими вимогами щодо інформаційної безпеки, надійності та затримки. Зв'язок, №3 2023. с. 8-15. URL: https://doi.org/10.31673/2412-9070.2023.032030 7. Якименко Ю. М., Рабчун Д. І., Мужанова Т.М., Запорожченко М.М., Щавінський Ю. В. Технічний аудит захищеності інформаційно - телекомунікаційних систем підприємств. Кібербезпека: освіта, наука, техніка. 2023. № 18 с. 45-61. URL: https://doi.org/10.28925/2663-4023.2023.20.4561 (фаховий журнал категорії Б) 8. Lehominova S.V., Shchainskyy YU.V.,

							Muzhanova T.M., Dzyuba T.M., Rabchun D.I. Legal mechanisms for ensuring information security in ukraine in the conditions of hybrid war. Телекомунікаційні та інформаційні технології, №1(2023). URL: https://doi.org/10.31673/2412-4338.2023.0101111 . (фаховий журнал категорії Б) 9. Щавінський Ю., Флис І., Красник Я., Бударецький Ю. Застосування дискримінантного аналізу для автоматизації розпізнавання зображень безпілотних літальних апаратів. Військово-технічний збірник № 28 (2023) (Т). Львів. – 2023. С. 28-37. (фаховий журнал категорії Б) 10. Юрій Щавінський, Олена Левчук, Віктор Левчук, Олександр Сирський. Організаційно-технічні і правові аспекти формування компетентностей військових фахівців /Збірник наукових праць “Військова освіта” Національного університету оборони України імені Івана Черняховського, м. Київ. 2022. № 2 (46). С. 311-324. URL: https://doi.org/10.33099/2617-1775/2022-02/311-324 (фаховий журнал категорії Б) 11. Щавінський Ю. В., Бударецький Ю. І., Красник Я. В., Іваник Є. Г. Використання методу динамічного програмування для структурно-алгоритмічної оптимізації процесу підготовки даних для стрільби артилерійських систем. Озброєння та військова техніка: Науково-технічний журнал №4 (75) ч.2(т). – К.: ЦНДІ ОВТ, 2019. – С. 75-94. (фаховий журнал категорії Б) 12. Yakovenko, V., Furmanova, N., Flys, I., Shchavinsky, Y., Farafonov, O., Malyi, O., & Samoylyk, S. (2022). Determining the components of the structural-automatic

							model of firing a single target in armor protection with fragmentation-beam projectiles of directed action in a series of three shots based on the reference graph of states. Eastern-European Journal of Enterprise Technologies, 5(3(119), 29–41. URL:https://doi.org/10.15587/1729-4061.2022.266275 (категорія «А», індексація Scopus) 13. Ю.В. Щавінський, О.А. Полоз, П.І. Ванкевич, І.М. Ільків, В.Д. Смичок, Є.Г. Іваник. Формування комплексу забезпечення польотів метеорологічних кульзондів для уточнення аерологічних вимірювань. Збірник наукових праць № 1(84) (Т) інв. 3681. Центральний науково-дослідний інститут ОВТ ЗСУ. Київ. – 2022. – С. 215-228 (фаховий журнал категорії Б) 14. Бударецький Ю.І., Щавінський Ю.В., Кузнецов В.В., Ніколаєв С.Т. Застосування методу аналізу ієрархій для оцінювання програмного забезпечення комплексів засобів автоматизації. Військово-технічний збірник. 2021. № 25. С. 3-12.URL: https://doi.org/10.33577/2312-4458.25.2021.3-12 (фаховий журнал категорії Б) 15. Петлюк І.В., Щавінський Ю.В. Використання військових систем імітаційного моделювання для визначення доцільних характеристик перспективного артилерійського озброєння. Зб. Наук. праць військової академії (м. Одеса): Одеса: ВА, 2020, - вип. 2(14). Ч.1. с. – 12-23. URL:https://doi.org/10.37129/2313-7509.2020.14.1.11-22 (фаховий журнал категорії Б) 16. Щавінський Ю., Полоз О., Ніколаєв С., Дубіль Р. Системно-технічні аспекти удосконалення метеорологічного забезпечення стрільби

							артилерійських систем. Військово-технічний збірник №23(т/2020). – Львів: НАСВ, 2020. – С. 54-64. (фаховий журнал категорії Б) 17. Бударецький Ю.І., Щавінський Ю.В., Бахмат М.В., Олійник М.Я., Іваник Є.Г. Удосконалення математичного забезпечення комплексу засобів автоматизації для ведення вогню артилерійськими системами. Озброєння та військова техніка: Науково-технічний журнал. №2 (26) – К.: ЦНДІ ОВТ, 2020. – С. 94-104. URL: https://doi.org/1034169/2414-0651.2020.2(26).94-102.10-4/4 (фаховий журнал категорії Б)
322264	Капелюшна Тетяна Вікторівна	доцент, Основне місце роботи	Навчально-науковий інститут Захисту інформації	Диплом бакалавра, Київська державна академія водного транспорту імені гетьмана Петра Конашевича-Сагайдачного, рік закінчення: 2005, спеціальність: 0502 Менеджмент, Диплом магістра, Київська державна академія водного транспорту імені гетьмана Петра Конашевича-Сагайдачного, рік закінчення: 2006, спеціальність: 0502 Менеджмент організацій, Диплом кандидата наук ДК 030756, виданий 29.09.2015, Атестат доцента АД 004582, виданий 14.05.2020	18	Організація проведення наукових досліджень	Освіта: 1. Київська державна академія водного транспорту ім. гетьмана П. Конашевича-Сагайдачного, 2005 р., спеціальність: менеджмент, кваліфікація: бакалавр менеджменту. (Диплом КВ №26350935) 2. Київська державна академія водного транспорту ім. гетьмана П. Конашевича-Сагайдачного, 2006 р., спеціальність: менеджмент організацій, кваліфікація: магістр з менеджменту. (Диплом КВ №30485151) Науковий ступінь: кандидат економічних наук. Наукова спеціальність: 08.00.04 – економіка і управління підприємствами (за видами економічної діяльності), (ДК №030756 від 29 вересня 2015 р., виданий МОН України) Вчене звання: доцент кафедри підприємництва, торгівлі та біржової діяльності, (АД №004582 від 14 .05.2020 р., виданий МОН України)

							п’ять публікацій у наукових виданнях, які включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection, протягом останніх п’яти років 1. Kapeliushna T., Lehominova S., Goloborodko A., Lysetskyi Yu., Nosova T. Methodological approaches to enterprise security management: traditional and transformed to the conditions of functioning. Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu. 2024. No. 3. P. 204-209. URL: https://doi.org/10.33271/nvngu/2024-3/204. (0,99 д.а., авторський внесок 0,2 д.а., полягає в аналізі методичних підходів до управління безпекою підприємства) (Scopus). 2. Kapeliushna T., Goloborodko A., Nesterenko S. Bezhenar I., Matviichuk B. Analysis of digitalization changes and their impact on enterprise security management under uncertainty. Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu. 2023. No. 4. P. 150–156. URL: https://doi.org/10.33271/nvngu/2023-4/150. (1,01 д.а., авторський внесок 0,21 д.а., полягає в обґрунтуванні врахування трансформаційних змін, що викликані діджиталізацією в управлінні безпекою) (Scopus). 3. Kapeliushna T., Dymenko R., Safonov Yu. Kachmala V., Borshch V., Sheremet O. Digital tools for effective student learning and training online in conditions of uncertainty. Financial and Credit Activity Problems of Theory and Practice. 2022. Vol. 6, No. 47. P. 469–479. URL: https://doi.org/10.55643/fcaptp.6.47.2022.3817. (0,9 д.а., авторський внесок 0,15 д.а., полягає в

							означенні електронних комунікаційних послуг та технологій, як основи забезпечення безпечного функціонування господарюючих одиниць за умов невизначеності) (Scopus, WoS). 4. Kryshtal H., Kapeliushna T., Kalina I., Shuliar N., Martynenko M. Trends of development of financial and economic activity of entrepreneurial structures during the period of quarantine restrictions. Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu. 2022. No. 1. P. 139–144. URL: https://doi.org/10.33271/nvngu/2022-1/139. (0,74 д.а., авторський внесок 0,14 д.а., полягає в аналізі трендів безпеки та можливостей забезпечення безперебійної роботи підприємства в умовах пандемії) (Scopus). 5. Zghurska O., Dymenko R., Semkina T., Kapeliushna T. Diversification Strategy of Entrepreneurial Activity in Conditions of European Integration. International Journal of Innovative Technology and Exploring Engineering. 2019. Vol. 9, no. 1. P. 4809–4815. URL: https://doi.org/10.35940/ijitee.j9443.119119. (0,7 д.а., авторський внесок 0,14 д.а., полягає в формуванні безпекових орієнтирів у функціонуванні підприємств в умовах євроінтеграції (Scopus). 6. Капелюшна Т. В. Методологічний концепт управління безпекою підприємства. Інвестиції: практика та досвід. 2024. № 10. С. 69-74. URL: https://doi.org/10.32702/2306-6814.2024.10.69 (0,4 д.а.). 7. Капелюшна Т. В. Формування площини безпеки підприємства під дією ризиків і загроз. Бізнес інформ. 2024. Т. 3, № 554. С. 255–262. URL:

							https://doi.org/10.32983/2222-4459-2024-3-255-262 (0,42 д.а.). 8. Капелюшна Т.В. Безпека даних підприємства у хмарному середовищі: аналіз загроз. Облік і фінанси, 2023. No 4(102). С. 97-104. https://afj.org.ua/ua/journals/2023/4/ (фахове видання, категорія В) 9. Капелюшна Т. В. Управління безпекою підприємства в умовах невизначеності: система контролю загроз. Відбудова для розвитку: зарубіжний досвід та українські перспективи: міжнародна колективна монографія. Київ : ДУ "Ін-т екон. та прогнозув. НАН України", 2023. С. 474-486. URL: http://ief.org.ua/wp-content/uploads/2023/08/Reconstruction-for-development.pdf 10. Капелюшна Т. В., Голобородько А.Ю. Врахування інформаційних викликів при управлінні безпекою підприємств у сьогоденних невизначених умовах. European Journal of Economics and Management. 2023. Volume 9, Issue 1 с. 12-21. https://eujem.cz/wp-content/uploads/2023/eujem_2023_9_1/04.pdf (фахове міжнародне видання) 11. Капелюшна Т.В. Врахування впливу загроз соціальної інженерії при управлінні безпекою підприємства. Інвестиції: практика та досвід. 2023. No 8 (2023). С. 125-130. URL: https://www.nayka.com.ua/index.php/investplan/article/view/1374/1384 (фахове видання, категорія В) 12. Капелюшна Т.В. Захист безпечного функціонування телекомунікаційних підприємств в умовах цифровізації та невизначеності. Агросвіт. 2023. No 7-8 С. 115-123. URL: https://www.nayka.com.ua/index.php/agrosvit/article/view/1351/1361 (фахове видання,

							категорія В) 13. Голобородько А.Ю., Капелюшна Т. В. Формування цифровізації інтегративного розвитку економіки та підприємств, як її елементів. European Journal of Economics and Management. 2022. Volume 8, Issue 6 с.5-13. URL: https://eujem.cz/wp-content/uploads/2022/eujem_2022_8_6/03.pdf (фахове міжнародне видання) 14. Капелюшна Т.В. Розширення базових складових економічної безпеки підприємства з урахуванням умов невизначеності. Ефективна економіка. 2022. No 10. URL: https://www.nayka.com.ua/index.php/ee/article/view/675/683 (фахове видання, категорія В) 15. Капелюшна Т.В., Пильнова В.П., Полякова А.О., Купрієнко Є.О. Роль електронної комерції в умовах формування цифрової держави та інформатизації суспільства. Економіка. Менеджмент. Бізнес. 2021. № (4). С. 68-75. 16. Капелюшна Т.В., Пильнова В.П., Овсійчук В.Я., Красник О.А. Місце інноваційних ризиків у системі економічної безпеки підприємства. Економіка. Менеджмент.Бізнес. 2021. № (4). С.61-68. 17. Пильнова В. П., Гавриш О. М., Капелюшна Т. В. Формування системи управління підприємницькими ризиками. Інвестиції: практика та досвід. 2020. № 24. С. 51-57. URL: http://www.investplan.com.ua/?op=1&z=7258&i=6
269004	Рабчун Дмитро Ігорович	доцент, Основне місце роботи	Навчально-науковий інститут Захисту інформації	Диплом бакалавра, Державний університет телекомунікацій, рік закінчення: 2014, спеціальність: Управління інформаційною безпекою, Диплом	8	Управління ризиками інформаційної безпеки	Освіта: Державний університет телекомунікацій, спеціальність: «Управління інформаційною та кібернетичною безпекою», кваліфікація: Професіонал із організації інформаційної безпеки, 2015,

				магістра, Державний університет телекомунікацій, рік закінчення: 2015, спеціальність: 8.17010301 управління інформаційною безпекою, Диплом кандидата наук ДК 052668, виданий 20.06.2019			(Диплом М15 № 007002) Науковий ступінь: Кандидат технічних наук Спеціальність: 21.05.01 Інформаційна безпеки держави. (АК № 052668, від 20 червня 2019 р.) Досвід професійної діяльності (заняття) за відповідним фахом: ТОВ «ІТ Спеціаліст» Провідний фахівець з тестування систем захисту інформації- з 2019 року. п'ять публікацій у наукових виданнях, які включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection, протягом останніх п'яти років 1. Рабчун Д.І., Бржевська З.М., Драгунцов Р.І. Принципи забезпечення безпеки архітектури інформаційної системи на базі клієнтських додатків для ОС Android. Кібербезпека: освіта, наука, техніка. м. Київ, 2020. Том 4, №8. С. URL: https://doi.org/10.28925/2663-4023.2020.8.4960 2. Якименко Ю.М., Рабчун Д.І., Запорожченко М.М. Місце соціальної інженерії в проблемі витоку даних та організаційні аспекти захисту корпоративного середовища від фішингових атак з використанням електронної пошти. Кібербезпека: освіта, наука, техніка. 2021. 1 (13). С. 6-15. URL: https://doi.org/10.28925/2663-4023.2021.13.615 3. Rabchun D.I., Drahuntsov R. I., Potential disguising attack vectors on security operation centers and siem systems. Cybersecurity: Education, Science, Technique, 2021. Т. 2(14). 6-16. URL: https://doi.org/10.28925/2663-4023.2021.14.614 4. Якименко, Ю.М., Рабчун, Д.І., Мужанова, Т.М., Запорожченко, М.М.,

							Щавінський, Ю.В. Технічний аудит захищеності інформаційно - телекомунікаційних систем підприємств. Кібербезпека: освіта, наука, техніка, 2023. Т 4(20). 45–61. URL: https://doi.org/10.28925/2663-4023.2023.20.4561 5. Svitlana Lehominova, Yurii Shchavinsky, Tetiana Muzhanova, Dmytro Rabchun, Mykhailo Zaporozhchenko. Application of Sentiment Analysis to Prevent Cyberattacks on Objects of Critical Information Infrastructure. International Journal of Computing. 2023. № 22(4), pp. 534-540. URL: https://doi.org/10.47839/ijc.22.4.3362 (Scopus). 6. Lehominova S.V., Shchainskyy YU.V., Muzhanova T.M., Dzyuba T.M., Rabchun D.I. Legal mechanisms for ensuring information security in Ukraine in the conditions of hybrid war. Телекомунікаційні та інформаційні технології, №1(2023). URL: https://doi.org/10.31673/2412-4338.2023.0101111 . (фаховий журнал категорії Б) 7. Рабчун Д.І., Тищенко В.С., Голобородько С.О. Ефективне розпізнавання дезінформації за допомогою нейронних мереж: фокус на виявленні емоційного впливу. Телекомунікаційні та інформаційні технології. 2024. № 2(83). С. 37-48. 8. Легомінова С.В., Щавінський Ю.В., Рабчун Д.І., Запорожченко М.М., Будзинський О.В. Небезпека інструментів OSINT та способи пом'якшення наслідків їх використання для організації. Кібербезпека: освіта, наука, техніка, 2024. Т 1 (25). 45–61.
269007	Савченко Віталій	професор, Основне	Навчально-науковий	Диплом спеціаліста,	19	Системи управління	Освіта: Національна академія оборони

	Анатолійвич	місце роботи	інститут Захисту інформації	Воронєжське вище військове авіаційно-інженерне училище, рік закінчення: 1990, спеціальність: Метеорологія, Диплом магістра, Національний університет оборони України імені Івана Черняховського, рік закінчення: 2002, спеціальність: бойове застосування та управління діями підрозділів (частин, з'єднань) авіації, Диплом доктора наук ДД 001633, виданий 25.01.2013, Атестат професора АП 000749, виданий 05.03.2019, Атестат старшого наукового співробітника (старшого дослідника) АС 007331, виданий 14.04.2010		інформаційною безпекою	України Рік закінчення: 2002 р. Спеціальність «Бойове застосування та управління діями підрозділів (частин, з'єднань) авіації». Кваліфікація згідно з документом про вищу освіту: «Магістр військового управління, офіцер військового управління оперативно-тактичного рівня». Науковий ступінь: доктор технічних наук. Наукова спеціальність: 122 Комп'ютерні науки (05.13.06 – інформаційні технології), тема дисертації: (спеціальна тема) (ДД №001633 від 25.01.2013 р., виданий МОН України) Вчене звання: професор кафедри Систем інформаційного та кібернетичного захисту, (АП № 000749 від 05.03.2019 р.) п'ять публікацій у наукових виданнях, які включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection, протягом останніх п'яти років 1. Savchenko V. Hidden Transmitter Localization Accuracy Model Based on Multi-Position Range Measurement / Vitalii Savchenko, Oleksandr Laptiev, Oleksandr Kolos, Rostyslav Lisnevskyi, Viktoriia Ivannikova, Ivan Ablazov // In Proceedings of the IEEE International Conference on Advanced Trends in Information Theory, ATIT`2020, Kyiv: IEEE Ukraine Section, 2020, pp. (SCOPUS) 2. Savchenko V. The new method for detecting signals of means of covert obtaining information / Oleksandr Laptiev, Savchenko Vitalii, Serhii Yevseiev, Halyna Haidur, Sergii Gakhov, Spartak Hohoniants // In Proceedings of the

							IEEE International Conference on Advanced Trends in Information Theory, ATIT`2020, Kyiv: IEEE Ukraine Section, 2020, pp.176-181 (SCOPUS) 3. Savchenko V. The method of improving the signal detection quality by accounting for interference / Oleksandr Laptiev, Igor Polovinkin, Savchenko Vitalii, Oleh Stefurak, Oleg Barabash, Olena Zelikovska // In Proceedings of the IEEE International Conference on Advanced Trends in Information Theory, ATIT`2020, Kyiv: IEEE Ukraine Section, 2020, pp. (SCOPUS) 4. Savchenko V. Detection of Slow DDoS Attacks based on User's Behavior Forecasting / Vitalii Savchenko, Oleh Ilin, Nikolay Hnidenko, Olga Tkachenko, Oleksander Laptiev, Svitlana Lehominova // International Journal of Emerging Trends in Engineering Research. Volume 8. No. 5, May 2020. 2019-2025. (SCOPUS) 5. Savchenko V. Air Defense Planning from an Impact of a Group of Unmanned Aerial Vehicles based on Multi-Agent Modeling / Pavlo Shchypanskyi, Vitalii Savchenko, Oleksii Martyniuk, Ihor Kostiuk // International Journal of Emerging Trends in Engineering Research. Volume 8. No. 4, April 2020. 1302-1308. (SCOPUS) 6. Savchenko V. Method of Detecting Radio Signals using Means of Covert by Obtaining Information on the basis of Random Signals Model / Oleksandr Laptiev, Vitalii Savchenko, Andrii Pravdyvyi, Ivan Ablazov, Rostyslav Lisnevsky, Oleksandr Koloss, Viktor Hudyma // International Journal of Communication Networks and Information Security (IJCNIS) Vol. 13, No. 1, April 2021. 48–54. (SCOPUS) 7. Savchenko V. Method of Determining Trust and Protection of Personal Data in Social

							Networks / Laptiev O.1, Savchenko V.1, Kotenko A.1, Akhramovych V.1, Samosyuk V. 1, Shuklin G1, Biehun A.2 // International Journal of Communication Networks and Information Security (IJCNIS) Vol. 13, No. 1, 2021. 15–21. (SCOPUS) 8. Fractal functions and their application to source data coding / Zamrii I., Sobchuk V., Laptiev O., Savchenko V., Shkapa V., Kovalenko V. and Kotok V. ARPN Journal of Engineering and Applied Sciences. Vol. 17, No. 4, February 2022. P.424-435. (SCOPUS) 9. Model of an Alternative Navigation System for High-Precision Weapons./ Vitalii Savchenko, Volodymyr Tolubko, Liubov Berkman, Anatolii Syrotenko, Pavlo Shchypanskyi, Oleksander Matsko, Vitalii Tiurin and Pavlo Open'ko // Journal of Defense Modeling and Simulation: Applications, Methodology, Technology. First published - May 27, 2020. Journal of Defense Modeling and Simulation, 2022, 19(3), pp. 255–262. https://doi.org/10.1177/1548512920921955 (SCOPUS) 10. Intensive Training Model for Artillery Cadets Using 3D Simulators // Vitalii Savchenko, Anatoliy Derevjanchuk, Taras Dzyuba, Denys Moskalenko // Advances in Military Technology. Vol. 18, No. 1, 2023, pp. 35-50. ISSN 1802-2308, eISSN 2533-4123. DOI 10.3849/aimt.01786 https://www.aimt.cz/index.php/aimt/article/view/1786/378 (SCOPUS)
150389	Легомінова Світлана Володимирівна	завідувач кафедри, Основне місце роботи	Навчально-науковий інститут Захисту інформації	Диплом спеціаліста, Латвійський університет, рік закінчення: 1993, спеціальність: економіка і соці-альне планування, Диплом магістра,	15	Управління проєктами інформаційної безпеки	Освіта: 1. Державний університет інформаційно-комунікаційних технологій, 2024. Ступінь вищої освіти: магістр, спеціальність: Кібербезпека. кваліфікація: магістр з кібербезпеки за освітньо-професійною програмою

				Державний університет інформаційно-комунікаційних технологій, рік закінчення: 2024, спеціальність: 125 Кібербезпека, Диплом доктора наук ДД 008898, виданий 15.10.2019, Диплом кандидата наук ДК 014670, виданий 12.06.2002, Атестат доцента 12ДЦ 046345, виданий 25.02.2016, Атестат професора АП 002374, виданий 15.12.2020			Інформаційна та кібернетична безпека. (Диплом М24 №012801 від 31.01.24). 2. Латвійський університет, 1993 р., Спеціальність: економічне і соціальне планування, Кваліфікація: економіст. (Диплом №103216 від 21.06.1993) Науковий ступінь: Доктор економічних наук, спеціальність 08.00.04. «Економіка та управління підприємствами, (за видами економічної діяльності)». (ДД №008898, від 15.10.2019 р.,) Вчене звання: професор кафедри управління інформаційною та кібернетичною безпекою. (АП №002374, від 9.02.2021 р.) керівництво (консультування) дисертації на здобуття наукового ступеня за спеціальністю, що була захищена в Україні або за кордоном: п’ять публікацій у наукових виданнях, які включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection, протягом останніх п’яти років 1. Korobchynskyi M., Slonov M., Maryliv O., Lysenko S., Lehominova S., S. Lytvynska S. Method of structural functional-value modeling of a complex system with a mixed combination of subsystems. Mathematical Modeling and Computing. 2021. Vol. 8, No. 2, pp. 215–227 (SCOPUS). 2. Viktoriia A. Hrosul, Alona Yu. Goloborodko, Svitlana V. Lehominova, Kseniia V. Kalienik, Natalia Yu. Balatska. Modelling balanced criteria system for business process management. RISUS - Journal on Innovation and Sustainability. 2021. Vol. 12, No. 2, pp.

							139-153. (Web of Science) URL: https://revistas.pucsp.br/index.php/risus/article/view/54314/pdf 3. Легомінова С.В., Мужанова Т.М., Якименко Ю.М. Системний аналіз технічних систем забезпечення інформаційної безпеки підприємств від компанії Fireeye. Кібербезпека: освіта, наука, техніка. 2021. № 4 (12). С. 36-50. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/251/2254. Мужанова Т.М., Легомінова С.В., Якименко Ю.М., Мордас І.В. Технології моніторингу й аналізу діяльності користувачів у запобіганні внутрішнім загрозам інформаційній безпеці організації. Кібербезпека: освіта, наука, техніка. 2021. № 1 (13). С. 50-62. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/281/2415. Легомінова С.В., Мужанова Т.М., Якименко Ю.М., Власенко В.О. Засоби інформування й навчання персоналу у сфері інформаційної безпеки в умовах цифровізації. Зв'язок. 2021. №4 (152). С.14-16. 6. Olena Klymenko, Svitlana Lehominova, Alona Goloborodko. Features of quality management of electronic services in Ukraine in the conditions of digitalization. RISUS - Journal on Innovation and Sustainability. 2022. Vol. 13, No. 1, pp. 72-85. (Web of Science) URL: https://revistas.pucsp.br/index.php/risus/article/view/57166/39383 7. Легомінова С.В., Голобородько А.Ю. Інтегрування штучного інтелекту до бізнес-процесів підприємства як ефективного інструменту його розвитку. Економічний форум. 2022. № 4. С. 99-107. 8. Savchenko, V., Lehominova, S., Dzyuba, T., Havryliuk,

							I., Novikova, I. Model of Connectivity in a Mobile MESH Network for a Group of Unmanned Aerial Vehicles. 2022 IEEE 4th International Conference on Advanced Trends in Information Theory, ATIT 2022 – Proceedings. 2022, pp. 142–147. (SCOPUS) URL: https://ieeexplore.ieee.org/document/10024235 https://www.scopus.com/authid/detail.uri?authorId=57217034683 9. Lehominova S.V., Shchavinskyy YU.V., Muzhanova T.M., Dzyuba T.M., Rabchun D.I. Legal mechanisms for ensuring information security in ukraine in the conditions of hybrid war. Телекомунікаційні та інформаційні технології. 2023. № 1 (78). С. 101-110. 10. Olena Klymenko, Svitlana Lehominova, Alona Goloborodko. A capsuled approach to analysis of the profitability of digitalization of business processes of telecommunications companies in Ukraine. RISUS - Journal on Innovation and Sustainability. 2023. Vol. 14, No. 3, pp. 123-137. (Web of Science) URL: https://revistas.pucsp.br/index.php/risus/article/view/59845/43178 11. Легомінова С. В., Голобородько А. Ю. Оцінка розвитку цифровізації на підприємствах інформаційно-комунікаційних послуг України. Бізнес Інформ. 2023. № 9. С. 104–110. 12. Легомінова С.В., Гайдур Г.І. Аналіз сучасних загроз інформаційній безпеці організацій та формування інформаційної платформи протидії їм. Кібербезпека: освіта, наука, техніка. 2023. № 2 (22). С. 57-64. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/535/41713. Lehominova S., Shchavinsky Y., Muzhanova T.,

							Rabchun D., Zaporozhchenko M. Application of Sentiment Analysis to Prevent Cyberattacks on Objects of Critical Information Infrastructure. International Journal of Computing. 2023.Vol. 22(4). P. 534-540. (SCOPUS) 14. Легомінова С.В., Мужанова Т.М., Якименко Ю.М., Щавінський Ю.В., Нестеренко Г.П. Розвиток політики кібербезпеки ЄС: підходи та рішення. Кібербезпека: освіта, наука, техніка. 2024. № 4 (24). С. 77-84. 15. Легомінова С.В., Щавінський Ю.В., Будзінський О.В. Аналіз сучасних підходів до забезпечення кібербезпеки корпоративних баз даних Сучасний захист інформації. 2024. №2(58). С. 84-91. 16. Легомінова С. В., Голобородько А. Ю. Інструменти діджиталізації забезпечення performans-маркетингу телекомунікаційних підприємств. Інвестиції: практика та досвід. 2024. № 12. С. 33-39. 17. Kapeliushna T., Lehominova S., Goloborodko A., Lysetskyi Yu., Nosova T. Methodological approaches to enterprise security management: traditional and transformed to the conditions of functioning. Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu. 2024, (3): 204 – 209. (SCOPUS)

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**	**Обов'язкові освітні компоненти, що забезпечують ПРН**	**Методи навчання**	**Форми та методи оцінювання**

	його)			
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.	☒	Науково-дослідна практика	практична робота, проведення експериментів, виконання індивідуальних завдань, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
		Прикладна загальна теорія систем інформаційної безпеки	лекція-візуалізація, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, вирішення практичних задач, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
		Переддипломна практика	практична робота, виконання індивідуальних завдань, консультації, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
		Кваліфікаційна робота	виконання індивідуальних завдань, консультації, самостійна робота	захист кваліфікаційної роботи.
РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.	☒	Кваліфікаційна робота	виконання індивідуальних завдань, консультації, самостійна робота	захист кваліфікаційної роботи.
		Переддипломна практика	практична робота, виконання індивідуальних завдань, консультації, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
		Науково-дослідна практика	практична робота, проведення експериментів, виконання індивідуальних завдань, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
		Організація проведення наукових досліджень	Лекція-візуалізація. Пояснювально – ілюстративний вид викладу, експрес-опитування здобувачів. Практичне застосування методів теоретичного та емпіричного наукового дослідження з поетапною розробкою структури написання наукової роботи. Усне опитування, тематична навчальна дискусія. Самостійна підготовка (опрацювання та систематизація матеріалу, узагальнення)	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - залік
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.	☒	Переддипломна практика	практична робота, виконання індивідуальних завдань, консультації, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
		Науково-дослідна практика	практична робота, проведення експериментів, виконання індивідуальних завдань, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових	☒	Кваліфікаційна робота	виконання індивідуальних завдань, консультації, самостійна робота	захист кваліфікаційної роботи.
		Переддипломна практика	практична робота, виконання індивідуальних завдань, консультації, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
		Науково-дослідна практика	практична робота, проведення експериментів,	підсумкове оцінювання - захист звіту за результатами

стандартів та кращих практик.			виконання індивідуальних завдань, самостійна робота	проходження практики
		Управління проєктами інформаційної безпеки	лекція-візуалізація, практична робота, розв'язання ситуативних завдань, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
		Організація проведення наукових досліджень	Лекція-візуалізація. Пояснювально – ілюстративний вид викладу, експрес-опитування здобувачів. Практичне застосування методів теоретичного та емпіричного наукового дослідження з поетапною розробкою структури написання наукової роботи. Усне опитування, тематична навчальна дискусія. Самостійна підготовка (опрацювання та систематизація матеріалу, узагальнення індукція, дедукція)	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - залік
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.	☒	Кваліфікаційна робота	виконання індивідуальних завдань, консультації, самостійна робота	захист кваліфікаційної роботи.
		Переддипломна практика	практична робота, виконання індивідуальних завдань, консультації, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
		Науково-дослідна практика	практична робота, проведення експериментів, виконання індивідуальних завдань, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.	☒	Науково-педагогічна практика	практична робота, самостійна робота, вирішення індивідуальних завдань	захист звіту за результатами проходження практики
		Педагогіка та психологія у вищій школі	лекція-візуалізація, лекція-дискусія, практична робота, розв'язання ситуативних завдань, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - залік
		Корпоративна та професійна етика в кібербезпеці	лекція-візуалізація, проблемна лекція, лекція-дискусія, практична робота, розв'язання ситуативних завдань, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
РН17. Мати навички	☒	Прикладна загальна теорія систем	лекція-візуалізація, експрес-опитування студентів, усне	поточний контроль, рубіжне оцінювання (модульний

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		інформаційної безпеки	опитування, індивідуальне тестування студентів, вирішення практичних задач, консультації, самостійна робота	контроль), підсумкове оцінювання - іспит
		Управління проєктами інформаційної безпеки	лекція-візуалізація, практична робота, розв'язання ситуативних завдань, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
		Педагогіка та психологія у вищій школі	лекція-візуалізація, лекція-дискусія, практична робота, розв'язання ситуативних завдань, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - залік
		Науково-педагогічна практика	практична робота, самостійна робота, вирішення індивідуальних завдань	захист звіту за результатами проходження практики
		Науково-дослідна практика	практична робота, проведення експериментів, виконання індивідуальних завдань, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
		Кваліфікаційна робота	виконання індивідуальних завдань, консультації, самостійна робота	захист кваліфікаційної роботи.
		Переддипломна практика	практична робота, виконання індивідуальних завдань, консультації, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
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.	☒	Прикладна загальна теорія систем інформаційної безпеки	лекція-візуалізація, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, вирішення практичних задач, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
		Корпоративна та професійна етика в кібербезпеці	лекція-візуалізація, проблемна лекція, лекція-дискусія, практична робота, розв'язання ситуативних завдань, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.	☒	Науково-педагогічна практика	практична робота, самостійна робота, вирішення індивідуальних завдань	захист звіту за результатами проходження практики
		Науково-технічний переклад	практична робота, самостійна робота, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, консультації	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
		Корпоративна та професійна етика в кібербезпеці	лекція-візуалізація, проблемна лекція, лекція-дискусія, практична робота, розв'язання ситуативних	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит

			завдань, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, консультації, самостійна робота	
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.	☒	Управління проєктами інформаційної безпеки	лекція-візуалізація, практична робота, розв'язання ситуативних завдань, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
		Системи управління інформаційною безпекою	лекція-візуалізація, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, вирішення практичних задач, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
		Управління ризиками інформаційної безпеки	лекція-візуалізація, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, вирішення практичних задач, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
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.	☒	Кваліфікаційна робота	виконання індивідуальних завдань, консультації, самостійна робота	захист кваліфікаційної роботи.
		Переддипломна практика	практична робота, виконання індивідуальних завдань, консультації, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
		Науково-дослідна практика	практична робота, проведення експериментів, виконання індивідуальних завдань, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
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.	☒	Кваліфікаційна робота	виконання індивідуальних завдань, консультації, самостійна робота	захист кваліфікаційної роботи.
		Переддипломна практика	практична робота, виконання індивідуальних завдань, консультації, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
		Науково-дослідна практика	практична робота, проведення експериментів, виконання індивідуальних завдань, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
		Управління ризиками інформаційної безпеки	лекція-візуалізація, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, вирішення практичних задач, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
РН9. Аналізувати, розробляти і	☒	Управління проєктами інформаційної	лекція-візуалізація, практична робота,	поточний контроль, рубіжне оцінювання (модульний

супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.		безпеки	розв'язання ситуативних завдань, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, консультації, самостійна робота	контроль), підсумкове оцінювання - іспит
		Системи управління інформаційною безпекою	лекція-візуалізація, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, вирішення практичних задач, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
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.	☒	Переддипломна практика	практична робота, виконання індивідуальних завдань, консультації, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
		Управління ризиками інформаційної безпеки	лекція-візуалізація, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, вирішення практичних задач, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
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.	☒	Переддипломна практика	практична робота, виконання індивідуальних завдань, консультації, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
		Науково-дослідна практика	практична робота, проведення експериментів, виконання індивідуальних завдань, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
		Прикладна загальна теорія систем інформаційної безпеки	лекція-візуалізація, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, вирішення практичних задач, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
		Системи управління інформаційною безпекою	лекція-візуалізація, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, вирішення практичних задач, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
		Управління ризиками інформаційної безпеки	лекція-візуалізація, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, вирішення практичних задач, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.	☒	Кваліфікаційна робота	виконання індивідуальних завдань, консультації, самостійна робота	захист кваліфікаційної роботи.
		Науково-дослідна практика	практична робота, проведення експериментів, виконання індивідуальних завдань, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
		Управління ризиками інформаційної безпеки	лекція-візуалізація, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, вирішення практичних	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит

			задач, консультації, самостійна робота	
		Організація проведення наукових досліджень	лекція-візуалізація, практична робота, проведення експериментів, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - залік
		Педагогіка та психологія у вищій школі	лекція-візуалізація, лекція-дискусія, практична робота, розв'язання ситуативних завдань, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - залік
		Переддипломна практика	практична робота, виконання індивідуальних завдань, консультації, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
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.	☒	Переддипломна практика	практична робота, виконання індивідуальних завдань, консультації, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
		Науково-дослідна практика	практична робота, проведення експериментів, виконання індивідуальних завдань, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
		Науково-технічний переклад	практична робота, самостійна робота, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, консультації	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання – залік, іспит
		Організація проведення наукових досліджень	лекція-візуалізація, практична робота, виконання практичних завдань, експрес-опитування студентів, усне опитування, тестування студентів, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - залік
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.	☒	Кваліфікаційна робота	виконання індивідуальних завдань, консультації, самостійна робота	захист кваліфікаційної роботи.
		Переддипломна практика	практична робота, виконання індивідуальних завдань, консультації, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
		Науково-дослідна практика	практична робота, проведення експериментів, виконання індивідуальних завдань, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
		Управління проєктами інформаційної безпеки	лекція-візуалізація, практична робота, розв'язання ситуативних завдань, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
РН1. Вільно спілкуватись державною та іноземною мовами,	☒	Науково-педагогічна практика	практична робота, самостійна робота, вирішення індивідуальних завдань	захист звіту за результатами проходження практики

усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес/операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.		Науково-технічний переклад	практична робота, самостійна робота, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, консультації	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - залік, іспит
		Педагогіка та психологія у вищій школі	лекція-візуалізація, лекція-дискусія, практична робота, розв'язання ситуативних завдань, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - залік
		Корпоративна та професійна етика в кібербезпеці	лекція-візуалізація, проблемна лекція, лекція-дискусія, практична робота, розв'язання ситуативних завдань, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	☒	Прикладна загальна теорія систем інформаційної безпеки	лекція-візуалізація, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, вирішення практичних задач, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	☒	Переддипломна практика	практична робота, виконання індивідуальних завдань, консультації, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
		Прикладна загальна теорія систем інформаційної безпеки	лекція-візуалізація, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, вирішення практичних задач, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
		Управління ризиками інформаційної безпеки	лекція-візуалізація, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, вирішення практичних задач, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
		Науково-технічний переклад	практична робота, самостійна робота, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, консультації	практична робота, самостійна робота, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, консультації
		Організація проведення наукових досліджень	олекція-візуалізація, практична робота, виконання практичних завдань, експрес-опитування студентів, усне опитування, тестування студентів, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - залік
		Корпоративна та	лекція-візуалізація,	поточний контроль, рубіжне

		професійна етика в кібербезпеці	проблемна лекція, лекція-дискусія, практична робота, розв'язання ситуативних завдань, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, консультації, самостійна робота	оцінювання (модульний контроль), підсумкове оцінювання - іспит
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.	☒	Організація проведення наукових досліджень	лекція-візуалізація, практична робота, виконання практичних завдань, експрес-опитування студентів, усне опитування, тестування студентів, консультації, самостійна робота5	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - залік
		Системи управління інформаційною безпекою	лекція-візуалізація, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, вирішення практичних задач, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
		Прикладна загальна теорія систем інформаційної безпеки	лекція-візуалізація, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, вирішення практичних задач, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
		Науково-дослідна практика	практична робота, проведення експериментів, виконання індивідуальних завдань, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
		Кваліфікаційна робота	виконання індивідуальних завдань, консультації, самостійна робота	захист кваліфікаційної роботи.
		Переддипломна практика	практична робота, виконання індивідуальних завдань, консультації, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	☒	Кваліфікаційна робота	виконання індивідуальних завдань, консультації, самостійна робота	захист кваліфікаційної роботи.
		Переддипломна практика	практична робота, виконання індивідуальних завдань, консультації, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
		Науково-дослідна практика	практична робота, проведення експериментів, виконання індивідуальних завдань, самостійна робота	підсумкове оцінювання - захист звіту за результатами проходження практики
		Управління проєктами інформаційної безпеки	лекція-візуалізація, практична робота, розв'язання ситуативних завдань, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит
		Системи управління інформаційною безпекою	лекція-візуалізація, експрес-опитування студентів, усне опитування, індивідуальне тестування студентів, вирішення практичних задач, консультації, самостійна робота	поточний контроль, рубіжне оцінювання (модульний контроль), підсумкове оцінювання - іспит