НАЦІОНАЛЬНЕ АГЕНТСТВО ІЗ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	**Державний університет інтелектуальних технологій і зв'язку**
Освітня програма	**58620 Кібербезпека та захист інформації**
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	**5780**
Повна назва ЗВО	**Державний університет інтелектуальних технологій і зв'язку**
Ідентифікаційний код ЗВО	**43997335**
ПІБ керівника ЗВО	**Назаренко Олександр Аскольдович**
Посилання на офіційний веб-сайт ЗВО	**https://suitt.edu.ua/**

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

https://registry.edbo.gov.ua/university/5780

3. Загальна інформація про ОП, яка подається на акредитацію

ID освітньої програми в ЄДЕБО	**58620**
Назва ОП	**Кібербезпека та захист інформації**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека та захист інформації**
Спеціалізація (за наявності)	*відсутня*
Рівень вищої освіти	**Магістр**
Тип освітньої програми	**Освітньо-професійна**
Вступ на освітню програму здійснюється на основі ступеня (рівня)	**Бакалавр, Магістр (ОКР «спеціаліст»)**
Структурний підрозділ (кафедра або інший підрозділ), відповідальний за реалізацію ОП	**Кафедра Кібербезпеки та технічного захисту інформації**
Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП	*відсутня*
Місце (адреса) провадження освітньої діяльності за ОП	**м. Одеса, вул. Кузнечна, 1**
Освітня програма передбачає присвоєння професійної кваліфікації	*не передбачає*
Професійна кваліфікація, яка присвоюється за ОП (за наявності)	***відсутня***
Мова (мови) викладання	**Українська**
ID гаранта ОП у ЄДЕБО	**388823**
ПІБ гаранта ОП	**Кільдішев Віталій Йосипович**
Посада гаранта ОП	**Доцент**
Корпоративна електронна адреса гаранта ОП	**v.y_kildishev@suitt.edu.ua**
Контактний телефон гаранта ОП	**+38(068)-202-76-45**
Додатковий телефон гаранта ОП	**+38(063)-011-46-86**

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

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

У 2018 році було створено освітньо-професійну програму «Кібербезпека» підготовки здобувачів вищої освіти другого (магістерського) рівня за спеціальністю 125 Кібербезпека, галузі знань 12 Інформаційні технології. У 2019 році дана програма була акредитована на 5 років.
У 2022 році у було вирішено оновити дану ОП відповідно до вимог нового професійного стандарту «Фахівець сфери захисту інформації» (за підтримки проєкту Агентства USAID «Кібербезпека критично важливої інфраструктури України» (https://www.facebook.com/CyberActivityUA/?locale=uk_UA, https://suitt.edu.ua/wp-content/uploads/2024/10/porivnialni-tablytsi-kompetentsij-dlia-dystsyplin-op.pdf).
Таким чином, було створено робочу групу з оновлення ОП (https://suitt.edu.ua/wp-content/uploads/2024/10/sklad-robochoi-hrupy-dlia-onovlennia-op.pdf), дії якої полягали у наступному: визначення основних потреб ринку, стану ресурсного забезпечення ЗВО та кафедри, аналіз наявних професійних стандартів (https://suitt.edu.ua/wp-content/uploads/2024/10/dii-z-onovlennia-osvitnoi-prohramy.pdf). Після аналізу професійного стандарту було визначено основні компетентності, які було доцільним включити до нової освітньої програми, а саме: було додано 7 фахових компетентностей та 11 програмних результатів навчання; створено опис вимог до ОП (https://suitt.edu.ua/wp-content/uploads/2024/10/vymohy-do-osvitnoi-prohramy.pdf). На цієї основі ОП було оновлено у 2023 році (https://suitt.edu.ua/osvitni-prohramy-2023/). ОП відповідала усім рекомендаціям: як від USAID, так й стейкголдерів (https://suitt.edu.ua/reformuvannia-opp/).
У 2024 році було вирішено знову оновити дану ОП, а саме приділити увагу оновленню деяких її основних освітніх компонентів (https://shorturl.at/kWF9g). Таким чином, дана ОП зазнала у 2024 р. деяких змін: було змінено зміст декількох освітніх компонентів, додано ОК11 – «Ділова іноземна мова», а також змінено навчальний план – 3 дисципліни для здобувачів вступу 2024 р. будуть викладатися на 2 курсі магістратури.

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

Рік навчання	Навчальний рік, у якому відбувся набір здобувачів відповідного року навчання	Обсяг набору на ОП у відповідному навчальному році	Контингент студентів на відповідному році навчання станом на 1 жовтня поточного навчального року		У тому числі іноземців	
			ОД	*З*	*ОД*	*З*
1 курс	2024 - 2025	70	31	14	0	0
2 курс	2023 - 2024	60	32	11	0	0

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

6. Інформація про інші ОП ЗВО за відповідною спеціальністю

Рівень вищої освіти	Інформація про освітні програми
початковий рівень (короткий цикл)	*програми відсутні*
перший (бакалаврський) рівень	**58531 Кібербезпека та захист інформації**
другий (магістерський) рівень	**58620 Кібербезпека та захист інформації**
третій (освітньо-науковий/освітньо-творчий) рівень	**58824 Кібербезпека та захист інформації**

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

	Загальна площа	Навчальна площа
Усі приміщення ЗВО	61587	29576
Власні приміщення ЗВО (на праві власності, господарського відання або оперативного управління)	61587	29576
Приміщення, які використовуються на іншому праві, аніж право власності, господарського відання або оперативного	0	0

управління (оренда, безоплатне користування тощо)		
Приміщення, здані в оренду	574	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	*op-125-masters-2024.pdf*	JaC+87JtBDG8T22Ugfg0KSbZ/6LIvqgy50O1VgrO05U=
Навчальний план за ОП	*np_125_masters_2024.pdf*	F2ss10MHDZILmvCtxeuszMwfrlKVRbcQQ4sscsZW90U=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Рецензія на ОПП ДУІТЗ - ГО Асоціація спеціалістів кібербезпеки.pdf*	nG5thGN2MsLtpAHHHXKZSKpcK37n1Q0qdK9gxx+IKLU=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Рецензія на ОПП ДУІТЗ - СІДКОН.pdf*	cVMkkTSoe3319XwP4qFbsDSzaEmaJiy+6HPYc8U+p14=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Рецензія на ОПП ДУІТЗ - БОШ.pdf*	9hSuVD57ZhvV20TRDS0OtSLR12vkYWd8S+l2329yhs8=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Перелік коментарів та пропозицій від стейкхолдерів.pdf*	JDrE6AlEGr0WGp72UW2ABrYWPEJS43xRyA0302igUkc=

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?

Освітня програма дає можливість досягти результатів навчання, визначених стандартом вищої освіти за спеціальністю 125 Кібербезпека другого (магістерського) рівня вищої освіти, оскільки під час проєктування та оновлення даної програми було проаналізовано відповідний стандарт вищої освіти за даною спеціальністю. Усі компетентності та програмні результати навчання відповідають даному стандарту.
Слід зазначити, що член групи забезпечення даної ОП - професор Василіу Є.В. - є членом Науково-методичної комісії Сектору вищої освіти Науково-методичної ради МОН України, підкомісія 125 "Кібербезпека", і брав участь у розробленні стандарту вищої освіти за спеціальністю 125 Кібербезпека другого (магістерського) рівня вищої освіти (затверджено наказом МОН України 18.03.2021 р., № 332).

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

Дана освітня програма оновлювалась також на основі змісту професійного стандарту «Фахівець сфери захисту інформації». Загальні та спеціальні компетентності програми, а також програмні результати навчання були

побудовані на основі визначених у професійному стандарті трудових функцій. Особливу увагу було приділено аналізу професійних компетентностей, знань, умінь та навичок цього стандарту з метою їхньої подальшої адаптації для здобувачів вищої освіти (https://suitt.edu.ua/wp-content/uploads/2024/10/porivnialni-tablytsi-kompetentsij-dlia-dystsyplin-op.pdf). До ОП було додано 7 фахових компетентностей з професійного стандарту до 10-ти, які визначені в стандарті вищої освіти, та 11 результатів навчання до 23 зі стандарту вищої освіти.

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

Регулярні зустрічі зі стейкголдерами, що включають представників керівництва підприємств і випускників минулих років, які вже працюють у відповідній галузі, організовуються для оперативного відгуку на зміни у галузі кібербезпеки та захисту інформації. При оновленні ОП було враховано інтереси та пропозиції здобувачів вищої освіти, які навчаються за цим напрямком. Було проведено опитування здобувачів щодо наповненості магістерської програми даної спеціальності освітніми компонентами. У результаті опитування здобувачі надали пропозиції щодо змісту деяких освітніх компонентів. Дані пропозиції були враховані під час перегляду таких освітніх компонентів як «Менеджмент інформаційної безпеки» (ОК5), та «Процесний менеджмент в системі корпоративної безпеки» (ОК9).

- роботодавці

Під час оновлення ОП були враховані пропозиції:
- ТОВ “Консалтинговна компанія “СІДКОН” (https://sidcon.com.ua);
- ГО “Асоціація спеціалістів кібербезпеки”(https://scsa.org.ua);
- ТОВ «Роберт Бош ЛТД» (https://www.bosch.ua).

У процесі обговорення проєкту ОП було взято до уваги усі зауваження та пропозиції представників даних організацій (https://suitt.edu.ua/wp-content/uploads/2024/10/perelik-komentariv-ta-propozytsij-vid-stejkkholderiv.pdf). На підприємствах роботодавців налагоджено проходження практики здобувачами вищої освіти даної ОП, тому роботодавці вносять пропозиції щодо оновлення/включення тих чи інших освітніх компонент в освітню програму, ґрунтуючись на потребах власного виробництва. Гарант ОП та робоча група намагаються враховувати дані пропозиції.
Кафедра Кібербезпеки та технічного захисту інформації (КБ та ТЗІ) постійно веде роботу над розширенням списку таких підприємств. Реєстр стейкголдерів на даний час https://suitt.edu.ua/partnery-ta-stejkholdery/

- академічна спільнота

Залучення та врахування інтересів академічної спільноти відбувається постійно. Найчастіше обговорення освітньої програми відбувається на засіданнях робочої групи. На них обговорюються усі пропозиції, які були отримані від здобувачів, роботодавців та стекголдерів щодо покращення змісту ОП (https://suitt.edu.ua/wp-content/uploads/2024/10/perelik-komentariv-ta-propozytsij-vid-stejkkholderiv-duitz.pdf). На кафедрі КБ та ТЗІ також регулярно проводяться засідання з метою обговорення тенденцій у підготовці фахівців у сфері кібербезпеки та захисту інформації для визначення перспектив подальшого оновлення освітньої програми (https://suitt.edu.ua/wp-content/uploads/2024/10/vytiah-kafedry-zatverdzhennia-pereliku-dystsyplin.pdf, https://shorturl.at/kWF9g).

- інші стейкхолдери

Пропозицій від інших стейкголдерів не надходило.

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

Однією із складових стратегії ДУІТЗ є реформування лабораторної бази університету, а саме відновлення навчальних та лабораторних корпусів, створення сучасних лабораторій з тестування, дослідження та експлуатації технологій та обладнання провідних виробників з країн-членів ЄС та світу, сертифікаційних лабораторій (https://shorturl.at/fLLYn), що є й однією з цілей даної ОП, оскільки підготовка професіоналів, здатних забезпечувати захищеність інформації, потребує відповідної лабораторної бази. На базі кафедри КБ та ТЗІ вже існують такі лабораторії (https://shorturl.at/f76Cu, https://shorturl.at/aaPfw), які у найближчому майбутньому будуть вдосконалюватись та розширятись.

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

Мета та програмні результати навчання освітньої програми визначаються з урахуванням розвитку науки та спеціальності. Однією з цілей програми є інтеграція науково-дослідної роботи, інноваційної діяльності і навчального процесу. Програма орієнтується на сучасні міжнародні вимоги та світові наукові досягнення та регулярно оновлюється. Таким чином, у 2023 р. дану програму було оновлено відповідно до професійного стандарту «Фахівець сфери захисту інформації» та пропозицій стейкголдерів, (https://suitt.edu.ua/wp-content/uploads/2024/10/dii-z-onovlennia-osvitnoi-prohramy.pdf, https://suitt.edu.ua/wp-content/uploads/2024/10/plan-onovlennia-osvitnoi-prohramy.pdf, https://suitt.edu.ua/wp-content/uploads/2024/10/perelik-komentariv-ta-propozytsij-vid-stejkkholderiv-duitz.pdf), а у 2024 р. на підставі аналізу кафедрою тенденцій розвитку кібербезпеки та опитувань здобувачів внесені додаткові зміни.

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

Мета та програмні результати освітньої програми визначаються з урахуванням тенденцій розвитку ринку праці, галузевого та регіонального контексту. Цілі програми другого (магістерського) рівня вищої освіти, випускники якої становляться фахівцями з кібербезпеки та захисту інформації високого рівня, повністю відповідають потребам цієї галузі, регіону та держави в цілому в таких фахівцях. В Одеській області багато державних установ та провідних високотехнологічних компаній, включаючи міжнародні, яким у зв'язку з постійно зростаючою кількістю кібератак потрібні професіонали-аналітики у галузі кібербезпеки та захисту інформації.
Однією з цілей програми є орієнтація на вимоги ринку праці. Програма регулярно переглядається та оновлюється відповідно до змін на ринку праці.

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

При формулюванні мети та програмних результатів ОП був врахований досвід провідних вітчизняних університетів, зокрема таких, як Харківський національний університет імені В.Н. Каразіна, КНУ ім. Тараса Шевченка, Національний авіаційний університет. Було проведено порівняння основних освітніх компонентів ОП за спеціальністю 125 Кібербезпека та захист інформації даних університетів з освітніми компонентами даної ОП та дещо модернізовано зміст таких освітніх компонентів як "Моніторинг та аудит інформаційно-комунікаційних систем" ("Аудит інформаційних систем" в ОП КНУ ім. Тараса Шевченка, "Аудит інформаційної безпеки" в ОП НАУ), "Кіберфізична безпека об'єктів критичної інфраструктури" ("Безпека критичної інформаційної інфраструктури" в ОП КНУ ім. Тараса Шевченка) тощо.

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

При оновлені освітньої програми у 2023 та 2024 рр. було враховано значний досвід, який отримали викладачі кафедри Кібербезпеки та технічного захисту інформації завдяки участі з 2020 р. у проєкті Агентства USAID "Кібербезпека критично важливої інфраструктури України", зокрема, підвищення кваліфікації в літніх школах для викладачів у 2021 та 2022 рр., які були організовані у межах цього проєкту (https://www.facebook.com/USAIDUkraine/posts/pfbid02u75M123L6anKNSU8Z4ZuRv2YEMSuf7Msui2sqCAdJQKfYQ17p7Xaj5t8639Rsj6Pl). Також оновлення ОП відповідно до трудових функцій та компетентностей професійного стандарту «Фахівець сфери захисту інформації» є врахуванням міжнародного досвіду, оскільки сам цей стандарт розроблено з урахуванням міжнародних вимог, зокрема стандартів американського NIST.

2. Структура та зміст освітньої програми

Яким є обсяг ОП (у кредитах ЄКТС)?

90

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

66

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

24

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

Зміст освітньо-професійної програми повністю відповідає предметній області заявленої спеціальності, яка охоплює різноманітні аспекти захисту інформації в інформаційних системах, управління інформаційною безпекою, розробку та впровадження технічних і організаційних засобів захисту даних.
Основні компоненти програми спрямовані на підготовку фахівців, здатних вирішувати складні завдання у сфері кібербезпеки та захисту інформації. Наприклад, дисципліна «Криптологія» (ОК8) готує здобувачів до роботи з алгоритмами шифрування, які є ключовим елементом захисту даних. «Кіберфізична безпека об'єктів критичної інфраструктури» (ОК7) навчає здобувачів захищати критичні інформаційно-комунікаційні системи, що є важливим для забезпечення національної безпеки в умовах цифрової трансформації.
Предметна область спеціальності включає вивчення сучасних інформаційних технологій, технічних систем та мереж, що забезпечують збереження, передавання, оброблення та захист інформації від несанкціонованого доступу, зломів і кіберзагроз. Це охоплює як фізичні засоби захисту інформації, так і сучасні програмні технології для забезпечення кіберзахисту на всіх етапах обробки даних.

ОП забезпечує набуття здобувачами як загальних, так і фахових компетентностей, необхідних для професійної діяльності в галузі кібербезпеки. Наприклад, серед ключових компетентностей можна виділити – СК11, СК13, СК14. Зазначені компетентності відповідають вимогам професійного стандарту «Фахівець сфери захисту інформації», затвердженого Адміністрацією Держспецзв'язку, що визначає основні завдання фахівців у сфері кібербезпеки та захисту інформації.
Програма також передбачає міждисциплінарний підхід, який полягає в інтеграції знань з технічних, організаційних, правових та управлінських аспектів кібербезпеки. Це відображено у таких освітніх компонентах, як «Менеджмент інформаційної безпеки» (ОК5), що поєднує знання з управління та технологій захисту інформації, а також у курсах з процесного менеджменту, які дають здобувачам змогу застосовувати принципи управління в галузі інформаційної безпеки.
Програма розроблена з урахуванням сучасних вимог ринку праці, що підтверджується участю стейкголдерів, таких як ГО «Асоціація спеціалістів кібербезпеки». ТОВ "Консалтинговна компанія "СІДКОН", а також представників компаній, що працюють у сфері інформаційної безпеки. Це дозволяє забезпечити актуальність програми та відповідність потребам роботодавців.
Освітньо-професійна програма «Кібербезпека та захист інформації» повністю відповідає предметній області заявленої спеціальності 125 «Кібербезпека та захист інформації». Вона забезпечує комплексну підготовку фахівців, здатних вирішувати дослідницькі та інноваційні завдання у сфері кібербезпеки, зокрема захисту критичної інфраструктури та інформаційних систем.

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

Формування індивідуальної освітньої траєкторії унормовується згідно з «Положенням про індивідуальний навчальний план здобувачів вищої освіти в ДУІТЗ» (https://suitt.edu.ua/wp-content/uploads/2023/05/PRO-INDYVIDUAL-NYY-NAVCHAL-NYY-PLAN-ZDOBUVACHIV-VYSHCHOYI-OSVITY-V-DUITZ.pdf).
Здобувачі вищої освіти мають можливість самостійно формувати свою освітню траєкторію на кожному етапі навчання згідно з Законом України "Про вищу освіту" (пункт 15 частини першої статті 62). Вони можуть обирати навчальні компоненти, орієнтуючись на власні інтереси та потреби. Для кращого розуміння специфіки різних вибіркових компонентів викладачі проводять співбесіди, під час яких роз'яснюють компетентності, що розвиваються завдяки вибору тієї чи іншої дисципліни. Також здобувачам надається доступ до навчальних програм і силабусів (https://shorturl.at/cNzre, https://suitt.edu.ua/vybirkovi-dystsypliny/), що дозволяє самостійно обирати компоненти з доступного каталогу. Для формування індивідуальної траєкторії в межах ОП передбачено вибіркові дисципліни обсягом 24 кредити ECTS.
Формуванням освітньої траєкторії здобувача опікується керівництво факультету, завідувач спеціальної кафедри КБ та ТЗІ та відповідальні за вибір дисциплін здобувачами.

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

Здобувачі мають можливість вибирати вибіркові компоненти загальним обсягом 24 кредитів ECTS із загальної кількості 90 кредитів ECTS, що дозволяє формувати власну індивідуальну навчальну траєкторію. Процедура вибору освітніх компонентів регулюється «Положенням про Порядок вибору навчальних дисциплін студентами ДУІТЗ» (https://suitt.edu.ua/wpcontent/uploads/2023/12/polozhennia_pro_poriadok_vyboru_navchalnykh_dystsyplin_studentamy_duitz.pdf). Механізм вибору навчальних дисциплін постійно вдосконалюється для полегшення процесу вибору здобувачами. Здобувачі вибирають дисципліни на основі їхніх інтересів та індивідуальних потреб. Для цього використовується каталог вибіркових навчальних дисциплін (https://suitt.edu.ua/vybirkovi-dystsypliny/), що дозволяє здобувачам гнучко підходити до вибору предметів та формувати освітню траєкторію, яка відповідає їх професійним цілям.

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

У програмі та навчальному плані передбачено практичні та лабораторні заняття, виконання курсових робіт та проектів, результатом яких є отримання практичних вмінь. Курсові роботи за всіма дисциплінами спрямовані на набуття необхідних для майбутньої професійної діяльності навичок.
Також на 2-му курсі здобувачі проходять виробничу практику на підприємствах в обсязі 12 кредитів. Метою переддипломної практики є досягнення практичних результатів навчання, передбачених в освітній програмі.

Положення про порядок проведення практичної підготовки здобувачів вищої освіти ДУІТЗ:
https://suitt.edu.ua/wpcontent/
uploads/2023/12/polozhennia_pro_poriadok_provedennia_praktychnoi_pidhotovky_zdobuvachiv.pdf

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

Навчальна програма містить компоненти, спрямовані на розвиток соціальних soft-навичок у здобувачів (ЗК3, ЗК4, СК10).
Дисципліна «Ділова іноземна мова» (ОК11) дозволяє здобувачам вдосконалити вміння вести переговори та складати ділову документацію іноземною мовою. Дисципліна «Методологія та організація наукових досліджень» (ОК1) сприяє оволодінню широкою панорамою методологічних принципів і підходів до наукового дослідження; формування методологічної і наукової культури, розвиває вміння чітко передавати інформацію, захищати дослідження перед аудиторією. Курсовий проєкт у дисципліні «Комплексні системи безпеки» (ОК6) передбачає

роботу в команді, що сприяє розвитку співпраці та розподілу обов'язків. Виробнича практика (ОК12) дає змогу здобути досвід практичної та командної роботи на підприємствах.
Дисципліни «Менеджмент інформаційної безпеки» (ОК5) та «Моніторинг та аудит інформаційно-комунікаційних систем» (ОК10) навчають приймати рішення в умовах невизначеності, аналізувати ризики й вирішувати проблеми кіберзагроз.
Дисципліна «Процесний менеджмент у корпоративній безпеці» (ОК9) розвиває управлінські навички, дозволяючи здобувачам планувати та керувати безпековими процесами. Дисципліна «Педагогіка та психологія» (ОК2) навчає розуміти емоції, управляти конфліктами та дотримуватись етики.
Захист магістерської роботи (ОК13) і робота в реальних умовах під час практики допомагають розвивати стресостійкість.

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

Освітня програма має чітку структуру, що забезпечує систематичність і послідовність навчання. Кожен компонент програми відіграє визначену роль у досягненні заявленої мети та програмних результатів навчання. Зміст програми розподілений на обов'язкові та вибіркові дисципліни. Обов'язкові дисципліни забезпечують фундаментальну та спеціальну підготовку, охоплюючи основи відповідної галузі, в той час як вибіркові дисципліни дозволяють здобувачам адаптувати навчання під свої професійні інтереси. Освітні компоненти взаємопов'язані: знання, отримані в одній дисципліні, використовуються і розвиваються в інших. Це створює інтегровану систему, що дозволяє глибше зрозуміти матеріал і застосовувати отримані навички в різних контекстах. Всі освітні компоненти спрямовані на досягнення конкретних результатів навчання, які були визначені як ключові для підготовки кваліфікованих фахівців.

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

В ДУІТЗ обсяг освітньої програми та студентське навантаження вимірюються в кредитах ECTS і регулюються відповідно до "Положення про організацію освітнього процесу в ДУІТЗ". При розробці навчальних планів і програм дотримуються встановлених нормативів. Загальний обсяг програми складає 90 кредитів ECTS (2700 годин), де 74% (66 кредитів) становлять обов'язкові компоненти, а 26% (24 кредити) — вибіркові. У навчальному плані за освітньою програмою передбачений такий розподіл годин для обов'язкових компонентів: 734 годин відводиться на аудиторні заняття, а 1966 годин — на самостійну роботу здобувачів.

Положення про організацію освітнього процесу в ДУІТЗ:
https://suitt.edu.ua/wp-content/uploads/2023/12/polozhennia_pro_orhanizatsiiu_osvitnoho_protsesu_v_duitz.pdf

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

Структура освітньої програми «Кібербезпека та захист інформації» забезпечує її практикоорієнтованість через поєднання теоретичних знань і реальних практичних завдань. Основні освітні компоненти, такі як виробнича практика (ОК12) та курсові проєкти у рамках дисциплін «Комплексні системи безпеки» (ОК6) і «Моніторинг та аудит інформаційних систем» (ОК10), дають змогу здобувачам застосовувати отримані знання у реальних умовах. Виробнича практика проходить на підприємствах, де здобувачі вирішують завдання кіберзахисту, адаптуючись до потреб ринку.
Дуальна форма освіти передбачає поєднання навчання у закладі освіти з професійною діяльністю. Модель дуальної освіти реалізується через:
- Чергування навчальних і виробничих періодів: здобувачі певний час навчаються в університеті, а потім працюють на підприємстві, де виконують завдання відповідно до програми.
- Залучення стейкголдерів: роботодавці активно беруть участь у розробці та вдосконаленні навчальних програм, а також у оцінюванні результатів практики здобувачів.
- Проєктне навчання: здобувачі працюють над реальними проєктами з кібербезпеки під керівництвом менторів від підприємств, що дозволяє їм отримати практичні навички ще під час навчання.

Положення про дуальну форму здобуття вищої освіти у ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2023/05/POLOZHENNYA-PRO-DUAL-NU-FORMU-ZDOBUTTYA-VYSHCHOYI-OSVITY-U-DUITZ.pdf
На даний час дуальна форма освіти за ОП у процесі впровадження.

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

ОП «Кібербезпека та захист інформації» спрямована на набуття здобувачами навичок і компетентностей, які

сприяють досягненню глобальних цілей сталого розвитку до 2030 року, зокрема:
-Ціль 4: Якісна освіта. ОП забезпечує доступ до інноваційної освіти у сфері кібербезпеки та захисту інформації, використовуючи сучасні методи навчання, залучення стейкголдерів та забезпечення дуальної освіти. Це сприяє підвищенню кваліфікації та розвитку критичного мислення у здобувачів.
-Ціль 8: Гідна праця та економічне зростання. ОП спрямована на підготовку висококваліфікованих фахівців для ринку праці, що відповідають потребам цифрової економіки. Здобувачі отримують навички, які дозволяють їм працювати у високотехнологічних сферах, забезпечуючи зростання продуктивності праці.
-Ціль 9: Інновації та інфраструктура. ОП спрямована на підготовку фахівців, здатних розробляти та впроваджувати інноваційні рішення для забезпечення кібербезпеки, що сприяє створенню надійної цифрової інфраструктури.
-Ціль 16: Мир, справедливість та сильні інститути. Навички захисту інформації, здобуті здобувачами, сприяють зміцненню кібербезпеки на рівні державних та приватних установ, що є важливим елементом забезпечення стійких інституцій.
ОП інтегрує ці глобальні цілі через освітні компоненти та практичну діяльність здобувачів.

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

https://suitt.edu.ua/vstup/

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

Вступники, які здобули перший рівень вищої освіти (бакалавр) приймаються на навчання за ОП на перший курс. Вони беруть участь у конкурсі за результатами ЗНО. Для спеціальності 125 конкурсним предметом у сертифікатах УЦОЯО є іноземна мова, високий рівень підготовки за яким відповідає профілю підготовки за ОП, а також ТЗНК та фаховий іспит за галуззю знань 12 Інформаційні технології.
Правила прийому на навчання за ОП оприлюднені на офіційному вебсайті ДУІТЗ (https://shorturl.at/RRkT5).

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?

Дане питання регулюється відповідно до наступних документів:
- Положення про організацію освітнього процесу в ДУІТЗ (https://shorturl.at/ZDXqU)
- Положення про порядок визнання результатів навчання отриманих у неформальній освіти в ДУІТЗ (https://shorturl.at/HEvuY)
- Положення про визнання (перезарахування) кредитів, отриманих здобувачами під час академічної мобільності в закордонних закладах вищої освіти ДУІТЗ (https://shorturl.at/Dq8qx)
- Положення про порядок відрахування, переривання навчання, поновлення і переведення осіб, а також надання їм академічної відпустки (https://shorturl.at/Fm55C)
- Положення про академічну мобільність здобувачів вищої освіти у ДУІТЗ (https://suitt.edu.ua/wp-content/uploads/2023/05/Polozhennya-pro-Akademicheskuyu-Mobilnost-ZVO-v-DUITZ.pdf)
- Положення про порядок визнання документів про освіту, виданих іноземними закладами освіти ДУІТЗ (https://suitt.edu.ua/wp-content/uploads/2023/05/pro-PORYADOK-VYZNANNYA-DOKUMENTIV-PRO-OCBITU-VYDANYKH-INOZEMNYMY-ZAKLADAMY-OSVITY-DUITZ.pdf)
- Положення про порядок визначення та ліквідації академічної різниці особами, що поновлюються або переводяться до ДУІТЗ (https://suitt.edu.ua/wp-content/uploads/2024/04/polozhennia_pro_poriadok_vyznannia_ta_likvidatsii_akademichnoi_riznytsi.pdf)
Всі зазначені документи оприлюднені на офіційному вебсайті ДУІТЗ.

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

За ОП, що акредитується, таких прикладів не було.

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

Здобувач вищої освіти має можливість подати заяву до ректора для визнання даних результатів, прикладаючи необхідні документи щодо отримання цих результатів. Для розгляду заяви створюється спеціальна предметна комісія згідно з розпорядженням декана факультету. У складі комісії можуть бути представники деканату, гарант освітньої програми та викладачі з відповідних дисциплін. Комісія надає здобувачеві 10 робочих днів для підготовки до підсумкового контролю з кожної дисципліни, що розглядається, в формі екзамену. Після оцінювання комісія складає протокол із висновками щодо зарахування або незарахування дисциплін. У разі позитивного результату відповідні дані вносяться до навчальної картки здобувача.

Положення про порядок визнання результатів навчання отриманих у неформальній освіті в ДУІТЗ (https://shorturl.at/HEvuY)

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

За ОП, що акредитується, таких випадків 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?

Методологія викладання базується на студентоцентрованому та проблемно-орієнтованому підході, що включає лекції, практичні заняття, проєктну діяльність та самостійну роботу. Інтерактивні мультимедійні лекції, дослідницькі та практичні завдання сприяють активному навчанню здобувачів. Курсові проєкти, реальні кейси, хакатони та практична підготовка забезпечують здобуття практичних навичок. Використання новітніх технологій кіберзахисту, симуляційних інструментів та кіберполігонів дозволяє моделювати й аналізувати кіберзагрози, сприяючи досягненню мети та програмних результатів навчання програми.
Також значну роль відіграє індивідуальна робота здобувачів з викладачами, яка забезпечується за допомогою електронної пошти, телеграм-каналів та платформ відеозв'язку, таких як Zoom та Meet (https://meet.suitt.edu.ua/). Важливо зазначити, що дистанційне навчання також використовується для досягнення програмних результатів згідно з Положенням про дистанційне навчання в ДУІТЗ. Для цього використовуються платформи відеозв’язку та система дистанційного навчання Moodle (http://e-learning2.suitt.edu.ua/)

Положення про організацію освітнього процесу в ДУІТЗ:
https://shorturl.at/AvOP6
Положення про дистанційне навчання в ДУІТЗ:
https://shorturl.at/vo7Up

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?

Методи, засоби та технології навчання і викладання в програмі «Кібербезпека та захист інформації» повністю відповідають вимогам студентоцентрованого підходу, який забезпечує індивідуалізацію навчального процесу. Це досягається через гнучкі освітні траєкторії, що дозволяють здобувачам самостійно обирати вибіркові компоненти навчання, а також через активне використання проєктного та проблемно-орієнтованого навчання. Практичні заняття, дослідницькі проєкти та інтерактивні мультимедійні лекції стимулюють здобувачів до самостійного прийняття рішень, розвитку критичного мислення та активної участі у навчальному процесі. Залучення роботодавців і експертів-практиків до навчального процесу забезпечує реальний зв'язок між теорією та практикою. Здобувачі мають доступ до сучасних технологій, кіберполігонів та симуляцій, що дозволяє їм працювати над реальними кейсами. Представники роботодавців регулярно проводять гостеві лекції для здобувачів (https://suitt.edu.ua/fakultet-itk/ підрозділ "Ініціативи")
Індивідуальна освітня траєкторія здобувача визначається через його можливість вибору навчальних дисциплін, що забезпечується «Положенням про Порядок вибору навчальних дисциплін студентами ДУІТЗ» (https://shorturl.at/WmEZN).
За результатами опитувань, рівень задоволеності здобувачів методами навчання високий (https://suitt.edu.ua/wp-content/uploads/2024/10/analitychna_zapyska_m_125.pdf).

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

Право на академічну свободу забезпечується для НПП та педагогічних працівників ЗВО згідно Закону України "Про освіту" №2145-VIII від 05.09.2017 року. Це означає, що вони мають можливість вільно обирати методи та засоби навчання. ЗВО не обмежує академічну свободу для своїх працівників і здобувачів, і не використовує їхні публічні заяви, включаючи соціальні мережі, як підставу для дисциплінарних санкцій, звільнень або відрахувань. Враховуючи це, викладачі здійснюють індивідуальний підхід у виборі форм, методів і засобів навчання, враховуючи потреби та особливості здобувачів, їхній рівень підготовки, інтереси, та інші аспекти.

Закон України "Про освіту" №2145-VIII від 05.09.2017 року:
https://zakon.rada.gov.ua/laws/show/2145-19

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

Мета, зміст і очікувані результати навчання чітко визначені в Освітніх програмах (ОП). Усі ОП, за якими в ДУІТЗ проводиться підготовка здобувачів вищої освіти, доступні для ознайомлення на офіційному сайті ЗВО, що забезпечує усім здобувачам доступ до цієї інформації (https://suitt.edu.ua/osvitni-prohramy-2024/).
У силабусах освітніх компонентів наведені цілі, зміст і очікувані результати навчання, а також критерії та порядок оцінювання (https://suitt.edu.ua/sylabusy-125-kiberbezpeka-ta-zakhyst-informatsii-mahistr-2024/). Крім того, здобувачі мають можливість звернутися до методичних матеріалів і рекомендацій щодо організації самостійної роботи (https://metod.suitt.edu.ua/).
Перед початком навчання гарант ОП організовує загальні збори, під час яких надає основну інформацію про очікувані результати навчання. Крім того, конкретні завдання, критерії оцінювання і методи навчання обов'язково пояснюються кожним викладачем на першому занятті для кожного окремого освітнього компоненту.

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

Поєднання навчання та досліджень у межах освітньо-професійної програми «Кібербезпека та захист інформації» забезпечується через інтеграцію науково-дослідної діяльності в усі ключові компоненти навчального процесу. Важливою частиною цієї інтеграції є дисципліни, що закладають основи наукових досліджень, зокрема «Методологія та організація наукових досліджень» (ОК1), яка дає здобувачам базові знання про проведення наукових досліджень, планування експериментів та наукового аналізу результатів. Здобувачі залучаються до проведення досліджень вже на початкових етапах навчання, що дозволяє їм розвивати критичне мислення, уміння формулювати наукові гіпотези та застосовувати методи системного аналізу для вирішення дослідницьких завдань у сфері кібербезпеки.
Особливістю програми є проєктне навчання, яке організоване таким чином, що здобувачі можуть поєднувати теоретичні знання з реальними дослідженнями в галузі кібербезпеки. Наприклад, у дисциплінах «Моніторинг та аудит інформаційно-комунікаційних систем» (ОК10) та «Кіберфізична безпека об'єктів критичної інфраструктури» (ОК7) здобувачі проводять дослідження в реальних умовах, використовуючи інструменти кіберполігонів та симуляційні моделі, які дозволяють їм відпрацьовувати сценарії кіберзагроз та вразливостей. Це поєднання дозволяє не лише набути практичних навичок, але й здійснити повноцінні наукові дослідження з оцінкою ризиків та рекомендаціями для вдосконалення інформаційної безпеки в реальних умовах. Окрім того, здобувачі працюють у дослідницьких групах під керівництвом викладачів, що займаються науковою роботою, та виконують індивідуальні дослідницькі завдання (https://drive.google.com/drive/folders/1_FfyT5vCrlRF3U1eH3_2onGl9ar9pPtO).
Фінальною фазою поєднання навчання і досліджень є підготовка та захист магістерської роботи (ОК13), де здобувачі демонструють здатність самостійно виконувати проєкти та наукові дослідження. Магістерські роботи включають аналіз актуальних проблем кібербезпеки, розробку нових методів захисту інформації, моделювання кіберінцидентів і оцінку ефективності систем захисту. Часто здобувачі використовують результати своїх досліджень для впровадження на підприємствах, де проходять практику, що дозволяє інтегрувати результати наукової роботи у практичну діяльність. Таким чином, освітня програма не лише готує фахівців з кібербезпеки та захисту інформації, але й надає їм можливість активно брати участь у науково-дослідних процесах та сприяти розвитку інновацій у цій сфері.

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

Викладачі освітньо-професійної програми «Кібербезпека та захист інформації» активно оновлюють зміст освітніх компонентів на основі сучасних наукових досягнень та практик у галузі кібербезпеки та захисту інформації, забезпечуючи актуальність навчання та його відповідність сучасним вимогам ринку. Це відбувається завдяки постійній участі викладачів у науково-дослідній роботі, їхній співпраці з практиками (https://suitt.edu.ua/partnery-ta-stejkholdery/) та залученню до міжнародних проєктів, зокрема, проєкту Агенства USAID «Кібербезпека критичної інфраструктури України» з 2020 року (https://www.facebook.com/CyberActivityUA/?locale=uk_UA, https://suitt.edu.ua/pidvyshchennia-kvalifikatsii-vykladachiv-kafedry-ktzi/)
Так, у 2023 році для урахування вимог професійного стандарту «Фахівець сфери захисту інформації» було оновлено зміст трьох фахових освітніх компонентів та введено два нових. Також, наприклад, дисципліна «Криптологія» (ОК8) оновлюється відповідно до останніх досліджень у сфері криптографічних методів захисту інформації. Викладачі, залучені до наукових конференцій з кібербезпеки, інтегрують у курс нові криптографічні протоколи, такі як квантова криптографія, що стають актуальними в умовах розвитку квантових обчислень. Крім того, вони використовують наукові статті та дослідження вітчизняних та закордонних експертів для оновлення навчальних матеріалів.
Інший приклад — курс «Моніторинг та аудит інформаційно-комунікаційних систем» (ОК10), який постійно адаптується до сучасних практик кібербезпеки. Викладачі впроваджують новітні технології моніторингу загроз та методи аудиту інформаційних систем, такі як використання штучного інтелекту для аналізу великих обсягів даних у режимі реального часу. Це відображає сучасні тренди у сфері кібербезпеки та забезпечує отримання здобувачами найсучасніших знань для своєї професійної діяльності.
Також, дисципліна «Кіберфізична безпека об'єктів критичної інфраструктури» (ОК7) постійно вдосконалюється на основі співпраці з підприємствами, що працюють у сфері захисту критичної інфраструктури. Викладачі програми оновлюють матеріали, враховуючи новітні загрози для об’єктів критичної інфраструктури та сучасні стандарти, як-от рекомендації Європейського агентства з кібербезпеки (ENISA).

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

Викладання та наукові дослідження в межах ОП тісно пов’язані з інтернаціоналізацією діяльності ДУІТЗ. Інтернаціоналізація діяльності реалізується, зокрема, через участь здобувачів у міжнародних наукових

конференціях, де вони отримують інформацію про новітні досягнення і тенденції розвитку галузі кібербезпеки, представляють результати своїх досліджень, обговорюють їх з провідними фахівцями (https://suitt.edu.ua/2024/10/20/sertyfikaty-mahistriv/).
Також здобувачі беруть участь у дистанційних вебінарах, що організуються у межах проєкту USAID «Кібербезпека критично важливої інфраструктури України» та проводяться відчизняними та іноземними провідними фахівцями з кібербезпеки, наприклад:
- Семінар з експертом галузі кібербезпеки Аллою Кобозєвою «Фундаментальні основи побудови крипто-стеганографічної системи», за підтримки Проєкту USAID "Кібербезпека критично важливої інфраструктури України"
https://www.facebook.com/CyberActivityUA/posts/pfbid07ogywixSJTqTa1c3UYR7NAJetUfQJGuzxJBwxYZ84JgA8JPn1giEhRVStcKRFBnjl
- Семінар з експертом галузі кібербезпеки Владиславом Радецьким "Основи перевірки файлів або як створити власний SandBox"», за підтримки Проєкту USAID "Кібербезпека критично важливої інфраструктури України"
https://www.facebook.com/CyberActivityUA/videos/931596165085248
- Семінар з експертом галузі кібербезпеки Микитою Книшем "Етичне полювання на неетичних хакерів", за підтримки Проєкту USAID https://www.facebook.com/CyberActivityUA/videos/792600099335875

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?

Протягом навчального семестру здобувачі періодично проходять перевірку своїх навчальних досягнень. Це включає усне та письмове опитування, виконання тестових завдань, звіти з лабораторних робіт, а також презентації. Форми контролю визначаються в ОП, навчальному плані, силабусах дисциплін і індивідуальних навчальних планах здобувачів. Семестровий екзамен або комбінований тест оцінює засвоєння здобувачами теоретичного та практичного матеріалу за семестр. Оцінка досягнень здобувачів за кожною навчальною дисципліною здійснюється за шкалами ECTS, 4-х бальною шкалою ("відмінно", "добре", "задовільно", "незадовільно" або "зараховано", "незараховано"), 100-бальною шкалою. Критерії оцінювання розробляються для кожної дисципліни і включаються в робочі програми (силабуси), які затверджуються на засіданнях кафедри.

ПОЛОЖЕННЯ ПРО ОЦІНЮВАННЯ ЗНАНЬ СТУДЕНТІВ ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2023/05/Polozhennya-pro-OTSININYUVANNYA-ZNAN-STUDENTIV.pdf

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

В університеті використовуються чіткі та зрозумілі критерії оцінювання досягнень здобувачів.
Для забезпечення ясності та зрозумілості контрольних заходів та критеріїв оцінювання навчальних досягнень здобувачів вищої освіти застосовуються наступні практики: уважне планування та формування контрольних заходів кафедрами та постійна роз’яснювальна робота із здобувачами.
У відповідності до ОП, контрольні заходи містять в собі поточний та підсумковий контроль, які спрямовані на перевірку рівня знань здобувачів. Поточний контроль проводиться під час різних видів навчальних занять і використовує рейтингову систему оцінювання, що відповідає встановленим стандартам. Підсумковий контроль може бути у формі заліку, екзамену, захисту курсової роботи або проекту, а також захисту результатів практики. Оцінювання курсових робіт (проектів) здобувачів також базується на рейтинговій системі оцінювання. Критерії оцінювання навчальних досягнень установлюються викладачем і роз'яснюються здобувачам на початку кожного курсу. Для зручності підсумкового контролю використовуються, зокрема, гугл форми, а також проводиться аудиторний та дистанційний спосіб проведення тестування, що дозволяє швидко отримати результати та забезпечує особисту ідентифікацію кожного здобувача.

ПОЛОЖЕННЯ ПРО ОЦІНЮВАННЯ ЗНАНЬ СТУДЕНТІВ ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2023/05/Polozhennya-pro-OTSININYUVANNYA-ZNAN-STUDENTIV.pdf

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

Інформація про форми контрольних заходів для здобувачів вищого навчального закладу надається і уточнюється кілька разів протягом навчального періоду:
- На початку навчального семестру здобувачам роз'яснюється загальний порядок оцінювання знань, критерії оцінювання, а також форми та види контрольних заходів для кожної навчальної дисципліни.
- Форми та критерії оцінювання включаються до силабусу (програми навчальної дисципліни), до якої здобувачі мають доступ через електронну систему навчання.
- Наприкінці вивчення кожної дисципліни, під час консультацій, викладачі ще раз уточнюють форму підсумкового контролю та критерії оцінювання.
- Щорічно проводяться соціологічні опитування серед здобувачів та випускників щодо якості та об'єктивності системи оцінювання, а також студентський моніторинг якості освітнього процесу.

ПОЛОЖЕННЯ ПРО ОЦІНЮВАННЯ ЗНАНЬ СТУДЕНТІВ ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2023/05/Polozhennya-pro-OTSININYUVANNYA-ZNAN-STUDENTIV.pdf

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

Здобувачі, що навчаються за ОП, після завершення навчального плану проходять атестацію згідно з вимогами стандарту вищої освіти другого (магістерського) рівня вищої освіти. Ця атестація включає публічний захист кваліфікаційної роботи перед спеціально утвореною екзаменаційною комісією (включаючи представників роботодавців), яку затверджує ректор університету. Згідно з вимогами стандарту вищої освіти, тема кваліфікаційної роботи передбачає вирішення складних спеціалізованих завдань або практичних проблем в галузі кібербезпеки та захисту інформації і передбачає проведення досліджень або здійснення інновацій.
Єдиний державний кваліфікаційний іспит за спеціальністю 125 – Кібербезпека та захист інформації на другому (магістерському) рівні не запроваджений.

ПОЛОЖЕННЯ ПРО ЕКЗАМЕНАЦІЙНУ КОМІСІЮ ТА АТЕСТАЦІЮ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2023/12/Polozhennia_pro_EK_ta_atestatsiiu_zdobuvachiv_DUITZ_6_12_23.pdf

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

Дана процедура регулюється наступними документами:
- Положення про ДИСТАНЦІЙНЕ НАВЧАННЯ В ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2023/05/Polozhennya-pro-DISTANTSIYNE-NAVCHANNYA-V-DUITZ.pdf
- Положення про ОРГАНІЗАЦІЮ ОСВІТНЬОГО ПРОЦЕСУ в ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2023/12/polozhennia_pro_orhanizatsiiu_osvitnoho_protsesu_v_duitz.pdf
- Положення про ОРГАНІЗАЦІЮ ПОТОЧНОГО, СЕМЕСТРОВОГО КОНТРОЛЮ ТА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ ІЗ ЗАСТОСУВАННЯМ ДИСТАНЦІЙНИХ ТЕХНОЛОГІЙ В ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2023/05/Polozhennya-pro-ORHANIZATSIYU-POTOCHNOHO-SEMESTROVOHO-KONTROLYU-TA-ATESTATSIYI.pdf
- Положення про ОЦІНЮВАННЯ ЗНАНЬ СТУДЕНТІВ ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2023/05/Polozhennya-pro-OTSININYUVANNYA-ZNAN-STUDENTIV.pdf

Дані документи доступні на офіційному сайті ЗВО

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

Для забезпечення об'єктивності та неупередженості екзаменаторів застосовуються наступні заходи. Спочатку, семестровий контроль проводиться у письмовій формі, а здобувачі ознайомлюються з прикладами завдань на початку семестру. Для підсумкового контролю екзаменаційна комісія має складатися не менше, ніж з двох осіб. Щоб запобігти конфліктам інтересів, оцінювання здобувачів проводиться публічно. Також, для забезпечення нейтральності, в якості голів та/або заступників голів екзаменаційних комісій для захисту кваліфікаційних робіт здобувачів залучаються сторонні фахівці, які представляють потенційних роботодавців.

ПОЛОЖЕННЯ ПРО ОЦІНЮВАННЯ ЗНАНЬ СТУДЕНТІВ ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2023/05/Polozhennya-pro-OTSININYUVANNYA-ZNAN-STUDENTIV.pdf

ПОЛОЖЕННЯ ПРО ВИРІШЕННЯ КОНФЛІКТНИХ СИТУАЦІЙ В ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2023/12/polozhennia_pro_vyrishennia_konfliknykh_sytuatsij_v_duitz.pdf

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

Здобувачам, які не з'явилися в день, визначений для складання контрольного заходу, або отримали незадовільну оцінку, надається право на перескладання екзамену або заліку протягом сесії за графіком ліквідації академічних заборгованостей, встановленого кафедрою. Ця оцінка вважається отриманою поза терміном, за виключенням випадків, коли здобувачі працюють за індивідуальним графіком. Для здобувачів з індивідуальним графіком своєчасним терміном є дата, вказана в індивідуальному графіку для певної освітньої компоненти. Перескладання екзаменів може відбутися не більше ніж двічі з кожної дисципліни: перший раз - перед провідним лектором, другий раз - перед комісією, яка створюється розпорядженням декана факультету. Здобувач не може перескладати екзамен з дисципліни, поки не виконає всі вимоги, передбачені навчальним планом на семестр з цієї дисципліни.

ПОЛОЖЕННЯ ПРО ОЦІНЮВАННЯ ЗНАНЬ СТУДЕНТІВ ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2023/05/Polozhennya-pro-OTSININYUVANNYA-ZNAN-STUDENTIV.pdf

Яким чином процедури ЗВО урегульовують порядок оскарження процедури та результатів

проведення контрольних заходів? Наведіть приклади застосування відповідних правил на ОП

Положення про організацію навчального процесу чітко визначає академічні права та обов'язки здобувачів ВО університету. Відповідно до цього документу, здобувачі мають можливість оскаржити дії керівництва університету та інших посадових осіб, науково-педагогічних і педагогічних працівників. У випадку незгоди з оцінкою, студент може подати письмову апеляцію завідувачеві кафедри в день оголошення оцінки або на наступний робочий день, вказавши конкретні причини своєї незгоди. Комісія, створена на основі цієї заяви, включає представників адміністрації, кафедри та студентського самоврядування. Ця комісія розглядає обставини скарги та приймає рішення щодо можливого призначення повторного екзамену чи невизнання скарги у випадку відсутності фактів порушення. Важливо зауважити, що за цією ОП не було випадків оскарження процедури та результатів проведення контрольних заходів.

ПРО СИСТЕМУ ВНУТРІШНЬОГО ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОСВІТНЬОЇ ДІЯЛЬНОСТІ ТА ЯКОСТІ ВИЩОЇ ОСВІТИ ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2024/01/polozhennia_pro_systemu_vnutrishnoho_zabezpechennia_iakosti_osvitnoi.pdf

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

Наступні документи ЗВО містять політику, стандарти і процедури академічної доброчесності:
Положення ПРО ЗАБЕЗПЕЧЕННЯ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ ТА ЕТИКИ В ДЕРЖАВНОМУ УНІВЕРСИТЕТІ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ
https://suitt.edu.ua/wp-content/uploads/2024/01/polozhennia_pro_zabezpechennia_akademichnoi_dobrochesnosti_ta_etyky_v.pdf
Положення про КОМІСІЮ З ПИТАНЬ ЕТИКИ ТА АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ В ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2023/05/POLOZHENNYA-PRO-KOMISIYU-Z-PYTAN-ETYKY-TA-AKADEMICHNOYI-DOBROCHESNOSTI-V-DUITZ.pdf
КОДЕКС ЕТИКИ
https://suitt.edu.ua/kodeks-etyky-zdobuvacha/
КОДЕКС ПРОФЕСІЙНОЇ ЕТИКИ
https://suitt.edu.ua/kodeks-profesijnoi-etyky-naukovo-pedahohichnoho-pratsivnyka/

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

У п.7 Положення Про забезпечення академічної доброчесності та етики в ДУІТЗ визначено, що перевірка всіх видів робіт проводиться за допомогою програмно-технічних засобів, централізовано придбаних ДУІТЗ, які дозволяють згенерувати звіт за результатами перевірки зі встановленням факту наявності чи відсутності текстових та/або ілюстративних запозичень. Програмно-технічні засоби надаються ДУІТЗ компаніями-розробниками на платній основ. Залежно від поставленого завдання (перевірка тексту, таблиць, ілюстрацій тощо) особа, яка здійснює перевірку, обирає програмно-технічний засіб, функціональні можливості якого в максимальній мірі задовольняють поставленому завданню та офіційно встановлені в ДУІТЗ.

Репозиторій ДУІТЗ http://193.186.15.27:4000

Положення ПРО ЗАБЕЗПЕЧЕННЯ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ ТА ЕТИКИ В ДЕРЖАВНОМУ УНІВЕРСИТЕТІ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ
- https://suitt.edu.ua/wp-content/uploads/2024/01/polozhennia_pro_zabezpechennia_akademichnoi_dobrochesnosti_ta_etyky_v.pdf

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

Перш за все, академічну доброчесність серед здобувачів ОП популяризують особистим прикладом викладачі. Також академічна доброчесність підтримується за допомогою систематичної інформаційної роботи відділу з забезпечення якості, проведення анкетування серед здобувачів та науково-педагогічних працівників, вивчення передового досвіду інших ЗВО.

Результати опитування випускників ОПП “Кібербезпека та захист інформації другого (магістерського) рівня ВО"
https://suitt.edu.ua/wp-content/uploads/2024/10/analitychna_zapyska_m_125.pdf

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

У ЗВО встановлено процедури реагування на випадки порушення академічної доброчесності, відповідно до встановлених норм. Здобувачі, які порушують ці принципи, можуть стати об'єктом наступних санкцій (п.6 Положення про забезпечення академічної доброчесності та етики в ДУІТЗ):
Викладач може призначити такі види академічної відповідальності:
- зниження результатів оцінювання контрольної роботи, іспиту, заліку, тощо;
- повторне проходження оцінювання контрольних робіт, іспитів, заліків, тощо;
- призначення додаткових контрольних заходів.

Керівник кваліфікаційної роботи може призначити такі види академічної відповідальності:
- зниження результатів оцінювання кваліфікаційної роботи;
- повторне виконання окремого розділу (розділів) кваліфікаційної роботи.
Завідувачі кафедр, декани факультетів можуть призначати такі види академічної відповідальності:
- повторне проходження відповідного ОК ОП;
- повторне виконання кваліфікаційної роботи;
Проте на цієї ОП не було зафіксовано випадків порушення академічної доброчесності здобувачами.

Положення ПРО ЗАБЕЗПЕЧЕННЯ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ ТА ЕТИКИ В ДЕРЖАВНОМУ УНІВЕРСИТЕТІ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ
https://suitt.edu.ua/wp-content/uploads/2024/01/polozhennia_pro_zabezpechennia_akademichnoi_dobrochesnosti_ta_etyky_v.pdf

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

Викладачі, залучені до реалізації освітньої програми «Кібербезпека та захист інформації», мають відповідну кваліфікацію та професійний досвід, що дозволяє їм ефективно забезпечувати освітні компоненти відповідно до вимог законодавства України, зокрема Закону України «Про вищу освіту» та Стандарту вищої освіти другого (магістерського) рівня за спеціальністю 125 «Кібербезпека». На ОП читають лекції 27% докторів технічних наук, професорів, інші кандидати наук. Викладачі мають наукові ступені, що відповідають їхнім навчальним дисциплінам. Деякі викладачі мають значний практичний досвід роботи в галузі. Наприклад, Кононович Володимир Григорович, який викладає курс «Кіберфізична безпека об'єктів критичної інфраструктури» (ОК7), працював спеціалістом із захисту інформації в Одеському регіональному центрі технічного захисту інформації, що дозволяє йому ефективно поєднувати теорію та практику в навчанні здобувачів.
Викладачі регулярно підвищують свою кваліфікацію на міжнародних курсах і стажуваннях. Наприклад, гарант ОП Кільдішев Віталій Йосипович, який викладає курс «Моніторинг та аудит інформаційно-комунікаційних систем» (ОК10), пройшов курс з аудиту безпеки та управління ризиками в рамках літніх шкіл для викладачів проєкту USAID, що підтверджує його відповідність сучасним вимогам галузі.
Троє професорів, які залучені до реалізації ОП, є членами спеціалізованої вченої ради Д41.113.03 в ДУІТЗ, двоє з них - за спеціальністю 05.13.21 - Системи захисту інформації.
Таким чином, завдяки науковим ступеням, публікаціям, професійному досвіду та регулярному підвищенню кваліфікації, викладачі здатні забезпечувати освітні компоненти програми відповідно до вимог законодавства.
Інформація про підвищення кваліфікації викладачами кафедри Кібербезпеки та технічного захисту інформації наведена за посиланням https://suitt.edu.ua/pidvyshchennia-kvalifikatsii-vykladachiv-kafedry-ktzi/

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

Професійний рівень науково-педагогічних працівників (НПП) під час конкурсу для вакантних посад визначається через аналіз досягнень всіх кандидатів відповідно до ліцензійних вимог, встановлених Постановою КМУ №365 від 24.03.2021 р. «Про внесення змін до постанови КМУ №1187 від 30.12.2015 р. «Про затвердження Ліцензійних умов провадження освітньої діяльності». Зокрема, береться до уваги наявність наукових публікацій за тематикою дисципліни, що викладається, досвід викладання у системі вищої освіти, науковий авторитет, який можна оцінити індексом цитуванням наукових робіт тощо.
Кандидатури розглядаються трудовим колективом відповідної кафедри, у присутності претендентів. Кафедра оцінює професійні якості кандидатів і надає пропозицію про обрання шляхом таємного голосування. Конкурсна комісія рекомендує претендентів для подальшого розгляду на Вченій Раді Університету. Претендентів запрошують на засідання Ради, де їм ставлять питання. На основі відповідей та таємного голосування лічильна комісія визначає переможця конкурсу, а Вчена Рада підтверджує результати голосування відкритим голосуванням.

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

Роботодавці беруть участь в удосконалені освітнього процесу на всіх рівнях вищої освіти через укладання договорів про співпрацю та участь у сумісних науково-дослідних та науково-технічних проектах. Вони надають підтримку здобувачам шляхом консультацій і беруть участь у відкритих заходах для здобувачів, наприклад, гостевих лекціях (https://suitt.edu.ua/fakultet-itk/ розділ Ініціативи).
Здобувачі, що навчаються на ОП, проходять виробничу практику на більш ніж двох десятках підприємств галузі кібербезпеки та захисту інформації (https://suitt.edu.ua/partnery-ta-stejkholdery/).
При оновленні та рецензуванні ОП до консультацій залучались представники ГО «Асоціація спеціалістів кібербезпеки», ТОВ «Консалтингова компанія «СІДКОН» та ТОВ “Робер Бош ЛТД”.
Відгуки на ОП від роботодавців https://suitt.edu.ua/retsenzii-na-opp-ktzi/

Відгуки роботодавців на проєкти програм навчальних дисциплін:
СІДКОН https://suitt.edu.ua/wp-content/uploads/2024/10/vidhuky_sidkon.pdf
Робер Бош ЛТД https://suitt.edu.ua/wp-content/uploads/2024/10/vidhuky_bosh.pdf

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

Підвищення кваліфікації науково-педагогічних працівників є важливою метою, що відповідає національній освітній політиці та сприяє високій якості освіти. Цей процес передбачає розвиток спеціальних фахових, науково-методичних, педагогічних, соціально-гуманітарних, психологічних, правових, економічних та управлінських навичок. Науково-педагогічні працівники мають можливість вибирати методи та форми підвищення кваліфікації, такі як навчання за спеціалізованими програмами, стажування, участь у семінарах, тренінгах, вебінарах та інших формах заходів. Заклад вищої освіти забезпечує підвищення кваліфікації та стажування протягом кожних п'яти років в обсязі не менше шести кредитів ЄКТС, зберігаючи середню заробітну плату. У разі підвищення кваліфікації або стажування з відривом від основного місця роботи, працівники мають право на гарантії і компенсації, визначені законодавством України.
Зокрема, 10 викладачів кафедри Кібербезпеки та технічного захисту інформації у 2021 та 2022 рр. підвищили кваліфікацію в обсязі 180 кредитів ЄКТС, пройшовши програму «Cybersecurity Summer Instructor Training Program» проекту Агентства USAID "Кібербезпека критично важливої інфраструктури України". Відповідні сертифікати викладачів та програми підготовки розміщені за посиланням https://suitt.edu.ua/pidvyshchennia-kvalifikatsii-vykladachiv-kafedry-ktzi/

Наведіть конкретні приклади заохочення розвитку викладацької майстерності

У ЗВО встановлені процедури, які сприяють розвитку викладацької майстерності та наукової активності, включаючи як матеріальні, так і нематеріальні заохочення. Матеріальні стимули призначені для підтримки педагогічної, наукової та творчої ініціативи викладачів та науковців університету. Нематеріальні заохочення включають в себе вручення відзнак за досягнення в науковій, педагогічній та громадській діяльності, а також за відзначення сумлінної праці тощо. Ці заохочення можуть надаватися як від адміністрації навчального закладу, так і від місцевих органів влади або Міністерства освіти та науки України. Наприклад:
- До дня науки відзначили кращих викладачів та здобувачів Університету
https://www.facebook.com/suitt.official/posts/pfbid0FoF48W4bYwehANT6Br87v9JvVCo19ZP7CNP6Gq7Vi8r2QuiMwvtQDDQMHxUky71el

7. Освітнє середовище та матеріальні ресурси

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

Матеріально-технічна база ЗВО відповідає вимогам Державних будівельних норм України, санітарним та пожежним нормам, а також нормам з охорони праці, що забезпечує якісне здійснення освітнього процесу. Ці ресурси сприяють досягненню визначених цілей та програм розвитку закладу вищої освіти.
Фінансова діяльність ЗВО відбувається відповідно до річного фінансового звіту, який обговорюється на засіданні Вченої ради щорічно.
Здобувачі можуть виконувати дослідження у лабораторіях кафедри (https://suitt.edu.ua/pro-laboratorii-ktzi/, https://suitt.edu.ua/2024/09/28/v-universyteti-stvoreno-proiektnu-laboratoriiu-internet-rechej-iot/).
Бібліотека ЗВО містить як друковані, так і електронні виданнями та інші інформаційні матеріали, що стосуються освітнього та наукового процесу (https://suitt.edu.ua/biblioteka/).
У всіх навчальних приміщеннях ЗВО забезпечено Wi-Fi доступ до мережі Інтернет.
Навчально-методичне забезпечення освітньої програми включає навчальні плани, конспекти лекцій, методичні вказівки для практичних та лабораторних робіт, а також матеріали для самостійної роботи здобувачів (https://drive.google.com/drive/folders/1AYeNz-T2tbo-nRsnMKTvHBIRQLPmUDdE?usp=sharing).
Для дистанційного навчання в ЗВО також використовується система Moodle (http://e-learning2.suitt.edu.ua/).

ТИПОВЕ ПОЛОЖЕННЯ ПРО КАФЕДРУ ДУІТЗ:
https://suitt.edu.ua/wp-content/uploads/2023/05/TYPOVE-POLOZHENNYA-PRO-KAFEDRU-DUITZ.pdf

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

Заклад надає викладачам і здобувачам доступ до електронних бібліотек, міжнародних наукових баз даних і спеціалізованих журналів з кібербезпеки та телекомунікацій, що сприяє використанню актуальних досліджень для підготовки до занять та наукової роботи. Бібліотека має електронні каталоги та надає доступ до наукових праць, що забезпечує якісну інформаційну підтримку навчального процесу (http://lib.onat.edu.ua/index2.php).
Для практичного навчання заклад оснащений сучасними лабораторіями з кібербезпеки та технічного захисту інформації. Лабораторії обладнані сучасним обладнанням з засобами технічного захисту інформації, комп'ютерами

та спеціалізованим програмним забезпеченням для моделювання кіберзагроз, захисту інформаційних систем і криптографії. Використовується також спеціалізоване ПЗ для моніторингу та аудиту безпеки.
Для дистанційного навчання використовується платформа Moodle, яка забезпечує доступ до матеріалів, тестів і завдань, а також інтерактивні форми навчання. Онлайн-лекції та семінари проводяться через платформи Zoom та/або Meet.
Здобувачі опановують сучасне обладнання у проєктних лабораторіях https://suitt.edu.ua/activity/nashi-studenty-opanovuyut-suchasne-obladnannya-u-proyektnykh-laboratoriyakh/

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

Університетське середовище, де навчаються здобувачі ОП, забезпечує їхню безпеку та враховує їхні потреби та інтереси. Всі приміщення, як навчальні, так і адміністративні, відповідають стандартам техніки безпеки та забезпечують необхідні умови для комфортного перебування, зокрема щодо освітлення, тепла та вентиляції, а також виконання спеціалізованих лабораторних робіт. Робочі режими навчального обладнання відповідають встановленим нормам. Здобувачі регулярно проходять інструктажі з охорони праці, а діяльність в цьому напрямку контролюється відділом охорони праці університету. Проводяться зустрічі з фахівцями з пожежного та цивільного захисту для забезпечення безпеки всіх працівників та здобувачів.
Два корпуси ДУІТЗ мають укриття.

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.

Здобувачам надається доступ до сучасних освітніх платформ, таких як Moodle, де розміщені всі необхідні навчальні матеріали, силабуси та завдання. Викладачі проводять регулярні консультації, як у форматі офлайн, так і онлайн, для допомоги в розумінні навчального матеріалу, підготовці до заліків та екзаменів, а також виконанні курсових і випускових кваліфікаційних робіт. Індивідуальні плани навчання дозволяють здобувачам адаптувати своє навчання відповідно до особистих потреб і ситуацій.
Заклад вищої освіти забезпечує здобувачів усією необхідною інформацією через офіційні канали, зокрема, веб-сайт, електронну пошту, месенджери та соціальні мережі (https://www.facebook.com/suitt.official, https://www.facebook.com/FacultyITC). Здобувачам надається інформація щодо навчального процесу, розкладу занять, екзаменів, а також про участь у конференціях, конкурсах і можливостях академічної мобільності. Регулярно проводяться зустрічі зі студентським самоврядуванням та адміністрацією, де здобувачі можуть висловити свої потреби та пропозиції.
Викладачі та куратори академічних груп регулярно надають консультації з академічних і професійних питань, допомагаючи здобувачам будувати індивідуальні траєкторії навчання та кар'єрного розвитку. Здобувачі мають можливість звертатися до викладачів за порадами стосовно науково-дослідницької діяльності, вибору дисциплін або підготовки до майбутньої професійної діяльності.
Заклад вищої освіти активно сприяє здоровому способу життя здобувачів через доступ до спортивних залів і секцій. Регулярно організовуються спортивні заходи, змагання та тренування. Для підтримки ментального здоров'я працює психологічна служба, яка проводить індивідуальні консультації та тренінги на теми стресостійкості, саморегуляції та подолання емоційних проблем.
Таким чином, університет забезпечує повноцінну підтримку здобувачів вищої освіти на всіх етапах їх навчання, сприяючи їхньому академічному, професійному та особистому розвитку.

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)

Правила прийому до вищого навчального закладу не обмежують можливість вступу осіб з особливими освітніми потребами. З метою забезпечення доступності освіти для цієї категорії осіб, у ДУІТЗ створено спеціальні умови. Наприклад, встановлено пандуси для зручного пересування на вході. Особам з особливими потребами надається можливість скласти індивідуальний графік навчання. При необхідності, навчальний процес може проводитися дистанційно.
Серед здобувачів ОПП «Кібербезпека та захист інформації» другого (магістерського) рівня вищої освіти не було осіб з особливими освітніми потребами.

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

Відповідно до законодавства України та Статуту ДУІТЗ прийнято Положення про комісію з питань етики та академічної доброчесності в ДУІТЗ. Для розгляду порушень створена Комісія з питань етики та академічної доброчесності. Університет також активно протидіє гендерному насильству, сексуальним домаганням, дискримінації та корупції шляхом проведення інформаційних та просвітницьких кампаній та створення Комісії для врегулювання конфліктних ситуацій та виявлення недоречної поведінки.
Серед здобувачів ОПП «Кібербезпека та захист інформації» конфліктні ситуації такого роду не зафіксовані.

Положення про комісію з питань етики та академічної доброчесності
https://suitt.edu.ua/wp-content/uploads/2023/05/POLOZHENNYA-PRO-KOMISIYU-Z-PYTAN-ETYKY-TA-AKADEMICHNOYI-DOBROCHESNOSTI-V-DUITZ.pdf

Положення про вирішення конфліктних ситуацій в ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2023/12/polozhennia_pro_vyrishennia_konfliknykh_sytuatsij_v_duitz.pdf

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

Наступними документами регулюються процедури розроблення, затвердження, моніторингу та періодичного перегляду ОП:
ПОЛОЖЕННЯ ПРО СИСТЕМУ ВНУТРІШНЬОГО ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОСВІТНЬОЇ ДІЯЛЬНОСТІ ТА ЯКОСТІ ВИЩОЇ ОСВІТИ ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2024/01/polozhennia_pro_systemu_vnutrishnoho_zabezpechennia_iakosti_osvitnoi.pdf
ПОЛОЖЕННЯ ПРО РОЗРОБЛЕННЯ ТА ЗАТВЕРДЖЕННЯ, МОНІТОРИНГ ТА ПЕРЕГЛЯД ОСВІТНІХ ПРОГРАМ В ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2023/05/Polozhennya-pro-ROZROBLENNYAO-ZATVERDZHENNYAO-MONITORYNH-TA-PEREHLYAD-OCBITHIX-PROHRAM-V-DUITZ.pdf

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

Періодичний моніторинг, огляд і оновлення освітніх програм націлені на забезпечення високої якості надання освітніх послуг і створення сприятливого й ефективного навчального та наукового середовища для здобувачів. Критерії для перегляду освітніх програм визначаються через аналіз та прогнозування розвитку наукового, виробничого та навчального середовища на національному та міжнародному рівнях та з врахуванням відгуків від роботодавців, випускників та здобувачів. Освітні програми переглядаються щорічно, а оновлюються - за потребою.
У 2023 ОП була суттєво оновлена за підтримці проєкту Агентства USAID «Кібербезпека критично важливої інфраструктури України» з метою інтеграції до неї професійних компетентностей, знань, умінь та навичок з професійного стандарту «Фахівець сфери захисту інформації» (https://suitt.edu.ua/reformuvannia-opp/), що обґрунтовано в першу чергу потребами сучасного ринку праці для фахівців з кібербезпеки та захисту інформації.
У 2024 році було оновлено дві освітні компоненти програми:
-ОК5 Менеджмент інформаційної безпеки
-ОК9 Процесний менеджмент в системі корпоративної безпеки

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

Під час перегляду освітніх програм увага приділяється думці всіх учасників навчального процесу, включаючи здобувачів. Здобувачам надається можливість висловити свої враження щодо навчального процесу, змісту освітніх складових та подати пропозиції щодо поліпшення програми за допомогою анонімних анкет. Аналіз відгуків допомагає виявити переваги та недоліки освітніх програм (https://suitt.edu.ua/wp-content/uploads/2024/10/analitychna_zapyska_m_125.pdf).

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

Представники студентського самоврядування залучаються до процесів забезпечення якості освітніх програм. Вони беруть участь у засіданнях кафедр для оцінки та перегляду програм, а також можуть приймати участь у розгляді та затвердженні програм на засіданнях Вченої Ради.

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

Роботодавці та стейкголдери залучені до періодичного перегляду ОП завдяки регулярним їх зустрічам з робочою групою та проведенню заходів в університеті.
Детальну інформацію про оновлення ОП за участю роботодавців та професійних об'єднань спеціалістів галузі кібербезпеки та захисту інформації розміщено за посиланням https://suitt.edu.ua/reformuvannia-opp/

Опишіть практику збирання, аналізу та врахування інформації щодо кар'єрного шляху та траєкторій

працевлаштування випускників ОП (зазначте в разі проходження акредитації вперше)

Інформацію про професійний розвиток випускників збирають і аналізують співробітники, що відповідають за якість освіти в ДУІТЗ, а також викладачі кафедри КБ та ТЗІ. Як свідчать результати опитувань, більше половини здобувачів ОП працюють за фахом вже на 2-му курсі магістратури.
Викладачі кафедри КБ та ТЗІ та адміністрація університету сприяють працевлаштуванню випускників ОП, а також мають з ними постійний зв'язок, що допомагає слідкувати за їх успіхом самореалізації у професії.

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

Система забезпечення якості закладу вищої освіти передбачає ефективний механізм моніторингу освітньої програми та освітньої діяльності, що реалізується через постійний аналіз результатів опитувань заінтересованих сторін, включаючи здобувачів, викладачів, роботодавців та випускників. Моніторинг здійснюється з використанням анкетувань, зворотного зв'язку та залучення стейкголдерів до обговорення результатів навчання.
Здобувачі заповнюють анкети щодо якості викладання, змісту освітніх компонентів, матеріально-технічного забезпечення та відповідності навчального процесу їхнім очікуванням ((https://suitt.edu.ua/wp-content/uploads/2024/10/analitychna_zapyska_m_125.pdf). Результати опитувань аналізуються відділом забезпечення якості освіти, і на їх основі вносяться зміни до освітніх програм.
Роботодавці, як заінтересовані сторони, також беруть участь в опитуваннях і надають відгуки, у тому числі в усній формі, про готовність випускників до роботи, необхідні навички та компетентності. На основі таких відгуків було внесено зміни до програми, зокрема оновлено зміст дисциплін, пов'язаних із кібербезпекою критичної інфраструктури, та впроваджено нові методи навчання, орієнтовані на практичні кейси.
Кожен навчальний рік проводиться комплексний аналіз результатів опитувань усіх заінтересованих сторін, і на його основі розробляються рекомендації для вдосконалення освітнього процесу. Це включає коригування навчальних планів, зміни у методах викладання, покращення технічного та інформаційного забезпечення.
Зокрема, значну користь для оновлення ОП, перегляду змісту освітніх компонентів, підвищення кваліфікації викладачів принесла участь кафедри в проєкті Агентства USAID «Кібербезпека критично важливої інфраструктури України» з 2021 р. (https://www.facebook.com/CyberActivityUA/?locale=uk_UA)
Таким чином, система забезпечення якості оперативно реагує на результати моніторингу та постійно вдосконалює освітню програму на основі відгуків усіх заінтересованих сторін.

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?

Під час удосконалення даної ОП було взято до уваги усі зауваження останньої акредитації (2019 р.):
1. Для подальшого удосконалення науково-методичної роботи збільшити кількість закордонних стажувань викладачів кафедри «Інформаційної безпеки та передачі даних» та розширити їх участь у міжнародних конференціях, симпозіумах, семінарах.
2. Розробити програму та організаційні заходи щодо подальшої професійної сертифікації викладачів кафедри, магістрів та аспірантів за освітньо-науковим напрямом роботи кафедри, зокрема, кандидату філософських наук, доценту Стайкуці С.В., завершити проходження довгострокового підвищення кваліфікації за спеціальністю 125 Кібербезпека.
3. Активізувати роботу щодо удосконалення організаційного і методичного забезпечення самостійної роботи здобувачів, посилити контроль за її виконанням.
4. Продовжити роботу з забезпечення навчального процесу сучасним лабораторним обладнанням, зокрема, звернути увагу на використання ліцензійного програмного забезпечення в лабораторії «Кібербезпека».
5. Підвищити ефективність набору та випуску докторів філософії з метою формування кадрового резерву кафедри.
Таким чином:
1. Більшість викладачів кафедри регулярно проходять міжнародні стажування, Однією з таких програм були літні школи проєкту Агентства USAID «Кібербезпека критичної інфраструктури України», що стало основою для оновлення даної ОП. Сертифікати викладачів розміщено за посиланням https://suitt.edu.ua/pidvyshchennia-kvalifikatsii-vykladachiv-kafedry-ktzi/ .
2. Усі викладачі кафедри регулярно проходять підвищення кваліфікації відповідно до графіку. Зокрема, доцент Стайкуці С.В. пройшов довгострокове підвищення кваліфікації за спеціальністю 125 Кібербезпека (сертифікат https://suitt.edu.ua/wp-content/uploads/2024/03/sergii-staikuca.pdf).
3. Кафедра регулярно оновлює усе методичне забезпечення своїх дисциплін, необхідне для самостійної роботи здобувачів. Методичне забезпечення розміщується на сайті бібліотеки університету (https://metod.suitt.edu.ua/) та на платформі Moodle (http://e-learning2.suitt.edu.ua/).
4. Кафедра регулярно розширює співпрацю з багатьма стейкголдерами (https://suitt.edu.ua/partnery-ta-stejkholdery/), які зацікавлені у вдосконаленні лабораторного забезпечення лабораторій (https://suitt.edu.ua/pro-laboratorii-ktzi/, https://suitt.edu.ua/2024/09/28/v-universyteti-stvoreno-proiektnu-laboratoriiu-internet-rechej-iot/). Окрім цього, участь у проєкті Агентства USAID «Кібербезпека критичної інфраструктури України» надала можливість у 2023-2024 рр. отримати сучасне серверне та мережеве обладнання для побудови власного кіберполігону (https://suitt.edu.ua/2024/02/28/derzhavnyj-universytet-intelektualnykh-tekhnolohij-i-zv-iazku-otrymav-obladnannia-vid-ahentstva-ssha-z-mizhnarodnoho-rozvytku-usaid/).
5. Кафедра постійно працює над створенням кадрового резерву. Так у 2023 р. викладачі кафедри Стайкуца С.В. та Рябуха О.М. вступили до докторантури за спеціальністю 05.13.21 – Системи захисту інформації.

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

Університет активно залучає академічну спільноту до внутрішніх аудитів системи управління якістю освітніх програм через наступні заходи:
- Розробка, моніторинг та регулярний перегляд освітніх програм за участю представників провідних кафедр відповідних спеціальностей.
- Регулярний аналіз навчальних планів та змісту робочих програм дисциплін за участю представників підприємств-партнерів.
- Обговорення проектів освітніх програм на засіданнях Вченої Ради із залученням усіх зацікавлених сторін академічної спільноти.
- Підвищення кваліфікації науково-педагогічних працівників у провідних наукових та навчальних закладах України та світу.
- Забезпечення ефективної системи виявлення та запобігання академічному плагіату в навчальному процесі.

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

Культура якості освіти формується завдяки організації внутрішнього забезпечення якості вищої освіти. Це відбувається на п'яти рівнях:
- Перший рівень – здобувачі та їхні ініціативні групи, які вносять пропозиції та зауваження щодо програм.
- Другий рівень – кафедри, гаранти програм, робочі групи, викладачі, а також представники стейхолдерів.
- Третій рівень – структурні підрозділи, які займаються освітньою діяльністю, включаючи деканів факультетів, представники студентського самоврядування.
- Четвертий рівень – Загально-університетські структурні підрозділи, відповідальні за забезпечення якості, навчально-методична та науково-технічна ради університету.
- П'ятий рівень – Наглядова Рада, Ректорат, Вчена рада, функції яких визначаються законодавством та статутом університету.

9. Прозорість і публічність

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

Права та обов'язки усіх учасників освітнього процесу забезпечуються наступним документом:
- ПОЛОЖЕННЯ ПРО ОРГАНІЗАЦІЮ ОСВІТНЬОГО ПРОЦЕСУ В ДУІТЗ
https://suitt.edu.ua/wp-content/uploads/2023/12/polozhennia_pro_orhanizatsiiu_osvitnoho_protsesu_v_duitz.pdf

Документи розміщені на офіційному сайті ЗВО та є загальнодоступними для всіх учасників освітнього процесу:
https://suitt.edu.ua/polozhennia/

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

Проєкт ОП, зауваження, пропозиції стейкголдерів, проєкти програм навчальних дисциплін та інші матеріали щодо оновлення ОП розміщені на сторінці https://suitt.edu.ua/reformuvannia-opp/
Затверджені ОП розміщені на сторінці https://suitt.edu.ua/prohramy-osvity/

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

Освітня програма: https://suitt.edu.ua/wp-content/uploads/2024/09/125-op-m-2024.pdf
Навчальний план: np_125_kbzi_m_2024.pdf (suitt.edu.ua)
Силабуси обов'язкових компонентів: https://suitt.edu.ua/sylabusy-125-kiberbezpeka-ta-zakhyst-informatsii-mahistr-2024/
Силабуси вибіркових компонентів: https://suitt.edu.ua/vybirkovi-dystsypliny/
Положення про індивідуальний навчальний план здобувачів вищої освіти: https://suitt.edu.ua/wp-content/uploads/2023/05/PRO-INDYVIDUAL-NYY-NAVCHAL-NYY-PLAN-ZDOBUVACHIV-VYSHCHOYI-OSVITY-V-DUITZ.pdf

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП?

Сильні сторони ОП:
- ОП базується на багаторічному досвіді успішної підготовки здобувачів другого (магістерського) рівня вищої освіти у галузі кібербезпеки та захисту інформації (з 2010 р.);
- ОП оновлена у 2023 р. з врахуванням частини професійних компетентностей, знань, вмінь та навичок професійного стандарту «Фахівець сфери захисту інформації»;
- індивідуальний підхід до кожного здобувача, включаючи можливість вибору спеціалізованих дисциплін з урахуванням особистих потреб у працевлаштуванні або професійного зростання;
- висока кваліфікація і досвід викладачів та керівників кваліфікаційних робіт здобувачів, що забезпечує високу якість підготовки здобувачів;
- залучення до освітнього процесу фахівців з практики, які є потенційними роботодавцями; співпраця кафедри Кібербезпеки та технічного захисту інформації з багатьма державними та приватними установами в галузі кібербезпеки та захисту інформації;
- збереження зв'язків між викладачами кафедри та випускниками ОП, зокрема, з метою відстеження їх кар'єрного зростання та отримання пропозицій щодо оновлення ОП.

Слабкі сторони ОП:
- недостатньо розвинена академічна мобільність здобувачів, які навчаються за даною ОП, особливо в останні роки;
- відсутність підготовки здобувачів за дуальною формою освіти в межах даної ОП, але з 2024/2025 навчального року дуальна форма освіти впроваджується.

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

- розширити коло фахівців, які беруть участь у навчальному процесі, зокрема залучити нових потенційних роботодавців, включаючи представників держав Європейського Союзу;
- збільшити кількість здобувачів, які обирають дуальну форму навчання шляхом розширення співпраці з вітчизняними підприємствами;
- підвищити ефективність профорієнтаційної роботи серед іноземних здобувачів та представників посольств їхніх країн з метою залучення на навчання за ОП іноземних здобувачів;
- раз на рік оновлювати зміст навчальних дисциплін ОП згідно новітніх тенденцій та перспективних напрямків розвитку галузі кібербезпеки та захисту інформації;
- максимально сприяти академічної мобільності здобувачів;
- збільшити активність викладачів у вивченні іноземних мов для розширення можливостей академічної мобільності та проведення занять англійською мовою

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: Назаренко Олександр Аскольдович

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**	
Методологія та організація наукових досліджень	навчальна дисципліна	*m_125_ok1_metodolohiia-ta-orhanizatsiia-naukovykh-doslidzhen.pdf*	hH0xIu5qk/niCo7SifWXYngFmILrDYiAkaMCWZEQCLo=	*Обладнання:* *1. Мультимедійна аудиторія з проектором BenQ MS506 та екраном:* *2. Комп'ютерний клас з ПК: Системний блок «Impression P», Монітор 19; Samsung SM - 10шт. OS Windows10.* *Література:* *1. Важинський С., Щербак Т. І. Методика та організація наукових досліджень: навч. посіб. Суми : СумДПУ ім. А. С. Макаренка, 2016. 260 с.* *2. Зацерковний В. І., Тішаєв І. В., Демидов В. К. Методологія наукових досліджень: навч. посіб. Ніжин : НДУ ім. М. Гоголя, 2017. 236 с.* *3. Основи методології та організації наукових досліджень: навч. посіб. для студентів, курсантів, аспірантів і ад'юнтів / ред. А. Є. Конверський. Київ : Центр учб. літ., 2010. 352 с.* *4. Юринець В. Є. Методологія наукових досліджень: навч. посіб. Львів : ЛНУ ім. Ів. Франка, 2011. 178 с.*
Педагогіка та психологія	навчальна дисципліна	*m_125_ok2_pedahohika_ta_psykholohiia.pdf*	W9AkraoJxGZbW0eg8MhqQmd+H2Ij50QpD/sIKGT3oYY=	*Обладнання* *1. Комп'ютер з доступом до інтернету* *2. ОС Windows* *Література:* *1. Шиліна Н.Є. Методичні рекомендації щодо організації самостійної та дистанційної роботи з дисципліни «Педагогіка та психологія» для магістрів заочного відділення. Методичний посібник. Одеса : ДУІТЗ, 2021. 81 с.* *2. Шиліна Н.Є. Конспект лекцій з дисципліни «Педагогіка та психологія» для магістрів усіх спеціальностей. Методичний посібник. Одеса.: ДУІТЗ, 2021. 92 с.* *3. Шиліна Н.Є. Робочий зошит з курсу «Педагогіка та психологія» для магістрів усіх спеціальностей. Методичний посібник. Одеса. : ДУІТЗ, 2021. 107 с.*
Спеціальні вимірювання в галузі ТЗІ	навчальна дисципліна	*m_125_ok3_spetsialni-vymiriuvannia-v-haluzi-tzi_edited.pdf*	gRqsv9E+p5PqnU9xfTUO/xInvMf5oCPXNAlqdFtqFKI=	*Обладнання* *1. Комп'ютер з доступом до інтернету* *2. ОС Windows* *Література:* *1. Антіпов І., Олейніков А., Ликов Ю. В. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спеціальності 125 "Кібербезпека"*

				спеціалізації "Системи технічного захисту інформації". Харків : ХНУРЕ, 2019. 216 с. *2. Богуш В., Кривуца В., Кудін А. Інформаційна безпека: термінологічний навчальний довідник / ред. В. Кривуца. Київ : ООО "Д.В.К.", 2004. 508 с.* *3.Кононович В., Гладиш С. Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування. частина 4: навч. посіб. Одеса : ОНАЗ ім. О.С. Поп., 2009.*
Управління доступом до інформаційних ресурсів	навчальна дисципліна	*m_125_ok4_upravlinnia_dostupom_do_informatsijnykh_resursiv.pdf*	3CguamIBTPdijR2eAQXBkPyXghJiomnHUKLD8qkerSw=	*Обладнання:* *1. ПК - 15шт* *2. ОС Windows* *3. Arduino IDE* *4. Симулятор Tinkercad* *5. Обладнання Arduino* *Література:* *1. Гребенюк А., Рибальченко Л. Основи управління інформаційною безпекою: навч. посібник. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 144 с.* *2. Інформаційна безпека інформаційно-комунікаційних систем. частина 1: лаб. практ. / М. Захарченко та ін. Одеса : ОНАЗ ім. О.С. Попова, 2011.* *3. Корчинський В. Конспект лекцій з дисципліни Управління доступом до інформаційних ресурсів. Одеса : ДУІТЗ, 2022.* *4. Корчинський В. Практикум до лабораторних робіт з дисципліни Управління доступом до інформаційних ресурсів. Одеса : ДУІТЗ, 2022.* *5. Корчинський В. Практикум до практичних робіт з дисципліни Управління доступом до інформаційних ресурсів. Одеса : ДУІТЗ, 2022*
Менеджмент інформаційної безпеки	навчальна дисципліна	*m_125_ok5_menedzhment-informatsijnoi-bezpeky.pdf*	r6hduLK4gLMp32vE839rxMmG2YehsRxjmfb5X4y2GJU=	*Обладнання:* *1. Комп'ютер із доступом до інтеренету* *2. ОС Windows* *3. MS Word* *Література:* *1. Information technology. Security techniques. Information security management systems. Requirements.* *2. ISO/IEC 27001:2013, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013.* *3. Jason Andress. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice.* *4. О.О. Цвілій, Безпека інформаційних технологій: сучасний стан стандартів ISO27K системи управління інформаційною безпекою, Телекомунікаційні та інформаційні технології., №2, с. 73-79, 2014.*
Комплексні системи безпеки	навчальна дисципліна	*m_125_ok6_kompleksni-systemy-bezpeky.pdf*	CbmoGmVgPqgCWGkB+lHLvJe+MgDOC7tqQVyskPdIthI=	*Обладнання* *1. Стенди «Алтосан», «TRASSIR», «ARCTIUM», «TIRAS»,*

				«GreenVision» з лабораторії «Технічних засобів охорони та захисту інформації» *Література:* *1.Конспект лекцій з дисципліни "Комплексні системи безпеки"" / С. Стайкуца Одеса : ДУІТЗ, 2021.* *2. Методичні вказівки для виконання курсу лабораторних робіт з дисципліни "Комплексні системи безпеки" / С. Стайкуца та ін. Одеса : ДУІТЗ, 2021.* *3. Концепція комплексної системи безпеки. Робочий документ компанії Bosch.*
Кіберфізична безпека об'єктів критичної інфраструктури	навчальна дисципліна	*m_125_ok7_kiberfizychna-bezpeka-obiektiv-krytychnoi-infrastruktury-1.pdf*	JB43t42JLDdQs1nWIBbNFmQfbOvCTiEnkpkbQkEwzEA=	*Обладнання:* *1. VirtualBox* *2. ОС Windows* *3. ОС Linux* *4. Nmap* *5. Wireshark* *6. APS* *7. Hashcat* *Література:* *1. Кононович В. Конспект лекцій з дисципліни «кіберфізична безпека об'єктів критичної інфраструктури». Одеса : ДУІТЗ, 2023.* *2. Кононович В. Лабораторний практикум з «Кіберфізичної безпеки об'єктів критичної інфраструктури» Методичний посібник та методичні вказівки. Одеса : ДУІТЗ. 40 с.* *3. Юдін О., Корченко О., Конахович І. Захист інформації в мережах передачі даних. Київ : ТОВ «НВП» ІНИЕРСЕРВІС», 2009. 716 с.*
Криптологія	навчальна дисципліна	*m_125_ok8_kryptolohiia.pdf*	uM5+acJ4dLUuxPVMGulC28EOFlIpaitRDX73RDSMQ2U=	*Обладнання* *1. Комп'ютер з доступом до інтернету* *2. ОС Windows* *3. Програмне забезпечення для виконання лабораторних робіт* *Література* *1. Shannon, Claude (4 October 1949). "Communication Theory of Secrecy Systems". Bell System Technical Journal. 28 (4): 662. doi:10.1002/j.1538-7305.1949.tb00928.x. Retrieved 20 June 2014.* *2. Cryptography, An Introduction by Nigel Smart. Springer International Publishing, 2015. 436 p.* *3. Cryptography Engineering: Design Principles and Practical Applications 1st Edition by Niels Ferguson (Author), Bruce Schneier (Author), Tadayoshi Kohno (Author) - Springer NewYork? 2008* *4. Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) 1st Edition - UK, Chapman and Hall/CRC; 1 edition - 2005, 368 p/* *5. A Course in Number Theory and Cryptography by Neal Koblitz.- Grade text in mathematics 114 p. - Springer NewYork – 1994*
Процесний	навчальна	*m_125_ok9_protses*	5WKV2A8Hv2D5x7t	*Обладнання*

менеджмент в системі корпоративної безпеки	дисципліна	*nyj_menedzhment_v_systemi_korporatyvnoi_bezpeky.pdf*	Cvi+R9zHg0bYDD1xPZce+0pjLX3I=	*1. Комп'ютер з доступом до інтернету* *2. ОС Windows* *Література:* *1. Довгий С., Воробієнко П., Гуляєв К. Сучасні телекомунікації: мережі, технології, безпека, економіка, регулювання: монографія / ред. С. Довгий. Київ : "АзимутУкраїна", 2013. 607 с.* *2. Тардаскіна Т. М., Кононович В. Менеджмент інформаційної безпеки в галузі зв'язку: [навч. посібник. Затверджено Міністерством освіти та науки України як посібник для вищих навчальних закладів. Лист № 1/11-7791 від 13 серпня 2010 року]. Одеса : ОНАЗ ім. О.С. Поп., 2011. 168 с.* *3. Керування ризиками на підприємстві / CIDCON CONSULTING COMPANY. - Київ, 2012.*
Моніторинг та аудит інформаційно-комунікаційних систем	навчальна дисципліна	*m_125_ok10_monitorinh_ta_audyt_informatsijno_komunikatsijnykh_system.pdf*	TsNOwvk9/G5ehVYZpSC76DFkHfv4TYUAWsMfScX83Bo=	*Обладнання:* *1. Обладнання з «Лабораторії Кібербезпеки 1»* *2. ОС Kali Linux та наявні у ній інструменти тестування* *Література:* *1. Богуш В.М., Кривуца В.Г. , Кудін А.М. Інформаційна безпека: термінологічний навчальний довідник / ред. В.Г. Кривуца. Київ : ООО "Д.В.К.", 2004. 508 с.* *2. Кононович В.Г., Гладиш С. Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування. частина 4: навч. посіб. Одеса : ОНАЗ, 2009.* *3. Програми та методики державної експертизи інформаційної захищеності телекомунікацій : навч. посіб. / Н.В. Горохов та ін. ; ред. В.Г. Кононович. Одеса : ОНАЗ, 2013. 252 с.*
Ділова іноземна мова	навчальна дисципліна	*m_125_ok11_dilova_inozemna_mova.pdf*	tO5Qtf5fWhYb88qjiEy4yn9bZZHojEtbt424FJCbc28=	*Обладнання:* *1. Практичні зошити з курсу «Ділова іноземна мова»* *2. Підручники з курсу «Ділова іноземна мова»* *3. Аудіо матеріали до підручнику* *Література:* *1. David Bonamy Technical English 1. Pearson Longman, 2008. 188 p.* *2. Eric H. Glending, Norman Glending Oxford English for Electrical and Mechanical Engineering. Oxford University Press 2001.198p.* *3. Lindsey White, Engineering. Oxford University Press, 2003.246p.* *4. Murphy R. English Grammar in Use. A self-study reference and practice book for intermediate learners of English. With Answers. Fourth Edition. Cambridge University Press, 2012. 398 p.* *5. Chaney, Lillian H. The essential guide to business etiquette / Lillian Hunt Chaney and Jeanette St. Clair Martin. 187 p.*

Практика (виробнича)	практика	*m_125_ok12_praktyka_vyrobnycha.pdf*	l7PPGqXd2Wy58i/GlSr2inokj24mxuopHQ8YGkdAE3g=	*Обладнання:* *1. Лабораторії кафедри Кібербезпеки та технічного захисту інформації* *2. Обладнання на підприємствах стейкголдерів* *Література:* *1. Програма практики для здобувачів вищої освіти другого (магістерського) рівня за спеціальністю 125 Кібербезпека та захист інформації* *2. Положення про порядок проведення практичної підготовки здобувачів вищої освіти ДУІТЗ*
Кваліфікаційна (магістерська) робота. Атестація	підсумкова атестація	*m_125_ok13_kvalifikatsijna_mahisterska_robota.pdf*	OhoTTMPM+2oYQZQNv6cL+r8WK9lCI/4Yvai028p4rtw=	*1. Положення про організацію поточного, семестрового контролю та атестації здобувачів вищої освіти із застосуванням дистанційних технологій в ДУІТЗ* *2. Положення про екзаменаційну комісію та атестацію здобувачів вищої освіти в ДУІТЗ* *3. Положення про забезпечення академічної доброчесності та етики в ДУІТЗ* *4. Положення про підготовку та захист кваліфікаційних робіт бакалаврів та магістрів денної та заочної форми навчання*

* 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)
468109	Кузьменко Юлія Олександрівна	Завідувач кафедри, Основне місце роботи	Бізнесу та соціальних комунікацій	Диплом спеціаліста, Південноукраїнський державний педагогічний університет ім. К.Д. Ушинського, рік закінчення: 2003, спеціальність: 030502 Мова та література (англійська, німецька), Диплом кандидата наук ДК 062068, виданий 06.10.2010, Атестат доцента ДЦ 044299, виданий	20	Ділова іноземна мова	Підвищення кваліфікації: Державний заклад «Південноукраїнський національний педагогічний університет ім. К.Д. Ушинського. Стажування за навчальною програмою на кафедрі «Кафедра західних і східних мов та методики їх навчання» з 01.02.2022 – 01.04.2022. ●Сертифікат № 718/04 від 19.05.2022 р.; ●Тема: «Діджитал-компетеність як складова процесу формування педагогічної

				29.09.2015			майстерності викладача іноземних мов у ВНЗ» ●Термін навчання та кількість кредитів ЄКТС (академ. год.): 2 місяці, 6 кредитів ЄКТС (180 год.) Наказ ректора ОНМА ім. Нежданової: № 10 від 31.01.2022. Наукові публікації: 1. Kuzmenko Yu., Kovalchuk T., Ivanitska I. Formation of foreign language communicative competence among future military officers: international experience. Порівняльна професійна педагогіка (Comparative professional pedagogy). ХНУ. Випуск 11 (1), наук. журнал / голов. ред. Н. М. Бідюк. Київ. Хмельницький, 2021. С. 101-108. (Cabell's directory, EBSCO, Discovery Service, Google Scholar, WorldCat) https://doi.org/10.31891/2308-4081 2. Кузьменко Ю.О., Ковальчук Т.С. Аналіз досвіду розвитку діагностичної компетентності викладачів іноземних мов у системі військової освіти. Науковий збірник Херсонського педагогічного університету. Випуск 96, Херсон, 2021. С. 89-96. (Index Copernicus) https://doi.org/10.32999/ksu2413-1865/2021-96-13 3. Кузьменко Ю.О., Левицька Л.Я, Терлецька Л.М. Впровадження інноваційних методик вивчення іноземної мови у вищій школі// Науковий журнал: Перспективи та інновації науки №12(17), 2022. С. 147-160. (Index Copernicus) https://doi.org/10.52058/2786-4952-2022-12(17)-147-160 4. Кузьменко Ю.О., Велущак М.О., Озарчук І.М Сучасні методи викладання у ЗВО: практичний аспект// Науковий журнал: Актуальні питання гуманітарних наук. Педагогіка. № 59, 2023. С. 156-170.

							(Index Copernicus) https://doi.org/10.24919/2308-4863/59-1-205. Булгару Н.Б., Кузьменко Ю.О. Основні переваги застосування засобів графічної візуалізації під час навчання іноземної мови// Науковий журнал: Актуальні питання гуманітарних наук. Педагогіка. № 70, Том 1, 2024. С. 284-288. (Index Copernicus) https://doi.org/10.24919/2308-4863/70-1-43
414119	Василіу Євген Вікторович	Професор, Суміщення	Інформаційних технологій та кібербезпеки	Диплом доктора наук ДД 001021, виданий 17.05.2012, Атестат професора 12ПР 010915, виданий 29.09.2015	31	Менеджмент інформаційної безпеки	Підвищення кваліфікації: 1. Foundations of Computer and Network Security within the 2022 Cybersecurity Summer Instructor Training Program under the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity 11 July – 31 August 2022 – 180 год. (6 кредитів) Професійний досвід: 1.Координатор проєкту USAID Cybersecurity for Critical Infrastructure in Ukraine: - Сертифікат про подяку від 28 грудня 2022 року за взірцеву підтримку в узгодженні направлень на навчання інструкторів в Державному університеті інтелектуальних технологій і зв'язку. - Сертифікат про визнання від 28 грудня 2021 року за максимальні зусилля та досягнення високих результатів у злагодженості, направлення на навчання вчителів (викладачів) та організацію заходів з Державним університетом інтелектуальних технологій і зв'язку за проектом USAID «Кібербезпека для критичної інфраструктури в Україні». Навчально-методичні публікації: 1. Лахно В.А., Василіу Є.В., Гладких В.М., Домрачев В.М., Сивкова Н.М.. Методи та засоби захисту інформації [Навчальний посібник] /– К. : ЦП «Компринт» О.В.,

							2021. 444 с. 2. Olena Rudnitska, Svitlana Kondakova, Anastasiia Kondakova, Yurii Khlaponin, Victoriia Ternavska, Yevhen Vasiliu. The Employer and Employee Reputation in the Ukrainian Cyberspace and Social Internet-Services // CEUR Workshop Proceedings. – Volume 2588, 2019. – P. 194 – 203.
388876	Онацький Олексій Віталійович	Доцент, Основне місце роботи	Інформаційних технологій та кібербезпеки	Диплом спеціаліста, Одеський державний політехнічний університет, рік закінчення: 1995, спеціальність: Радіотехніка, Диплом кандидата наук ДК 007533, виданий 27.06.2000, Атестат доцента 12ДЦ 045225, виданий 15.12.2015	29	Спеціальні вимірювання в галузі ТЗІ	Підвищення кваліфікації: Сертифікат про підвищення кваліфікації з 11 липня 2022 р. по 31 серпня 2022 р. за програмою «Foundations of Computer and Network Security» в рамках літньої програми підготовки інструкторів з кібербезпеки 2022 року в рамках проекту USAID «Кібербезпека для критичної інфраструктури в Україні» (180 годин). Наукові публікації: 1. Onatskiy O.V. Cryptographic authentication protocol zero-knowledge secret on elliptic curves using public keys and random messages / Onatskiy O.V., Garova O.V. – Цифрові технології. Одеса: ОНАЗ ім. О.С. Попова – 2019. – Вип. 26. – pp. 16-23. 2. Onatskyi O., Dykyi O., Zharova O., Yona L. Modification of the Shamir and Blakley threshold secret sharing schemes with elliptic curves. Інфокомунікаційні та комп'ютерні технології. № 1(03), 2022. – С. 267-283. 3. Onatskiy O. Two-factor authentication protocol with zero-knowledge over an extended field of elliptic curves. 2023 IEEE Sixth International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo, 13 November – 16 November, 2023.
400423	Стайкуца Сергій Володимирович	Доцент, Основне місце роботи	Інформаційних технологій та кібербезпеки	Диплом спеціаліста, Українська державна	19	Процесний менеджмент в системі корпоративної	Підвищення кваліфікації: Сертифікат про підвищення

				академія зв'язку імені О.С. Попова, рік закінчення: 2001, спеціальність: 092401 Автоматичний електрозв'язок, Диплом кандидата наук ДК 055529, виданий 14.10.2009, Атестат доцента 12ДЦ 044266, виданий 29.09.2015		безпеки	кваліфікації з 11 липня 2022 р. по 31 серпня 2022 р. за програмою «Audit and Risk Management» в рамках літньої програми підготовки інструкторів з кібербезпеки 2022 року в рамках проекту USAID «Кібербезпека для критичної інфраструктури в Україні» (180 годин). Професійний досвід: 1. З листопада 2016 р. - керівник лабораторії технічних засобів охорони та технічного захисту інформації кафедри КБ та ТЗІ ДУІТЗ (Протокол №3 кафедри ІБ та ПД від 18 листопада 2016 р. 2. З травня 2018 р. - зам.голови ГО “Технологічний кластер Одеського регіону” Наукові публікації: 1. Кононович В.Г. Контури систем забезпечення кібербезпеки цифровізованого суспільства та кібернетизованого виробництва, бізнесу й управління / Кононович В.Г., Стайкуца С.В., Кононович І.В., Романюков М.Г. // Збірник тез VI-ї міжнародної науково-практичної конференції"перспективні напрями захисту інформації ", ОНАЗ ім. О.С. Попова. – 2020. – С. 70-76. 2. Стайкуца С. В. Щодо побудови комплексної системи захисту в закладі середньої освіти / С. В. Стайкуца, В. Й. Кільдішев, Д. Р. Зайченко, С. С. Роман // «Наука, освіта та суспільство: актуальні наукові дослідження» (м. Київ, 25-26 лютого 2022 р.). — Херсон : Видавничий дім "Гельветика", 2022. 3. Стайкуца, С. В., К. С. Сєдов, А. С. Гусак. "Актуальність впровадження принципів неперервності бізнесу в українських компаніях." Молодий вчений (2022). 4. Рябуха, О. М., С. В. Стайкуца, М. Є. Самохін. "Застосування

							елементів аудиту безпеки та ризик-менеджменту в роботі сучасної компанії." Молодий вчений (2022). 5. Стайкуца, С. В., В. Й. Кільдішев, В. В. Афанасьєв. "Дослідження екосистеми інсайдерів як ключової складової внутрішніх загроз підприємства." Молодий вчений (2022). 6. Стайкуца, С. В., В. Й. Кільдішев, Є. В. Карнаухий. "Щодо використання систем охоронної сигналізації." Молодий вчений (2022).
388437	Ложковський Анатолій Григорович	В.о. завідувача кафедри, Основне місце роботи	Телекомунікацій та радіотехніки	Диплом спеціаліста, Одеській електротехнічний інститут зв'язку ім. О.С. Попова, рік закінчення: 1981, спеціальність: автоматическая электросвязь, Диплом доктора наук ДД 008949, виданий 22.12.2010, Атестат професора 12ПР 007337, виданий 10.11.2011	42	Методологія та організація наукових досліджень	Підвищення кваліфікації (стажування): Університет Миколаса Ромереса (Вільнюс, Литва) Свідоцтво № 344 від 19.06.2024 р.; Тема «Соціальні та технологічні трансформації в умовах, що змінюються»; 15.04.2024-30.06.2024 р., 6 кредитів ЄКТС (180 год.) Наказ ректора ДУІТЗ: № 01-14-10 від 11.04.2024. Професійний досвід: 1. Голова Спеціалізованої вченої ради Д 41.113.03 з 2022 р. до т.ч. (наказ МОН №1166 від 23.12.2022 р) https://suitt.edu.ua/specializovana-vcena-rada-d-41-113-03/ 2.Науковий керівник НДР № 0118U100372, 2019 «Прогнозування характеристик самоподібного трафіка». Науковий керівник НДР № 0116U003632, 2020 «Прогнозування параметрів трафіка Internet IoT». 3. Науковий редактор фахового журналу "Наукові праці ОНАЗ ім. О.С. Попова" (до 2021 року) 4. Член технічного комітету стандартизації ТК 157 «Телекомунікації» ДП "Одеський науково-дослідний інститут зв'язку" (65026, м. Одеса, вул. Буніна, 23)

							Наукові публікації: 1. Lozhkovskyi A.G. Calculation the service waiting probability with self-similar network traffic / A.G. Lozhkovskyi // Journal of Engineering Science. (TECHNICAL UNIVERSITY OF MOLDOVA) – Vol. XXVI (2), 2019. – P. 35-39. DOI: 10.5281/zenodo.3249178 2. Ложковський А.Г. Вплив точності розрахунку показника самоподібності трафіка на характеристики якості обслуговування / А.Г. Ложковський, В.А. Турчин., В.С. Андріяка // Наукові праці ОНАЗ ім. О.С. Попова. – 2020. – № 1. – С. 88-94. DOI: https://doi.org/10.33243/2518-7139-2020-1-1 3. Ложковський А.Г. Метод розрахунку пропускної здатності пакетної мережі доступу для пристроїв IoT / А.Г. Ложковський, К.Д. Гуляєв // Наукові праці ОНАЗ ім. О.С. Попова. – 2020. – № 2. – С. 31-40. DOI: https://doi.org/10.33243/2518-7139-2020-1-2 4. Lozhkovskyi A. Method for evaluating the quality of service characteristic of a packet access network for IoT devices / A. Lozhkovskyi, M. Klymash, Yu. Pyrih, O. Shpur // 2021 IEEE 4th International Conference on Advanced Information and Communication Technologies, AICT-2021 – Proceedings. 21-25 Sept. 2021 – Lviv-Slavske, Ukraine, 2021. – P. 79-73. (Scopus) DOI: 10.1109/AICT52120.2021.9628912 https://ieeexplore.ieee.org/document/9628912
388804	Корчинський Володимир Вікторович	Завідувач кафедри, Основне місце роботи	Інформаційних технологій та кібербезпеки	Диплом спеціаліста, Одеський електротехнічний інститут зв'язку ім. О.С. Попова, рік закінчення: 1987, спеціальність: Автоматичний електрозв'язок, Диплом доктора наук	32	Управління доступом до інформаційних ресурсів	Підвищення кваліфікації: 1. Довідка про підвищення кваліфікації за програмою науково-педагогічного працівника з 11 грудня 2018 року по 13 лютого 2019 року на кафедрі Інформатики та управління захистом інформаційних систем

				ДД 004043, виданий 26.02.2015, Атестат доцента 12ДЦ 030616, виданий 17.02.2012			Одеського національного політехнічного університету (108 годин) 2. Підвищення кваліфікації Університету «КРОК». «Розвиток інформаційно-комунікаційних навичок в організації дистанційного формату навчального процесу». 2 кредити ЄКТС (з урахуванням самостійної (позааудиторної) роботи). 3. Підвищення кваліфікації на тему «Освіта дорослих: досвід країн Європейського Союзу та України» 1,5 кред. (45год) з 11 березня по 20 березня 2024 року Професійний досвід: Інженер-конструктор 1 категорії Спеціального конструкторського бюро "Молнія" Наукові публікації: 1. Корчинський Володимир. Атаки на основі BADUSB / Володимир Корчинський, Ірина Тарасенко, Юлія Бєлова, Сергій Рациборинський, Олександр Акаєв / Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах» , 2023, № 4 – С. 134-139. https://vottp.khmnu.edu.ua/index.php/vottp/article/view/206 2. Корчинський В. Автоматизовані системи керування доступом / В. Корчинський, Ірина Тарасенко, Сергій Рациборинський, Олександр Акаєв, Артем Хаджиогло // Вісник Хмельницького національного університету, №1, 2024 (331), С.291-296. file:///C:/Users/Volodymyr/Downloads/(331)+VKNU-TS-2024-N1-44-1.pdf 3. Корчинський В. В. Дослідження платформи arduino для проєктування системи керування доступом

							підприємства / Корчинський, О.О. Донченко, М.Я. Гоцул, Д.С. Кенджаєв // 76-а Науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів, Одесса, ДУІТЗ, грудень 2021
388685	Басов Віктор Євгенович	Старший викладач, Основне місце роботи	Інформаційних технологій та кібербезпеки	Диплом спеціаліста, Одеський електротехнічний інститут зв'язку ім. О.С. Попова, рік закінчення: 1993, спеціальність: Автоматичний електрозв'язок, Диплом кандидата наук ДК 036629, виданий 12.10.2006	30	Криптологія	Підвищення кваліфікації 1. USAID Project "Cybersecurity for Critical Infrastructure in Ukraine" Course Malware Analysyst 12 June – 12 august 2021, 90 год Професійний досвід: З 2009-2011 р.р. брав участь у розробці системи автоматизованого обліку та збору інформації зі споживачів електроенергії «Matrix-AMM» в КБ ТОВ Телекомунікаційні технології (ТТ). У ній був розроблений і запрограмований PLC модем для передачі інформації з електричних лічильників по проводах лінії електропередач 220 вольт на мікроконтролері Microchip PIC24F32GA002, який використаний в якості DSP. Програмування в середовищі MPLAB мовою С. З листопада 2010 р модем виробляється серійно. З 2000 по 2008 рік у складі КБ ТТ займався розробкою і підтримкою ПЗ для DSP нових цифрових телефонних станцій (ЦАТС) «F2000» і «Матриця». У складі цих станцій для всіх DSP типових елементів заміни (ТЕЗ) спільно або повністю розроблено програмне забезпечення. Це процесори TMS320C5409A і TMS320C5416 розташовані в наступних ТЕЗ, а саме: - ТЕЗ абонентських ліній ЦАТС «Матриця» - спільно, - ТЕЗ комутатора ЦАТС «Матриця» - тільки мною; - ТЕЗ цифрових

							сполучних ліній ЦАТС «Матриця»; - ТЕЗ комутатора F2000. Програми написані в середовищі Code Composer Studio мовою асемблера TMS320F54xx. В даний час станцію «Матриця» можна придбати в ТОВ ТТ.
388829	Кононович Володимир Григорійович	Доцент, Основне місце роботи	Інформаційних технологій та кібербезпеки	Диплом спеціаліста, Одеський електротехнічний інститут зв`язку ім. О.С. Попова, рік закінчення: 1968, спеціальність: телеграфний та телефоний звязок, Диплом кандидата наук МТН 97444, виданий 14.06.1974, Атестат доцента ДЦ 039534, виданий 24.09.1980	54	Кіберфізична безпека об'єктів критичної інфраструктури	Підвищення кваліфікації: 1. Підвищення кваліфікації з 14 червня 2021 р. по 23 липня 2021 р. за програмою «Cyber-Physical System Security» в рамках літньої навчальної програми з кібербезпеки за проектом USAID «Кібербезпека для критичної інфраструктури в Україні» 2. Підвищення кваліфікації з 11 липня 2022 р. по 31 серпня 2022 р. за програмою «Advanced Malware» в рамках літньої програми підготовки інструкторів з кібербезпеки 2022 року в рамках проекту USAID «Кібербезпека для критичної інфраструктури в Україні» (180 годин). 3. Участь у другій міжнародній науковій і практичній конференції з 22 січня по 24 січні 2024 року «Science and society: modern trends in a changing world», Відень, Австрія(24 години). Професійний досвід: Працював з 12.10.2000 по 01.08.2009 р провідним фахівцем з експлуатації, модернізації та ремонту засобів технічного захисту інформації «Одеського регіонального центру технічного захисту інформації» в Одеській дирекції ВАТ «Укртелеком».
388823	Кільдішев Віталій Йосипович	Доцент, Суміщення	Інформаційних технологій та кібербезпеки	Диплом магістра, Українська державна академія зв'язку імені О.С. Попова, рік закінчення: 2001,	21	Моніторинг та аудит інформаційно-комунікаційних систем	Доцент. Основне місце роботи. Підвищення кваліфікації: 1. Security Audit and Risk Management Course, 40 (forty) continuing professional education hours, ISACA

				спеціальність: 092402 Багатоканальний електрозв'язок, Диплом кандидата наук ДК 046943, виданий 21.05.2008, Атестат доцента 12ДЦ 034732, виданий 28.03.2013			Kyiv Chapter, 12 July – 23 august 2022, Certificate of 29.08.2022, 40 год. 2. USAID Project "Cybersecurity for Critical Infrastructure in Ukraine" Course Security Audit and Risk Management 12 July – 23 august 2022, 90 год; 3. Одеський Національний Політехнічний Університет, 13.02.2019, 782/03-07, за спеціальністю 125 - Кібербезпека, 108 годин. Наукові публікації: 1. Корчинський В.В. Підвищення захищеності користувацьких даних веб-серверів шляхом впровадження гомоморфного шифрування, Кільдішев В.Й., Онищук В. В., Аль-Файюми Халед, ОНАЗ ім. О.С. Попова, 2020.
388997	Шиліна Наталія Євгенівна	Доцент, Основне місце роботи	Бізнесу та соціальних комунікацій	Диплом спеціаліста, Рівненський державний гуманітарний університет, рік закінчення: 2000, спеціальність: 010101 Дошкільне виховання і практична психологія, Диплом кандидата наук ДК 022219, виданий 11.02.2004, Атестат доцента 12ДЦ 022082, виданий 23.12.2008	21	Педагогіка та психологія	Підвищення кваліфікації (стажування): 1. 04.11.19-15.12.19 ПДПУ ім. К.Д. Ушинського «Педагогіка закладів вищої освіти» Довідка №3416/14 від 23.12.2019 2. Освітній курс "Протидія та попередження булінгу (цькування) в закладах освіти" - 2,6 кредити ЄКТС (80 год.). ГО Prometeus. Сертифікат від 24.08.2022 р. 3. Навчання за освітньою програмою "Робота з ПТСР в умовах воєнного часу: від болю до відродження" - 1,5 кредити ЄКТС (42 год.). Міжнародна тренінгова компанія "Основа". Сертифікат № 606233 від 19.07.2022 р. 4. Scientifik and practical training at Karaganda Buketov University (180 hours) «Information and communication technologies in the digital economy: the socio-economic, political, psychological aspects and their impact on education system. Certificate №000020-EF від 08.02.2023 5. Участь у проекті за підтримки Unicef та

							ГО «Волонтер» «Основи психологічної основи дітям та їхнім батькам/особам, які їх замінюють» Сертифікат від 08.02.2023 6. Участь у Міжнародному воркшопі з теми «Методи ефективної взаємодії в умовах конфлікту» (15-16 травня 2023) Сертифікат 7. Сертифікатна програма «Базова підготовка медіаторів», 150 год. Професійний досвід: 1. Керівництво постійно діючим студентським науковим гуртком з психології. (Витяг №1 з протоколу №1 засідання кафедри психології,педагогіки та лінгводидактики від 30.08.2022) Наукові публікації: 1. Проблема емоційного стану біженців та переселенців за умов військового конфлікту в Україні на прикладі студентів 5 курсу // Вчені записки таврійського національного університету імені В.І. Вернадського Серія: Психологія Том 34 (73) № 2 2023, с.30-36 https://doi.org/10.32782/2709-3093/2023.2/06 (фахове видання з психології, Index Copernicus) 1. 2. Особливості освітнього простору в Україні в умовах війни: проблеми і перспективи розвитку / Актуальні питання гуманітарних наук. Вип 59, Том 3, 2023, С. 319-325 https://doi.org/10.24919/2308-4863/59-3-50 (фахове видання з педагогіки, Index Copernicus) 3. Розвиток творчого мислення магістрів засобами метафоричних карт // Актуальні питання гуманітарних наук. Вип 49, том 2, 2022, С. 254-260 https://doi.org/10.24919/2308-4863/49-2-40 (фахове видання з педагогіки, Index

							Copernicus) 4. Соціально-психологічний комфорт як критерій успішного навчання студентів в умовах карантину // Науковий вісник ПДПУ ім. К.Д. Ушинського. – Вип. 1(138), 2022, С.94-100 DOI: https://doi.org/10.24195/2617-6688-2022-1-12 (фахове видання з педагогіки, Index Copernicus) 5. Проблема мотивації щодо використання інформаційних технологій під час дистанційного навчання в умовах карантину // Вісник Запорізького національного університету. Педагогічні науки. – Том 2 № 1 (2021), С. 193-199. DOI: https://doi.org/10.26661/2522-4360-2021-1-2-30 (фахове видання з педагогіки, Index Copernicus) 6. Проблема дистанційного навчання у вищих навчальних закладах в умовах карантину // Науковий вісник Південноукраїнського національного педагогічного університету імені К. Д. Ушинського. Випуск 3 (136). Одеса, 2021, С. 120-127 DOI: https://doi.org/10.24195/2617-6688-2021-3-16 (фахове видання з педагогіки, Index Copernicus) 7. Дистанційне навчання в умовах пандемії: труднощі та переваги // Науковий вісник Південноукраїнського національного педагогічного університету імені К. Д. Ушинського. Випуск 1 (134). Одеса, 2021, С. 16-23. DOI https://doi.org/10.24195/2617-6688-2021-1-2 (фахове видання з педагогіки, Index Copernicus) 2. 8. Процеси несвідомого людини як фактор формування навколишнього світу та соціальних взаємодій // Психологія і особистість. Науковий журнал. – Київ-

							Полтава, 2019. – №1 (15). – С. 73-85 DOI: https://doi.org/10.33989/2226-4078.2019.1.163987 (фахове видання з психології, Index Copernicus) 3. 9. Проблема виховання дітей з особливими освітніми потребами в умовах сім'ї та освітніх установ // Науковий вісник ПНПУ ім. К.Д. Ушинського, Випуск 3 (128). Одеса, 2019, с. 42-49; DOI https://doi.org/10.24195/2617-6688-2019-3-6 (фахове видання з педагогіки, Index Copernicus)
400423	Стайкуца Сергій Володимирович	Доцент, Основне місце роботи	Інформаційних технологій та кібербезпеки	Диплом спеціаліста, Українська державна академія зв'язку імені О.С. Попова, рік закінчення: 2001, спеціальність: 092401 Автоматичний електрозв'язок, Диплом кандидата наук ДК 055529, виданий 14.10.2009, Атестат доцента 12ДЦ 044266, виданий 29.09.2015	19	Комплексні системи безпеки	Підвищення кваліфікації: Сертифікат про підвищення кваліфікації з 11 липня 2022 р. по 31 серпня 2022 р. за програмою «Audit and Risk Management» в рамках літньої програми підготовки інструкторів з кібербезпеки 2022 року в рамках проекту USAID «Кібербезпека для критичної інфраструктури в Україні» (180 годин). Професійний досвід: 1. З листопада 2016 р. - керівник лабораторії технічних засобів охорони та технічного захисту інформації кафедри КБ та ТЗІ ДУІТЗ (Протокол №3 кафедри ІБ та ПД від 18 листопада 2016 р. 2. З травня 2018 р. - зам.голови ГО "Технологічний кластер Одеського регіону" Наукові публікації: 1. Кононович В.Г. Контури систем забезпечення кібербезпеки цифровізованого суспільства та кібернетизованого виробництва, бізнесу й управління / Кононович В.Г., Стайкуца С.В., Кононович І.В., Романюков М.Г. // Збірник тез VI-і міжнародної науково-практичної конференції"перспективні напрями захисту інформації ", ОНАЗ ім. О.С. Попова. –

							2020. – С. 70-76. 2. Стайкуца С. В. Щодо побудови комплексної системи захисту в закладі середньої освіти / С. В. Стайкуца, В. Й. Кільдішев, Д. Р. Зайченко, С. С. Роман // «Наука, освіта та суспільство: актуальні наукові дослідження» (м. Київ, 25-26 лютого 2022 р.). — Херсон : Видавничий дім "Гельветика", 2022. 3. Стайкуца, С. В., К. С. Сєдов, А. С. Гусак. "Актуальність впровадження принципів неперервності бізнесу в українських компаніях." Молодий вчений (2022). 4. Рябуха, О. М., С. В. Стайкуца, М. Є. Самохін. "Застосування елементів аудиту безпеки та ризик-менеджменту в роботі сучасної компанії." Молодий вчений (2022). 5. Стайкуца, С. В., В. Й. Кільдішев, В. В. Афанасьєв. "Дослідження екосистеми інсайдерів як ключової складової внутрішніх загроз підприємства." Молодий вчений (2022). 6. Стайкуца, С. В., В. Й. Кільдішев, Є. В. Карнаухий. "Щодо використання систем охоронної сигналізації." Молодий вчений (2022).

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

Програмні результати навчання ОП	**ПРН відповідає результату навчання, визначеному стандартом вищої освіти (або охоплює його)**	**Обов'язкові освітні компоненти, що забезпечують ПРН**	**Методи навчання**	**Форми та методи оцінювання**
ПРН34 Приймати участь в організації та навчанні (підвищенні кваліфікації) працівників структурних	☒	Спеціальні вимірювання в галузі ТЗІ	Наочні (дискусія, групова робота); Практичні (практичне заняття, лабораторна робота, самостійна робота, завдання); Дистанційного навчання (платформа Zoom; онлайн-дискусії, онлайн-	Поточне оцінювання результатів самостійної роботи здобувачів з обговоренням питань створення програм підвищення кваліфікації для організації для подальшої підтримки

підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки, з відповідних питань.			опитування та онлайн-консультації)	працездатності створюваної КСЗІ.
ПРН19 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.	☒	Комплексні системи безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу «Вивчення досвіду щодо впровадження в містах України та світу КСБ в проектах типу “Безпечне місто”. Технології, бренди, компонентний склад, результати.», «Моделювання компонентного складу систему, складання специфікації в залежності від ТЗ на об’єкт. Використання спеціалізованих калькуляторів на корпоративних сайтах»; «Компонентний склад та сценарії роботи обладнання в екосистемі Bosch Building Integration System»
		Менеджмент інформаційної безпеки	Наочні (лекція-презентація, демонстраційні відеоролики, групова робота); Практичні (практичне заняття, захист і обговорення рефератів, дискусія, самостійна робота, завдання); Дистанційного навчання (платформа Zoom; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу «Економіка ІБ», «Інформаційні технології і е-бізнес», «Впровадження та контроль над реалізованими стратегіями»
		Методологія та організація наукових досліджень	Метод кейсів: Аналіз реальних сценаріїв та проблем, що допомагає розвивати навички критичного мислення та вирішення проблем. Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Письмові та усні відповіді: Оцінка теоретичних знань і здатності аналізувати інформацію.
		Кваліфікаційна (магістерська) робота. Атестація	Наочні (дискусія щодо теми кваліфікаційної роботи з керівником) Практичні (написання кваліфікаційної роботи); Дистанційного навчання (захист кваліфікаційної роботи, робота з керівником з допомогою платформ дистанційного навчання)	Захист кваліфікаційної роботи здобувачем
		Процесний менеджмент в системі корпоративної безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання);	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з

			Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	наступних тем курсу «Основні етапи забезпечення принципів неперервності бізнесу.», «Моделювання бізнес-процесів підприємства.», «Оптимізація бізнес-процесів підприємства.», «Експрес-аудит стану безпеки підприємства в фокусі впровадження ВСМ»
ПРН20 Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.	☒	Кваліфікаційна (магістерська) робота. Атестація	Наочні (дискусія щодо теми кваліфікаційної роботи з керівником) Практичні (написання кваліфікаційної роботи); Дистанційного навчання (захист кваліфікаційної роботи, робота з керівником з допомогою платформ дистанційного навчання)	Захист кваліфікаційної роботи здобувачем
		Методологія та організація наукових досліджень	Метод кейсів: Аналіз реальних сценаріїв та проблем, що допомагає розвивати навички критичного мислення та вирішення проблем. Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Практичні завдання: Оцінка практичних навичок у застосуванні аналітичних, розрахункових і експериментальних методів.
ПРН21 Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.	☒	Моніторинг та аудит інформаційно-комунікаційних систем	Наочні (дискусія, групова робота); Практичні (практичне заняття, лабораторна робота, самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	Тематичне оцінювання групових практичних робіт, що спрямовані на розв'язання завдань: здійснювати обґрунтування варіантів побудови автоматизованої системи моніторингу інформаційної безпеки та її основних складових
		Криптологія	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання – результатів самостійної роботи здобувачів з розробки питань: Лекції 1-8, практичні 1-6, лабораторні 1-6.
ПРН22 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 (магістерська) робота. Атестація	Наочні (дискусія щодо теми кваліфікаційної роботи з керівником) Практичні (написання кваліфікаційної роботи); Дистанційного навчання (захист кваліфікаційної роботи, робота з керівником з допомогою платформ дистанційного навчання)	Захист кваліфікаційної роботи здобувачем
		Комплексні системи безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з теми курсу «Дослідження рішень щодо сучасних систем відеоаналітики, представлених на ринку України та світу»

		Методологія та організація наукових досліджень	Метод кейсів: Аналіз реальних сценаріїв та проблем, що допомагає розвивати навички критичного мислення та вирішення проблем. Гіпотетичні експерименти: Висування і перевірка гіпотез у контрольованих умовах. Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Звіти про дослідження: Письмові звіти, що описують проведені експерименти, їх результати та висновки. Презентації: Усні або мультимедійні презентації, де здобувачі представляють свої дослідження та аргументують висновки перед аудиторією.
ПРН23 Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.	☒	Кваліфікаційна (магістерська) робота. Атестація	Наочні (дискусія щодо теми кваліфікаційної роботи з керівником) Практичні (написання кваліфікаційної роботи); Дистанційного навчання (захист кваліфікаційної роботи, робота з керівником з допомогою платформ дистанційного навчання)	Захист кваліфікаційної роботи здобувачем
		Практика (виробнича)	Використання наочних та практичних методів навчання завдяки проходженню здобувачем практики на підприємствах стейкхолдерів	Поточне оцінювання відповідно до проходження практичної підготовки здобувачем на підприємствах стейкхолдерів
		Криптологія	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання – результатів самостійної роботи здобувачів з розробки питань: Лекції 1-8, практичні 1-6, лабораторні 1-6
		Комплексні системи безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу «Визначення термінів АС, ІАС, ІСБ, КСБ тощо. Загальна структура інтегрованої системи безпеки, базові рівні мережевої взаємодії. принципів проектування ІСБ, основні вимоги при реалізації універсальної апаратної платформи ІСБ. Інтеграція на проектному, програмному, апаратному та апаратно-програмному рівнях (платформах) інтеграції.»
		Менеджмент інформаційної безпеки	Наочні (лекція-презентація, демонстраційні відеоролики, групова робота); Практичні (практичне заняття, захист і обговорення рефератів, дискусія, самостійна робота, завдання); Дистанційного навчання (платформа Zoom; онлайн-	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступної теми курсу «Класифікація програмних рішень»

			дискусії, онлайн-опитування та онлайн-консультації)	
		Управління доступом до інформаційних ресурсів	Наочні (дискусія, групова робота); Практичні (практичне заняття, лабораторна робота, самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	Поточне оцінювання – результатів самостійної роботи здобувачів з обговорення питань: впровадження заходів протидії НСД, розроблених рішень у практику, що включає моніторинг мережі та систем, автоматизацію процедур відповіді на інциденти, захист від атак на різних рівнях (мережевий, системний, прикладний).
		Кіберфізична безпека об'єктів критичної інфраструктури	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання – результатів самостійної роботи здобувачів з розробки питань: «Практичне заняття 2. Розділи 2, 4. Принцип модельованості та цілеспрямованості. Задачі вибору й оцінки програмно-технічних засобів захисту інформації».
ПРН24 Розроблювати плани аварійного відновлення та безперервності операцій в інформаційних, електронних, комунікаційних та інформаційно-комунікаційних системах.	☒	Процесний менеджмент в системі корпоративної безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу «Забезпечення неперервності бізнесу в "нетипові" періоди», «Експрес-аудит стану безпеки підприємства в фокусі впровадження BCM.»
		Кіберфізична безпека об'єктів критичної інфраструктури	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання – результатів самостійної роботи здобувачів з розробки питань: «Практичне заняття 4. Методи розрахунків показників надійності та безпеки кіберфізичних систем». Тематичне оцінювання – групових самостійних робіт (за варіантами), що спрямовані на розв'язання проблемних ситуацій та обґрунтування методів їх вирішення за темою «Етап здавально-приймальних робіт комплексу захисту інформації (КСЗІ) в інформаційно-телекомунікаційній системі (ІТС)».
ПРН33 Здійснювати перевірку повноти і відповідності реалізованих заходів із захисту інформації вимогам технічного завдання на створення комплексу ТЗІ (або на створення КСЗІ в інформаційно-	☒	Спеціальні вимірювання в галузі ТЗІ	Наочні (дискусія, групова робота); Практичні (практичне заняття, лабораторна робота, самостійна робота, завдання); Дистанційного навчання (платформа Zoom; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів самостійної роботи здобувачів з обговоренням питань використання нормативної документації при створені КСЗІ.

комунікаційних системах в частині вимог до захисту інформації від витоку технічними каналами), нормативно-правових актів та нормативних документів системи ТЗІ.				
ПРН25 Застосовувати сервіс-орієнтовані принципи архітектури безпеки, щоб задовольнити вимоги конфіденційності, цілісності та доступності організації.	☒	Кіберфізична безпека об'єктів критичної інфраструктури	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Семестрове оцінювання – індивідуальна робота здобувача з тематичного модуля «Тема 2. Основи теорії, техніки і технології кіберфізичної безпеки". Поточне оцінювання – результатів самостійної роботи здобувачів з розробки питань: «Лекція 2. Моделі та характеристики кіберфізичних систем як об'єкта безпеки індустріальні системи управління, АСУ ТП (SKADA) та їх елементи, розширений кіберпростір, транспортні протоколи, функції». «Лекція 3. Розділ 3. Стандартизована архітектура протоколів».
ПРН27 Здійснювати моніторинг та аудит загроз для інформації в інформаційних системах та мережах та оцінку ризиків безпеки інформації	☒	Моніторинг та аудит інформаційно-комунікаційних систем	Наочні (дискусія, групова робота); Практичні (самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	Поточне оцінювання – результатів самостійної роботи здобувачів з обговорення питання: оцінка ефективності впровадження навчання та інформування користувачів та персоналу аспектів інформаційної безпеки.
ПРН28 Здійснювати моніторинг та аудит загроз для інформації, що озвучується.	☒	Моніторинг та аудит інформаційно-комунікаційних систем	Наочні (дискусія, групова робота); Практичні (практичне заняття, лабораторна робота, самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	Поточне оцінювання – результатів самостійної роботи здобувачів з обговорення питання: впровадження протоколювання процесів у центрі інформаційної безпеки та ведення системного журналу.
ПРН29 Використовувати інструменти та технології безперервного моніторингу з метою оцінки ризиків, користуватися прикладними програмами моніторингу та аудиту загроз для інформації в інформаційних системах та мережах	☒	Моніторинг та аудит інформаційно-комунікаційних систем	Наочні (дискусія, групова робота); Практичні (практичне заняття, лабораторна робота, самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	Тематичне оцінювання групових практичних робіт, що спрямовані на розв'язання завдань: організовувати та здійснювати збирання, попередній аналіз даних та планування заходів з підготовки та проведення аудиту.
ПРН30 Проводити сканування вразливостей і розпізнавання вразливостей в ІКС	☒	Моніторинг та аудит інформаційно-комунікаційних систем	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (курсова робота, самостійна робота,	Тематичне оцінювання групових практичних робіт, що спрямовані на розв'язання завдань: створення системи

і системах безпеки.			завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	комплексного дослідження захищеності інформаційно-комунікаційної системи; розробка рекомендації щодо удосконалення системи інформаційної безпеки.
		Кіберфізична безпека об'єктів критичної інфраструктури	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання – результатів самостійної роботи здобувачів з розробки питань: «Лекція 6. Атаки на АСУ ТП, вразливості комунікаційних протоколів". "Лекція 7 .Загрози та вразливості індустріальних систем управління".
ПРН31 Використовувати моделі та симуляції інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації.	☒	Кіберфізична безпека об'єктів критичної інфраструктури	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання – результатів самостійної роботи здобувачів з розробки питань: «Лекція 1.Роздыл 2. Модель типового об'єкта захисту".«Лекція 2. Моделі та характеристики кіберфізичних систем як об'єкта безпеки індустріальні системи управління, АСУ ТП (SKADA) та їх елементи, розширений кіберпростір, транспортні протоколи, функції». "Лекція 7 .Загрози та вразливості індустріальних систем управління".
ПРН32 Складати програму та методику атестації комплексу технічного захисту інформації (ТЗІ)	☒	Спеціальні вимірювання в галузі ТЗІ	Наочні (дискусія, групова робота); Практичні (практичне заняття, лабораторна робота, самостійна робота, завдання); Дистанційного навчання (платформа Zoom; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів лабораторних робіт, пов'язаних з комплексами КТЗІ, а також самостійної роботи здобувачів з обговоренням питань атестації даних комплексів відповідно до вимог.
ПРН26 Визначати вимоги до показників (характеристик) апаратних засобів технічного захисту інформації, які необхідні для забезпечення захищеності інформації в системі або на об'єкті інформаційної діяльності.	☒	Кіберфізична безпека об'єктів критичної інфраструктури	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання – результатів самостійної роботи здобувачів з розробки питань: «Практичне заняття 2. Розділи 2, 4. Принцип модельованості та цілеспрямованості. Задачі вибору й оцінки програмно-технічних засобів захисту інформації». "Розрахунки та вимірювання показників функціональної безпеки кіберфізичних систем".
ПРН18 Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.	☒	Педагогіка та психологія	Наочні (тренінгові завдання, групова робота, самостійний перегляд навчально-пізнавальних фільмів); Практичні (практичне заняття, захист і обговорення рефератів, дискусія, самостійна робота, тести здібностей, тест інтелекту); Дистанційного навчання (платформа Zoom; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів самостійної роботи здобувачів з обговоренням питання пройдених тестів.

ПРН15 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.	☒	Практика (виробнича)	Використання наочних та практичних методів навчання завдяки проходженню здобувачем практики на підприємствах стейкхолдерів	Поточне оцінювання відповідно до проходження практичної підготовки здобувачем на підприємствах стейкхолдерів
ПРН16 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.	☒	Менеджмент інформаційної безпеки	Наочні (лекція-презентація, демонстраційні відеоролики, групова робота); Практичні (практичне заняття, захист і обговорення рефератів, дискусія, самостійна робота, завдання); Дистанційного навчання (платформа Zoom; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу «Постановка цілей і організаційне планування», «Стандарт ISO 2700», «Стандарт COBIT»
		Моніторинг та аудит інформаційно-комунікаційних систем	Наочні (дискусія, групова робота); Практичні (самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	Поточне оцінювання – результатів самостійної роботи здобувачів з обговорення питання: дослідження центру управління безпекою за допомогою передових практик та стандартів (наприклад, ITIL, COBIT та PCI DSS).
		Процесний менеджмент в системі корпоративної безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу «Аналіз рішень щодо управління бізнес-процесами підприємства», «Забезпечення неперервності бізнесу в "нетипові" періоди»
		Кваліфікаційна (магістерська) робота. Атестація	Наочні (дискусія щодо теми кваліфікаційної роботи з керівником) Практичні (написання кваліфікаційної роботи); Дистанційного навчання (захист кваліфікаційної роботи, робота з керівником з допомогою платформ дистанційного навчання)	Захист кваліфікаційної роботи здобувачем
		Комплексні системи безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу «Ситуаційні центри комплексних систем безпеки. Цілі, завдання та суб'єкти ситуаційних центрів. Масштаби ситуаційних центрів. Вимоги до фізичної та інформаційної

				інфраструктури, рівні оснащення ситуаційних центрів.»; «Принципи системності та комплексності. Синергія та синергетичний ефект.»
ПРН17 Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.	☒	Педагогіка та психологія	Наочні (презентація теми реферату, самостійний перегляд навчально-пізнавальних фільмів); Практичні (практичне заняття, самостійна робота, завдання, проходження онлайн-крусу від ГО "Волонтер" при підтримці Unicef "Булінг та кібербулінг: як ідентифікувати і зупинити); Дистанційного навчання (платформа Zoom; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів самостійної роботи здобувачів з обговоренням його теоретичного дослідження з тематики курсу.
		Практика (виробнича)	Використання наочних та практичних методів навчання завдяки проходженню здобувачем практики на підприємствах стейкхолдерів	Поточне оцінювання відповідно до проходження практичної підготовки здобувачем на підприємствах стейкхолдерів
		Кваліфікаційна (магістерська) робота. Атестація	Наочні (дискусія щодо теми кваліфікаційної роботи з керівником) Практичні (написання кваліфікаційної роботи); Дистанційного навчання (захист кваліфікаційної роботи, робота з керівником з допомогою платформ дистанційного навчання)	Захист кваліфікаційної роботи здобувачем
ПРН1 Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	☒	Кваліфікаційна (магістерська) робота. Атестація	Наочні (дискусія щодо теми кваліфікаційної роботи з керівником) Практичні (написання кваліфікаційної роботи); Дистанційного навчання (захист кваліфікаційної роботи, робота з керівником з допомогою платформ дистанційного навчання)	Захист кваліфікаційної роботи здобувачем
		Практика (виробнича)	Використання наочних та практичних методів навчання завдяки проходженню здобувачем практики на підприємствах стейкхолдерів	Поточне оцінювання відповідно до проходження практичної підготовки здобувачем на підприємствах стейкхолдерів
		Ділова іноземна мова	Комунікативний (learner-centered approach, підхід, орієнтований на здобувача, language fluency method/метод вільного мовлення, language skills method/метод мовних навичок, trial and error method/метод проб і помилок); Практичні (метод вправ; практична робота; ділова гра;); Інтерактивні (внутрішні (зовнішні) кола (inside/outside circles), мозковий штурм (brain storm), обмін думками (think-pair-share), парні інтерв'ю (pair-interviews) та інші.	Тематичне оцінювання – групових практичних робіт (малі групи 3-5 осіб), що спрямовані на діалогічне мовлення та презентації.

		Моніторинг та аудит інформаційно-комунікаційних систем	Наочні (дискусія, групова робота); Практичні (самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	Поточне оцінювання результатів самостійної роботи здобувачів з обговоренням питань: загальні принципи аудиту інформаційної безпеки; принципів проведення аудиту; основні цілі та задачі моніторингу та аудиту інформаційних систем.
		Процесний менеджмент в системі корпоративної безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з основних тем курсу.
		Криптологія	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання – результатів самостійної роботи здобувачів з розробки питань:Лекції 1-8, практичні 1-6, лабораторні 1-6
		Кіберфізична безпека об'єктів критичної інфраструктури	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання – результатів самостійної роботи здобувачів з розробки питань: «Лекція 3. Розділ 4. Incident organization and security incident handling: Guidelines for telecommunication organizations (Rec. ITU-T E.409). Тематичне оцінювання – групових самостійних робіт (за варіантами), що спрямовані на розв'язання проблемних ситуацій та обґрунтування методів їх вирішення за темою "Future networks. Functional architecture of software-defined networking (Rec. ITU-T Y.3302)".
		Комплексні системи безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з основної тематики курсу.
		Менеджмент інформаційної безпеки	Наочні (лекція-презентація, демонстраційні відеоролики, групова робота); Практичні (практичне заняття, захист і обговорення рефератів, дискусія, самостійна робота, завдання); Дистанційного навчання	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з обговорення питань курсу.

			(платформа Zoom; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	
		Управління доступом до інформаційних ресурсів	Наочні (дискусія, групова робота); Практичні (практичне заняття, лабораторна робота, самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	Поточне оцінювання результатів самостійної роботи здобувачів з обговоренням питань: базові визначення понять інформаційних ресурсів та інтелектуальної мережі; національні інформаційні ресурси; принципи побудови та архітектура інтелектуальної мережі.
		Педагогіка та психологія	Наочні (лекція-презентація, демонстраційні відеоролики, групова робота); Практичні (практичне заняття, захист і обговорення рефератів, дискусія, самостійна робота, завдання); Дистанційного навчання (платформа Zoom; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з обговорення питань курсу.
		Методологія та організація наукових досліджень	Наочні (лекція-презентація, демонстраційні відеоролики, групова робота); Практичні (практичне заняття, захист і обговорення рефератів, дискусія, самостійна робота, завдання); Дистанційного навчання (платформа Zoom; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на практичних заняттях, оцінювання самостійної роботи здобувача з обговорення питань курсу.
ПРН2 Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисципліна рних контекстах.	☒	Кваліфікаційна (магістерська) робота. Атестація	Наочні (дискусія щодо теми кваліфікаційної роботи з керівником) Практичні (написання кваліфікаційної роботи); Дистанційного навчання (захист кваліфікаційної роботи, робота з керівником з допомогою платформ дистанційного навчання)	Захист кваліфікаційної роботи здобувачем
		Практика (виробнича)	Використання наочних та практичних методів навчання завдяки проходженню здобувачем практики на підприємствах стейкхолдерів	Поточне оцінювання відповідно до проходження практичної підготовки здобувачем на підприємствах стейкхолдерів
		Моніторинг та аудит інформаційно-комунікаційних систем	Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Тематичне оцінювання групових практичних робіт, що спрямовані на розв'язання завдань: здійснювати моніторинг та аудит загроз для інформації в інформаційних системах та мережах та оцінку ризиків безпеки інформації.
		Процесний менеджмент в системі корпоративної безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу «Моделювання бізнес-процесів підприємства.»,

			дискусії, онлайн-опитування та онлайн-консультації)	«Аналіз рішень щодо управління бізнес-процесами підприємства»; «Забезпечення неперервності бізнесу в "нетипові" періоди»
		Криптологія	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання – результатів самостійної роботи здобувачів з розробки питань: Лекції 1-8, практичні 1-6, лабораторні 1-6
		Кіберфізична безпека об'єктів критичної інфраструктури	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Семестрове оцінювання – індивідуальна робота здобувача з тематичного модуля «Тема 1. Процеси міждисциплінарної інтеграції, конвергенції та авторизації безпеки» Поточне оцінювання – результатів самостійної роботи здобувачів з розробки «Лекція 1. Дисципліна «Кіберфізична безпека об'єктів критичної інфраструктури», «Розділ Лекції 3. Короткий огляд теорії систем управління». «Розділ Лекції 4. Міра критичності складових кіберфізичної системи». «Розділ Лекції 6. Огляд основ кібербезпеки». «Практичне заняття 2. Системні принципи теорії захисту інформації. Принцип модельованості та цілеспрямованості. Критерії системного мислення». «Практичне заняття 5. ALARP – підхід до управління ризиком». «Практичне заняття 6. Методології категоріювання об’єктів кіберфізичної інфраструктури». «Лабораторна робота 7. Математичні методи категоріювання об’єктів критичної інфраструктури. Формальні задачі математичної статистики в термінах категоріювання об’єктів
		Комплексні системи безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з теми курсу «Системи інтелектуального відеоспостереження та відеоаналітика.», «Моделювання компонентного складу систему, складання специфікації в залежності від ТЗ на об’єкт. Використання спеціалізованих калькуляторів на корпоративних сайтах»

		Менеджмент інформаційної безпеки	Наочні (лекція-презентація, демонстраційні відеоролики, групова робота); Практичні (практичне заняття, захист і обговорення рефератів, дискусія, самостійна робота, завдання); Дистанційного навчання (платформа Zoom; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу: «Економічна ефективність інформаційних систем»; « Аудит стану ІБ на підприємстві»
		Управління доступом до інформаційних ресурсів	Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Тематичне оцінювання групових практичних робіт (малі групи 3-5 осіб), що спрямовані на розв'язання завдань, що пов'язані з моделюванням загроз та керування ризиками від дій несанкціонованого доступу до інтелектуальної мережі.
		Методологія та організація наукових досліджень	Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Тематичне оцінювання групових практичних робіт (малі групи 3-5 осіб), що спрямовані на розв'язання завдань, що пов'язані з моделюванням загроз та керування ризиками від дій несанкціонованого доступу до інтелектуальної мережі.
ПРН3 Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	☒	Кіберфізична безпека об'єктів критичної інфраструктури	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Семестрове оцінювання – індивідуальна робота здобувача з тематичного модуля «Тема 2. Основи теорії, техніки і технології кіберфізичної безпеки Поточне оцінювання – результатів самостійної роботи здобувачів з проробки «» Лекція 3. Короткий огляд властивостей безпеки у складі кіберфізичних систем». «Лекція 6. Системи та алгоритми шифрування. Порівняння симетричного ключа проти відкритого ключа».
		Комплексні системи безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу «Дослідження рішень щодо сучасних систем відеоаналітики, представлених на ринку України та світу»; «Вивчення досвіду щодо впровадження в містах України та світу КСБ в проектах типу "Безпечне місто". Технології, бренди, компонентний склад, результати»
		Менеджмент інформаційної безпеки	Наочні (лекція-презентація, демонстраційні відеоролики, групова робота); Практичні (практичне заняття, захист і обговорення рефератів,	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступної теми курсу «

			дискусія, самостійна робота, завдання); Дистанційного навчання (платформа Zoom; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Формулювання та впровадження стратегії»
		Управління доступом до інформаційних ресурсів	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів самостійної роботи здобувачів з обговоренням питань: послуги, що надаються інтелектуальною мережею; створення системи управління інтелектуальною надбудовою; захист інформації в сучасних інтелектуальних мережах.
		Методологія та організація наукових досліджень	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів самостійної роботи здобувачів з обговоренням питань: послуги, що надаються інтелектуальною мережею; створення системи управління інтелектуальною надбудовою; захист інформації в сучасних інтелектуальних мережах.
		Криптологія	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання – результатів самостійної роботи здобувачів з розробки питань: Лекції 1-8, практичні 1-6, лабораторні 1-6
		Процесний менеджмент в системі корпоративної безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу «Експрес-аудит стану безпеки підприємства в фокусі впровадження ВСМ.», « Оптимізація бізнес-процесів підприємства.», «Міжнародні стандарти та практики ВСМ»
		Моніторинг та аудит інформаційно-комунікаційних систем	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів самостійної роботи здобувачів з обговоренням питань: ієрархічна модель реалізації послуг аудиту; модель реалізації послуг аудиту та тривожної сигналізації.
		Ділова іноземна мова	Комунікативний (learner-centered approach, підхід, орієнтований на здобувача, language fluency method/метод вільного мовлення, language skills method/метод мовних навичок, trial and error method/метод проб і помилок); Практичні (метод вправ; практична робота; ділова гра;);	Тематичне оцінювання – групових практичних робіт (малі групи 3-5 осіб), що спрямовані на діалогічне мовлення та презентації.

			Інтерактивні (внутрішні (зовнішні) кола (inside/outside circles), мозковий штурм (brain storm), обмін думками (think-pair-share), парні інтерв'ю (pair-interviews) та інші.	
		Кваліфікаційна (магістерська) робота. Атестація	Наочні (дискусія щодо теми кваліфікаційної роботи з керівником) Практичні (написання кваліфікаційної роботи); Дистанційного навчання (захист кваліфікаційної роботи, робота з керівником з допомогою платформ дистанційного навчання)	Захист кваліфікаційної роботи здобувачем
ПРН4 Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.	☒	Кваліфікаційна (магістерська) робота. Атестація	Наочні (дискусія щодо теми кваліфікаційної роботи з креівником) Практичні (написання кваліфікаційної роботи); Дистанційного навчання (захист кваліфікаційної роботи, робота з керівником з допомогою платформ дистанційного навчання)	Захист кваліфікаційної роботи здобувачем
		Моніторинг та аудит інформаційно-комунікаційних систем	Практичні (практичне заняття, лабораторна робота, самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	Поточне оцінювання результатів самостійної роботи здобувачів з обговоренням питання: аналіз і оцінка ризиків інформаційної безпеки.
		Процесний менеджмент в системі корпоративної безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу « Оптимізація бізнес-процесів підприємства.», «Аналіз рішень щодо управління бізнес-процесами підприємства.», «Забезпечення неперервності бізнесу в "нетипові" періоди»; « Експрес-аудит стану безпеки підприємства в фокусі впровадження BCM»
		Криптологія	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання – результатів самостійної роботи здобувачів з розробки питань: Лекції 1-8, практичні 1-6, лабораторні 1-6
		Кіберфізична безпека об'єктів критичної інфраструктури	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-	Поточне оцінювання – результатів самостійної роботи здобувачів з проробки «Лекція 8. Безпечні версії сучасних протоколів для кібер-фізичних систем» «Лекція 4. Мережеві комунікаційні протоколи для

			дискусії, онлайн-опитування та онлайн-консультації)	індустріальних систем управління». «Практичне заняття 3. Основні показники надійності та формули для їх обчислення. Показники кібер-фізичної безпеки та формули для їх обчислення». «Практичне заняття 4. Марківську модель та проведіть за його допомогою розрахунок та аналіз показників безпеки та надійності». «Практичне заняття 6. Багаторівнева методика категоріювання». Лабораторна робота 7. розрахункових формулах, сітках, областях категоріювання, та розрахунку очікуваного ризику».
		Комплексні системи безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу «Вивчення досвіду щодо впровадження в містах України та світу КСБ в проектах типу “Безпечне місто”. Технології, бренди, компонентний склад, результати.», «Моделювання компонентного складу систему, складання специфікації в залежності від ТЗ на об’єкт. Використання спеціалізованих калькуляторів на корпоративних сайтах»
		Менеджмент інформаційної безпеки	Наочні (лекція-презентація, демонстраційні відеоролики, групова робота); Практичні (практичне заняття, захист і обговорення рефератів, дискусія, самостійна робота, завдання); Дистанційного навчання (платформа Zoom; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу «Формулювання та впровадження стратегії», «Впровадження та контроль над реалізованими стратегіями»
		Управління доступом до інформаційних ресурсів	Практичні (практичне заняття, лабораторна робота, самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	Поточне оцінювання результатів самостійної роботи здобувачів з обговоренням питання аналізу інформаційних ресурсів на основі моделі інтелектуальної мережі і взаємодії її основних компонентів.
ПРН5 Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння	☒	Кваліфікаційна (магістерська) робота. Атестація	Наочні (дискусія щодо теми кваліфікаційної роботи з керівником) Практичні (написання кваліфікаційної роботи); Дистанційного навчання (захист кваліфікаційної роботи, робота з керівником з допомогою платформ дистанційного навчання)	Захист кваліфікаційної роботи здобувачем

нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.		Моніторинг та аудит інформаційно-комунікаційних систем	Наочні (дискусія, групова робота); Практичні (курсова робота, самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	Поточне оцінювання – результатів самостійної роботи здобувачів з обговорення питання: щодо способів сканування та розпізнавання вразливостей у системах безпеки для інформації в інформаційних системах і мережах.
		Процесний менеджмент в системі корпоративної безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу «Аналіз рішень щодо управління бізнес-процесами підприємства», «Оптимізація бізнес-процесів підприємства»; «Моделювання бізнес-процесів підприємства»
		Кіберфізична безпека об'єктів критичної інфраструктури	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання – результатів самостійної роботи здобувачів з обробки розділу «Характерні відмінності інформаційних (комп'ютерних) систем від індустріальних систем. «Лекція 7. Розділ 2. Уразливості комунікаційних протоколів». «Лекція 8. Розділ 1. Захищені версії застарілих протоколів". "Практичне заняття 4. Варіант 4. Проаналізувати повноту діагностичного покриття, отриманого в результаті FMECA. Чи є можливість підвищити повноту безпеки.
		Комплексні системи безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу «Визначення термінів АС, ІАС, ІСБ, КСБ тощо. Загальна структура інтегрованої системи безпеки, базові рівні мережевої взаємодії. принципів проектування ІСБ, основні вимоги при реалізації універсальної апаратної платформи ІСБ. Інтеграція на проектному, програмному, апаратному та апаратно-програмному рівнях (платформах) інтеграції.»
		Менеджмент інформаційної безпеки	Наочні (лекція-презентація, демонстраційні відеоролики, групова робота); Практичні (практичне заняття, захист і обговорення рефератів, дискусія, самостійна робота, завдання); Дистанційного навчання (платформа Zoom; онлайн-дискусії, онлайн-опитування	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу « Постановка цілей і організаційне планування»; «Інтернет і е-бізнес»

			та онлайн-консультації)	
		Управління доступом до інформаційних ресурсів	Наочні (дискусія, групова робота); Практичні (практичне заняття, лабораторна робота, самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	Поточне оцінювання – результатів самостійної роботи здобувачів з обговорення питань використання спеціалізованого програмного забезпечення для захисту інформації від НСД та засобів радіотехнічної розвідки.
		Криптологія	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання – результатів самостійної роботи здобувачів з розробки питань: Лекції 1-8, практичні 1-6, лабораторні 1-6
ПРН7 Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	☒	Спеціальні вимірювання в галузі ТЗІ	Наочні (дискусія, групова робота); Практичні (практичне заняття, лабораторна робота, самостійна робота, завдання); Дистанційного навчання (платформа Zoom; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів самостійної роботи здобувачів з обговоренням нормативних акти, документи, стандартів що визначають вимоги із захисту інформації на об'єкті інформаційної діяльності. Результатів самостійної роботи здобувачів на тему «Протокол інструментального контролю захищеності інформації на об'єкті інформаційної діяльності». Лекція 6. Система технічних документів щодо систем і комплексів захисту інформації.
		Моніторинг та аудит інформаційно-комунікаційних систем	Практичні (самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації). Наочні (дискусія, групова робота); Практичні (самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	Поточне оцінювання результатів самостійної роботи здобувачів з обговоренням питання: відповідність аудиту інформаційної безпеки національним та міжнародним стандартам.
		Процесний менеджмент в системі корпоративної безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу «Міжнародні стандарти та практики BCM»; «Забезпечення неперервності бізнесу в "нетипові" періоди»
		Криптологія	Наочні (лекція, консультація, ілюстрація,	Поточне оцінювання – результатів самостійної

			дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	роботи здобувачів з розробки питань: Лекції 1-8, практичні 1-6, лабораторні 1-6
		Кіберфізична безпека об'єктів критичної інфраструктури	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання – результатів самостійної роботи здобувачів з проробки «Лекція 3. Розділ 3. Стандартизована архітектура протоколів». «Лекція 5. Протоколи індустріальних мереж Modbus, DNP3, IEC 61850».
		Комплексні системи безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу «Дослідження рішень щодо сучасних систем відеоаналітики, представлених на ринку України та світу», «Концепція ІАС “Безпечне місто”. Вимоги до побудови, основні підсистеми, приклади реалізації.», «Компонентний склад та сценарії роботи обладнання в екосистемі Bosch Building Integration System»; «Комплексні системи безпеки на основі екосистем Ajax та Tiras. Технології, компонентний склад, можливості застосування»
		Управління доступом до інформаційних ресурсів	Практичні (практичне заняття, лабораторна робота, самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	Поточне оцінювання результатів самостійної роботи здобувачів з обговоренням питання вибору методів захисту інформації у залежності від вимог до якості для конкретних умов передавання сигналів.
		Кваліфікаційна (магістерська) робота. Атестація	Наочні (дискусія щодо теми кваліфікаційної роботи з керівником) Практичні (написання кваліфікаційної роботи); Дистанційного навчання (захист кваліфікаційної роботи, робота з керівником з допомогою платформ дистанційного навчання)	Захист кваліфікаційної роботи здобувачем
ПРН6 Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	☒	Моніторинг та аудит інформаційно-комунікаційних систем	Наочні (дискусія, групова робота); Практичні (практичне заняття, лабораторна робота, самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	Поточне оцінювання результатів самостійної роботи здобувачів з обговоренням питання: здатність здійснювати постійний моніторинг та аудит загроз для інформації та відповідну модернізацію систем і комплексів захисту інформації.

		Криптологія	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання – результатів самостійної роботи здобувачів з розробки питань: Лекції 1-8, практичні 1-6, лабораторні 1-6
		Кіберфізична безпека об'єктів критичної інфраструктури	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Семестрове оцінювання – індивідуальна робота здобувача з тематичного модуля «Тема 1. Процеси міждисциплінарної інтеграції, конвергенції та авторизації безпеки» та «Тема 2. Основи теорії, техніки і технології у кіберфізичної безпеки». Поточне оцінювання – результатів самостійної роботи здобувачів з розробки питань: «Лекція 1. Розділ 3. Розподіл рівнів безпеки засобів телекомунікацій у координатах міри важливості систем для безпеки установки підприємства промисловості та транспорту та степені засобів захисту». «Модель типового об’єкта захисту». «Лекція 4. Розділ 3. Міра критичності складових кіберфізичної системи». Питання практичного заняття 1. «Визначення основних переваг та недоліків використання стандартів САН». «Практичне заняття 3. Розділ 4. Чому необхідно аналізувати одночасно і показник безпеки і показник надійності». «Практичне заняття 5. Методи аналізу ризиків». Тематичне оцінювання – групових самостійних робіт (за варіантами), що спрямовані на розв’язання проблемних ситуацій та обґрунтування методів їх вирішення за темою «Розробка та реалізація програми та методики проведення державної експертизи комплексних систем безпеки інформації».
		Комплексні системи безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу «Введення в дисципліну. Методологія в питаннях безпеки. Визначення термінів функціональний ресурс системи, системотехніка та комплексотехніка, принципи комплексотехніки. Моделювання комплексної

				системи безпеки об'єкта.», «Принципи системності та комплексності. Синергія та синергетичний ефект.»
		Управління доступом до інформаційних ресурсів	Наочні (дискусія, групова робота); Практичні (практичне заняття, лабораторна робота, самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	Поточне оцінювання результатів самостійної роботи здобувачів з обговоренням питання аналізу умов передавання конфіденційної інформації при дії засобів радіоелектронної розвідки.
		Спеціальні вимірювання в галузі ТЗІ	Наочні (дискусія, групова робота); Практичні (практичне заняття, лабораторна робота, самостійна робота, завдання); Дистанційного навчання (платформа Zoom; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів самостійної роботи здобувачів з обговоренням питань: базові визначення та поняття. Результати самостійної роботи здобувачів на тему «Розробка моделі загроз на об'єкті інформаційної діяльності». Лекція 4. Створення комплексів технічного захисту інформації.
ПРН9 Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	☒	Кіберфізична безпека об'єктів критичної інфраструктури	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання – результатів самостійної роботи здобувачів з проробки «Лекція 3. Розділ 4. Короткий огляд теорії систем управління безпекою».
		Менеджмент інформаційної безпеки	Наочні (лекція-презентація, демонстраційні відеоролики, групова робота); Практичні (практичне заняття, захист і обговорення рефератів, дискусія, самостійна робота, завдання); Дистанційного навчання (платформа Zoom; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу «Завдання, ролі і методи, використовувані на різних рівнях організаційної роботи в сфері інформаційної безпеки»; «Основні напрями забезпечення безпеки інформації та інформаційних ресурсів»
ПРН10 Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	☒	Процесний менеджмент в системі корпоративної безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу «Моделювання бізнес-процесів підприємства.», «Експрес-аудит стану безпеки підприємства в фокусі впровадження ВСМ»
		Менеджмент інформаційної безпеки	Наочні (лекція-презентація, демонстраційні відеоролики, групова робота); Практичні (практичне заняття, захист і обговорення рефератів,	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу

			дискусія, самостійна робота, завдання); Дистанційного навчання (платформа Zoom; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	«Процес стратегічного менеджменту», «Формулювання та впровадження стратегії»
		Управління доступом до інформаційних ресурсів	Наочні (дискусія, групова робота); Практичні (практичне заняття, лабораторна робота, самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	Поточне оцінювання – результатів самостійної роботи здобувачів з обговорення питань щодо уразливості інформаційних ресурсів у випадку доступу до них на основі бездротових мереж, забезпечення захисту інформації від НСД в сучасних телекомунікаційних системах.
ПРН11 Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	☒	Менеджмент інформаційної безпеки	Наочні (лекція-презентація, демонстраційні відеоролики, групова робота); Практичні (практичне заняття, захист і обговорення рефератів, дискусія, самостійна робота, завдання); Дистанційного навчання (платформа Zoom; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу «Завдання, ролі і методи, використовувані на різних рівнях організаційної роботи в сфері інформаційної безпеки»; «Основні напрями забезпечення безпеки інформації та інформаційних ресурсів»
		Управління доступом до інформаційних ресурсів	Наочні (дискусія, групова робота); Практичні (практичне заняття, лабораторна робота, самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	Поточне оцінювання – результатів самостійної роботи здобувачів з обговорення питань щодо захисту інформації в сучасних інтелектуальних мережах, характеристик захищеності телекомунікаційних систем.
ПРН12 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.	☒	Управління доступом до інформаційних ресурсів	Наочні (дискусія, групова робота); Практичні (практичне заняття, лабораторна робота, самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	Поточне оцінювання – результатів самостійної роботи здобувачів з обговорення наступних питань: аналіз різних типів атак, їх походження, векторів та способів впровадження є першим кроком для ефективної протидії; рекомендації щодо покращення захисту, зокрема впровадження багатофакторної автентифікації, регулярного оновлення програмного забезпечення, навчання персоналу правилам кібергігієни і створення резервних копій даних.
		Моніторинг та аудит інформаційно-комунікаційних систем	Наочні (дискусія, групова робота); Практичні (практичне заняття, лабораторна робота, самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	Поточне оцінювання – результатів самостійної роботи здобувачів з обговорення питання: дослідження методів та технологій моніторингу та аудиту загроз для конфіденційності, цілісності та доступності інформації.

ПРН13 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.	☒	Кіберфізична безпека об'єктів критичної інфраструктури	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання – результатів самостійної роботи здобувачів з розробки питань: «Лекція 6. Розділи 3, 4. Послуги, функції та механізми інформаційної та кібербезпеки. Системи та алгоритми шифрування». «Практичне заняття 3. Методи розрахунку ризиків кібернетичної безпеки кіберфізичних систем. Якісний підхід».
		Криптологія	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання – результатів самостійної роботи здобувачів з розробки питань: Лекції 1-8, практичні 1-6, лабораторні 1-6
		Комплексні системи безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу «Ситуаційні центри комплексних систем безпеки. Цілі, завдання та суб'єкти ситуаційних центрів. Масштаби ситуаційних центрів. Вимоги до фізичної та інформаційної інфраструктури, рівні оснащення ситуаційних центрів.»; «Загрози та ризики ситуаційних центрів, модель загроз, методи та засоби підвищення рівня безпеки ситуаційних центрів.»
		Спеціальні вимірювання в галузі ТЗІ	Наочні (дискусія, групова робота); Практичні (практичне заняття, лабораторна робота, самостійна робота, завдання); Дистанційного навчання (платформа Zoom; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів самостійної роботи здобувачів з обговоренням питань: типів, видів, класів, функції засобів криптографічного захисту інформації; програмно-технічних методів та засобів захисту інформації їх використання в інформаційних системах та на об'єктах інформаційної діяльності.
ПРН14 Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або	☒	Моніторинг та аудит інформаційно-комунікаційних систем	Наочні (дискусія, групова робота); Практичні (самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	Поточне оцінювання – результатів самостійної роботи здобувачів з обговорення питання: організація взаємозв'язку бізнес-стратегій з процесами розробки та управління операційною безпекою.

кібербезпеки в цілому.				
ПРН8 Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	☒	Кваліфікаційна (магістерська) робота. Атестація	Наочні (дискусія щодо теми кваліфікаційної роботи з креівником) Практичні (написання кваліфікаційної роботи); Дистанційного навчання (захист кваліфікаційної роботи, робота з керівником з допомогою платформ дистанційного навчання)	Захист кваліфікаційної роботи здобувачем
		Моніторинг та аудит інформаційно-комунікаційних систем	Практичні (самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації). Наочні (дискусія, групова робота); Практичні (самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	Поточне оцінювання – результатів самостійної роботи здобувачів з обговоренням питання: проведення безперервного внутрішнього аудиту інформаційної безпеки інформаційно-комунікаційних систем.
		Процесний менеджмент в системі корпоративної безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу «Моделювання бізнес-процесів підприємства.», «Експрес-аудит стану безпеки підприємства в фокусі впровадження ВСМ»
		Кіберфізична безпека об'єктів критичної інфраструктури	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання – результатів самостійної роботи здобувачів з проробки «Лекція 6. Розділи 2, 3. Послуги, функції та механізми інформаційної та кібербезпеки. Системи та алгоритми шифрування». «Практичне заняття 6. Методика категоризації об'єктів критичної інфраструктури№. «Лабораторна робота 7. Практика категоріювання об'єктів кіберфізичної інфраструктури».
		Комплексні системи безпеки	Наочні (лекція, консультація, ілюстрація, дискусія, групова робота) Практичні (практичне заняття, лабораторна робота, завдання); Дистанційного навчання (платформа Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації)	Поточне оцінювання результатів групової та індивідуальної роботи на семінарських заняттях, оцінювання самостійної роботи здобувача з наступних тем курсу «Ситуаційні центри комплексних систем безпеки. Цілі, завдання та суб'єкти ситуаційних центрів. Масштаби ситуаційних центрів. Вимоги до фізичної та інформаційної інфраструктури, рівні оснащення ситуаційних

				центрів.»; «Моделювання компонентного складу систему, складання специфікації в залежності від ТЗ на об'єкт. Використання спеціалізованих калькуляторів на корпоративних сайтах»
		Управління доступом до інформаційних ресурсів	Наочні (дискусія, групова робота); Практичні (практичне заняття, лабораторна робота, самостійна робота, завдання); Дистанційного навчання (платформи Moodle, Zoom та інші месенджери; онлайн-дискусії, онлайн-опитування та онлайн-консультації).	Поточне оцінювання – результатів самостійної роботи здобувачів з обговоренням питання розробки методів захисту передавання інформації від НСД та засобів радіотехнічної розвідки противника (зловмисника).