НАЦІОНАЛЬНЕ АГЕНТСТВО ІЗ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	**Державний університет інформаційно-комунікаційних технологій**
Освітня програма	**71152 Інформаційна та кібернетична безпека**
Рівень вищої освіти	**Магістр**
Спеціальність	**F5 Кібербезпека та захист інформації**

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

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

Використані скорочення:

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

Загальні відомості

1. Інформація про ЗВО (ВСП ЗВО)

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

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

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

3. Загальна інформація про ОП, яка подається на акредитацію

ID освітньої програми в ЄДЕБО	**71152**
Назва ОП	**Інформаційна та кібернетична безпека**
Галузь знань	**F Інформаційні технології**
Спеціальність	**F5 Кібербезпека та захист інформації**
Спеціалізація (за наявності)	*відсутня*
Рівень вищої освіти	**Магістр**
Тип освітньої програми	**Освітньо-професійна**
Вступ на освітню програму здійснюється на основі ступеня (рівня)	**Бакалавр, Магістр (ОКР «спеціаліст»)**
Структурний підрозділ (кафедра або інший підрозділ), відповідальний за реалізацію ОП	**Навчально-науковий інститут кібербезпеки та захисту інформації, кафедра систем та технологій кібербезпеки**
Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП	**Навчально-науковий інститут кібербезпеки та захисту інформації (кафедра управління кібербезпекою та захистом інформації); Навчально-науковий інститут телекомунікацій (кафедра української мови)**
Місце (адреса) провадження освітньої діяльності за ОП	**03110, Україна, м. Київ, вулиця Солом'янська, буд. 7**
Освітня програма передбачає присвоєння професійної кваліфікації	*не передбачає*
Професійна кваліфікація, яка присвоюється за ОП (за наявності)	***відсутня***
Мова (мови) викладання	**Українська**
ID гаранта ОП у ЄДЕБО	**81112**
ПІБ гаранта ОП	**Гайдур Галина Іванівна**
Посада гаранта ОП	**Завідувач кафедри**
Корпоративна електронна адреса гаранта ОП	**g.haidur@duikt.edu.ua**
Контактний телефон гаранта ОП	**+38(067)-345-33-38**
Додатковий телефон гаранта ОП	*відсутній*

Форми здобуття освіти на ОП	Термін навчання
заочна	1 р. 10 міс.
очна денна	1 р. 5 міс.

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

Освітньо-професійна програма «Інформаційна та кібернетична безпека» другого (магістерського) рівня вищої освіти визначає мету, цілі та зміст підготовки фахівців за спеціальністю F5 «Кібербезпека та захист інформації» освітньої кваліфікації магістра з кібербезпеки та захисту інформації. Потреба в реалізації зазначеної програми зумовлена необхідністю підготовки висококваліфікованих магістрів, здатних проводити наукові дослідження, впроваджувати інноваційні результати для захисту інформаційних систем, розслідувати кіберінциденти та вирішувати складні управлінські й науково-дослідні завдання, а також формуванням кадрового резерву висококласних фахівців і викладачів для галузі. Набуті здобувачами компетентності знаходять практичне застосування в дослідницькій, управлінській, освітній та бізнесовій сферах.
Стратегія розвитку ДУІКТ (https://duikt.edu.ua/uploads/p_949_78903289.pdf ikt.edu.ua/uploads/p_949_11377077.pdf) акцентує увагу на підготовці конкурентоспроможного людського капіталу для інноваційного розвитку держави та ґрунтується на принципах підтримки учасників освітнього процесу й розвитку сучасної цифрової освіти і науки. Університет забезпечує послідовну ступеневу підготовку за спеціальністю F5 «Кібербезпека та захист інформації» — від бакалаврського рівня до рівня доктора філософії.
Оновлена редакція ОПП «Інформаційна та кібернетична безпека» була схвалена Вченою радою університету (протокол № 3 від 17 березня 2026 року) та введена в дію наказом ректора № 105 від 20 березня 2026 року. Проєкт програми розроблено робочою групою на основі детального аналізу ринку праці, вимог роботодавців та положень Державного стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для магістерського рівня, затвердженого наказом МОН України від 18.03.2021 р. № 332. Відповідно до ОПП сформовано навчальний план підготовки та індивідуальні плани здобувачів.
Освітній процес забезпечується провідними кафедрами Навчально-наукового інституту захисту інформації за участю кафедри української мови Навчально-наукового інституту телекомунікацій.

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

Рік навчання	Навчальний рік, у якому відбувся набір здобувачів відповідного року навчання	Обсяг набору на ОП у відповідному навчальному році	Контингент студентів на відповідному році навчання станом на 1 жовтня поточного навчального року		У тому числі іноземців	
			ОД	*З*	*ОД*	*З*
1 курс	2025 - 2026	120	36	9	0	0
2 курс	2024 - 2025	120	66	13	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	*програми відсутні*
другий (магістерський) рівень	**71152 Інформаційна та кібернетична безпека** **71156 Технічні системи інформаційного та кібернетичного захисту** **71163 Управління інформаційною та кібернетичною безпекою**
третій (освітньо-науковий/освітньо-творчий) рівень	*програми відсутні*

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

	Загальна площа	Навчальна площа
Усі приміщення ЗВО	16518	7032
Власні приміщення ЗВО (на праві власності, господарського	16518	7032

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

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

8. Документи щодо ОП

Документ	Назва файла	Хеш файла
Освітня програма	*ОППмаістр_2026 т.pdf*	XxTynHAMCosWJqhfXETz4vTdC674ywMLn3q1VAdFeBk=
Освітня програма	*ОПП_магістр_2025.pdf*	V/SZpRJo8PoM6AWFKpqDivYCv3DiNAsRycpcAmYcHsw=
Навчальний план за ОП	*Навчальний план_денна_2026.pdf*	qikG4b6+DX+VH4AYaMmkoNk6tWrgdHxUFQqedLOBV7s=
Навчальний план за ОП	*Навчальний план_заочка_2026.pdf*	BtkuGhDzZnNvBZi2Ik1wjLVaf6XsQIj39Imp5x39Tr4=
Навчальний план за ОП	*Навчальний план_денна+заочка_2025.pdf*	zQFJXmz9MPLL4hAC3AZNCm+Sh9I/SEBeyPDOMc2qpek=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*КНУ_Наконечний_2026.pdf*	AFGUTNt/RmVLXXp5DYiSTltj2WzX1DojgQARLqMyTAU=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Світ_IT_Порошин_2026.pdf*	GBfDnQC4Rr1xtbXREtzHEo/jbOGlEv93DKE6qTxOUzw=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*КНУ_Толюпа_2025.pdf*	vG89T6aQKY/8daXXTRRx3mVFPr9Lz+GxBVdY9+w3BIo=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Світ_IT_Порошин_2026.pdf*	GBfDnQC4Rr1xtbXREtzHEo/jbOGlEv93DKE6qTxOUzw=

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?

Стандарт вищої освіти України за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти містить чіткий перелік із 23 нормативних результатів навчання (РН1 – РН23) для освітньо-професійних програм. Усі ці 23 програмні результати навчання (РН1 – РН23) повністю та без змін імплементовані у Розділ 7 ОПП «Інформаційна та кібернетична безпека».
Механізм досягнення цих результатів наочно продемонстрований у Розділі 5 ОПП «Матриця забезпечення програмних результатів навчання (ПРН) відповідними компонентами освітньої програми». Кожен нормативний результат навчання підкріплений циклом обов'язкових (ОК1-ОК13) або вибіркових компонентів.
Такі результати, як здатність застосовувати технології кіберзахисту та обґрунтовувати світові стандарти (РН4, РН6, РН7, РН8), досягаються під час вивчення профільних дисциплін «Прикладна загальна теорія систем кібербезпеки» (ОК6), «Управління проектами інформаційної безпеки» (ОК7) «Технології забезпечення безпеки мережевої інфраструктури» (ОК8) та «Технології виявлення уразливостей мережевих ресурсів» (ОК9).
Дослідницькі та інноваційні результати навчання (РН3, РН22, РН23) закріплюються завдяки проходженню науково-дослідної (ОК11) та переддипломної (ОК12) практик, а також виконанню кваліфікаційної роботи (ОК13).
Досягнення програмних результатів навчання підтверджується також активною позааудиторною та практичною діяльністю студентів, про що свідчать новини кафедри систем та технологій кібербезпеки. Зокрема:
Студенти отримують навички використання сучасних інструментів кіберзахисту, успішно завершуючи сертифіковані курси від партнерів (наприклад, курс HCIA-Security V4.0 від Huawei, CISCO та IBM).
Здобувачі освіти беруть участь у реальних хакерських турнірах у форматі Capture the Flag (CTF), що допомагає безпосередньо відпрацьовувати здатність до аналізу кіберінцидентів.
Постійний зв'язок з ринком праці та компаніями-роботодавцями (наприклад, ТОВ «Світ ІТ», ТОВ «IT Specialist», ТОВ «Євротелеком» та участь у «2U Tech Forum») забезпечує актуальність компетенцій. Також на кафедрі регулярно проводяться заходи, присвячені принципам академічної доброчесності та питань безбар'єрності та інклюзивності.
Кваліфікація магістра за ОПП офіційно відповідає 7 рівню Національної рамки кваліфікацій України (НРК).

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

Програма розроблена та оновлена з урахуванням Професійного стандарту на групу професій «Викладачі закладів вищої освіти» (затвердженого наказом Міністерства економіки від 23.03.2021 № 610). Крім того, враховано вимоги Національного класифікатора професій ДК 003:2010 (зі змінами) щодо кваліфікацій фахівця з реагування на інциденти кібербезпеки та фахівця з підтримки інфраструктури кіберзахисту.
https://duikt.edu.ua/ua/news-1-574-14839-strategichni-vektori-formuvannya-novoi-paradigmi-kiber-osviti-duikt-doluchivsya-do-fahovogo-dialogu_kafedra-informaciynoi-ta-kibernetichnoi-bezpeki

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

Мета та результати навчання оновлюються з урахуванням безпосередніх пропозицій і побажань здобувачів та випускників. До офіційного складу робочої групи з розробки ОПП входить здобувач магістерського рівня Антоніна КОРЖ. Крім того, програма офіційно погоджена Головою студентської ради ННІКБЗІ.

- роботодавці

Потреби ринку праці та ІТ-компаній безпосередньо формують практичну складову ОПП та профіль компетенцій випускника. До складу робочої групи включено представника роботодавців – директора ТОВ «Світ ІТ» Максима ПОРОШИНА, який надав позитивну рецензію. Випускники програми можуть бути залучені до виконання професійних функцій на посадах аналітика кібербезпеки, інженера з інформаційної безпеки, спеціаліста з реагування на інциденти, аудитора безпеки та адміністратора систем захисту інформації.
https://duikt.edu.ua/ua/news-1-574-15193-v-duikt-vidbulosya-obgovorennya-onovlenih-osvitnih-program-za-specialnistyu--f5-kiberbezpeka-ta-zahist-informacii_kafedra-informaciynoi-ta-kibernetichnoi-bezpeki

- академічна спільнота

ОПП базується на загальновідомих наукових результатах та враховує досвід вітчизняних і зарубіжних науково-педагогічних працівників. До розробки програми безпосередньо залучені професори та доценти профільної кафедри (зокрема, професор Сергій ЗИБІН та доцент Сергій ГАХОВ). Додатково, програма пройшла експертну оцінку та отримала зовнішню рецензію від представника академічної спільноти – професора Київського національного університету ім. Тараса Шевченка професора Володимира Наконечного).
https://duikt.edu.ua/ua/news-1-574-12729-spivpracya-mizh-duikt-ta-knu-im-tarasa-shevchenka-obgovorennya-navchalnih-osvitnih-program-za-specialnistyu-kiberbezpeka-ta-zahist-informacii_kafedra-informaciynoi-ta-kibernetichnoi-bezpeki

- інші стейкхолдери

Зміст ОПП відповідає вимогам державних регуляторів, професійних спільнот та узгоджується з міжнародними освітніми проєктами. ОПП оновлено з урахуванням наказів МОН (Державний стандарт) та Мінекономіки (Професійний стандарт, Класифікатор професій). Крім того, у програму впроваджені результати академічної співпраці з компанією IBM «Skills Build», Hu та результати проєкту Європейського союзу Tempus щодо освіти експертів у галузі кібербезпеки.

https://duikt.edu.ua/ua/news-1-574-13664-studenti-kafedri-sistem-ta-tehnologiy-kiberbezpeki-proyshli-specializovaniy-kurs-vid-ibm_kafedra-informaciynoi-ta-kibernetichnoi-bezpeki

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

Відповідно до Стратегії розвитку ДУІКТ (https://duikt.edu.ua/uploads/p_949_78903289.pdf), місія Університету — забезпечення якісної освіти, досліджень та інновацій у сфері ІКТ для підготовки конкурентоспроможних фахівців цифрової епохи. Стратегічні напрями охоплюють якість освіти за євростандартами, міжнародну інтеграцію, науку, підтримку молоді, розвиток персоналу, партнерство та безпечне середовище.
Мета ОПП ІКБ повністю узгоджена з цією місією та спрямована на підготовку фахівців для розв'язання дослідницьких і інноваційних завдань у галузі кібербезпеки.
Виконання означених Стратегією завдань у межах реалізації програми забезпечується:
Тісною співпрацею з ІТ-компаніями та держустановами. (https://surl.li/zqonnc).
Формуванням навчальних планів з урахуванням новітніх досягнень ІТ. (https://surl.li/fkaulj).
Залученням студентів до науки через олімпіади та конкурси (https://surl.li/bkcxxh).
Підготовкою магістрів із дотриманням принципів безбар'єрності, інклюзивності та академічної доброчесності (https://surli.cc/qflpur; https://surl.li/wjxykq; https://surl.li/zbucge).
Зворотний зв'язок та вдосконалення якості підготовки реалізуються через https://duikt.edu.ua/uploads/p_1352_68098088.pdf ; https://duikt.edu.ua/uploads/p_1352_35046282.pdf, https://surl.li/dlpnhk.

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

Зміст програми відображає передові напрями досліджень кафедри. Зокрема, у навчальний процес та тематику кваліфікаційних робіт активно інтегруються такі сучасні тенденції, як архітектура нульової довіри, застосування машинного навчання для виявлення мережевих вторгнень.
Здобувачі вищої освіти регулярно апробують свої наукові здобутки на фахових науково-практичних конференціях організованих кафедрою та університетом, які враховують тенденції розвитку науки та спеціальності (https://surl.li/xesqxd; https://surl.li/ohxonm; https://surl.li/mzwidfздобувачі-магістри публікують наукові праці під керівництвом, що підтверджує актуальність їхніх досліджень.
Здобувачі приймають участь у спеціально організованих заходах, а саме:
- відкритих заняттях, де демонструють прикладні навички https://surl.li/yrejsa;
- спеціалізованих курсах від провідних вендорів https://surli.cc/nbyiqi;
- профільних змаганнях у форматі Capture the Flag https://surl.lt/lyiyft.
Під час таких заходів, а також за результатами участі здобувачів у турнірах та спілкування зі стейкхолдерами, регулярно обговорювались пропозиції щодо вдосконалення ОПП. Зокрема, акцентувалась увага на посиленні таких програмних результатів навчання: РН7: порушувалось питання імплементації кращих світових стандартів і корпоративних практик управління безпекою при роботі з рішеннями провідних галузевих компаній; РН17: дискутувались шляхи розширення навичок щодо автономного і самостійного навчання у сфері кібербезпеки та захисту інформації.

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

Мета освітньої програми та програмні результати (РН) повністю відображають актуальні потреби ринку праці, що підтверджено позитивними рецензіями стейкхолдерів. Компетентності магістрів формуються з урахуванням реальних очікувань роботодавців завдяки залученню партнерів до освітнього процесу.
Галузевий контекст реалізується шляхом тісної співпраці з провідними державними та приватними організаціями галузі. Завдяки рекомендаціям Департаменту Кіберполіції НПУ (Меморандум від 18.03.2021 № 21/ННІЗІ/342), ТОВ «Світ ІТ» (договір від 20.03.19 № 19-0320-1), ТОВ «Євротелеком» (договір від 03.03.2020 № 07/2020) та ТОВ «ІТ Спеціаліст» (договір від 23.01.2020 № 34/1294) було посилено фокус на захисті об’єктів інформаційної діяльності, системах аудиту та моніторингу. Ці галузеві вимоги були безпосередньо враховані при формуванні РН 8, РН 13, РН 14, РН 19 та РН 20.
Регіональний контекст формується на співпраці переважно з комерційними підприємствами та приватними закладами освіти, які провадять професійну дослідницьку діяльність у галузі кібербезпеки та захисту інформації, зокрема Міжнародною Кіберакадемією (договір від 28.10.2019 № 10/2019), Check Point Software Technologies Ltd. Рекомендації цих партнерів були імплементовані у РН 8, РН 11, РН 13, РН 21 та РН 22.
Наявність зазначених договорів і тісна база контактів дозволяють Університету не лише своєчасно оновлювати освітні компоненти під пріоритети ринку, а й забезпечувати бази для проходження практик і проведення спільних наукових досліджень.

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

Так, під час розроблення та періодичного перегляду освітньо-професійної програми (ОПП) «Інформаційна та кібернетична безпека» робочою групою здійснюється системний моніторинг та аналіз передового досвіду провідних вітчизняних закладів вищої освіти. Це дозволяє впроваджувати кращі освітні практики у формування програмних результатів навчання (РН), зберігаючи при цьому унікальний практично-орієнтований фокус нашої ОПП.
Під час оновлення ОПП було проаналізовано відповідні програми інших ЗВО України, зокрема:
КНУ ім. Тараса Шевченка ОНП Кібербезпека https://kbzi.knu.ua/magistr_specialty_125/ .

Київський столичний університет імені Бориса Грінченка ОПП «Безпека інформаційних і комунікаційних систем» https://fitm.kubg.edu.ua/struktura1/kafedry/kafedra-informatsiinoi-ta-kibernetychnoi-bezpeky-im-profesora-volodymyra-buriachka/navchalno-metodychna-robota/obhovorennia-osvitnikh-prohram-ta-proiektiv-osvitnikh-prohram/2295-obhovorennia-osvitnikh-prohram.html.
НУ «Львівська політехніка» ОПП Безпека інформаційних і комунікаційних системhttps://directory-new.lpnu.ua/majors/ikta/8.F5.00.01/19/2026/ua/full
Порівняльний аналіз зазначених ОПП підтвердив, що наша програма структурно та змістовно відповідає загальнонаціональним стандартам і тенденціям підготовки магістрів з кібербезпеки, водночас вирізняючись глибокою орієнтацією на потреби ринку праці завдяки залученню вендорів та IT-компаній.

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

Мета ОПП «Інформаційна та кібернетична безпека» та її програмні результати навчання (РН) системно формуються з урахуванням передового досвіду іноземних закладів вищої освіти, дослідницьких інститутів, європейських стандартів якості та міжнародних корпоративних практик у сфері кібербезпеки. Це забезпечує інтеграцію української освіти до глобального ринку праці та світового наукового простору.
З метою запозичення кращих закордонних практик підготовки фахівців з інформаційної та кібербезпеки вивчено досвід реалізації магістерських програм у провідних іноземних ЗВО:
Mississippi State University (США) (програма The Master of Science in Cyber Security and Operations (MS CYSO), https://www.cse.msstate.edu/grad/ms-cyso/) – на основі досвіду цієї програми було сформовано РН 2, РН 16 та РН 23.
Capitol Technology University (США) (курс Master of Science in Cybersecurity, https://www.captechu.edu/degrees-and-programs/masters-degrees/cybersecurity-ms) – аналіз освітніх складових дав підстави для коригування та посилення РН 9 та РН 10.
Dakota State University (США) (програма Cyber Defense Master of Science (MSCD), https://dsu.edu/programs/mscd/index.html) – з урахуванням змісту й очікуваних результатів цієї програми було вдосконалено обов'язкову дисципліну «Корпоративна та професійна етика в кібербезпеці» (ОК1), що забезпечило краще формування РН 15 та РН 16.
При формуванні освітніх компонентів було також ретельно вивчено та успішно впроваджено досвід Канадського інституту кібербезпеки (Canadian Institute for Cybersecurity). Зокрема, їхні передові підходи до методології та організації дослідницької діяльності були безпосередньо імплементовані в обов'язкову дисципліну «Проведення наукових досліджень в кібербезпеці» (ОК3). Це дозволило суттєво посилити підготовку здобувачів до виконання самостійних досліджень за міжнародними стандартами (РН 3, РН 20).
При розробці та вдосконаленні освітньої програми безпосередньо враховано досвід європейських університетів через реалізацію міжнародних грантових проєктів. У програму впроваджені результати масштабного проєкту Європейського союзу Tempus (№544455-TEMPUS-1-2013-1-SE-TEMPUS-JPCR) «Освіта експертів наступного покоління в галузі кібербезпеки: нова програма магістерської програми ЄС». Завдяки цьому результати навчання адаптовані до актуальних моделей підготовки європейських магістрів.

2. Структура та зміст освітньої програми

Яким є обсяг ОП (у кредитах ЄКТС)?

90

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

65

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

25

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

Компоненти освітньо-професійної програми повністю забезпечують реалізацію поставленої мети та структурно відповідають предметній області спеціальності F5 «Кібербезпека та захист інформації» для магістерського рівня. Базові обов'язкові компоненти ОПП, зокрема «Проведення наукових досліджень в кібербезпеці» (ОК3), «Прикладна загальна теорія систем кібербезпеки» (ОК6) та «Управління проектами інформаційної безпеки» (ОК7), забезпечують опанування теоретичних засад системного аналізу, теорії управління ризиками та фундаментальних знань у галузі кібербезпеки. Процес вивчення цих компонентів формує навички використання системного підходу до вирішення професійних та наукових завдань.
Дисципліни професійної підготовки, такі як «Технології забезпечення безпеки мережевої інфраструктури» (ОК8) та «Технології виявлення уразливостей мережевих ресурсів» (ОК9), спрямовані на вивчення технологій захисту інформаційних ресурсів, методів виявлення кіберзагроз та підтримки інфраструктури кіберзахисту, що є ключовими

об'єктами вивчення спеціальності.
Компоненти ОПП, спрямовані на поглиблене оволодіння окремими аспектами кібербезпеки для їх теоретичного осмислення та практичного застосування у розрізі індивідуальної тематики наукових досліджень, вільно обираються здобувачами (дисципліни ВК 1 – ВК 5 загальним обсягом 25 кредитів) з відповідного каталогу освітніх компонентів вільного вибору Університету: https://duikt.edu.ua/ua/2994-katalog-osvitnih-komponentiv-vilnogo-viboru.
У результаті аналізу освітньої програми можна зробити висновок, що її зміст повною мірою охоплює всі об'єкти вивчення предметної області (сучасні процеси дослідження, інформаційні системи, інфраструктури об'єктів та системи управління кібербезпекою). Здобувачі засвоюють необхідні знання й навички з метою якісного проведення наукових досліджень, практичного впровадження інноваційних результатів та ефективного вирішення інженерно-технічних і управлінських завдань у сфері кібербезпеки.

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

Основним інструментом формування індивідуальної освітньої траєкторії (ІОТ) є дисципліни вільного вибору (ВК 1 – 5), загальний обсяг яких становить 25 кредитів ЄКТС. Це складає понад 27% від загального обсягу освітньої програми , що повністю відповідає законодавчим вимогам.
Формування ІОТ базується на індивідуальному виборі кожного студента та регламентується внутрішньою нормативною базою ДУІКТ, зокрема:
Положенням про організацію освітнього процесу в ДУІКТ (https://duikt.edu.ua/uploads/p_447_49109699.pdf);
Положенням про формування індивідуальних освітніх траєкторій здобувачів вищої освіти у ДУІКТ (https://duikt.edu.ua/uploads/p_447_22834975.pdf);
Положенням про порядок організації права на академічну мобільність (https://duikt.edu.ua/uploads/p_447_36289291.pdf).
Формування ІОТ базується на індивідуальному виборі кожного студента-магістра, що передбачено
Положенням про організацію освітнього процесу в ДУІКТ https://duikt.edu.ua/uploads/p_447_49109699.pdf,
Положенням про порядок організації права на академічну мобільність
https://duikt.edu.ua/ua/447-polozhennya-normativni-dokumenti,
Положенням про формування індивідуальних освітніх траєкторій здобувачів вищої освіти у Державному університеті інформаційно-комунікаційних технологій
https://duikt.edu.ua/uploads/p_447_22834975.pdf .
Додатковим інструментом розширення ІОТ є визнання результатів неформальної освіти (https://duikt.edu.ua/uploads/p_447_35048489.pdf), що дозволяє офіційно зараховувати здобуті студентами сертифікатиІТ-компаній як складову оцінювання в межах ОП.

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

Вибір навчальних дисциплін здобувачами освітньо-професійної програми «Інформаційна та кібернетична безпека» регламентовано Положенням про формування індивідуальних освітніх траєкторій здобувачів вищої освіти у ДУІКТ (https://duikt.edu.ua/uploads/p_447_22834975.pdf).
Положення містить основні вимоги щодо здійснення права вибору відповідно до пункту 15 частини першої статті 62 Закону України «Про вищу освіту». Для магістрів нашої ОПП процес реалізації цього права є прозорим і структурованим у чотири етапи:
• Перший крок (Ознайомлення): На початку навчального року здобувачі знайомляться на офіційному сайті з переліком вибіркових компонентів та їхніми силабусами, які підготовлені кафедрою систем та технологій кібербезпеки, іншими кафедрами Навчально-наукового інституту кібербезпеки та захисту інформації (ННІКБЗІ), а також іншими інститутами Університету.
• Другий крок (Вибір та консультація): Після аналізу запропонованих матеріалів та відповідно до особистих кар'єрних цілей, здобувачі самостійно формують перелік вибіркових дисциплін для свого індивідуального навчального плану. На цьому етапі студенти мають можливість звернутися за фаховою консультацією безпосередньо до гаранта освітньої програми або кураторів від кафедри.
• Третій крок (Організація): Навчальна частина ННІКБЗІ опрацьовує заяви студентів, організовує роботу з формування списків навчальних груп для вивчення обраних дисциплін та формує відповідний розклад занять.
• Четвертий крок (Затвердження): Обрані здобувачем вибіркові компоненти ОПП офіційно вносяться до його індивідуального навчального плану.
В освітній програмі «Інформаційна та кібернетична безпека» на дисципліни вільного вибору (ВК 1 – ВК 5) виділено 25 кредитів ЄКТС із загальних 90 кредитів. Це складає понад 27% від загального обсягу ОПП, що гарантовано перевищує законодавчо встановлений мінімум у 25%.
Перелік дисциплін для вибору наведено у загальноуніверситетському Каталозі освітніх компонентів вільного вибору (https://duikt.edu.ua/ua/2994-katalog-osvitnih-komponentiv-vilnogo-viboru). Здобувачі ОПП мають повне право вільно обирати дисципліни не лише за своєю спеціальністю, а й ті, що запропоновані іншими кафедрами Університету, за погодженням з директором навчально-наукового інституту, що дозволяє максимально гнучко формувати власну освітню траєкторію.

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

За ОПП передбачено проходження студентами науково-педагогічної практики (6 кредитів), яке регламентується Положенням про проведення практики в ДУІКТ https://duikt.edu.ua/uploads/p_447_23214805.pdf , програмами практики для спеціальності F5 «Кібербезпека та захист інформації» галузі знань F «Інформаційні технології».
Загальні засади організації, проведення, звітування й оцінювання результатів проходження науково-педагогічної

(НПП), науково-дослідної (НДП) і переддипломної практики (ПП) студентів магістратури визначені у силабусах (програмах).
Базою НПП є кафедри ННІКБЗІ ДУІКТ. НПП проводиться під керівництвом досвідчених викладачів кафедри.
https://surl.li/djtzme
https://surl.li/fjsxgl
https://surl.li/glgwgs
Базою НДП і ПП може бути компанія-партнер кафедри або, в разі самостійного обрання здобувачем місця практики, підприємства й організації муніципального, державного та корпоративного управління.

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

Невід'ємною складовою підготовки сучасного фахівця з КБ є навички soft skills, які допомагають успішно працювати в команді та спілкуватися із замовниками. ОПП ІКБ забезпечує набуття таких соціальних навичок через цикл дисциплін загальної та професійної підготовки. Зокрема, програма дозволяє студенту набути:
Навичок етичного поводження та ефективної комунікації: дис-ни «Корпоративна та професійна етика в кібербезпеці» (РН1, 15, 16, 17, 18) та «Наукова комунікація та технічне документування в кібербезпеці» (РН1, 2, 17, 20, 23).
Здатності спілкуватися іноземною мовою в діловому середовищі: «Англійська мова для ділової комунікації» (РН1, РН15).
Здатності до автономного навчання, організації часу та психологічної роботи з колективом: «Педагогіка та психологія у вищій школі» (РН2, РН17, РН18) та «Проведення наукових досліджень в кібербезпеці» (РН3, 17, 19, 20, 23).
Крім того, розвиток лідерства, навичок командної роботи й ефективної взаємодії в проєктній групі забезпечується під час вивчення фахової дисципліни «Управління проектами інформаційної безпеки» (РН4, 8, 9, 14, 17, 20). Ці освітні компоненти дозволяють випускнику успішно доносити власні висновки до фахівців і нефахівців , працювати в колективі та приймати обґрунтовані рішення в складних умовах.
Все це дозволяє випускнику на належному рівні проводити наукові дослідження, реалізувати отримані наукові результати на практиці, ефективно бути застосовані в дослідницькій, управлінській, освітній, бізнесовій та інших дисциплінарно-професійних полях.

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

Зміст освітньо-професійної програми «Інформаційна та кібернетична безпека» має чітку логічну структуру, що складається з циклів загальної і професійної підготовки та відображена у структурно-логічній схемі ОПП.
У рамках циклу загальної підготовки (ОК1–ОК5) здобувачі оволодівають навичками наукової, етичної, комунікаційної та викладацької діяльності. До цього блоку належать такі компоненти, як «Педагогіка та психологія у вищій школі», «Проведення наукових досліджень в кібербезпеці», «Наукова комунікація та технічне документування в кібербезпеці» та «Корпоративна та професійна етика в кібербезпеці».
Цикл професійної та практичної підготовки (ОК6–ОК13) спрямований на формування ключових фахових компетентностей магістра з кібербезпеки. Він охоплює глибокі знання, передбачені компонентами «Прикладна загальна теорія систем кібербезпеки», «Технології забезпечення безпеки мережевої інфраструктури», «Технології виявлення уразливостей мережевих ресурсів» та «Управління проектами інформаційної безпеки».
Логічна послідовність вивчення теоретичних дисциплін, підкріплена проходженням науково-педагогічної, науково-дослідної та переддипломної практик, формує цілісну систему, яка забезпечує досягнення заявленої мети та всіх програмних результатів навчання (РН1–РН23) і завершується виконанням кваліфікаційної роботи.

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

Підхід до співвіднесення обсягу освітніх компонентів ОПП «Інформаційна та кібернетична безпека» із фактичним навантаженням здобувачів базується на забезпеченні досяжності програмних результатів навчання та адекватності розподілу кредитів ЄКТС. Відповідно до Положення про організацію освітнього процесу в ДУІКТ (https://duikt.edu.ua/uploads/p_447_49109699.pdf), загальний бюджет навчального часу для магістрів становить 90 кредитів ЄКТС (2700 годин).
Розподіл часу здійснюється з урахуванням оптимального балансу навантаження: орієнтовно 24,4% (660 годин) відводиться на аудиторні заняття, а 75,6% (2040 годин) - на самостійну роботу здобувачів.
Загальний обсяг часу, необхідного на виконання всіх видів семестрових завдань, підготовку до практичних занять та виконання кваліфікаційної роботи (ОК13), не перевищує кількості передбачених навчальним планом годин на самостійну роботу. Ефективність самостійної роботи забезпечується комплексною системою навчально-методичних засобів. Підручники, конспекти лекцій та методичні рекомендації до кожної дисципліни знаходяться у вільному доступі в системі дистанційного навчання (електронній бібліотеці) університету. Крім того, навчально-методичні матеріали з усіх освітніх компонентів розміщені на електронних платформах викладачів Google Classroom), що забезпечує безперервний доступ здобувачів до контенту протягом усього періоду навчання.

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

Структура ОПП гарантує високу практикоорієнтованість через поєднання теорії з інтенсивною практикою та використанням спеціалізованих лабораторій. Набуття практичних умінь науково-педагогічної та дослідницької діяльності забезпечується компонентами «Педагогіка та психологія у вищій школі» (ОК2), «Проведення наукових досліджень в кібербезпеці» (ОК3) та проходженням науково-педагогічної (ОК10), науково-дослідної (ОК11) і переддипломної (ОК12) практик.
У рамках циклу професійної підготовки здобувачі відпрацьовують прикладні фахові компетентності через дисципліни: «Технології забезпечення безпеки мережевої інфраструктури» (ОК8), «Технології виявлення уразливостей мережевих ресурсів» (ОК9), «Управління проектами інформаційної безпеки» (ОК7) та «Прикладна загальна теорія систем кібербезпеки» (ОК6). Ці компоненти спрямовані на забезпечення потреб ринку праці при вирішенні реальних професійних задач.
Навчання за дуальною формою регламентується Положенням про дуальну форму здобуття вищої освіти у ДУІКТ (https://duikt.edu.ua/uploads/p_447_91663915.pdf). Хоча безпосередньо за цією ОПП підготовка за дуальною формою наразі не здійснюється, подолання розриву між теорією і практикою забезпечується активним залученням до освітнього процесу та розробки програми професіоналів-практиків і роботодавців (зокрема, ТОВ «Світ ІТ» та інших), впровадженням сертифікаційних курсів і тренінгів від компаній-партнерів і і працевлаштування випускників ОПП на посадах НПП в Університеті (А. Бойко, Д. Шулімова, В. Марченко).

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

ОПП ІКБ забезпечує набуття здобувачами актуальних професійних навичок (реагувата на інциденти) та соціальних навичок (soft skills: робота в команді, комунікація), що дозволяє випускникам зробити вагомий внесок у досягнення глобальних цілей сталого розвитку до 2030 року. Зокрема, реалізуються такі цілі:
Ціль 4 (Якісна освіта): Програма ґрунтується на концепції навчання впродовж життя, формує навички автономного навчання та готує магістрів до науково-педагогічної діяльності.
Ціль 8 (Гідна праця та економічне зростання): Набуття фахових навичок аналізу вразливостей і реагування на кіберінциденти спільно з вивченням професійної етики забезпечує випускникам стійку та продуктивну зайнятість.
Ціль 9 (Промисловість, інновації та інфраструктура): Здатність розробляти та супроводжувати системи КБ на оОКІ і провадити інноваційну дослідницьку діяльність сприяє створенню стійкої інформаційно-комунікаційної інфраструктури.
Ціль 5 (Забезпечення гендерної рівності, розширення прав і можливостей усіх жінок та дівчат): Програма активно сприяє подоланню гендерних стереотипів у сфері ІТ та кібербезпеки та заохоченню студенток до участі у профільних змаганнях і воркшопах (зокрема, активна участь керівництва кафедри у національному воркшопі «Шлях жінок у кібербезпеці», що слугує прикладом для здобувачок (https://surl.li/vrqcyd).
Підготовка висококваліфікованих фахівців за цією ОПП комплексно підвищує рівень захищеності інформаційних ресурсів та інфраструктури України, сприяючи безпечному і сталому розвитку цифрової економіки.

3. Доступ до освітньої програми та визнання результатів навчання

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

Інформація про правила прийому на навчання для здобуття освітнього ступеня магістра містяться за посиланнями:
Правила прийому до ДУІКТ у 2026 році
https://duikt.edu.ua/uploads/p_108_54084336.pdf
Вступ в магістратуру
https://duikt.edu.ua/ua/1866-vstup-v-magistraturu-priymalna-komisiya
Абітурієнти, які закінчили бакалаврат у 2024-2026 роках, вступають в магістратуру на загальних підставах за результатами ЄДКІ та ЄВІ. Абітурієнти, які закінчили бакалаврат раніше 2024 року, вступають в магістратуру за результатами ЄВІ та ЄФВВ.
Усі питання, пов'язані зі вступом до Університету, вирішуються Приймальною комісією на її засіданнях. Рішення Приймальної комісії оприлюднюються на офіційному веб-сайті (https://duikt.edu.ua/ua/363-vstup-2026-priymalna-komisiya) в день прийняття або не пізніше наступного дня після прийняття відповідного рішення.

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

Нормативним документом для організації вступної кампанії до ДУІКТ, у тому числі на освітньо-професійну програму ІКБ, є Правила прийому до ДУІКТ у 2026 році (https://surl.li/yqqaqw), які детально визначають умови доступу до навчання.
Правила прийому повністю враховують специфіку магістерського рівня та особливості даної ОПП через такі вимоги до вступників:
Передумови здобуття освіти. Наявність ступеня бакалавра, магістра або освітньо-кваліфікаційного рівня спеціаліста, причому правила враховують можливість вступу осіб як за спеціальністю «Кібербезпека», так і з інших

спеціальностей (через проходження необхідних фахових вступних випробувань, що передбачено Стандартом вищої освіти та реалізується приймальною комісією).
Форма оцінювання компетентностей. Відповідно до правил на магістерський рівень, вступники подають результати єдиного вступного іспиту (ЄВІ) з іноземної мови та єдиного фахового вступного випробування (ЄФВВ), що гарантує наявність у здобувачів базових знань, необхідних для успішного засвоєння спеціальних фахових компетентностей ОПП (КФ1–КФ10).
Спеціальні умови та категорії. Правила чітко регламентують перелік необхідних документів для конкурсного відбору та особливості вступу для різних категорій здобувачів (зокрема військовослужбовців), забезпечуючи прозорий і регламентований відбір на програму.

Яким документом ЗВО регулюється питання визнання результатів навчання та кваліфікацій, отриманих на інших освітніх програмах? Яким чином забезпечується доступність цієї процедури для учасників освітнього процесу?

Питання визнання результатів навчання, отриманих в інших ЗВО чи через неформальну освіту (зокрема здобуті сертифікати компаній-партнерів у межах ОПП «Інформаційна та кібернетична безпека»), регулюється такими внутрішніми документами ДУІКТ:
Положенням про організацію освітнього процесу у ДУІКТ (https://duikt.edu.ua/uploads/p_447_49109699.pdf);
Положенням про порядок організації права на академічну мобільність (https://duikt.edu.ua/uploads/p_447_36289291.pdf);
Положенням про формування індивідуальних освітніх траєкторій здобувачів вищої освіти – зокрема розділом щодо порядку зарахування та перезарахування кредитів (https://duikt.edu.ua/uploads/p_447_22834975.pdf);
Положення про неформальну та інформальну освіту у Державному університеті інформаційно-комунікаційних технологій (https://duikt.edu.ua/uploads/p_447_35048489.pdf).
Доступність та прозорість цієї процедури для учасників освітнього процесу забезпечуються постійним вільним доступом до всієї нормативної бази на офіційному сайті Університету, а також обов'язковим консультуванням здобувачів гарантом та викладачами кафедри під час формування індивідуальних навчальних планів, оформлення академічної мобільності чи зарахування сертифікатів міжнародних вендорів (IBM, Cisco, Huawei), що підтримують нашу освітню програму.

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

Прикладом практичного застосування цих процедур є успішна участь представників і здобувачів ДУІКТ у програмах міжнародної академічної мобільності з подальшим офіційним визнанням здобутих результатів і отриманням сертифікатів європейського зразка (наприклад, стажування та освітня мобільність в Університеті Національної комісії з питань освіти у Кракові (https://surl.li/aeksjl).
На підставі успішного проходження таких програм і надання офіційних документів (сертифікатів, академічних довідок із переліком кредитів ЄКТС та кредити/дисципліни), університетською комісією приймаються рішення щодо перезарахування відповідних освітніх компонентів, що забезпечує прозорість процедури та повну інтеграцію європейського досвіду в індивідуальні освітні траєкторії здобувачів.

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

Визнання результатів навчання, отриманих здобувачем за програмами неформальної освіти, регулюються Положенням про неформальну та інформальну освіту https://duikt.edu.ua/uploads/p_447_35048489.pdf та Положенням про порядок перезарахування результатів навчання https://duikt.edu.ua/uploads/p_949_73284553.pdf?file=p_949_73284553.pdf.
До результатів навчання, які зараховуються при виконанні ОПП, враховуючи особливості спеціальності F5 Кібербезпека та захист інформації в межах галузі F Інформаційні технології, відносяться результати отримані, зазвичай, у формальній освіті.
Результати навчання здобувачів освітнього рівня магістра, отриманих у неформальній освіті, визнаються у частині виконання ними професійної складової індивідуального плану здобувача.

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

Застосування практики визнання результатів навчання, отриманих у неформальній освіті, для здобувачів даної ОПП не було

4. Навчання і викладання за освітньою програмою

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

Освітній процес на освітньо-професійній програмі ІКБсуворо відповідає вимогам чинного законодавства України, зокрема Закону України «Про вищу освіту» (https://zakon.rada.gov.ua/laws/show/1556-18#Text) у частині конкурсного відбору, дотримання форм здобуття освіти та організації навчального процесу. Відповідно до Положення про організацію освітнього процесу у ДУІКТ (https://duikt.edu.ua/uploads/p_447_49109699.pdf), підготовка магістрів здійснюється за денною та заочною формами за кошти державного бюджету або фізичних/юридичних осіб.
Методи, засоби та технології навчання і викладання безпосередньо сприяють досягненню мети та програмних результатів навчання (РН1–РН23) завдяки поєднанню класичних і новітніх підходів:
Види занять. Основними видами навчальних занять є лекції, практичні, лабораторні, семінарські, індивідуальні заняття та консультації, зміст яких детально розписано в силабусах дисциплін.
Практична інфраструктура. Засоби навчання включають спеціалізовані навчальні лабораторії Університету (реагування на кіберінциденти SOC з рішеннями IBM QRadar та Tenable, захисту кінцевих точок Eset, мережевої безпеки Cisco та Huawei), що гарантує набуття прикладних фахових компетентностей.
Інноваційні методики. Застосовуються інтерактивні методи, робота з кейсами від партнерів кафедри, участь у хакатонах і CTF-змаганнях, а також використання сертифікатних курсів вендорів, що повністю відображено в освітній програмі (https://surl.li/cxrcco) та силабусах освітніх компонентів кафедри (https://surl.lt/tfsklv).

Продемонструйте, яким чином методи, засоби та технології навчання і викладання відповідають вимогам студентоцентрованого підходу. Яким є рівень задоволеності здобувачів вищої освіти методами навчання і викладання відповідно до результатів опитувань?

Студентам ОПП забезпечено постійний доступ до підручників, навчальних посібників, конспектів лекцій та інших навчально-методичних матеріалів, які розміщені в електронній бібліотеці Університету й кафедри за посиланням https://duikt.edu.ua/ua/lib/1/category/2122. Доступ є відкритим упродовж усього терміну навчання.
Форми і методи навчання й викладання відповідають вимогам студентоцентрованого підходу, який забезпечується вибором індивідуальних завдань з окремих освітніх компонентів, в тому числі вибіркових https://duikt.edu.ua/ua/2080-katalog-osvitnih-komponentiv-vilnogo-viboru-studentami-navchannya.
Зворотний зв'язок зі студентами, який здійснюється систематично шляхом безпосереднього спілкування з викладачами, дозволяє науково-педагогічним працівникам коригувати власну стратегію викладання й обирати оптимальні методи навчання для підвищення рівня засвоєння здобувачами необхідних знань і навичок, а також їх задоволеності якістю і змістом навчання https://duikt.edu.ua/ua/1352-rezultati-opituvan-vnutrishnya-sistema-zabezpechennya--yakosti-vischoi-osviti-ta-osvitnoi-diyalnosti.
Як свідчать опитування рівень задоволеності здобувачів вищої освіти та випускників методами навчання і викладання досягає до 90% (https://duikt.edu.ua/ua/3142-opituvannya-uchasnikiv-osvitnogo-procesu-diyalnist-kafedri)

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

Відповідність методів, засобів та технологій навчання і викладання на освітній програмі «Інформаційна та кібернетична безпека» принципам академічної свободи гарантується внутрішніми нормативними документами Університету. Зокрема, згідно з пунктом 18 Положення про організацію освітнього процесу в ДУІКТ (https://duikt.edu.ua/uploads/p_447_49109699.pdf), науково-педагогічні, наукові та педагогічні працівники мають законне право на академічну свободу, що передбачає вільний вибір форм, методологій, методів і засобів викладання, які забезпечують високу якість навчання та реалізуються через розроблені ними силабуси освітніх компонентів.
Принцип академічної свободи викладання тісно поєднується з інтересами здобувачів вищої освіти магістерського рівня, оскільки викладачі застосовують особистісно орієнтований підхід з урахуванням рівня підготовки та інтересів студентів. Зі свого боку, академічні свободи здобувачів ОПП виявляються у можливості вільного вибору освітньої траєкторії через дисципліни вільного вибору, самостійному обранні наукового керівника та пріоритетної тематики для майбутнього кваліфікаційного дослідження, а також у захищеності освітнього процесу від стороннього впливу

Опишіть, яким чином і у які строки учасникам освітнього процесу надається інформація щодо цілей, змісту та очікуваних результатів навчання, порядку та критеріїв оцінювання у межах окремих освітніх компонентів

Освітніми ресурсами ДУІКТ є офіційний сайт, на якому зосереджена уся інформація стосовно освітньої діяльності Університету, в тому числі й щодо ОПП, що акредитується.
Загальна мета, структура та програмні результати ОПП розміщені у вільному доступі на офіційній сторінці кафедри систем та технологій кібербезпеки: https://surl.li/fygvts .
Здобувачі вищої освіти мають доступ до навчально-методичних матеріалів (конспекти лекцій, методичних вказівок до практичних/лабораторних/семінарських занять, тестів) з усіх освітніх компонентів ОПП у Google Class, дистанційні заняття проводяться з використанням Google Meet або ZOOM.
На перших лекційних та організаційних заняттях кожен викладач презентує освітній компонент, детально висвітлюючи його цілі, завдання, зміст, очікувані РН, форми контролю, а також чіткі критерії та шкалу оцінювання навчальних досягнень здобувачів.
Деталізовані силабуси всіх освітніх компонентів, конспекти лекцій, завдання для самостійної роботи та критерії оцінювання публікуються на платформах дистанційного навчання (Google Classroom) перед початком вивчення дисципліни, що забезпечує постійний відкритий доступ здобувачів до всієї необхідної інформації протягом усього семестру.

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

Під час реалізації освітньо-професійної програми «Інформаційна та кібернетична безпека» поєднання навчання і наукових досліджень забезпечується через інтеграцію освітнього процесу з практичною лабораторною базою, залученням здобувачів до прикладних розвідок та активною публікаційною діяльністю.
Навчальні заняття та дослідження проводяться у спеціалізованих високотехнологічних лабораторіях кафедри систем та технологій кібербезпеки: Центрі управління інформаційною та кібербезпекою (SOC), Навчальній лабораторії реагування на кіберінциденти, Навчальній лабораторії захисту кінцевих точок та Навчальній лабораторії мережевої безпеки (https://surl.li/yhuxfp). Це дозволяє проводити експерименти, моделювати кібератаки та досліджувати вразливості.
Здобувачі магістратури регулярно представляють результати власних досліджень на щорічних усеукраїнських конференціях, зокрема «Цифрова трансформація кібербезпеки» (https://duikt.edu.ua/uploads/p_3086_30075970.pdf) та «Актуальні проблеми кібербезпеки» (https://duikt.edu.ua/uploads/p_2779_58326207.pdf).
Студенти публікують результати кваліфікаційних досліджень у фахових виданнях ДУІКТ та провідних вітчизняних журналах («Сучасний захист інформації», «Телекомунікаційні та інформаційні технології» (https://surl.li/nmlhnf), «Кібербезпека: освіта, наука, техніка»). Приклади успішних публікацій у співавторстві з викладачами кафедри:
Гайдур Г. І., Гахов С. О., Бригинець А. А. Виявлення мережевих аномалій з використанням алгоритмів нейронних мереж.
Гайдур Г. І., Бригинець А. А. (2024). Захист конфіденційних даних у снепшотах Amazon Elastic Block Store. Сучасний захист інформації, 1(57), 15–21.
Гайдур Г., Марченко В., Борсуковський Ю., Дмітрієв В., Царьова С. (2025). DLP-система як компонент протидії інсайдерським загрозам конфіденційності інформації. Кібербезпека: освіта, наука, техніка, 2(30), 583–592.
Найвищий рівень поєднання навчання і досліджень демонструють статті магістрантів у співавторстві з викладачами у престижних міжнародних виданнях, що індексуються у базі Scopus:
Bryhynets A., Haidur H., Gakhov S., Marchenko V. Quantitative WEB Application Vulnerability Assessment using SAST Methodology. International Journal of Computing, 2025, 24(1), pp. 163–170.
Bryhynets A., Klymenko Y., Haidur H., Gakhov S., Marchenko V. (2025). Random Forest Approach for pdf Malware Detection. Baltic Journal of Modern Computing, 13(3), 694–719.
Такий підхід гарантує, що виконання обов'язкових компонентів програми (зокрема дисципліни «Проведення наукових досліджень в кібербезпеці», науково-дослідної практики та кваліфікаційної роботи) перетворюється на реальний внесок здобувачів у розвиток галузі інформаційної та кібернетичної безпеки ще до завершення навчання.

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

Зміст освітніх компонентів освітньо-професійної програми «Інформаційна та кібернетична безпека» регулярно оновлюється на основі новітніх наукових досягнень, результатів держбюджетних і госпдоговірних науково-дослідних робіт (НДР), а також практичного досвіду викладачів як розробників національних професійних стандартів.
Так, протягом 2021-2026 рр. на кафедрі виконувалися науково-дослідні роботи:
НДР за темою: «Розробка методів та засобів підвищення живучості інформаційно-комунікаційних систем в умовах впливу кібернетичних атак» (реєстраційний номер НДР шифр «Живучість К14» РК №0114U000391);
НДР за темою: «Методологія виявлення шкідливих процесів в інформаційних системах (реєстраційний номер НДР 0121U113613);
НДР «Розробка науково-методичних рекомендацій виявлення шкідливих процесів в інформаційній системі організації» (ТОВ «АЛЬФА-МЕТАЛ», м. Київ).
Отримані теоретичні та практичні моделі виявлення шкідливої активності і забезпечення живучості систем безпосередньо увійшли до змістових модулів таких освітніх компонентів, як «Прикладна загальна теорія систем кібербезпеки» (ОК6), «Проведення наукових досліджень в кібербезпеці» (ОК3) та «Технології виявлення уразливостей мережевих ресурсів» (ОК9).
Викладачі кафедри виступали безпосередніми розробниками базових державних професійних стандартів у галузі кібербезпеки, серед яких:
«ФАХІВЕЦЬ З ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ» https://register.nqa.gov.ua/uploads/0/572-fahivec_z_tehnicnogo_zahistu_informacii_v_2.pdf ;
«ФАХІВЕЦЬ З ОЦІНКИ ЗАХОДІВ ЗАХИСТУ ІНФОРМАЦІЇ (КІБЕРБЕЗПЕКИ)» https://register.nqa.gov.ua/uploads/0/579-fahivec_z_ocinki_zahodiv_zahistu_informacii_kiberbezpeki_v_2.pdf ;
«ФАХІВЕЦЬ З КРИПТОГРАФІЧНОГО ЗАХИСТУ» https://register.nqa.gov.ua/uploads/0/569-fahivec_z_kriptograficnogo_zahistu_informacii_v_2.pdf ;
«ФАХІВЕЦЬ З ПЛАНУВАННЯ ПОЛІТИКИ ТА СТРАТЕГІЇ КІБЕРБЕЗПЕКИ» https://cip.gov.ua/ua/news/proyekt-profesiinogo-standartu-fakhivec-z-planuvannya-politiki-ta-strategiyi-kiberbezpeki;
«ФАХІВЕЦЬ З РЕАГУВАННЯ НА ІНЦИДЕНТИ КІБЕРБЕЗПЕКИ»;
«ФАХІВЕЦЬ ІЗ КІБЕРДОСЛІДЖЕНЬ ТА РОЗРОБОК СИСТЕМ БЕЗПЕКИ» https://cip.gov.ua/ua/news/proyekt-profesiinogo-standartu-fakhivec-iz-kiberdoslidzhen-ta-rozrobok-sistem-bezpeki;
«АНАЛІТИК ЗАГРОЗ БЕЗПЕКИ».
Положення та трудові функції, закладені в ці національні стандарти, були повною мірою імплементовані в ОПП.
Окрім цього, розроблені за результатами НДР кафедри рекомендації використовуються НПП під час консультування фахівців компаній-партнерів, які є стейкхолдерами та надають офіційні рецензії й відгуки на освітню програму «Інформаційна та кібернетична безпека».

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

Навчання, викладання та наукові дослідження в межах ОПП тісно інтегровані з процесами інтернаціоналізації діяльності ДУІКТ та реалізуються через такі ключові напрями як міжнародна академічна мобільність студентів і викладачів, співпраця зі світовими ІТ-вендорами, участь у глобальних проєктах та конференціях.
Здобувачі магістратури отримують постійну консультативну підтримку щодо участі у програмах міжнародного обміну (зокрема Erasmus+). Яскравим прикладом реалізації такої мобільності є успішне стажування та навчання здобувачки магістратури з кібербезпеки Антоніни Корж в Університеті Національної комісії з питань освіти у Кракові з отриманням сертифікатів європейського зразка (https://surl.li/mnttnz). Викладачі кафедри також активно проходять міжнародні стажування (https://surl.li/blmsyn).
У межах викладання та практичної підготовки студенти ОПП залучаються до заходів і сертифікаційних програм провідних міжнародних компаній – CISCO, IBM та HUAWEI.
https://surl.li/izmaos
https://surl.li/mernqc.
Будучи базою для діяльності організацій світового рівня (ДУКТ є членом Міжнародного союзу електрозв'язку – МСЕ), університет щорічно проводить міжнародні науково-практичні конференції за участю викладачів, аспірантів і магістрантів (https://surl.li/hkzqfm).
Такий комплексний підхід гарантує інтеграцію української освітньої та наукової діяльності до європейського та світового простору вищої освіти й ринку праці.

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?

Форми контрольних заходів у межах освітньо-професійної програми «Інформаційна та кібернетична безпека» утворюють цілісну та прозору систему діагностики, яка дозволяє об'єктивно перевірити досягнення здобувачами всіх заявлених програмних результатів навчання.
Організація та проведення контролю базуються на вимогах Положення про організацію освітнього процесу в ДУІКТ (https://duikt.edu.ua/uploads/p_447_49109699.pdf). Згідно з Положенням, здобувачі зобов'язані відвідувати заняття, проходити практики та всі форми поточного й підсумкового контролю, передбачені навчальним планом.
Контрольні заходи є важливим елементом зворотного зв'язку, що забезпечує перевірку рівня сформованості знань, умінь і навичок на кожному етапі навчання. Залежно від специфіки дисципліни застосовуються усні й письмові опитування, тестування, захист лабораторних та практичних робіт, виконання індивідуальних завдань, а також семестровий контроль у формі екзаменів або заліків.
Реалізація завдань контролю досягається системним підходом до оцінювання вимірюваних результатів навчання та комплексністю застосування різних видів контролю. Оцінювання сформованих компетенцій проводиться під час контрольних заходів, передбачених освітньою програмою та навчальним планом.
Критерії оцінювання знань і навичок розроблені відповідно до законодавства та затверджені у Положенні про організацію освітнього процесу в ДУІКТ.
Також з метою отримання додаткових балів у межах дисциплін студентам зараховуються сертифікати відомих компаній за тематикою курсів.
Кожен вид контролю має чітко визначені форми проведення та критерії оцінювання навчальних досягнень, націлені на визначення здобутого рівня компетентності. Така система контролю дозволяє перевірити досягнення результатів навчання в межах усіх освітніх компонентів програми та об'єктивно їх оцінити. Для стимулювання планомірної роботи здобувачів результати складання іспитів оцінюються за національною (чотирибальною), уніфікованою семибальною шкалою ECTS - A (відмінно), B,C (добре), D,E (задовільно), FX,F (незадовільно), і рейтинговою 100-бальною шкалою, а заліків – за двобальною, семибальною шкалою A,B,C,D,E (зараховано), FX,F (не зараховано) і 100-бальною шкалою. оцінюються за національною чотирибальною шкалою, уніфікованою шкалою ECTS (A, B, C, D, E, FX, F) та рейтинговою 100-бальною шкалою.

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

Забезпечення чіткості та зрозумілості форм контрольних заходів і критеріїв оцінювання навчальних досягнень здобувачів відбувається шляхом ґрунтовного планування заходів контролю кафедрою і викладачем, точного формулювання вимог до їх проведення, встановлення чітких критеріїв оцінювання та постійної роз'яснювальної роботи зі студентами.
Метою проведення контрольних заходів є комплексне оцінювання якості освітньої діяльності в рамках ОПП та досягнення РН.
Оцінювання здобувачів з кожного освітнього компонента здійснюється за 100-бальною шкалою з подальшим переведенням в оцінку за національною шкалою та шкалою ЄКТС, що відповідає загальним принципам організації освітнього процесу в ДУІКТ.
Згідно з програмою, використовуються такі види контролю знань: поточний, рубіжний (модульний, тематичний) та підсумковий контроль.
Поточний контроль проводиться під час аудиторних занять, а його конкретні форми і критерії визначаються в силабусах дисциплін. Результати оцінювання оперативно доводяться до відома студентів і за потреби роз'яснюються викладачами в індивідуальному порядку.

Підсумковий контроль оцінює результати навчання на проміжних або заключному етапах і охоплює семестровий контроль та атестацію.
Детальні критерії оцінювання навчальних досягнень обов'язково описуються в силабусах освітніх компонентів ОПП, де чітко зазначено розподіл балів за виконання конкретних видів робіт (лабораторних, практичних, тестових чи індивідуальних завдань), що гарантує повну прозорість для здобувачів вищої освіти.

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

Інформація про форми контрольних заходів та критерії оцінювання доводиться до здобувачів вищої освіти завчасно і системно.
Викладач знайомить студентів із формами контролю і критеріями оцінювання за кожним освітнім компонентом на першому занятті на початку семестру, детально роз'яснюючи структуру курсу та процедуру перевірки знань і навичок. У подальшому під час проведення кожного контрольного заходу викладач додатково нагадує студентам конкретні вимоги щодо оцінювання.
Строки проведення контрольних заходів чітко регламентуються графіком навчального процесу та розкладом занять на поточний семестр, які затверджуються ректором ДУІКТ і розміщуються на офіційному сайті Університету до початку навчального семестру.

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

Форми атестації здобувачів вищої освіти за освітньо-професійною програмою «Інформаційна та кібернетична безпека» повністю відповідають вимогам Державного стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти, затвердженого наказом МОН України від 18.03.2021 р. № 332.
Засади та порядок проведення атестації визначаються Положенням про атестацію здобувачів вищої освіти та організацію роботи екзаменаційної комісії у ДУІКТ (https://duikt.edu.ua/uploads/p_447_63335719.pdf). Відповідно до вимог стандарту та ОПП, атестація магістрів здійснюється у формі публічного захисту кваліфікаційної роботи.
Графіки захистів та результати роботи екзаменаційної комісії прозоро оприлюднюються на офіційному сайті університету (https://surl.li/zsyysz).
Загальні вимоги до змісту, обсягу та структури кваліфікаційних робіт, порядок їх виконання та організаційного супроводу регламентуються Положенням про кваліфікаційні роботи здобувачів вищої освіти у ДУІКТ. Усі магістерські роботи обов'язково проходять перевірку на наявність академічного плагіату відповідно до Положення про систему запобігання та виявлення академічного плагіату в ДУІКТ (https://duikt.edu.ua/uploads/p_447_61575036.pdf), що гарантує самостійність і високу якість досліджень.
Проведення єдиного державного кваліфікаційного іспиту (ЄДКІ) за результатами навчання за цією ОПП наразі не передбачено чинними нормативно-правовими актами для даної спеціальності.

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

Проведення контрольних заходів у ДУІКТ регламентується Положенням про організацію освітнього процесу (https://duikt.edu.ua/uploads/p_447_49109699.pdf), Положенням про атестацію здобувачів вищої освіти та організацію роботи екзаменаційної комісії у ДУІКТ (https://duikt.edu.ua/uploads/p_447_63335719.pdf) та Положенням про кваліфікаційні роботи здобувачів вищої освіти у ДУІКТ (https://duikt.edu.ua/uploads/p_447_53363267.pdf).
Положенням про кваліфікаційні роботи здобувачів встановлює можливість про дистанційний захист у разі форс-мажорів та з використання дистанційних технологій (Google Classroom, Meet, Zoom) за умови визначення додаткового резервного дня атестації, завчасного надсилання здобувачем необхідних документів і проведення захисту в синхронному режимі (відеоконференція). Цифровий запис процесу захисту кваліфікаційних робіт зберігається на кафедрі, яка здійснює набір, протягом одного року.
Доступність документів для учасників освітнього процесу забезпечується їх розміщенням у відкритому доступі на офіційному сайті ДУІКТ у розділі нормативних документів (https://duikt.edu.ua/ua/447-polozhennya-normativni-dokumenti). Крім того, детальна процедура проведення контрольних заходів з кожного освітнього компонента ОПП прописана в силабусах дисциплін, які опубліковані на сторінці кафедри (https://surl.li/bteруг).

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

Об'єктивність екзаменаторів та запобігання конфліктам інтересів в ОПП забезпечуються нормативною базою ДУІКТ і прозорими процедурами.
Порядок вирішення спірних ситуацій і врегулювання конфлікту інтересів визначається Положенням про вирішення конфліктних ситуацій (https://surl.li/mvdkgb), яке регламентує алгоритми дій у разі виникнення розбіжностей під час оцінювання навчальних досягнень.
Діяльність НПП і здобувачів ґрунтується на Положенні про систему внутрішнього забезпечення якості вищої освіти (https://surl.li/swzrrk) та Кодексі академічної доброчесності (https://surl.li/wnsxgv), які вимагають неупередженості, об'єктивності й дотримання етичних норм.
Перевірка академічних текстів і кваліфікаційних робіт здійснюється за допомогою спеціалізованого програмного забезпечення StrikePlagiarism.com відповідно до Положення про систему запобігання та виявлення академічного

плагіату (https://surl.li/awjtkz). Кожного року проводиться моніторинг обізнаності здобувачів про академічну доброчесність (https://surl.li/taaeve). В університеті призначено уповноважену особу з питань запобігання і протидії корупції, а відповідна інформація та заходи публікуються у відкритому доступі (https://surl.li/fqvwwh). Усі нормативні документи постійно оновлюються та доступні у розділі нормативної бази Університету (https://surl.li/hdsrdh).
Додатковою гарантією є відеоспостереження в аудиторіях. За весь час реалізації ОПП випадків оскарження об'єктивності чи конфліктів інтересів не зафіксовано.

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

Порядок повторного проходження контрольних заходів та ліквідації академічної заборгованості в ДУІКТ чітко врегульований Положенням про організацію освітнього процесу (https://duikt.edu.ua/uploads/p_447_49109699.pdf). Здобувачу, який не склав не більше двох заліків у встановлений термін, директор навчально-наукового інституту може дозволити їх перескладання після завершення сесії до початку наступного семестру (у визначені терміни ліквідації заборгованості).
Перескладання екзамену з дисципліни допускається не більше двох разів: вперше – викладачу, вдруге – спеціальній комісії, створеній директором інституту. Оцінка комісії є остаточною.
Якщо здобувач отримує незадовільну оцінку (F, FX) під час складання екзамену комісії, або якщо під час сесії накопичено три і більше незадовільних оцінок, такий здобувач відраховується з Університету за невиконання індивідуального навчального плану (академічну неуспішність).
Загальні строки ліквідації академічної заборгованості, як правило, не перевищують трьох місяців.
На практиці реалізація цих правил на ОПП здійснюється прозоро та відповідно до встановлених графіків ліквідації заборгованостей. Завдяки високому рівню мотивації магістрантів та постійному супроводу з боку викладачів і гаранта програми критичні випадки відрахувань є поодинокими, а переважна більшість студентів успішно закриває поточні проміжні результати вчасно.

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

Порядок оскарження процедури та результатів проведення контрольних заходів у ДУІКТ чітко урегульований внутрішніми нормативними документами Університету.
Зокрема, відповідно до Положення щодо вирішення конфліктних ситуацій (https://surl.li/mvdkgb), у разі виникнення скарги чи конфлікту щодо оцінювання знань розгляд звернення відбувається згідно з визначеною процедурою.
За розпорядженням директора інституту не пізніше наступного робочого дня після подання заяви створюється апеляційна комісія, до складу якої входять керівництво інституту, завідувач кафедри, куратор групи та представники студентського самоврядування.
Комісія розглядає звернення здобувача вищої освіти у строк не пізніше п'яти робочих днів після його подання.
Результати розгляду апеляції повідомляються студенту одразу після прийняття рішення, після чого оформлюється відповідний протокол за підписами заявника та членів комісії, який реєструється і зберігається в навчальній частині інституту. Крім того, за мотивованою заявою може створюватися спеціальна комісія для повторного приймання екзамену чи заліку.
На практиці в межах ОПП завдяки прозорості критеріїв оцінювання та відкритому діалогу між викладачами й магістрантами випадків офіційного оскарження результатів контрольних заходів за весь час навчання не виникало.

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

Політика, стандарти і процедури дотримання академічної доброчесності в ДУІКТ чітко визначені у ключових внутрішніх нормативних документах Університету:
Кодекс академічної доброчесності (https://duikt.edu.ua/uploads/p_447_96297052.pdf);
Положення про систему внутрішнього забезпечення якості вищої освіти (https://duikt.edu.ua/uploads/p_447_18879118.pdf);
Положення про систему запобігання та виявлення академічного плагіату (https://duikt.edu.ua/uploads/p_447_61575036.pdf).
Безпосередніми повноваженнями щодо реалізації цієї політики, контролю за дотриманням стандартів та виконання встановлених процедур наділені Комісія з питань академічної доброчесності, директори інститутів, завідувачі кафедр і члени групи забезпечення освітньо-професійної програми

Які технологічні рішення використовуються на ОП як інструменти протидії порушенням академічної доброчесності? Вкажіть посилання на репозиторій ЗВО, що містить кваліфікаційні роботи здобувачів вищої освіти ОП

В якості інструментів щодо запобігання проявам академічної недоброчесності використовуються: інформування здобувачів вищої освіти про неприпустимість наявності плагіату кваліфікаційних робіт, перевірка наукових та кваліфікаційних робіт на плагіат з використанням комп'ютерної програми для внутрішньої перевірки текстів на наявність академічного плагіату StrikePlagiarism.com (https://panel.strikeplagiarism.com/#/).
Процедура інформування НПП щодо потреби запобігати академічній недоброчесності при вивченні освітніх компонентів в Університеті закріплена обов'язковим підписанням відповідної декларації.
Крім того, всі навчальні аудиторії, в яких ведеться підготовка здобувачів за ОПП, обладнані відеокамерами, що унеможливлює використання під час проведення заходів контролю навчальних досягнень здобувачів недозволених

матеріалів.
В Університеті діє репозиторій, що містить кваліфікаційні роботи здобувачів вищої освіти ОПП https://surl.li/fqsjfb.

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

Популяризація академічної доброчесності серед здобувачів ОПП здійснюється через комплекс організаційних, освітніх та інформаційних заходів (https://duikt.edu.ua/uploads/p_1352_45939071.pdf).
Нормативне інформування та етична культура: Створення середовища взаємної довіри й поваги, обов'язкове ознайомлення здобувачів із Кодексом академічної доброчесності ДУІКТ (https://duikt.edu.ua/uploads/p_447_96297052.pdf) та підписання відповідних декларацій.
Вивчення принципів академічного письма та коректного цитування безпосередньо в межах освітніх компонентів, а також технічна перевірка робіт на плагіат.
Участь науково-педагогічних працівників і здобувачів у профільних освітніх ініціативах (зокрема проходження онлайн-курсів на платформі Prometheus із отриманням сертифікатів), а також регулярні обговорення питань академічної етики на засіданнях кафедри й інформаційно-роз'яснювальна робота кураторів академічних груп (https://surli.cc/ximodh).

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

Реагування ЗВО на порушення академічної доброчесності здійснюється відповідно до чинних нормативних документів та передбачає чітко визначені заходи відповідальності:
Для здобувачів вищої освіти: У разі виявлення порушень застосовуються такі види відповідальності, як повторне проходження оцінювання чи відповідного освітнього компонента ОПП, позбавлення академічної стипендії, позбавлення пільг з оплати за навчання або відрахування з Університету.
Для науково-педагогічних працівників: Передбачено відмову у присудженні наукового ступеня чи присвоєнні вченого звання, а також позбавлення права брати участь у роботі визначених законом органів чи займати відповідні посади.
За весь час реалізації ОПП випадків виявлення порушень академічної доброчесності як з боку здобувачів, так і з боку науково-педагогічних працівників не зафіксовано, що свідчить про високу етичну культуру та свідомість учасників освітнього процесу

6. Людські ресурси

Продемонструйте, що викладачі, залучені до реалізації освітньої програми, з огляду на їх кваліфікацію та/або професійний досвід спроможні забезпечити освітні компоненти, які вони реалізують у межах освітньої програми, з урахуванням вимог щодо викладачів, визначених законодавством

Усі НПП, залучені до реалізації освітньо-професійної програми «Інформаційна та кібернетична безпека», повністю відповідають ліцензійним вимогам, визначеним у Постанові Кабінету Міністрів України від 30 грудня 2015 року № 1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності». Їхня кваліфікація, профільна освіта, наукові ступені та практичний досвід гарантують високу якість викладання освітніх компонентів:
Гайдур Галина Іванівна (доктор технічних наук, професор) забезпечує викладання таких компонентів, як «Наукова комунікація та технічний переклад в кібербезпеці», «Прикладна загальна теорія систем інформаційної та кібербезпеки» тощо; має профільну освіту, науковий ступінь за предметною спеціалізацією та значний досвід наукового керівництва здобувачів ступеня доктора філософії за спеціальністю 125 «Кібербезпека та захист інформації».
Легомінова Світлана Володимирівна (доктор економічних наук, професор) викладає компонент «Управління проєктами інформаційної безпеки»; володіє глибокими дослідницькими та практичними навичками в галузі управління проєктами.
Гахов Сергій Олександрович (кандидат військових наук, доцент) викладає дисципліну «Технології виявлення вразливостей мережевих ресурсів», спираючись на багаторічний практичний та науковий досвід у сфері кіберзахисту.
Щавінський Юрій Віталійович (кандидат технічних наук, доцент) забезпечує реалізацію освітнього компонента «Корпоративна та професійна етика в кібербезпеці» для розуміння проблем професійної та корпоративної етики в управлінні кібербезпекою, умінь застосовувати знання для аналізу, супроводу і контролю ефективної роботи колективу, вирішення проблем та впровадження заходів протидії кіберінцидентам.
Марченко Віталій Вікторович (доктор філософії з кібербезпеки, доцент) забезпечує реалізацію освітнього компонента «Технології забезпечення безпеки мережевої інфраструктури» відповідно до сучасних технічних стандартів.
Колісниченко Анна Віталіївна викладає дисципліну «Англійська мова для ділової комунікації», забезпечуючи формування професійних лінгвістичних компетентностей магістрантів.
Кондратенко Наталія Юріївна (кандидат педагогічних наук, доцент, доцент кафедри української мови) викладає дисципліну «Педагогіка та психологія у вищій школі», забезпечуючи формування психолого-педагогічних компетентностей, навичок педагогічної майстерності та підготовку майбутніх фахівців до науково-педагогічної діяльності.
Усі викладачі мають необхідний стаж професійної діяльності за спеціальністю F5 «Кібербезпека та захист інформації», регулярно публікуються у фахових виданнях та міжнародних наукометричних базах Scopus і Web of

Science, а також проходять стажування, що повністю відповідає ліцензійним умовам та забезпечує практичну спрямованість навчання.

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

Формування науково-педагогічного колективу для забезпечення освітньої діяльності за ОПП здійснюється відповідно до чинних нормативно-правових вимог, Ліцензійних умов провадження освітньої діяльності, Статуту й нормативних документів Університету.
Відповідальність за визначення відповідності кваліфікації НПП і його рівня професійної та наукової активності, який забезпечує викладання освітніх компонентів, покладається на завідувача кафедри або групи забезпечення спеціальності на підставі Ліцензійних умов.
Процедури проведення конкурсу на заміщення вакантних посад та порядок перевиборів здійснюється відповідно до нормативних документів Університету:
Положення про порядок проведення конкурсу на заміщення вакантних посад НПП (https://duikt.edu.ua/uploads/p_447_91164126.pdf);
Положення про щорічну рейтингову оцінку діяльності НПП ДУІКТ (https://duikt.edu.ua/uploads/p_447_89539392.pdf).
Кандидатури на заміщення посад НПП попередньо обговорюються на кафедрі в їх присутності. Претендент проводить відкриту лекцію або практичне заняття, після чого здійснюється обговорення рівня його професійної майстерності. По закінченню терміну контракту НПП у повному обсязі подає документи до конкурсної комісії на продовження роботи на посаді та бере участь у конкурсі на рівних умовах з іншими претендентами. Для оцінки рівня відповідності НПП долучається рейтингова картка, звіт за попередній рік роботи й перелік наукових публікацій. Рішення конкурсної комісії затверджується Вченою радою Університету

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

ДУІКТ запровадив в освітній процес модель інноваційного змісту навчання з метою підготовки конкурентоспроможних фахівців, яка передбачає: підготовку здобувачів вищої освіти за компетенціями роботодавців; залучення їх до освітнього процесу та атестації випускників; обговорення змін до ОПП з урахуванням сучасних тенденцій розвитку галузі ІТ, кібербезпеки та захисту інформації; включення в навчальний процес курсів з подальшою видачею сертифікатів компанії-партнера; стажування НПП у компаніях-партнерах.
ДУІКТ активно залучає до проведення окремих занять на ОПП провідних фахівців, експертів галузі та представників роботодавців і партнерських організацій, зокрема:Приклади залучення до навчальних занять представників роботодавців:
Владислав Негода (Світ ІТ) https://surl.li/nwetfr;
Представники компанії Epson https://surl.lt/nfyfly;
Анна Корченко – доктор технічних наук, професор кафедри Комп'ютерної інженерії та кібербезпеки Інституту безпеки та інформатики Краківського педагогічного університету (UKEN, Uniwersytecie Komisji Edukacji Narodowej w Krakowie) https://surl.li/inmjhy;
Роман Орлов (Кіберполіція) https://surl.lt/qhhvoh;
Фахівці компанії ESET Україна https://surl.lt/rtqoyf;
Представники BakoTech https://surl.li/wmhzbn;
А. Кузьменко (IBM) https://surl.li/wvqjdk.
Також до проведення занять та практичних ініціатив залучаються фахівці з КБ провідних вітчизняних і міжнародних компаній, таких як Євротелеком, Дата-центр «Парковий», ST&T, СВІТ ІТ, ІТ Спеціаліст, Netwave LLC та ESET (https://surl.li/tkgred).

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

ДУІКТ сприяє викладачам ОПП у проходженні підвищення кваліфікації відповідно до Положення про підвищення кваліфікації науково-педагогічних працівників (офіційне посилання на університетському ресурсі: https://duikt.edu.ua/uploads/p_447_82499307.pdf).
Прикладами такого сприяння є:
Віталій Марченко пройшов міжнародне стажування в Сілезькій політехніці (https://surl.li/tggtcq);
Собчук Андрій взяв участь у програмі академічної мобільності, у межах якої представив наукову доповідь на тему «A Method for Covert Monitoring of Heterogeneous Sensor Networks Based on Chaotic Dynamics: a cybersecurity perspective: synchronization, stealth, and reliability in distributed monitoring systems» (https://surl.li/argiiu);
Галина Гайдур Сергій Гахов Віталій Марченко успішно пройшли навчання за програмою Check Point Security Administrator (https://surl.li/dutsef);
В'ячеслав Дмітрієв, Юрій Борсуковський взяли участь у програмі міжнародної академічної мобільності в Університеті Національної комісії з питань освіти у Кракові (https://surl.li/mnttnz).
Євгеній Педченко прийняв участь у тренінгу «Training on Critical Infrastructure and Malware Information Sharing Platform», організований Western Balkans Cyber Capacity Centre (WB3C) спільно з Міжнародним союзом електрозв'язку (ITU) (https://surl.li/mlqjhn).

Наведіть конкретні приклади заохочення розвитку викладацької майстерності

Система заходів зі стимулювання підвищення фаховості та викладацької майстерності науково-педагогічних працівників ДУІКТ передбачає матеріальні й моральні заохочення та регламентується внутрішніми нормативними документами Університету:
Статутом Університету https://surl.li/lkuqgj,
Колективним договором на 2023-2025 р.р. https://surl.li/ukrpip,
Положенням про підвищення кваліфікації науково-педагогічних та педагогічних працівників (https://surl.li/cmpfot),
Положенням про порядок заохочення осіб, які працюють, навчаються в Державному університеті інформаційно-комунікаційних технологій (https://surl.li/fgfrnc),
Положенням про надання щорічної грошової винагороди педагогічним працівникам за сумлінну працю зразкове виконання службових обовязків (https://surl.li/kelodc).
Зокрема, здійснюється матеріальне стимулювання НПП, що мають вагомі успіхи у науково-педагогічній діяльності.
Моральні заохочення передбачають нагородження такими видами: оголошення подяки ректора, грамота ректора, а також за поданням керівництва ДУІКТ на відзначення регіональними та відомчими відзнаками.
Прикладом такого заохочення є:
Подяка ректора ДУІКТ завідувачці кафедри СТКБ Галині Гайдур та завідувачці кафедри УКЗІ Світлані Легоміновій (https://surl.li/akkkra).
Премія Верховної Ради України молодим ученим за 2025 рік присуджена професорці кафедри СТКБ Світлані Казмірчук за роботу «Ризикоорієнтований підхід до управління кібербезпекою в умовах дії гібридних загроз у секторі цивільної безпеки України» (https://surl.li/jzoxdj).

7. Освітнє середовище та матеріальні ресурси

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

Основними джерелами фінансування діяльності ДУІКТ є кошти державного бюджету, доходи від надання платних освітніх послуг і господарської діяльності, а також виконання науково-дослідних робіт.
Університет має у своєму складі розширену інфраструктуру (навчальні приміщення, комп'ютерні та спеціалізовані лабораторії, організаційно-методичний центр новітніх технологій, редакційний відділ, бібліотеку, студентський центр та інші приміщення, доступ до високошвидкісного WiFi (5 Gb/s)), що сприяє забезпеченню досягнення цілей і програмних результатів навчання. Зокрема, перелік комп'ютерних класів і спеціалізованих лабораторій Навчально-наукового інституту захисту інформації доступний за посиланням https://surl.li/rlvvkw .
Загальний фонд електронної бібліотеки (https://surl.li/vfshdr) становить понад 160 тис. примірників, серед яких навчальні посібники, конспекти лекцій і методичні рекомендації з освітніх компонентів ОПП.
Інформаційна платформа Google Workspace for Education (GWE) використовується для організації дистанційного навчання і спільної роботи в межах закладу (https://surl.li/kdvwfn). Викладачі, які забезпечують викладання освітніх компонентів ОПП, розмістили необхідні навчально-методичні матеріали на сторінках курсів у GWE. Всі студенти ОПП отримали персональні облікові записи для роботи в системі GWE, а також коди і посилання на сторінки курсів. Дистанційні заняття проходять із використанням Google Meet або Zoom.

Продемонструйте, яким чином заклад вищої освіти забезпечує доступ викладачів і здобувачів вищої освіти до відповідної інфраструктури та інформаційних ресурсів, потрібних для навчання, викладацької та/або наукової діяльності в межах освітньої програми, відповідно до законодавства

ДУІКТ забезпечує вільний доступ викладачів і здобувачів вищої освіти до інфраструктури та інформаційних ресурсів, потрібних для навчання, викладацької та/або наукової діяльності в межах ОПП.
Перелік та силабуси освітніх компонентів ОПП розміщені на сторінці кафедри, а навчально-методичні матеріали (методичні розробки для проведення практичних/лабораторних/семінарських занять, конспекти лекцій, завдання для підготовки до підсумкових заходів контролю, тести та інші форми оцінювання навчальних досягнень здобувачів тощо) розміщені на сторінках викладачів у Google Class. Окрім цього, діє електронна бібліотека, де у постійному доступі знаходяться навчальні посібники, підручники та конспекти лекцій з усіх дисциплін.
Для проведення занять, самостійної освітньої та наукової дослідницької діяльності здобувачів ОПП використовуються спеціалізовані лабораторії ННІКБЗІ та кафедри з урахуванням їх оновлених назв і аудиторного фонду, зокрема: навчальна лабораторія реагування на кіберінциденти, навчальна лабораторія захисту кінцевих точок, навчальна лабораторія мережевої безпеки, навчальна лабораторія Центр управління інформаційною та кібербезпекою (https://surl.li/dkjyna).
Науково-педагогічні працівники і здобувачі ступеня магістра мають можливість користуватися високошвидкісним Інтернетом від компанії Lanet (5 Гб/с) для навчання, викладацької та науково-дослідницької діяльності.

Опишіть, яким чином освітнє середовище надає можливість задовольнити потреби та інтереси здобувачів вищої освіти, які навчаються за освітньою програмою, та є безпечним для їх життя, фізичного та ментального здоров'я

У ДУІКТ створене сприятливе та безпечне освітнє середовище, яке повноцінно задовольняє потреби, інтереси й запити здобувачів вищої освіти та забезпечує захист їхнього життя, фізичного й ментального здоров'я.

Забезпечуються умови для розвитку й реалізації творчих здібностей здобувачів освіти (https://surl.li/gigthv, https://surl.li/rjaspb). На кафедрі функціонують два наукових гуртка за фаховим напрямом (https://surl.li/pvoaay), а також організовуються закордонні стажування та залучення грантів на проведення наукових досліджень (http://surl.li/ojkabd). Здобувачі активно беруть участь у різноманітних фахових конкурсах і змаганнях (https://surl.li/posteo, https://surl.li/hyflvw).
Організовано дистанційні заняття і віддалений доступ до навчальних матеріалів завдяки використанню платформи Google Workspace for Education (https://surl.li/ifqobb).
Для задоволення інтересів і потреб студентів постійно діють студентський центр, тренажерна зала та фітнес-центр, їдальня. Окрім цього, фінансуються численні соціальні ініціативи, зокрема надання матеріальної допомоги, виплата соціальних стипендій та поліпшення умов проживання у гуртожитках.
Значна увага приділяється безпеці освітнього середовища: проводяться вступні інструктажі щодо видів та джерел небезпеки у навчальних приміщеннях і загальних правил поведінки під час освітнього процесу, забезпечується ознайомлення з правилами пожежної безпеки та планами евакуації, налагоджено систему оповіщення про ракетну небезпеку й узгоджено план розміщення студентів в укриттях.

Опишіть, яким чином заклад вищої освіти забезпечує освітню, організаційну, інформаційну, консультативну та соціальну підтримку, підтримку фізичного та ментального здоров'я здобувачів вищої освіти, які навчаються за освітньою програмою.

ДУІКТ створює та забезпечує ефективні механізми різнобічної підтримки здобувачів освіти у ході навчання.
Освітня, організаційна та консультативна підтримка. Надається організаційна та консультативна підтримка з метою реалізації студентами індивідуальної освітньої траєкторії. Завідувач кафедри, куратори груп та науково-педагогічні працівники спільно з адміністрацією Університету здійснюють підтримку здобувачів освітньо-професійної програми з усіх організаційних питань навчання. Студенти отримують сприяння щодо можливостей додаткового навчання, професійного й кар'єрного зростання та працевлаштування за фахом. Зокрема, в університеті функціонує Рада молодих вчених (https://duikt.edu.ua/ua/896-rada-molodih-vchenih-nauka), яка активно просуває та захищає інтереси науковців-початківців.
Інформаційна підтримка і зворотний зв'язок. У разі виникнення конфліктних або складних ситуацій до вирішення питань залучаються завідувачі кафедр, працівники деканату чи ректорату. Крім того, здобувачі мають можливість звернутися через електронний ресурс «Скринька довіри» (https://surl.li/ksxwyg) і залишити анонімне звернення, яке розглядається адміністрацією Університету.
Соціальна підтримка. Студентам пільгових категорій надається активна підтримка у вигляді соціальних стипендій та інших видів соціальної допомоги. Передбачено необхідні умови для навчання осіб з особливими потребами з метою їх ефективної соціалізації, забезпечення доступності й результативності освітнього процесу. Відділ по роботі зі студентами займається вивченням і вирішенням соціальних проблем студентів, надає консультаційну допомогу для поліпшення навчального середовища, а за потреби бере участь у вирішенні конфліктних ситуацій.
Підтримка ментального здоров'я та психологічного клімату. Постійно здійснюється моніторинг психологічного клімату й міжособистісних відносин здобувачів вищої освіти, а також їхньої обізнаності щодо безпечного вирішення конфліктних ситуацій (https://duikt.edu.ua/uploads/p_1352_52264797.pdf).
Роль студентського самоврядування. Важливу роль у забезпеченні різнопланової підтримки здобувачів та їх залученні до життя університету відіграє Студентська рада Університету. Вона реалізує проєкти для вдосконалення професійних умінь і навичок студентів, сприяє налагодженню конструктивної комунікації між студентами й викладачами, залучає до освітнього процесу провідні компанії ІТ-галузі та консультує студентів з питань соціального захисту, зокрема осіб пільгових категорій (https://duikt.edu.ua/ua/929-zagalna-informaciya-studentska-rada). Окрім цього, Студентська рада організовує спортивні змагання та культурно-просвітницькі заходи, забезпечує роботу студентів-кураторів молодших курсів (https://duikt.edu.ua/ua/929-zagalna-informaciya-studentska-rada).
Діяльність та обов'язки самоврядування регламентуються Положенням про студентське самоврядування (https://duikt.edu.ua/ua/933-polozhennya-pro-studentske-samovryaduvannya-studentska-rada).

Яким чином ЗВО створює достатні умови для реалізації права на освіту особами з особливими освітніми потребами? Наведіть посилання на конкретні приклади створення таких умов на ОП (якщо такі були)

ДУІКТ створює інклюзивне освітнє середовище для спільного навчання, виховання та розвитку здобувачів освіти з урахуванням їхніх потреб та можливостей. Згідно з ч. 2 ст. 30 Закону України «Про освіту» щодо умов доступності закладу освіти для навчання осіб з особливими освітніми потребами в ЗВО проведено обстеження будівель та прилеглої до них території з метою визначення доступності навчальних приміщень для осіб з особливими освітніми потребами й інших маломобільних груп населення (МГН).
Враховуючи вимоги та нормативи Державних будівельних норм України і ДСТУ-Н В.2.2-31-2011, розроблено Положення про порядок організації інклюзивного навчання (https://duikt.edu.ua/uploads/p_447_39062918.pdf), яке містить Порядок супроводу (надання допомоги) осіб з інвалідністю та інших маломобільних груп населення.
В Університеті створені умови для вільного пересування осіб з особливими освітніми потребами: встановлені пандуси і підйомні платформи для інвалідів, біля аудиторій та інших приміщень розміщені таблички, надруковані шрифтом Брайля, обладнані спеціальні санвузли для людей з обмеженими можливостями. Відповідно до Правил прийому під час вступу в ДУІКТ створюються пільгові умови вступу для осіб з особливими освітніми потребами.
Конкретним прикладом реалізації таких умов на освітній програмі є навчання студентки Царьової Софії (група БСДМ-61), яка має особливі потреби.

Продемонструйте наявність унормованих антикорупційних політик, процедур реагування на випадки цькування, дискримінації, сексуального домагання, інших конфліктних ситуацій, які є

доступними для всіх учасників освітнього процесу та яких послідовно дотримуються під час реалізації освітньої програми

Освітня діяльність ДУІКТ побудована на принципах дотримання цінностей свободи, справедливості, рівності прав і можливостей, інклюзивності, толерантності, недискримінації, відкритості та прозорості.
В Університеті функціонує відділ з питань соціальних та навчальних проблем студентів (https://surl.li/wmmxqt), діяльність якого регламентується відповідним Положенням (https://duikt.edu.ua/uploads/p_2146_85078892.pdf). Положення про вирішення конфліктних ситуацій (https://duikt.edu.ua/uploads/p_447_88699516.pdf) визначає чіткий порядок і процедури врегулювання ситуацій у разі виникнення конфлікту інтересів, порушення прав людини, міжособистісних зіткнень чи суперечок у навчальному та освітньому процесі. За потреби вступники та здобувачі можуть звернутися до Апеляційної комісії (https://duikt.edu.ua/uploads/p_447_93714477.pdf).
У здобувачів ОПП є можливість скористатися електронною скринькою довіри (https://surl.li/ksxwyg) для подання письмового звернення щодо вирішення будь-якої конфліктної ситуації, у тому числі пов'язаної із сексуальними домаганнями, корупцією чи дискримінацією. У разі потреби створюється тимчасова комісія, яка ретельно перевіряє викладені факти, після чого приймається рішення відповідно до чинного законодавства.
Врегулювання конфліктних ситуацій, пов'язаних із корупцією, здійснюється згідно із Законом України «Про запобігання корупції». В Університеті призначено уповноважену особу з питань запобігання та регулярно проводяться антикорупційні заходи (https://duikt.edu.ua/uploads/p_1471_85184024.pdf).
Розгляд звернень, скарг і заяв, що надходять до Університету, відбувається відповідно до Законів України «Про доступ до публічної інформації» та «Про звернення громадян». Врегулювання скарг здійснюється шляхом особистого прийому громадян адміністрацією ДУІКТ, а про результати розгляду заявникам повідомляється письмово або усно за їхнім бажанням.
За період реалізації освітньо-професійної програми випадків звернень щодо вирішення конфліктних ситуацій (у тому числі пов'язаних із сексуальними домаганнями, корупцією чи дискримінацією) зафіксовано не було.

8. Внутрішнє забезпечення якості освітньої програми

Яким документом ЗВО регулюються процедури розроблення, затвердження, моніторингу та періодичного перегляду ОП? Наведіть посилання на цей документ, оприлюднений у відкритому доступі на своєму вебсайті

Розробка, затвердження, моніторинг та актуалізація освітньо-професійної програми ґрунтуються на Положенні про систему внутрішнього забезпечення якості освіти (https://duikt.edu.ua/uploads/p_447_18879118.pdf) та Положенні про запровадження та оновлення освітніх програм (https://duikt.edu.ua/uploads/p_447_50872585.pdf). Ці нормативні документи стандартизують процеси для всіх спеціальностей університету, гарантуючи єдиний методичний підхід до контролю якості та вдосконалення освітнього контенту.
Для створення ОПП формується спеціальна робоча група, до якої входять науково-педагогічні працівники з високим рівнем професійної активності, необхідною кваліфікацією та стажем. До цього процесу також залучаються профільні роботодавці, студенти та провідні галузеві експерти. Безпосередню відповідальність за якість виконання та реалізації програми несе група забезпечення спеціальності.
Порядок перегляду та оновлення ОП регламентується Положенням про запровадження й оновлення освітніх програм. З метою оцінки ефективності програми щороку проводиться моніторинг її відповідності стандартам вищої освіти, здатності гарантувати досягнення запланованих програмних результатів навчання, а також рівня задоволеності студентів і працедавців (https://surli.cc/fzwqty). Коригування до ОПП та окремих навчальних дисциплін вносяться оперативно – з огляду на актуальні зміни в законодавстві та технологічні інновації у сфері інформаційних технологій і кіберзахисту.

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

Процедура перегляду й оновлення ОПП чітко регламентована Положенням про запровадження й оновлення освітніх програм. Згідно з цим документом, перегляд програми здійснюється за чітко визначеною періодичністю: щорічно за результатами внутрішнього моніторингу, а також по завершенню повного циклу реалізації ОПП.
З метою своєчасного оновлення програми щороку проводяться комплексні заходи щодо моніторингу змін у чинному законодавстві, а також аналізуються тенденції інноваційного розвитку галузей ІТ, кібербезпеки та захисту інформації.
За результатами останнього перегляду до ОПП було внесено низку обґрунтованих змін:
До структури основного блоку програми додано освітню компоненту «Англійська мова для ділової комунікації» – відповідно до розпорядження ректора для посилення лінгвістичних компетентностей магістрантів.
Введено освітню компоненту «Наукова комунікація та технічне документування в кібербезпеці» – з метою покращення навичок роботи з технічною документацією та правильного оформлення наукових здобутків, що покращення принципів академічного письма та коректного цитування. Цю зміну було реалізовано за рекомендацією академічної спільноти, зокрема професора кафедри кібербезпеки та захисту інформації факультету інформаційних технологій Київського національного університету імені Тараса Шевченка Володимира Наконечного.
Оновлено блок, що стосується працевлаштування та подальшого навчання: у результаті обговорення перспектив актуалізації ОПП директором ТОВ «Євротелеком» у 2024 році було внесено рекомендації щодо деталізації професійних ролей випускників (зокрема, «Фахівець з реагування на інциденти кібербезпеки» та «Фахівець з підтримки інфраструктури кіберзахисту»).
Зміцненню та стратегічному розвитку програми також сприяла участь представників університету у фахових

діалогах, зокрема в рамках ініціативи «Стратегічні вектори формування нової парадигми кібер-освіти: ДУІКТ долучився до фахового діалогу», що дозволило інтегрувати передові підходи до підготовки фахівців з урахуванням сучасних викликів 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

Пропозиції від здобувачів одержуються в особистому спілкуванні, на засіданнях кафедр і під час опитувань https://duikt.edu.ua/uploads/p_3142_86456738.pdf.
Здобувачі свої пропозиції можуть надавати через форму зворотного зв'язку, розміщену на сторінці публічного обговорення освітньо-професійних програм https://surl.li/nreoau та скриньку довіри https://surl.li/ksxwyg.
Також, ефективним засобом моніторингу ОПП є зустрічі з магістрантами щодо поточних питань організації навчального процесу та проведення різних заходів, де обговорюються проблемні питання
https://surl.li/kksjlh
Найбільш актуальні зміни обговорюються під час зустрічей з представниками компаній-партнерів
https://surl.li/ihqlkg
https://surli.cc/nlcvtg
https://surl.li/zfrfcc

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

Студентське самоврядування ДУІКТ бере активну та системну участь у процедурах внутрішнього забезпечення якості ОП, виконуючи представницьку, контрольну та консультативну функції. Відповідно до Положення про студентське самоврядування, основними формами такої участі є:
Представники студентського самоврядування входять до складу Вченої ради університету, рад інститутів та інших робочих органів, де розглядаються та затверджуються питання розробки, моніторингу, періодичного перегляду та вдосконалення освітньо-професійних програм.
Студентське самоврядування аналізує та узагальнює зауваження та пропозиції Студентів щодо організації освітнього процесу та умов навчання. На основі цих даних формуються пропозиції щодо коригування силабусів чи змісту ОП.
Органи самоврядування здійснюють моніторинг дотримання академічної доброчесності, прозорості оцінювання та створення комфортного освітнього середовища, беручи участь у врегулюванні спірних або конфліктних ситуацій через механізми зворотного зв'язку.
Студентське самоврядування долучається до організації зустрічей з роботодавцями, випускниками та експертами галузі, сприяючи обговоренню актуальності програмних результатів навчання з урахуванням сучасних ринкових тенденцій у сфері ІТ та кібербезпеки.

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

Оскільки переважна більшість здобувачів ступеня магістра працевлаштовуються в компаніях галузі ІТ, кібербезпеки та захисту інформації, компанії-партнери кафедри, які є потенційними роботодавцями випускників, беруть безпосередню участь у процесі періодичного перегляду програми.
До ключових представників роботодавців, залучених до забезпечення якості та оновлення ОПП, належать:
Максим Порошин – представник компанії ТОВ «СвітІТ»;
Олександр Іллюша – технічний директор компанії ESET в Україні;
Павло Булавін – директор ТОВ «ЄВРОТЕЛЕКОМ» (https://surl.li/ihqlkg).
Обговорення з роботодавцями перспектив розвитку галузі, ринкових трендів і необхідних змін до програм здійснюється під час науково-практичних конференцій та семінарів, засідань вчених рад і кафедри, а також робочих зустрічей. Окрім того, до регулярного перегляду освітньо-професійної програми долучається широка академічна спільнота (https://surli.cc/nlcvtg)

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

Інформація про працевлаштування випускників освітньо-професійної програми постійно і системно збирається та аналізується. Оскільки переважна більшість здобувачів ступеня магістра успішно працевлаштовуються в компаніях галузі ІТ, кібербезпеки та захисту інформації, кафедра підтримує постійний зв'язок із випускниками та аналізує їхні кар'єрні траєкторії для подальшого вдосконалення освітнього процесу (https://surl.li/woyhuj).
Зокрема, серед випускників ОПП попередніх років слід відзначити:
Серед випускників ОПП 2026 року:
Ярослав Клименко – менеджер з інформаційної безпеки АТ «УкрПошта»;
Анастасія Бригинець – головний інженер CSIRT-NBU, Національний банк України;
Ярослав Шандровський – інженер з кібербезпекиТОВ «Євротелеком»;
Артем Мурав'єв – інженер з інформаційної безпеки «ESET Україна»;
Андрій Баранов – аналітик SOC NBU, Національний банк України.
Зокрема, серед випускників ОПП попередніх років слід відзначити:
Анастасія Чаплієва – провідний експерт з ІТ аудиту, АТ «Райффайзен банк»;
Анастасія Шайкова – керівник програм Управління інформаційної безпеки, АТ «Державний експортно-імпортний банк України»;

Ілля Калабухов – системний адміністратор у сфері баз даних та комп'ютерних мереж, ADEON International, spol. s r. o.;
Тетяна Парфенюк – TENTENS Tech, Security Team Lead;
Артем Мурав'єв – провідний технічний спеціаліст ТОВ "центр інформаційної та технічної підтримки «САПФОРІС».
Роман Драгунцов - керівник департаменту кіберзахисту ТОВ ІТ Спеціаліст;
Владислав Оліферчук - керівник 2-ї лінії SOC ТОВ ІТ Спеціаліст.

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

Процедури щодо забезпечення якості реалізації, контролю та моніторингу внутрішніх показників освітньої діяльності за освітньо-професійною програмою (ОПП) багаторівневі та охоплюють усі ланки управління університетом:
На рівні кафедри систем та технологій кібербезпеки: здійснюється поточний контроль діяльності науково-педагогічних працівників, зокрема перевірка з боку завідувача кафедри, проведення відкритих занять, а також заслуховування, активне обговорення та прийняття управлінських рішень на засіданнях кафедри.
На рівні навчально-наукового інституту: проводиться контроль діяльності випускаючих кафедр, заслуховування звітів, відвідування занять НПП, обговорення ключових питань і прийняття рішень на засіданні Вченої ради інституту щодо затвердження нормативних документів із реалізації ОПП.
На рівні ЗВО: моніторинг щодо виконання прийнятих рішень та загальний контроль реалізує Навчально-методичний відділ.
Кафедра систем та технологій кібербезпеки проводить опитування здобувачів освіти за ОПП щодо рівня їхнього задоволення змістом і якістю освітнього процесу (https://duikt.edu.ua/uploads/p_3142_86456738.pdf).
За результатами таких опитувань здобувачів та аналізу зворотного зв'язку заінтересованих сторін вчасно формуються обґрунтовані пропозиції щодо оновлення змісту освітніх компонентів і підвищення загальної якості ОПП, що безпосередньо розглядається на засіданнях кафедри (https://surl.li/rjskgl) для подальшого вдосконалення підготовки магістрів із кібербезпеки.

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

У зв'язку із введенням воєнного стану акредитація ОПП, яка була запланована на 2023 рік, була продовжена автоматично.
Водночас, під час оновлення програми було розглянуто недоліки і рекомендації щодо їх виправлення за результатами акредитації ОП «управління інформаційною та кібернетичною безпекою"».
У ході оновлення ОПП враховано зауваження експертів до ОПП, зокрема:
Критерій 7 Внутрішнє забезпечення якості освітньої програми
Додано вкладку оприлюднення для громадського обговорення проект ОПП та змін до нього на сторінці кафедри.
Впроваджено опитування стейкголедерів, випускників та здобувачів, з метою проведення своєчасного моніторингу ОПП та внесення відповідних змін.
Створено опитування серед випускників щодо їх кар'єрного шляху для підвищення рівня якості забезпечення освітнього процесу.

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

Відповідно до Положення про систему внутрішнього забезпечення якості вищої освіти (https://duikt.edu.ua/uploads/p_447_18879118.pdf) ДУІКТ всіляко сприяє активному залученню учасників академічної спільноти до процесу внутрішнього забезпечення якості освіти.
Представники академічної спільноти залучаються до здійснення моніторингу та періодичного перегляду освітніх програм, а також до оцінювання освітньої та науково-технічної діяльності кафедр інституту. Питання підвищення якості освіти та вдосконалення освітніх компонентів регулярно виносяться на обговорення під час засідань кафедр, вчених рад Інституту та Університету.
Протягом 2022–2026 років до зовнішньої експертизи та перегляду освітньо-професійної програми долучалися провідні фахівці з інших закладів вищої освіти:
Наконечний Володимир Семенович — доктор технічних наук, професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка;
Толюпа Сергій Володимирович — доктор технічних наук, професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка;
Молодецька Катерина Сергіївна — доктор технічних наук, професор Поліського національного університету.
Окрім цього, фахове обговорення змісту ОПП та перспектив її розвитку систематично проводиться в рамках круглих столів, наукових семінарів і тематичних заходів (https://surl.li/zfrfcc).

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

Формування стійкої культури якості освіти в університетському середовищі ґрунтується на систематичному діалозі, відкритому висвітленні питань модернізації навчального процесу та залученні всіх учасників на рівні кафедри, Інституту й Університету. Така культура охоплює спільні цінності, академічні норми та стандарти професійної

поведінки, розділені як науково-педагогічним колективом, так і здобувачами.
Питання постійного вдосконалення освітньо-професійних програм та моніторингу їхньої ефективності регулярно виносяться на розгляд засідань кафедри систем та технологій кібербезпеки, Вченої ради Навчально-наукового інституту захисту інформації та Вченої ради Університету. Важливим інструментом підтримки та розвитку цієї культури є систематичні опитування стейкхолдерів і студентів задля оцінки рівня задоволеності якістю навчання й збору ініціатив щодо оновлення освітнього контенту (https://surl.li/hhhjnz, https://surl.li/hkmwba).

9. Прозорість і публічність

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

Права та обов'язки всіх учасників освітнього процесу ДУІКТ регулюються:
Статутом Університету, погодженого загальними зборами трудового колективу й затвердженого наказом МОН України від 16 грудня 2025 року, протокол №1 https://duikt.edu.ua/uploads/p_949_82462133.pdf;
Положенням про організацію освітнього процесу у ДУІКТ https://duikt.edu.ua/uploads/p_447_49109699.pdf,
Колективним договором ДУІКТ https://duikt.edu.ua/uploads/p_949_61639574.pdf,
Кодексом академічної доброчесності ДУІКТ https://duikt.edu.ua/uploads/p_447_96297052.pdf?file=p_447_96297052.pdf,
Положенням про систему внутрішнього забезпечення якості вищої освіти та освітньої діяльності ДУІКТ https://duikt.edu.ua/uploads/p_447_18879118.pdf ;
договором про навчання у закладі вищої освіти та надання платної освітньої послуги між ЗВО та фізичною (юридичною) особою, контрактами з науково-педагогічними працівниками, посадовими інструкціями.
Доступність документів учасників освітнього процесу, забезпечується їх розміщенням на сайті Університету.

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

https://duikt.edu.ua/ua/3141-publichne-obgovorennya-osvitno-profesiynih-program-osvitni-programi

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

ОПП, навчальні плани https://duikt.edu.ua/ua/1822-osvitno-profesiyni-programi-kafedra-informaciynoi-ta-kibernetichnoi-bezpeki
силабуси освітніх компонентів, освітні компоненти вільного вибору студента
https://duikt.edu.ua/ua/840-navchalni-disciplini-kafedra-informaciynoi-ta-kibernetichnoi-bezpeki
освітні компоненти вільного вибору студента
https://duikt.edu.ua/ua/2994-katalog-osvitnih-komponentiv-vilnogo-viboru

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП?

Запровадження ОПП «Інформаційна та кібернетична безпека» другого (магістерського) рівня за спеціальністю 125 «Кібербезпека та захист інформації» у Державному університеті інформаційно-комунікаційних технологій забезпечує чітку послідовність і неперервність підготовки фахівців від бакалаврського до освітньо-наукового рівня. Проведений самоаналіз засвідчує, що структура програми повністю ґрунтується на компетентнісному підході, містить детально визначені програмні результати навчання (РН1–РН23) та гармонізована з вимогами Національної рамки кваліфікацій. Зміст навчального плану, обсяги кредитів ЄКТС, а також якісний склад науково-педагогічних працівників і групи забезпечення повністю відповідають чинним ліцензійним умовам і державним стандартам вищої освіти.
Серед ключових сильних сторін освітньої програми слід виокремити потужне матеріально-технічне забезпечення, зокрема наявність сучасних спеціалізованих лабораторій (Центр управління інформаційною та кібербезпекою, навчальні лабораторії реагування на кіберінциденти, захисту кінцевих точок і мережевої безпеки), створених на основі технологій провідних вітчизняних та світових ІТ-компаній. Суттєвою перевагою освітнього процесу є активне залучення професіоналів-практиків і роботодавців до аудиторних занять, розробки змісту компонентів та атестації здобувачів. Водночас гнучкі внутрішні механізми університету гарантують кожному здобувачеві реальну можливість формувати індивідуальну освітню траєкторію (зокрема через вибіркові дисципліни обсягом понад 27% та визнання результатів неформальної освіти) відповідно до його професійних інтересів.
Узагальнюючи наведені показники, можна зробити обґрунтований висновок, що освітня діяльність за ОПП «Інформаційна та кібернетична безпека» повною мірою відповідає критеріям акредитації та забезпечує високу

державну гарантію якості підготовки конкурентоспроможних фахівців.

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

Стратегічний розвиток ОПП «Інформаційна та кібернетична безпека» на найближчі три роки орієнтований на її глибоку інноваційну модернізацію, посилення практичної спрямованості та гармонізацію з провідними європейськими й світовими стандартами. Усвідомлюючи стрімке зростання масштабів кіберзагроз і вимог до цифрової стійкості держави, кафедра систем та технологій кібербезпеки спрямовує зусилля на виведення підготовки магістрів на якісно новий міжнародний рівень. Головними векторами еволюції програми визначено розширення інтернаціоналізації освітнього середовища, інтеграцію новітніх наукових розробок у навчальний процес та зміцнення партнерства з ключовими гравцями ІТ-ринку й сектора безпеки.
Задля досягнення поставлених цілей та реалізації перспективних завдань ДУІКТ у межах ОПП планує здійснити низку цілеспрямованих заходів:
Активація міжнародної академічної мобільності за рахунок систематичного залучення здобувачів і науково-педагогічних працівників до програм академічної мобільності, стажувань та спільних наукових проєктів із провідними закордонними закладами вищої освіти.
Технологічне оновлення навчальної бази за рахунок постійної модернізації спеціалізованих лабораторій та Центру управління інформаційною і кібербезпекою з урахуванням актуальних трендів ринку (зокрема впровадження платформ класу SOC, систем штучного інтелекту для виявлення аномалій та архітектур Zero Trust).
Практико-орієнтоване оновлення змісту за рахунок регулярного коригування освітніх компонентів і тем кваліфікаційних робіт за безпосередньої участі роботодавців (представників Держспецзв'язку, Кіберполіції та провідних ІТ-компаній) на основі актуальних викликів безпеки.
Стимулювання наукових публікацій у Scopus та Web of Science шляхом активізації спільних наукових досліджень викладачів і магістрантів із подальшим висвітленням результатів у високорейтингових міжнародних фахових виданнях.
Впровадження сертифікаційних програм вендорів з метою поглиблення інтеграції курсів світових ІТ-лідерів (таких як Cisco, IBM, Huawei, Check Point) безпосередньо в освітній процес із можливістю отримання міжнародних сертифікатів.
Розвиток проєктного навчання та командної взаємодії: розширення практики участі студентських команд у національних та міжнародних змаганнях у форматі CTF (Capture the Flag) і хакатонах як ефективного інструменту формування прикладних компетентностей.

Запевнення

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

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

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

Додатки:

Таблиця 1. Інформація про обов'язкові освітні компоненти ОП

Таблиця 2. Зведена інформація про викладачів ОП

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

***

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

Документ підписаний кваліфікованим електронним підписом/кваліфікованою електронною печаткою.

Інформація про КЕП

ПІБ: ШУЛЬГА ВОЛОДИМИР ПЕТРОВИЧ

Дата: 07.09.2026 р.

Таблиця 1. Інформація про освітні компоненти ОП

Назва освітнього компонента	Вид освітнього компонента	Силабус або інші навчально-методичні матеріали		Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього*
		Назва файла	Хеш файла	
Корпоративна та професійна етика в кібербезпеці	навчальна дисципліна	*ОК 1 (2).pdf*	Q6ho8WzvTNsNoYDiZlOkUFS4boQhduTu+e8nEladgH4=	*Навчальна лабораторія Security Operation Center:* *1.Комп'ютери Asus p5gc-mx - 3шт.; ITS 5400 - 7 шт.* *2. Мультимедійна система Acer X113 DLP – 1шт.* *3. Монітор Panasonic TX 32" FR 250K LED HD – 6 шт.* *4. Системний блок Everest Enterprise 7600.* *5. Монітор Aser SA 240 Ydid – 1 шт.* *Програмно-апаратні комплекси:* *1. Програмно-апаратний комплекс USM/SIEM від AlienVault: платформа USM (All-In-One) для збору, моніторингу, аналізу подій і загроз інформаційної безпеки; SIEM для управління інформацією та подіями безпеки. ПЗ вільного доступу.* *2. Програмні засоби тестування та підтримки прийняття рішень у сфері кібербезпеки:* *– для тестування на проникнення (Kali Linux). Ліцензія – відкритий код;* *– для аналізу даних (KNIME, Orange, RapidMiner). Ліцензія – відкритий код;* *– для багатокритеріального аналізу (D-Sight, SuperDecisions). Ліцензія – безкоштовна з обмеженнями;* *– системи підтримки прийняття рішень (DSS) (LibreOffice Calc, OpenSolver). Ліцензія – безкоштовна для навчання.*
Педагогіка та психологія у вищій школі	навчальна дисципліна	*ОК 2 (2).pdf*	/m9asVHxzMurgBXwTKK5TmbfFQ7Hk50NEfYhZyMwMk4=	*Спеціального матеріально-технічного забезпечення не потребує, Мультимедійна система*
Англійська мова для ділової комунікації	навчальна дисципліна	*ОК 5.pdf*	siWxFFHs5MjZsP9Z3wIA5YPjrjfC7FlblIa5EsvDa3Q=	*Спеціального матеріально-технічного забезпечення не потребує, Мультимедійна система*
Проведення наукових досліджень в кібербезпеці	навчальна дисципліна	*ОК 3.pdf*	I/n7Dhdo9GTHDGdUamiWoX6ZMNByTuDUksuDgqOJLBM=	*Навчальна лабораторія реагування на кіберінциденти:* *1. Комп'ютери Dell OptiPlex 3050/Core i5 7500T – 14 шт.* *2. Мультимедійна система Acer 113 – 1 шт.* *3. Набір серверів Server Dell PE R530 – 3шт.* *4. Робочі станції Dell Precision Tower 3620 i7 – 14 шт. Dell OptiPlex 3050 i5;* *5. Маршрутизатор Mikrotik CSS326-24G-2S+RM. – 1 шт.* *6. Комутатор Mikrotik CSS326-24G-2S+ RM – 1шт.* *Програмно-апаратні комплекси: програмне забезпечення мови програмування Python 3.11.1,*

				платформа Google Colab або програмне забезпечення Jupyter Notebook, бібліотека програм Scikit-learn, бібліотека програм Pandas, бібліотека програм NumPy, бібліотека програм Matplotlib, бібліотека програм Seaborn, Canadian Institute for Cybersecurity datasets.
Управління проектами інформаційної безпеки	навчальна дисципліна	*ОК 7.pdf*	dUvlUFlHT3xpajpJXvemgzzEoFILY905/vl5iYuLgxU=	*Навчальна лабораторія Security Operation Center:* *1.Комп'ютери Asus p5gc-mx - 3шт.; ITS 5400 - 7 шт.* *2. Мультимедійна система Acer X113 DLP – 1шт.* *3. Монітор Panasonic TX 32" FR 250K LED HD – 6 шт.* *4. Системний блок Everest Enterprise 7600.* *5. Монітор Aser SA 240 Ydid – 1 шт.* *Програмне забезпечення:* *1. Apache OpenOffice URL: https://www.openoffice.org/ 2. Microsoft Project URL: https://www.microsoft.com/uk-ua/microsoft-365/project/project-management-software*
Технології забезпечення безпеки мережевої інфраструктури	навчальна дисципліна	*ОК 8.pdf*	6U0aijX5e2DHLwEpPkZrybEKvNJg8kXlwXf9+EW8LHk=	*Навчальна лабораторія мережевої безпеки:* *1.Комп'ютери Intel Cougar Point H61 2x, 2700 MGhz на МП H61b-K, 2 Гб ОЗУ DDR3 – 15 шт.* *2. Мультимедійна система Acer 113 – 1шт.* *3.Маршрутизатор TP–Link ARCHER C60 AC 1350 – 1 шт.;* *4.Маршрутизатор Huawei AR120 – 1шт.;* *5.Комутатор L2+24ZIXEL – 1шт.;* *6.Мережеве сховище My Cloud Home – 1шт.* *Програмно-апаратні комплекси:* *1. Cisco Packet Tracer – програмний комплекс для проведення досліженнь взаємодії між елементами мережі. ПЗ вільного доступу.*
Технології виявлення уразливостей мережевих ресурсів	навчальна дисципліна	*ОК 9.pdf*	mR3rvqX2rZ3EIu+aCyUVYv6QOy5oolJwaIwq9hXdCoE=	*Навчальна лабораторія реагування на кіберінциденти:* *1. Комп'ютери Dell OptiPlex 3050/Core i5 7500T – 14 шт.* *2. Мультимедійна система Acer 113 – 1 шт.* *3. Набір серверів Server Dell PE R530 – 3шт.* *4. Робочі станції Dell Precision Tower 3620 i7 – 14 шт. Dell OptiPlex 3050 i5;* *5. Маршрутизатор Mikrotik CSS326-24G-2S+RM. – 1 шт.* *6. Комутатор Mikrotik CSS326-24G-2S+ RM – 1шт.* *Програмно-апаратні комплекси:* *1. ESET PROTECT Enterprise On-Prem. № ліцензії – A33-AMJ-UTU, до 30.11.2026. Кількість пристроїв – 60.* *2. IBM QRadar SIEM. № ліцензії – 31XX-SIEM-QRM-QVM. . Навчальна ліцензія* *3. IBM i2 Analyst's Notebook Premium. Навчальна ліцензія* *4. Tenable Nessus Professional. Навчальна ліцензія*
Науково-педагогічна	практика	*ОК 10.pdf*	EbR+a5aKnKAutGfB	*Спеціального матеріально-*

практика			SsrPpAw44kOzGAr7uqZQ5/VtrHU=	*технічного забезпечення не потребує,*
Науково-дослідна практика	практика	*ОК 11 НДП.pdf*	/T4Boizwra7sJuukd6vHeFPY/FBQCqplAhRoCC1QCN8=	*Використовується матеріально-технічне та інформаційне забезпечення бази практики. Мультимедійний проектор*
Переддипломна практика	практика	*ОК 12 ПД.pdf*	i41O5j5Z5rvlGweXt1CirBwQw4rYm8Qz3FdDNcatWDA=	*Використовується матеріально-технічне та інформаційне забезпечення бази практики. Мультимедійний проектор*
Кваліфікаційна робота	підсумкова атестація	*ОК 13.pdf*	Cz4t+SxLSDbqu5tUQmbCw5zpdLdgxOB3cCfRXex3PRo=	-
Наукова комунікація та технічний переклад в кібербезпеці	навчальна дисципліна	*ОК 4.pdf*	pC+IoPJpcx98YUwFt+gqFafPeJmHELM5/3loxWqnPz0=	*Спеціального матеріально-технічного забезпечення не потребує, Мультимедійна система*
Прикладна загальна теорія систем кібербезпеки	навчальна дисципліна	*ОК 6.pdf*	KHKZ/xNiKsSoQztTqnWthSvvtQgMT4DeDw8sirfO1FY=	*Навчальна лабораторія захисту кінцевих точок:* *1. Комп'ютери:* *DualCore Intel Pentium E2180, 2000 Ghz на МП ASUS P5Л SE/EPU, 1 Гб ОЗУ DDR2 – 13 од.* *DualCore Intel Core 2 Duo, 2666 Mhz на МП ASUS P5E Deluxe, 4 Гб ОЗУ DDR2 – 4 од.– 17 шт.* *2. Мультимедійна система Acer 113 – 1шт.* *Програмно-апаратні комплекси:* *1. ESET PROTECT Enterprise On-Prem: № ліцензії – A33-AMJ-UTU. Кількість пристроїв – 60.* *Навчальна лабораторія реагування на кіберінциденти:* *1. Комп'ютери Dell OptiPlex 3050/Core i5 7500T – 14 шт.* *2. Мультимедійна система Acer 113 – 1 шт.* *3. Набір серверів Server Dell PE R530 – 3шт.* *4. Робочі станції Dell Precision Tower 3620 i7 – 14 шт. Dell OptiPlex 3050 i5;* *5. Маршрутизатор Mikrotik CSS326-24G-2S+RM. – 1 шт.* *6. Комутатор Mikrotik CSS326-24G-2S+ RM – 1шт.* *Програмно-апаратні комплекси:* *1. ESET PROTECT Enterprise On-Prem. № ліцензії – A33-AMJ-UTU, до 30.11.2026. Кількість пристроїв – 60.* *2. IBM QRadar SIEM. № ліцензії – 31XX-SIEM-QRM-QVM. . Навчальна ліцензія* *3. IBM i2 Analyst's Notebook Premium. Навчальна ліцензія* *4. Tenable Nessus Professional. Навчальна ліцензія*

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

Таблиця 2. Зведена інформація про відповідність НПП освітнім компонентам

ID викладача	ПІБ	Посада	Структурний підрозділ	Кваліфікація викладача	Стаж	Навчальні дисципліни, що їх викладає викладач на ОП	Обґрунтування відповідності освітньому компоненту (кваліфікація, професійний

							досвід, наукові публікації)
143226	Гахов Сергій Олександрович	Доцент, Основне місце роботи	Навчально-науковий інститут Кібербезпеки та захисту інформації	Диплом спеціаліста, Харківським вищим військовим училищем радіозв'язку, рік закінчення: 1993, спеціальність: , Диплом магістра, Національна академія оборони України, рік закінчення: 2006, спеціальність: Організація бойового та оперативного забезпеченнгя військ (за видами та родами військ і сил), Диплом кандидата наук ДК 008375, виданий 26.10.2012, Атестат доцента АД 006511, виданий 09.02.2021	32	Технології виявлення уразливостей мережевих ресурсів	Види і результати професійної діяльності за спеціальністю відповідно до п.38 Ліцензійних умов провадження освітньої діяльності: п.п. 38.1), 38.3), 38.4), 38.8), 38.11), 38.12), 38.19), 38.20) наявність сертифіката відповідно до Загальноєвропейської рекомендації з мовної освіти В2 з англійської мови 1.наявність не менше п’яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection; 1. Bryhynets, A. Haidur, H. Gakhov, S.Marchenko, V. Quantitative WEB Application Vulnerability Assessment using SAST Methodology International Journal of Computing, 2025, 24(1), pp. 163–170 DOI: 10.1016/j.egyr.2025.04.056. (Scopus) 2. Sobchuk V., Gakhov S., Smoliev Y., Haidur H. Enhancing Intrusion Detection in Organizational Information Systems through AI-Powered Traffic Analysis (2024) CEUR Workshop Proceedings, 3933, pp. 190 - 203. https://www.scopus.com/inward/record.uri?eid=2-s2.0-86000713893&partnerID=40&md5=f59cab3a67f02a57321b8172f4b75ed6 . (Scopus) 3. Haidur, H., Gakhov, S., & Hamza, D. (2024). USING SUPPORT VECTORS TO BUILD A RULE-BASED SYSTEM FOR DETECTING MALICIOUS PROCESSES IN AN ORGANISATION’S NETWORK TRAFFIC. Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska, 14(4), 90–96. https://doi.org/10.35784/iapgos.6366. (Scopus

							) 4. Гайдур, Г. І., Гахов, С. О., Марченко, В. В., & Гайдур, К. В. (2024). Концептуальна модель виявлення фішингових атак на основі використання методів опорних векторів. Сучасний захист інформації, 2(58), 24–33. https://doi.org/10.31673/2409-7292.2024.020003 5. Гайдур Г. І. Гахов С. О, Сич М. В., Дмітрієв В. Є. Аналіз загроз мережевого трафіку рівнів моделі OSI для динамічного розрахунку RTO в контексті боротьби з DDOS атаками. Телекомунікаційні та інформаційні технології. № 3 (2023). С. 12-21. DOI: 10.31673/2412-4338.2023.031221. 6. Гайдур Г. І., Гахов С. О., Бригинець А. Виявлення мережевих аномалій з використанням алгоритмів нейронних мереж. Телекомунікаційні та інформаційні технології. № 1 (2023). С. 61-73. DOI: 10.31673/2412-4338.2023.016173. 3.наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора); 1. Козачок В.А., Гайдур Г.І., Гахов С.О., Власенко В.О., Чумак Н.С. Політики безпеки. Навчальний посібник підготовлено для студентів вищих навчальних закладів – Київ: ДУТ ННІЗІ, 2020. – 167 с. 2. Haidur H. I., Gakhov S. O., Skybun O. Z. Cyber education in the context of the formation of ukraine's modern educational space: interdisciplinary approaches. Ukraine's capacity to implement the sustainable development program in the context of full-scale armed aggression: Scientific monograph.

							Riga, Latvia : “Baltija Publishing”,Volume 1. 2025. p. 48-60. DOI https://doi.org/10.30525/978-9934-26-570-9-4 . 4.наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування; 1. Методичні рекомендації до виконання магістерських робіт на ступінь вищої освіти «Магістр» для здобувачів спеціальності 125 Кібербезпека / Гайдур Г.І., Гахов С.О., Марченко В.В. ,Чумак Н.С. /– К.: ДУІКТ, 2024. 44 с. 2. Методичні рекомендації до виконання кваліфікаційної роботи першого (бакалаврського) рівня вищої освіти спеціальності 125 Кібербезпека ОП Інформаційна та кібернетична безпека // Гайдур Г.І., Гахов С.О., Марченко В.В., Дмітрієв В.Є. / – К.: ДУІКТ, 2024. – 46 с. 3. Електроний курс «Проведення наукових досліджень в кібербезпеці». 4. Електроний курс «Технології виявлення уразливостей мережевих ресурсів». 5. Електроний курс «SIEM системи». 6. Електроний курс «Цифрова криміналістика». 8.виконання функцій (повноважень, обов’язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента)

							наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах; 1. Відповідальний виконавець ініціативної держбюджетної науково-дослідної роботи за темою: «Розробка методів та засобів підвищення живучості інформаційно-комунікаційнихсистем в умовах впливу кібернетичних атак» (реєстраційний номер НДР шифр «Живучість К14» РК №0114U000391) 2. Науковий керівник ініціативної держбюджетної науково-дослідної роботи за темою: «Методологія виявлення шкідливих процесів в інформаційних системах» (реєстраційний номер НДР 0121U113613). 11.наукове консультування підприємств, установ, організацій не менше трьох років, що здійснювалося на підставі договору із закладом вищої освіти (науковою установою); Консультація відповідно договору № 0203від 02 березня 2020 року з ТОВ « Центр інформаційної та технічної підтримки «Сапфоріс». 12.наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п’яти публікацій; 1. Гайдур Г. І., Гахов С. О., Скибун О. Ж. Кібербезпека у контексті формування міждисциплінарних підходів використання іт-технологій для відновлення України. Відновлення України: міжгалузевий теоретико-прикладний аналіз та потенціали розвитку :

Міжнародний науково-практичний форум, 11 квітня 2025 року, м. Одеса. Львів – Торунь : Liha-Pres, 2025. – Ч. 2. – 81-83.
2. Gakhov S. Samoilenko V., Analysis of machine learning methods for detecting malicious processes in a corporate network. VII International Scientific and Practical Conference «GRUNDLAGEN DER MODERNEN WISSENSCHAFTLICHEN FORSCHUNG», December 13, 2024; Zurich, Switzerland, 244-246. DOI: 10.36074/logos-13.12.2024.050
3. Гайдур Г. І., Гахов С. О. Врахування тенденцій штучного інтелекту під час підготовки фахівців з кібербезпеки. Штучний інтелект у вищій освіті: ризики та перспективи інтеграції: матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, 1 липня – 11 серпня 2024 року. – Львів –Торунь : Liha-Pres, 2024. С. 50-53. ISBN 978-966-397-412-5
4. Haidur H., Gakhov S. Detection of malicious processes in the organization's network traffic using synthetic data. Cybersecurity of energy, scientific-practical conference of the G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine: materials, May 31, 2023. Kyiv: PIMEE NAS of Ukraine, 2023. P. 30–33.
5. Гайдур Г.І., Гахов С.О., Скибун О.Ж. Готові програмні продукти захисту персональних даних в рамках використання концепції BYOD. / Modern tools and methods of scientific investigations: collection of scientific papers «SCIENTIA» with Proceedings of the II International Scientific and Theoretical Conference, December 8, 2023. Antwerp, Kingdom of Belgium: International Center of Scientific Research. 347 p.

							pp.160-166. 6. Гайдур Г.І., Гахов С.О., Скибун О.Ж. Аналіз вимог нормативних документів щодо захисту персональних даних. / Scientific review of the actual events, achievements and problems: collection of scientific papers «SCIENTIA» with Proceedings of the I International Scientific and Theoretical Conference, December 1, 2023. Berlin, Federal Republic of Germany: International Center of Scientific Research. 347p. pp.167-173. 19.діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях; Учасник робочої групи з розробки професійних стандартів: «ФАХІВЕЦЬ З ПЛАНУВАННЯ ПОЛІТИКИ ТА СТРАТЕГІЇ КІБЕРБЕЗПЕКИ» «ФАХІВЕЦЬ З РЕАГУВАННЯ НА ІНЦИДЕНТИ КІБЕРБЕЗПЕКИ» «ФАХІВЕЦЬ ІЗ КІБЕРДОСЛІДЖЕНЬ ТА РОЗРОБОК СИСТЕМ БЕЗПЕКИ» «АНАЛІТИК ЗАГРОЗ БЕЗПЕКИ» 20. досвід практичної роботи за спеціальністю не менше п'яти років (крім педагогічної, науково-педагогічної, наукової діяльності). 1989-2013- Служба у Збройних Силах України за спеціальністю. 2013-2014 – начальник режимно-секретного відділу ТОВ «Прогноз Україна».
291861	Марченко Віталій Вікторович	Доцент, Основне місце роботи	Навчально-науковий інститут Кібербезпеки та захисту інформації	Диплом бакалавра, Черкаський державний технологічний університет, рік закінчення: 2016, спеціальність: 6.170101 безпека інформаційних і комунікаційних систем, Диплом магістра,	7	Технології забезпечення безпеки мережевої інфраструктури	Види і результати професійної діяльності за спеціальністю відповідно до п.38 Ліцензійних умов провадження освітньої діяльності: п.п. 38.1), 38.3), 38.4), 38.5), 38.7), 38.11), 38.12), 38.14) наявність сертифіката відповідно до Загальноєвропейської рекомендації з мовної

				Державний університет телекомунікацій, рік закінчення: 2018, спеціальність: 125 Кібербезпека, Диплом доктора філософії Н23 000683, виданий 21.06.2023			освіти В2 з англійської мови 1. Наявність не менше п’яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection; 1. Гайдур Г. І., Гахов С. О., Марченко В. В. Метод побудови динамічної моделі логічного об’єкта інформаційної системи та визначення закону його функціонування. RADIOELECTRONIC AND COMPUTER SYSTEMS. 2022. № 1. С. 129–140. DOI: 10.32620/reks.2022.1.10 (Scopus). 2. Концептуальна модель виявлення фішингових атак на основі використання методів опорних векторів / Г. І. Гайдур та ін. Сучасний захист інформації №2(2024). 2024. С. 24–33. DOI: 10.31673/2409-7292.2024.020003. 3. Марченко В.В, Чайківський В.В., Прийма О.О. Метод підвищення обізнаності особового складу з інформаційної безпеки за допомогою програмного застосунку GOPHISH. Системи і технології зв’язку, інформатизації та кібербезпеки. 2024. № 6. С. 116–126. DOI: 10.58254/viti.6.2024.09.116. 4. Лаптєв О., Марченко В. Застосування завад для захисту інформації від витоку радіоканалом. Сучасний захист інформації. 2025. Т. 1, № 61. С. 89–97. DOI: 10.31673/2409-7292.2025.013057. 5. Quantitative WEB Application Vulnerability Assessment using SAST Methodology / A. Bryhynets et al. International Journal of Computing. 2025. Vol. 24, no. 1. P. 163–170. DOI:10.47839/ijc.24.1.3888 (Scopus). 6. Ensuring efficient power system operation

							in partial phase modes / V. Kuchanskyy et al. Energy Reports. 2025. Vol. 13. P. 5187–5195. DOI:10.1016/j.egyr.2025.04.056 (Scopus). 3. Наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора); 1. Математичні методи криптології: Навчальний посібник [Електронний ресурс] (Для студентів техн. спец. вищ. навч. закл.) / [А.Д. Кожухівський, І.Д. Горбенко, Г.І. Гайдур, О.А. Кожухівська, В.В. Марченко]; М-во освіти і науки України, Державний університет телекомунікацій.- К.: ДУТ, 2021 – 244 с.. 2. Вступ до квантової криптології [Текст]: Навчальний посібник (Для студентів техн. спец. вищ. навч. закл.) / [А.Д. Кожухівський, І.Д. Горбенко, В.К. Задірака, О.М. Хіміч, Ю.І. Горбенко, Г.І. Гайдур, О.А. Кожухівська, В.В. Марченко.]; М-во освіти і науки України, Державний університет інформаційно-комунікаційних технологій.- К.: ДУІКТ, 2024. – 597 с. 3. Г.І Гайдур., З.З. Бондаренко, В.В. Марченко, Н.С. Чумак. Лабораторний практикум з навчальної дисципліни “Теорія інформації та кодування” Навчальний посібник для студентів вищих навчальних закладів – Київ: ДУТ, ННІЗІ, 2021. – 50с 4. Наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів,

							конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування; 1. Методичні рекомедації до виконання лабораторних робіт з дисципліни “Прикладна криптологія”: [Електронний ресурс] (Для студентів техн. спец. вищ. навч. закл.) / [А.Д. Кожухівський, І.Д. Горбенко, Г.І. Гайдур, В,А. Савченко, В.В. Марченко, О.А. Кожухівська]; М-во освіти і науки України, Державний університет телекомунікацій. – К: ДУІКТ, 2025. – 109 с. 2. А.Д. Кожухівський, Г.І. Гайдур, О.А. Кожухівська, В.В. Марченко, С.О. Алексенко. Імітаційне моделювання Систем та процесів кібербезпеки В середовищі matlab Практикум. К.: ДУТ, 2020. – 78 с. 3. Методичні рекомендації до виконання кваліфікаційної роботи першого рівня вищої освіти «Бакалавр» для студентів спеціальності 125 «Кібербезпека та захист інформації» // Гайдур Г.І., Гахов С.О., Марченко В.В. Собчук А.В., Дмітрієв В.Є./ – К.: ДУІКТ, 2025. – 44 с. 4. Методичні рекомендації до виконання кваліфікаційної роботи другого (магістерського) рівня вищої освіти здобувачів спеціальності 125 Кібербезпека та захист інформації кафедри систем та технологій кібербезпеки освітньо-професійної програми «Інформаційна та кібернетична безпека» / Гайдур Г.І., Гахов С.О., Марченко В.В. ,Чумак Н.С. /– К.: ДУІКТ, 2024. 44 с/ 5. Захист дисертації на здобуття наукового ступеня;

							Доктор філософії Спеціальність 125 Кібербезпека Тема: «Метод виявлення шкідливих процесів в інформаційній системі підприємства на основі ідентифікації та діагностування станів логічних об'єктів» Диплом Н23 №000683 від 01 червня 2023 р. 11. Наукове консультування підприємств, установ, організацій не менше трьох років, що здійснювалося на підставі договору із закладом вищої освіти (науковою установою); 1. Консультація відповідно договору № 0203 від 02 березня 2020 року з ТОВ « Центр інформаційної та технічної підтримки «Сапфоріс». 12. Наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п'яти публікацій; 1. Марченко В.В., Макеєв М.Б., Програмні вразливості, як загроза мережевій безпеці. Науково-практична інтернет-конференція «Цифрова трансформація кібербезпеки», м. Київ, 25 березня 2021 / ДУТ. – С. 82-85. 2. Savchenko, V., Haidur, H., Dzyuba, T., Marchenko, V., Matsko, O., & Havryliuk, I. (2021). Providing of data center information security on the basis of Performance Balance. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT). DOI: 10.1109/atit54053.2021.9678679 (Scopus). 3. Веселков Н.Л., Марченко В.В., Метод оптимізації процесів розслідування Кіберінцидентів в розгалужених SOC командах.

							Всеукраїнська науково-практична конференція «Актуальні проблеми кібербезпеки», м. Київ, 27 жовтня 2023 / ДУІКТ. – С. 54-56. 4. Марченко В.В., Коліда В.П., Метод виявлення шкідливого програмного забезпечення в корпоративній мережі на основі методів машинного навчання в реальному часі. Всеукраїнська науково-практична конференція «Актуальні проблеми кібербезпеки», м. Київ, 27 жовтня 2023 / ДУІКТ. – С. 383-384. 5. Марченко В.В. Штучний інтелект в освітньому процесі закладів вищої освіти. Штучний інтелект у вищій освіті: ризики та перспективи інтеграції: матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, 1 липня – 11 серпня 2024 року. – Львів –Торунь : Liha-Pres, 2024. С. 201-203. ISBN 978-966-397-412-5. 6. Марченко В., Гайдур Г., Кушнір Д. Використання OSINT-інструментів для створення профілю державних службовців. Кібероборотьба: розвідка, захист та протидія : III Міжнар. науково-практ. конф., м. Київ, 6–7 трав. 2025 р. Київ, 2025. С. 34–36. DOI: 10.61929/viti.mnpk.3.2025. 14. Керівництво студентом, який зайняв призове місце на І або ІІ етапі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт), або робота у складі організаційного комітету / журі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт), або керівництво постійно діючим студентським науковим гуртком / проблемною групою; керівництво

							студентом, який став призером або лауреатом Міжнародних, Всеукраїнських мистецьких конкурсів, фестивалів та проектів, робота у складі організаційного комітету або у складі журі міжнародних, всеукраїнських мистецьких конкурсів, інших культурно-мистецьких проектів (для забезпечення провадження освітньої діяльності на третьому (освітньо-творчому) рівні); керівництво здобувачем, який став призером або лауреатом міжнародних мистецьких конкурсів, фестивалів, віднесених до Європейської або Всесвітньої (Світової) асоціації мистецьких конкурсів, фестивалів, робота у складі організаційного комітету або у складі журі зазначених мистецьких конкурсів, фестивалів); керівництво студентом, який брав участь в Олімпійських, Паралімпійських іграх, Всесвітній та Всеукраїнській Універсіаді, чемпіонаті світу, Європи, Європейських іграх, етапах Кубка світу та Європи, чемпіонаті України; виконання обов'язків тренера, помічника тренера національної збірної команди України з видів спорту; виконання обов'язків головного секретаря, головного судді, судді міжнародних та всеукраїнських змагань; керівництво спортивною делегацією; робота у складі організаційного комітету, суддівського корпусу: 1. Керівник гуртка «Основи інформаційної та кібернетичної безпеки» затверджено протоколом кафедри від 27 серпня 2020року № 1.
150389	Легомінова Світлана Володимирів	Завідувач кафедри, Основне	Навчально-науковий інститут	Диплом спеціаліста, Латвійський	16	Управління проектами інформаційної	Види і результати професійної діяльності за

	на	місце роботи	Кібербезпеки та захисту інформації	університет, рік закінчення: 1993, спеціальність: економіка і соці-альне планування, Диплом магістра, Державний університет інформаційно-комунікаційних технологій, рік закінчення: 2024, спеціальність: 125 Кібербезпека, Диплом доктора наук ДД 008898, виданий 15.10.2019, Диплом кандидата наук ДК 014670, виданий 12.06.2002, Атестат доцента 12ДЦ 046345, виданий 25.02.2016, Атестат професора АП 002374, виданий 15.12.2020		безпеки	спеціальністю відповідно до п.38 Ліцензійних умов провадження освітньої діяльності: п. 1, 3, 4, 5, 7, 8, 10, 11, 12,14, 19 Сертифікат про рівень володіння державною мовою УМД N 00190455 від 11.08.2023. наявність сертифіката відповідно до Загальноєвропейської рекомендації з мовної освіти В2 з англійської мови реєстраційний номер 5221/25 від 02.07.2025 1 - Наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection; 1. Savchenko, V., Lehominova, S., Dzyuba, T., Havryliuk, I., Novikova, I. Model of Connectivity in a Mobile MESH Network for a Group of Unmanned Aerial Vehicles. 2022 IEEE 4th International Conference on Advanced Trends in Information Theory, ATIT 2022 – Proceedings. 2022, pp. 142–147. (SCOPUS) URL: https://ieeexplore.ieee.org/document/10024235 https://www.scopus.com/authid/detail.uri?authorId=57217034683 2. Lehominova S., Zaporozhchenko M., Shchavinsky Yu., Muzhanova T., Tyshchenko V., Yushchenko M. Methodology for Determining Means of Monitoring Information Security by the Method of Expert Assessment. International Journal of Computing. 2024. Vol. 23 (4). P. 681-691. URL: https://computingonline.net/files/journals/1/archieve/IJC_2024_23_4_17.pdf (SCOPUS) 3. Vitalii Savchenko, Halyna Haidur, Svitlana Lehominova, Taras Dzyuba and Oleksandr Laptiev. Modeling of

							media influence on personal information security. 2024 IT&I. Information technology and implementation. November 20-21, 2024 Taras Shevchenko National University of Kyiv pp. 196-206. URL: https://ceur-ws.org/Vol-3909/Paper_15.pdf. (Scopus). 4. 27. Легомінова С.В., Примаченко Д.В. Роль ризик-менеджменту в підвищенні кіберстійкості організації за умов гібридних загроз. Кібербезпека: освіта, наука, техніка. 2025. Том 3 №31. С. 792–800. DOI: https://doi.org/10.28925/2663-4023.2025.31.1060. URL: https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/1060 5. 28. Мужанова Т., Легомінова С., Капелюшна Т., Щавінський Ю., Запорожченко М. Особливості сучасних кібероперацій за підтримки держав як новітньої форми міждержавного протиборства. Кібербезпека: освіта, наука, техніка. 2026. 4(32), С. 71–89. https://doi.org/10.28925/2663-4023.2026.32.1116 6. 29. Легомінова С.В., Запорожченко М.М., Рабчун Д.І. Формалізація системи показників оцінювання результативності програм навчання персоналу з інформаційної безпеки. Кібербезпека: освіта, наука, техніка. 2026. №1(33). С. 55–64. DOI: https://doi.org/10.28925/2663-4023.2026.33.1179 3.наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора);

							1. Легомінова С. В., Мужанова Т. М. Безпечне використання захищеної інформації про критичну інфраструктуру: досвід США.Challenges and threats to critical infrastructure: Collective monograph. NGO Institute for Cyberspace Research. Detroit, Michigan, USA, 2023. pp. 191-194. URL: https://conference.cyberspace.org.ua/wp-content/uploads/2023/06/Monograph-09-06-2023.pdf 2. Голобородько А.Ю., Гусєва О.Ю., Легомінова С.В. Цифрова економіка: підручник. Київ: Видавництво “Міленіум” , 2020. 400 с. 3. Легомінова С.В., Якименко Ю.М., Савченко В.А. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник, Київ: Державний університет телекомунікацій, 2022. 306с. 4. Легомінова С. В., Щавінський Ю. В., Мужанова Т. М., Якименко Ю. М., Капелюшна Т. В., Рабчун Д. І. Професійна етика управлінської діяльності в кібербезпеці : навч. посіб. Київ : ДУТ, 2023. 198 с. 5. Легомінова С. В., Мужанова Т. М., Щавінський Ю. В., Якименко Ю. М., Запорожченко М. М., Рабчун Д. І. Аудит інформаційної безпеки : навч. посіб. Київ : ДУТ, 2023. 125 с. 6. Якименко Ю. М., Легомінова С. В., Щавінський Ю. В., Рабчун Д. І. Управління інцидентами інформаційної безпеки. Сучасні методи і засоби : навч. посіб. Київ : ДУТ, 2023. 7. Шульга В.П., Легомінова С. В., Гайдур Г.І., Щавінський Ю. В., Мужанова Т.М., Якименко Ю. М. Застосування програмно–технічних комплексів в

							управлінні кібербезпекою та захистом інформації. Alient Vault, IBM QRadar, Nessus, Kali Linux. Київ: ДУІКТ, 2024, 220 с.. 4.наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування; 1. Електронний курс у системі Google Classroom «Основи управління інформаційною та кібербезпекою». 2. Електронний курс у системі Google Classroom «Аудит інформацыйної безпеки». 3. Електронний курс у системі Google Classroom «Основи а кібербезпеки та захисту інформації». 4. Електронний курс у системі Google Classroom «Управління проєктами інформаційної безпеки». 5 Легомінова С.В., Мужанова Т.М., Рабчун Д.І., Щавінський Ю.В. Методичні рекомендації до виконання кваліфікаційної роботи другого магістерського рівня вищої освіти для студентів спеціальності 125 «Кібербезпека» : метод. реком. Київ: ДУТ, 2022. 39 с.. 5.захист дисертації на здобуття наукового ступеня; Доктор економічних наук, спеціальність 08.00.04. «Економіка та управління підприємствами, (за видами економічної діяльності)». Тема докторської дисертації: “Управління

							конкурентними перевагами телекомунікаційних підприємств: теорія і методологія". Диплом ДД №008898 від 15.10.2019 р. Захист відбувся у 2019 році в Державному університеті телекомунікацій Міністерства освіти і науки України. 6) наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня (прізвище, ім'я, по батькові дисертанта, здобутий науковий ступінь, спеціальність, назва дисертації, рік захисту, серія, номер, дата, ким виданий диплом) Капелюшна Тетяна Вікторівна, доктор економічних наук, 08.00.04 – Економіка та управління підприємствами (за видами економічної діяльності). Тема: Управління безпекою підприємств: теорія та методологія. Диплом DD №13616 від 10.12.2024, Державний університет інформаційно-комунікаційних технологій. Запорожченко Михайло Михайлович, доктор філософії, 125 Кібербезпека. Тема дисертації: «Методи прогнозування соціоінженерних атак на корпоративні інформаційні системи на основі профілю захищеності користувача». Диплом доктора філософії Н25 № 000720 (рішення від 17.04.2025), Державний університет інформаційно-комунікаційних технологій. 7.участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад; Офіційний опонент на захисті дисертацій: 1. Шамін М.В. "Науково-прикладні

							основи розвитку інтелектуального потенціалу працівників підприємства зв’язку”, поданої на здобуття наукового ступеня кандидата економічних наук зі спеціальності 08.00.04 - економіка та управління підприємствами (за видами економічної діяльності), 2020 рік. Одеська національна академія зв’язку ім. О. С. Попова, 2020. 2. Глухов Микита Олексійович “Організаційно-економічний механізм розвитку суб’єктів ринку телекомунікаційних послуг в Україні,” на здобуття ступня доктора філософії за спеціальністю 073 “Менеджмент”, 2025 рік. Європейський університет, 2025 1. Член спеціалізованої вченої ради Д 26.861.03 з правом прийняття до розгляду та проведення захисту дисертацій на здобуття наукового ступеня доктора (кандидата) економічних наук за спеціальністю 08.00.04 “Економіка та управління підприємствами (за видами економічної діяльності)”. 2. Член разової СР в ДУІКТ із захисту Асан Айсулу, 15.08.2025. 3. Член разової СР в ДУІКТ із захисту МІШКУРА Юрія Валентиновича, 2.07.2026. 4. Член разової СР в ДУІКТ із захисту СНІТКА Артема Сергійовича, 3.07.2026. 5. Член разової СР в ДУІКТ із захисту ГАМЗИ Дмитра Євгенійовича, 3.07.2026. 8.виконання функцій (повноважень, обов’язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до

							переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах; 1. Керівник ініціативної науково-дослідної роботи за темою: “Конкурентна розвідка як складова забезпечення інформаційної безпеки підприємства”, шифр “CompInt” (2018-2020 рр.) № держреєстрації 0118U100058. 2. Керівник ініціативної науково-дослідної роботи за темою: “Кадрові технології в управлінні інформаційною безпекою підприємства”, (2020-2022 рр.) № держреєстрації 0120U105132. 3. Керівник ініціативної науково-дослідної роботи за темою: “Розробка рекомендацій щодо засад запобігання і протидії методам соціальної інженерії у забезпеченні інформаційної безпеки підприємства”, (2022-2024 рр.) № держреєстрації 0123U100743. 4. Член редакційної колегії наукового фахового журналу «Економіка.Менеджмент.Бізнес», включеного до переліку фахових видань України. 5. Член редакційної колегії наукового фахового журналу «Journal of Scientific Papers Social development and Security», включеного до переліку фахових видань України. 10.участь у міжнародних наукових та/або освітніх проектах, залучення до міжнародної експертизи, наявність звання “суддя міжнародної категорії”; 1. Державний навчально-науковий заклад післядипломної освіти» Дипломатична Академія України

							імені Геннадія Удовенка при Міністерстві закордонних справ України, «War in Ukraine and its impact on EU Economy», міжнародний проєкт з розвитку професійної компетентності державних службовців у сфері зовнішніх зносин, навчання за спеціалізованою програмою, сертифікат – реєстраційний номер № ЦП20062173/024/23,10 годин /0,3 кредити ЄКТС, 12 січня, 2023, м. Київ. 11.наукове консультування підприємств, установ, організацій не менше трьох років, що здійснювалося на підставі договору із закладом вищої освіти (науковою установою); 1. ТОВ «ІТ - Спеціаліст», договір №34/1294 від 23.01.2020 2. ТОВ «СМАРТ ТЕХНОЛОДЖІС», договір №31/1035 від 03.02.2020 3. ТОВ “РЕАЛЛАЙН”, договір № 34/1295 від 04.12.2020 4. ДП «ЕС ЕНД ТІ УКРАЇНА», договір №8/28.11.2022 5. ТОВ «ІНФОРМАЦІЙНІ СПЕЦІАЛІЗОВАНІ СИСТЕМИ», договір № 1901-24/1.12.2023 6. ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА СИСТЕМ НАН УКРАЇНИ, договір № 9 07.03.2025 7. Госпдоговір № 02/21 від 25.02.2021 ТОВ «БУХГАЛТЕРСЬКА КОМПАНІЯ ПРОФІТ» («Кадрові технології в управлінні інформаційною безпекою підприємства»). 8. Госпдоговір № 2025/1212 від 12.12.2025 ТОВ “АЛЬФА-МЕТАЛ” (“Розробка рекомендацій для створення системи виявлення шкідливих процесів в інформаційній системі організації”). 12.наявність апробаційних та/або

							науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п’яти публікацій; 1. Легомінова С.В., Мужанова Т.М., Коврига М. Стратегії захисту від кібератак, що спонсоруються державами. Актуальні проблеми кібербезпеки: матеріали Всеукраїн. наук.-практ. конф., (м. Київ, Україна, 29 жовтня 2025 р.). Київ: ДУІКТ, 2025. С.218-220. URL: https://duikt.edu.ua/uploads/p_2779_58326207.pdf 22. Савченко В., Гайдур Г., Легомінова С. Прогнозування повільних DDoS атак на основі кореляційного аналізу індивідуальних траєкторій трафіку. Безпека сучасних інформаційно-комунікаційних систем: матеріали Міжнар. наук.-техн. конф., м. Львів, 16-18 жов. 2025 р. Львів: ЛНУ ім. І. Франка, 2025. С. 194-199. 2. Svitlana Lehominova, Tetiana Kapeliushna, Tetiana Muzhanova. The concept of the principles of information warfare in the context of hybrid aggression against Ukraine. Digital Transformation: Strengthening the Cybersecurity Capacities in the Modern World: materials of International scientific-practical conf., (c. Krakow, Poland, 4-5 November 2025). Krakow: 2025. pp. 67-68. URL: https://duikt.edu.ua/uploads/p_2779_38079537.pdf 3. Svitlana Lehominova, Mykhailo Zaporozhchenko. An analysis of organizational determinants of corporate vulnerability to social engineering attacks. Digital Transformation: Strengthening the Cybersecurity Capacities in the

							Modern World: materials of International scientific-practical conf., (c. Krakow, Poland, 4-5 November 2025). Krakow: 2025. p. 60. URL: https://duikt.edu.ua/uploads/p_2779_38079537.pdf 4. Легомінова С. В., Лугін М.О.Аналіз сучасних векторів атак на хмарні технології в корпоративному середовищі та розробка комплексних засобів захисту. Стратегії кіберстійкості: управління ризиками та безперервність бізнесу: матеріали VI Всеукраїн. наук.-практ. конф., (м. Київ, Україна, 25 лютого 2026 р.). Київ: ДУІКТ, 2026. С. 108-110. URL: https://duikt.edu.ua/uploads/p_3086_48908725.pdf 5. Легомінова С. В., Мужанова Т. М., Щавінський Ю. В. Основні чинники формування культури кібербезпеки організації. Стратегії кіберстійкості: управління ризиками та безперервність бізнесу: матеріали VI Всеукраїн. наук.-практ. конф., (м. Київ, Україна, 25 лютого 2026 р.). Київ: ДУІКТ, 2026. С. 202-205. URL: https://duikt.edu.ua/uploads/p_3086_48908725.pdf 6. Капелюшна Т., Легомінова С., Мужанова Т. Протидія когнітивним викривленням як чинник стійкості суспільства в умовах гібридних загроз. Проблеми кібербезпеки інформаційно-комунікаційних систем (PCSICS): матеріали IX Міжнар. наук.-техн. конф., (м. Київ, Україна, 24 квітня 2026 р.) Київ: Київський національний університет імені Тараса Шевченка. ВПЦ "Київський університет", 2026. С.194 14.керівництво студентом, який зайняв призове місце на І або ІІ етапі Всеукраїнської студентської

							олімпіади (Всеукраїнського конкурсу студентських наукових робіт), або робота у складі організаційного комітету / журі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт), або керівництво постійно діючим студентським науковим гуртком / проблемною групою; керівництво студентом, який став призером або лауреатом Міжнародних, Всеукраїнських мистецьких конкурсів, фестивалів та проектів, робота у складі організаційного комітету або у складі журі міжнародних, всеукраїнських мистецьких конкурсів, інших культурно-мистецьких проектів (для забезпечення провадження освітньої діяльності на третьому (освітньо-творчому) рівні); керівництво здобувачем, який став призером або лауреатом міжнародних мистецьких конкурсів, фестивалів, віднесених до Європейської або Всесвітньої (Світової) асоціації мистецьких конкурсів, фестивалів, робота у складі організаційного комітету або у складі журі зазначених мистецьких конкурсів, фестивалів); керівництво студентом, який брав участь в Олімпійських, Паралімпійських іграх, Всесвітній та Всеукраїнській Універсіаді, чемпіонаті світу, Європи, Європейських іграх, етапах Кубка світу та Європи, чемпіонаті України; виконання обов'язків тренера, помічника тренера національної збірної команди України з видів спорту; виконання обов'язків головного секретаря, головного судді, судді міжнародних та всеукраїнських змагань; керівництво

							спортивною делегацією; робота у складі організаційного комітету, суддівського корпусу; Робота у складі журі Всеукраїнського конкурсу студентських наукових робіт з кібербезпеки (І етап) 2025 рік, ДУІКТ. Робота у складі журі Всеукраїнського конкурсу студентських наукових робіт з кібербезпеки (ІІ етап) 2026 рік, ДУІКТ. 19) діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях 1. Учасник робочої групи з розробки професійних стандартів: «ФАХІВЕЦЬ З ТЕСТУВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ» «АНАЛІТИК З ОЦІНКИ ВРАЗЛИВОСТЕЙ» «АУДИТОР ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ (З КІБЕРБЕЗПЕКИ)»
435683	Щавінський Юрій Віталійович	Доцент, Основне місце роботи	Навчально-науковий інститут Кібербезпеки та захисту інформації	Диплом спеціаліста, Хмельницьке вище артилерійське командне училище, рік закінчення: 1982, спеціальність: командна, тактична, артилерійське озброєння, Диплом кандидата наук ДК 055434, виданий 16.12.2019	16	Корпоративна та професійна етика в кібербезпеці	діяльності за спеціальністю відповідно до п.38 Ліцензійних умов провадження освітньої діяльності: п.п. 1, 3, 4, 5, 8, 12, 14 1.наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection 1. Будзинський, О., Щавінський, Ю., Мужанова, Т., Якименко, Ю., & Примаченко, Д. (2026). МЕТОДИКА ІНТЕЛЕКТУАЛЬНОЇ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАТИВНИХ БАЗ ДАНИХ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(33), 399–413. https://doi.org/10.28925/2663-4023.2026.33.1221 2. Мужанова, Т., Легомінова, С., Капелюшна, Т., Щавінський, Ю., &

							Запорожченко, М. (2026). ОСОБЛИВОСТІ СУЧАСНИХ КІБЕРОПЕРАЦІЙ ЗА ПІДТРИМКИ ДЕРЖАВ ЯК НОВІТНЬОЇ ФОРМИ МІЖДЕРЖАВНОГО ПРОТИБОРСТВА. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(32), 71–89. https://doi.org/10.28925/2663-4023.2026.32.1116 3. Легомінова С.В., Капелюшна Т.В., Щавінський Ю.В., Мужанова Т.М. (2025) Модель оцінювання етичної зрілості системи інформаційної безпеки організації. Телекомунікаційні та інформаційні технології №3(2025), стр. 194-203. https://doi.org/10.31673/2412-4338.2025.038722 4. Легомінова С.В., Капелюшна Т.В., Щавінський Ю.В., Мужанова Т.М. (2025) Концептуальні підходи інтеграції етичних норм у політику інформаційної безпеки. Сучасний захист інформації, 3(63), 90–98. https://doi.org/10.31673/2409-7292.2025.031152 5. Lehominova, S., Kapeliushna, T., Shchavinskyi, Y., Zaporozhchenko, M., & Budzynskyi, O. (2025a). CONCEPT OF AUTOMATED RESPONSE TO THREATS IN CORPORATE DATABASES IN REAL-TIME MODE. Cybersecurity: Education, Science, Technique, 1(29), 676–686. https://doi.org/10.28925/2663-4023.2025.29.927 . 6. Shchavinsky Yu. APPLICATION OF ETHICAL PRINCIPLES IN CYBERSECURITY/ Modern vision of implementing innovations in scientific studies: collection of scientific papers «SCIENTIA» with Proceedings of the VI International Scientific and Theoretical

							Conference, July 25, 2025. Marseille, French Republic: International Center of Scientific Research. pp. 83-87. https://doi.org/10.36074/scientia-25.07.2025 . 3.наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора); 1. ЗАСТОСУВАННЯ ПРОГРАМНО–ТЕХНІЧНИХ КОМПЛЕКСІВ В УПРАВЛІННІ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ. ALIENVAULT, QRADAR, NESSUS, KALI LINUX. Навчально–методичний посібник / В.П. Шульга, С.В. Легомінова, Г.І. Гайдур, Ю.В. Щавінський, Т.М. Мужанова, Ю.М. Якименко, К. : ДУІКТ, 2024, 220 с. 2. ПРОФЕСІЙНА ЕТИКА УПРАВЛІНСЬКОЇ ДІЯЛЬНОСТІ В КІБЕРБЕЗПЕЦІ. Навчальний посібник / С.В. Легомінова, Ю.В. Щавінський, Т.М. Мужанова, Ю.М. Якименко, Т.В. Капелюшна, Д.І. Рабчун, К. : ДУТ, 2023, 198 с. 3. Легомінова С. В., Мужанова Т. М., Щавінський Ю. В., Якименко Ю. М., Запорожченко М. М., Рабчун Д. І. Аудит інформаційної безпеки : навч. посіб. Київ : ДУТ, 2023. 125 с. 4. Якименко Ю. М., Легомінова С. В., Щавінський Ю. В., Рабчун Д. І. Управління інцидентами інформаційної безпеки. Сучасні методи і засоби: навч. посіб. Київ : ДУТ, 2023. 5. Мужанова Т. М., Щавінський Ю. В., Рабчун Д. І. Управління безпекою інформаційних мереж : навч. посіб. Київ : ДУТ, 2023.

							4.наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування; 1. Легомінова С.В., Мужанова Т.М., Якименко Ю.М., Рабчун Д.І., Щавінський Ю.В. Методичні рекомендації до виконання кваліфікаційної роботи першого бакалаврського рівня вищої освіти для студентів спеціальності 125 «Кібербезпека» : метод. реком. Київ: ДУТ, 2022. 30 с. URL: https://dut.edu.ua/uploads/p_366_87119203.pdf 2. Легомінова С.В., Мужанова Т.М., Рабчун Д.І., Щавінський Ю.В. Л 38 Методичні рекомендації до виконання кваліфікаційної роботи другого магістерського рівня вищої освіти для студентів спеціальності 125 «Кібербезпека» : метод. реком. Київ: ДУТ, 2022. 39 с.URL: https://dut.edu.ua/uploads/p_366_58878899.pdf 3. Інформаційні технології у психології ч. 2. Електронний навчально-методичний комплекс /Щавінський Ю.В., Баранюк Н.І.// Львів : Національний університет «Львівська політехніка», 2020. № Е41-139-326/2020 від 12.10.2020 4. Корпоративна та професійна етика у кібербезпеці. Навчальна програма 2022. 5. Корпоративна та професійна етика у

							кібербезпеці. Робоча навчальна програма 2022. 5. захист дисертації на здобуття наукового ступеня Кандидат технічних наук, спеціальність 20.02.14 «Озброєння та військова техніка». Тема дисертації «Методика підвищення точності і оперативності підготовки даних для стрільби артилерійських систем». Диплом ДК № 055434 від 16.12.2019 р. Захист відбувся 2019 року в Національній академії Сухопутних військ ЗС України. 12.наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п'яти публікацій; 1. Олександр Будзинський, Юрій Щавінський. Застосування штучного інтелекту для визначення аномалій доступу до баз даних.Зб. тез доповідей IX Міжнародної науково-практичної конференції «Проблеми кібербезпеки інформаційно-комунікаційних систем» (PCSICS). 24 квітня 2026 року. К.: ВПЦ «київський університет». С. 128-131. https://drive.google.com/drive/folders/1dVUr1WyfUSNzx1-6IZv0gKi-sqRCT_Kt?usp=drive_link 2. Щавінський Ю.В., Будзинський О.В. Застосування інструментів симуляції кіберінцидентів для перевірки захисту корпоративних баз даних. Наукові відкриття та фундаментальні наукові дослідження: світовий досвід: збірник наукових праць з матеріалами VII Міжнародної наукової конференції,

							м. Житомир, 2025 р. / Міжнародний центр наукових досліджень. Вінниця. «Укрлогос-груп», 2025. С. 246-249. URL: https://doi.org/10.62731/mcnd-24.10.2025 3. Бортник Л.Л., Щавінський Ю.В., Будзинський О.В. Проблеми та перспективи забезпечення кібербезпеки логістичних систем підрозділів Збройних Сил України. Збірник тез доповідей Всеукр. наук.-практ. конф., Львів, 26-27 лист. 2025 р. / Львів: НАСВ 2025. С. 466-467. URL: https://asv.mil.gov.ua/sites/default/files/2026-01/1-zbirnyk-tez_2025_hotovo_0.pdf 4. Shchavinsky Yu., Budzynskyi O., Prymachenko D., Sviatska N. Applying structural-functional analysis to protect corporate databases. Digital Transformation: Strengthening the Cybersecurity Capacities in the Modern World, Krakow, 4-5 November 2025. P. 73-75. URL: https://duikt.edu.ua/uploads/p_2779_38079537.pdf 5. Щавінський Ю.В., Будзинський О.В. Technological requirements for the protection of corporate databases in connection with the development of network infrastructure. Актуальні проблеми кібербезпеки: зб. тез доп. міжнар. наук.-практ. конф., Київ, 2023. С. 226-228 https://duikt.edu.ua/uploads/p_2626_52007398.pdf 6. Щавінський Ю. В., Будзинський О. В. Шляхи удосконалення захисту корпоративних баз даних в комп'ютерних системах. Актуальні проблеми кібербезпеки: Матеріали Всеукраїнської науково-практичної конференції (м. Київ, 27 жовтня 2023 року). Навчально-науковий інститут захисту інформації, Державний університет

							інформаційно-комунікаційних технологій . Київ, 2023. С. 44-46. https://duikt.edu.ua/uploads/p_2626_52007398.pdf 14. керівництво студентом, який зайняв призове місце на І або ІІ етапі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт), або робота у складі організаційного комітету / журі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт), або керівництво постійно діючим студентським науковим гуртком / проблемною групою; керівництво студентом, який став призером або лауреатом Міжнародних, Всеукраїнських мистецьких конкурсів, фестивалів та проектів, робота у складі організаційного комітету або у складі журі міжнародних, всеукраїнських мистецьких конкурсів, інших культурно-мистецьких проектів (для забезпечення провадження освітньої діяльності на третьому (освітньо-творчому) рівні); керівництво здобувачем, який став призером або лауреатом міжнародних мистецьких конкурсів, фестивалів, віднесених до Європейської або Всесвітньої (Світової) асоціації мистецьких конкурсів, фестивалів, робота у складі організаційного комітету або у складі журі зазначених мистецьких конкурсів, фестивалів); керівництво студентом, який брав участь в Олімпійських, Паралімпійських іграх, Всесвітній та Всеукраїнській Універсіаді, чемпіонаті світу, Європи, Європейських іграх, етапах Кубка світу та Європи,

							чемпіонаті України; виконання обов'язків тренера, помічника тренера національної збірної команди України з видів спорту; виконання обов'язків головного секретаря, головного судді, судді міжнародних та всеукраїнських змагань; керівництво спортивною делегацією; робота у складі організаційного комітету, суддівського корпусу Керівництво постійно діючим студентським науковим гуртком «Розробка та технічна підтримка пристроїв для роботи в сфері кібербезпеки».
487740	Колісниченко Анна Віталіївна	Завідувач кафедри, Основне місце роботи	Навчально-науковий інститут Інформаційних технологій	Диплом спеціаліста, Ніжинський державний університет імені Миколи Гоголя, рік закінчення: 2006, спеціальність: 010103 Педагогіка і методика середньої освіти. Українська мова і література та мова і література (англійська), Диплом кандидата наук ДК 044200, виданий 11.10.2017, Атестат доцента АД 015082, виданий 24.04.2024	18	Англійська мова для ділової комунікації	Види і результати професійної діяльності за спеціальністю відповідно до п.38 Ліцензійних умов провадження освітньої діяльності: п.п. 1, 3, 4, 8,10, 12, 14, 19 1) публікації у наукових виданнях, включених до переліку наукових фахових видань України: 1.Anna Kolisnychenko, Svitlana Kharytska. Indian myths as the basis of Hart Crane's mythmaking. Alfred Nobel University Journal of Philology. – Vol. 2 (26/1) – Dnipro, 2023. – P. 89-104. (Scopus) https://doi.org/10.32342/2523-4463-2023-2-26/1-7 2. Харицька, С. В., Колісниченко, А. В. (2025). Інтеграція професійної англійської мови в підготовку ІТ-фахівців. Наукові записки. Серія «Психолого-педагогічні науки» (Ніжинський державний університет імені Миколи Гоголя), (4), 218–225. https://doi.org/10.31654/2663-4902-2025-PP-4-218-225 3. Колісниченко А. В., Харицька С. В. Художня ретрансляція етноментальних констант та сучасної

							соціально-історичної конкретики в імагінативному просторі ліричної творчості Анни Малігон. Рідне слово в етнокультурному вимірі». № 10. Дрогобич, 2025. С. 45-51 4. Харицька С.В., Колісниченко А.В., Конопляник Л.М. Національна складова стандартизації перекладних словників у процесі формування національної термінології і галузевих наукових тезаурусів. Науковий вісник Вінницької академії безперервної освіти. Серія «Педагогіка. Психологія». Вип. 7. Вінниця, 2025. С. 246-253. 5. Харицька С. В., Колісниченко А. В. Search-informational competence of future biomedical engineers and economists as an important component of adjustment of safety professional activity standards. Перспективи та інновації науки. Серія «Педагогіка». Серія «Психологія». Серія «Медицина». № 15(33). Київ, 2023. С. 38-54. https://doi.org/10.52058/2786-4952-2023-15(33)-38-54 6. Харицька С. В., Колісниченко А. В. Інтенсифікація концепції інклюзії в сучасних соціально-педагогічних доктринах та літературних студіях дизабіліті. Актуальні питання гуманітарних наук. – Випуск 47. Том 1– Дрогобич, 2022. – С. 207-213. https://doi.org/10.24919/2308-4863/47-1-31 7. Харицька С. В., Колісниченко А. В. Проблема адаптації форм виховних заходів до сучасних вимог дистанційного навчання. Перспективи та інновації науки. Серія: Педагогіка. Психологія. Медицина. – Випуск №8 (13), 2022. – С. 306-315. https://doi.org/10.52058/2786-4952-2022-8(13)-306-315

							8. Колісниченко. А. В. Конфлікт культур крізь призму індійської національної свідомості у оповіданні Порошурама «Сватання». Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Філологія. Журналістика. – Том 32 (71). – №2, 2021. – С. 178-182. https://doi.org/10.32838/2710-4656/2021.2-2/31 9. Харицька С. В, Колісниченко А. В. Інтеграція професійної англійської мови в підготовку ІТ фахівців. Психолого-педагогічні науки. № 4. Ніжин, 2025. С. 218-225. 10. Стежко С. О., Колісниченко А. В., Кондратенко Н. Ю., Павлов В. О. Методика формування академічної мовної компетентності українською та англійською мовами засобами цифрових освітніх платформ. Вісник науки та освіти: журнал. 2026. № 3(45) 2026. С. 1354-1368. 3) наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора); 1. Professional English. Information Technology: навч. посібник / О.В. Ковтун, Л. М. Конопляник, Ю. Ю. Пришупа, А. В. Колісниченко, С. В. Харицька. – Київ: ДУ «КАІ», 2025. 160 с. (20%). 2. Харицька С. В., Колісниченко А. В. The metaspace of the functioning of the concept of academic integrity as a factor in the formation of the identity of moral and ethical patterns.

							MODERNÍ ASPEKTY VĚDY. Svazek XL mezinárodní kolektivní monografie (Modern aspects of science. 40-th volume of the international collective monograph). Česká republika, 2024. – С. 166-180. 3. Харицька С. В., Колісниченко А. В. Патріотичне татуювання як виразник національної самоідентифікації. MODERNÍ ASPEKTY VĚDY. Svazek XXI mezinárodní kolektivní monografie (Modern aspects of science. 21-th volume of the international collective monograph). Česká republika, 2022. – С. 150-158. 4) наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування; 1. А. В. Колісниченко, С. В. Харицька. English for academis purposes. Методичні рекомендації для самостійної роботи здоьбувачів наукового ступеня доктора філософії з дисципліни «Англійська мова наукового спрямувавння» . – Київ: ДУІКТ, 2026. 30 с. 2.Professional English. Information Technology: навч. посібник / О.В. Ковтун, Л. М. Конопляник, Ю. Ю. Пришупа, А. В. Колісниченко, С. В. Харицька. – Київ: ДУ «КАІ», 2025. 160 с. (20%). 3. Колісниченко А. В. Professional English. Biomedical engineering: практикум з

							англійської мови / А. В. Колісниченко. – К.:НАУ, 2021. – 53 с. 4. Колісниченко А. В. Professional English. Ecology: практикум з англійської мови / А. В. Колісниченко. – К.:НАУ, 2021. – 53 с. 8) виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах; «Експлікація концептосфери національної ідентичності у мета дискурсі сучасних соціальних комунікацій» (реєстраційний номер: 44 – 2020 / 12.01.04) – держбюджетна (кафедральна) науково-дослідна робота (2020-2022), відповідальний виконавець «Культурна мультимодальність як визначник національної ідентичності у світовій літературно-художній спадщині» (реєстраційний номер: 45-2022/12.01.04) – держбюджетна (кафедральна) науково-дослідна робота (2022-2025), науковий керівник «Методи та засоби оптимізації параметрів та ресурсів електронних комунікаційних мереж та ІКС із застосуванням ШІ» (2025-2026 р.) , виконавець 10) участь у міжнародних наукових та / або освітніх проєктах, залучення до міжнародної експертизи, наявність звання «суддя міжнародної

							категорії»; 1. Міжнародна науково-практична конференція «Національна ідентичність в мові і культурі», член оргкомітету, відповідальна за секцію «Інтерпретація творів зарубіжної літератури» (2021-2025 р.) 2. VII Всеукраїнська студентська науково-практична конференція «Мова і світ: мовознавчі, літературознавчі і перекладознавчі аспекти взаємодії», член оргкомітету (2026). 12) наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п'яти публікацій; 1. Харицька С. В., Колісниченко А. В. Лінгвокультурні аспекти перекладу кулінаронімів. Проблеми ефективності професійної мовної комунікації в умовах інформаційної агресії: матеріали II Всеукр. наук.-практ. конф. з міжнародною участю (м. Київ, 28 листопада 2025 року). Київ : Київський інститут Національної гвардії України, 2025. С. 302-305. 2. Харицька С. В., Колісниченко А. В. Екстраполяція національної ідентичності в кулінарні патерни України. Нові перспективи національної ідентичності мові, мистецтві та літературі: збірник наукових праць. К., 2025. С. 145-150. 3. Романчук В. Ю., Колісниченко А. В. Revolutionizing creativity: the impact of AI on modern creative industries. Проблеми ефективності професійної мовної комунікації в умовах інформаційної агресії: матеріали II Всеукр.

							наук.-практ. конф. з міжнародною участю (м. Київ, 28 листопада 2025 року). Київ : Київський інститут Національної гвардії України, 2025. С. 223-225. 4.Колісниченко А. В., Харицька С. В. Мультимодальність інкорпорування STEM-освіти у процес формування Soft Skills та професійних компетентностей. Importance of Soft Skills for Life and Scientific Success: Proceedings of the 4th International Scientific and Practical Internet Conference, March 6-7, 2025. FOP Marenichenko V.V., Dnipro, Ukraine, 2025. С. 108-109. 5. Харицька С. В., Колісниченко А. В. Транслітерація фольклорних жанрів як засіб популяризації української культурної спадщини: кейс vesnianky. Global trends in science and education. Proceedings of XI International Scientific and Practical Conference. Kyiv, Ukraine, 2025. С. 915-919 6. Kharytska S., Kolisnychenko A. English texts reading strategies across professionally oriented training. Similarities and differences in teaching philological disciplines in Ukraine and Latvia. Proceedings of the scientific and pedagogical internship, December 4 – January 14, 2024. Riga, the Republic of Latvia, 2024. P. 41-45. 7. Kolisnychenko A., Kharytska S. Fake vs critical consumption of information. Interaction of the experience of post-Yugoslav and Ukrainian areas: cultural, linguistic, literary, artistic, historical, and journalistic aspects (February 23–24, 2024. Ljubljana, Slovenia). Riga, Latvia: Baltija Publishing, 2024. P. 10-1 8. Kharytska S., Kolisnychenko A. Inappropriate technologies of business administration of the Ukrainian aviation industry in the

							21st century. Proceedings of the 11th World Congress «Aviation in the XXI-st century». September 25-25, 2024. P. 433-437. 9. Колісниченко А. В. Застосування дизайн-мислення при створенні мистецької студії як креативного студентського простору. Дизайн-мислення в освітній діяльності : матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, 1 липня – 11 серпня 2024 року. Львів – Торунь: Liha-Pres, 2024. С. 16-17. 10. Колісниченко А. В., Харицька С. В. Роль асистента вчителя в системі національної освіти України. Integration of Education, Science and Business in Modern Environment: Summer Debates: Proceedings of the 6th International Scientific and Practical Internet Conference, August 1-2, 2024. FOP Marenichenko V.V., Dnipro, Ukraine, C. 155-157. 11. Колісниченко А. В. Особливості трансформації позитивного мислення: від поліаннізму до синдрома Поліанни (за романом Елеонор Портнр «Поліанна»). Proceedings of I International Scientific and Practical Conference «Scientific Acheievements of Contemporary Society», 15-17 August 2024. London, United Kingdom, 2024. C. 315-318. 12. Харицька С. В., Колісниченко А. В. Дотримання принципів академічної доброчесності як чинник формування морально-етичної ідентичності студентів-спеціалістів у сфері захисту інформації: матеріали V Міжнародного науково-практичного форуму «Ефективне врядування та виховання доброчесності в секторі безпеки та оборони» (11 грудня 2024 р.). Київ, 2024. С.

							59-50. 13. А. Колісниченко. Концепт «Фастівської культури» у творах Гарта Крейна. Національна ідентичність в мові і культурі: збірник наукових праць / за заг. ред. О. Г. Шостак. К.: Талком, 2023. С. 83-85. 14. А. Колісниченко, С. Харицька. Фейк як одиниця медіаманіпуляції соціальною думкою. Подолання мовних та комунікативних бар'єрів: освіта, наука, культура: збірник наукових праць / за заг. ред.. О. В. Ковтун. К.: НАУ, 2023. С. 159-162. 15. Харицька С. В., Колісниченко А. В. Виховна функція роботи гуртка під час кризової трансформації національної самосвідомості. Формування резильєнтних компетентностей здобувача освіти в період трансформацій, сучасних викликів та кризових станів суспільства: матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, 3 липня – 13 серпня 2023 року. Одеса: Видавничий дім «Гельветика», 2023. С. 155-159. 16. A. Kolisnychenko, S. Kharytska. Localization of video games as the important component of national / cultural patterns expressing. Національна ідентичність в мові і культурі: збірник наукових праць / за заг. ред. О. Г. Шостак. К.: Талком, 2021. С. 169-172. 17. Kharytska S., Kolisnychenko A. Features of foreign language competence of future aviation industry engineers. Modern problems in science: Proceedings of the XIX International Scientific and Practical Conference. Vancouver, Canada. 2022. Pp. 456-459. 18. Колісниченко А. В., Харицька С. В. Жанрова парадигма лірики Гарта Крейна. Філологічні науки:

							сучасні тенденції та фактори розвитку: Міжнародна науково-практична конференція, м. Одеса, 28–29 січня 2022 року. Одеса: Південноукраїнська організація «Центр філологічних досліджень», 2022. С. 68-70. 19. С. Харицька, А. Колісниченко. Проблеми адаптації студентів ВЗО до навчання у період воєнного стану. Подолання мовних та комунікативних бар'єрів: освіта, наука, культура: збірник наукових праць / за заг. ред.. О. В. Ковтун. К.: НАУ, 2022. С. 249-253. 20. Колісниченко А. В. Концепт «гендер» як базис гендерних студій. Мова та література у полікультурному просторі: Міжнародна науково-практична конференція, м. Львів 11–12 лютого 2022 року. Львів: Наукова філологічна організація «Логос», 2022. С. 7-8. 21. С. Харицька, А. Колісниченко. Інтегрування засад національної ідентичності у виховний процес у закладах вищої освіти. Інновації в сучасній освіті: український та світовий контекст: матеріали V Міжнар. наук.-практ. Інтернет-конф. (Умань, 20 жовтня 2022 р.) / МОН України, Уманський держ. пед. ун-т імені Павла Тичини [та ін.]; [редкол.: О. І. Безлюдний, Т. Л. Годованюк, І. С. Постоленко [та ін.]; відпов. за вип. І. Ю. Гурський]. Умань: Візаві, 2022. С. 198-201. 22. Колісниченко А. В. Національні традиції Емілі Дікінсон та Волта Вітмена vs модерністські новації Езри Паунда й Томаса Стірнза Еліота в формуванні оригінальності письма Гарта Крейна. Fundamental and applied research in the modern world. Abstracts of the 6th International scientific

							and practical conference. BoScience Publisher, Boston, USA. 2021. Pp. 580-587. 23. Романчук В. Ю., Колісниченко А. В. Revolutionizing creativity: the impact of AI on modern creative industries. Проблеми ефективності професійної мовної комунікації в умовах інформаційної агресії: матеріали ІІ Всеукр. наук.-практ. конф. з міжнародною участю (м. Київ, 28 листопада 2025 року). Київ : Київський інститут Національної гвардії України, 2025. С. 223-225. 24. 1. Харицька С. В., Колісниченко А. В. Розвиток навичок критичного аналізу англомовних джерел як складова професійної підготовки студентів ІТ. Лінгвістичні та методологічні аспекти викладання іноземних мов професійного спрямування: матеріали VII Міжнародної науково-практичної конференції 26–27 березня 2026 р. / За заг. ред. О. М. Акмалдінової. К.: НУ «КАІ». 2026. С. 64-65. 14) керівництво студентом, який зайняв призове місце на І або ІІ етапі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт), або робота у складі організаційного комітету / журі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт), або керівництво постійно діючим студентським науковим гуртком / проблемною групою; керівництво студентом, який став призером або лауреатом Міжнародних, Всеукраїнських мистецьких конкурсів, фестивалів та проектів, робота у складі організаційного комітету або у складі журі міжнародних,

							всеукраїнських мистецьких конкурсів, інших культурно-мистецьких проектів (для забезпечення провадження освітньої діяльності на третьому (освітньо-творчому) рівні); керівництво здобувачем, який став призером або лауреатом міжнародних мистецьких конкурсів, фестивалів, віднесених до Європейської або Всесвітньої (Світової) асоціації мистецьких конкурсів, фестивалів, робота у складі організаційного комітету або у складі журі зазначених мистецьких конкурсів, фестивалів); керівництво студентом, який брав участь в Олімпійських, Параолімпійських іграх, Всесвітній та Всеукраїнській Універсіаді, чемпіонаті світу, Європи, Європейських іграх, етапах Кубка світу та Європи, чемпіонаті України; виконання обов'язків тренера, помічника тренера національної збірної команди України з видів спорту; виконання обов'язків головного секретаря, головного судді, судді міжнародних та всеукраїнських змагань; керівництво спортивною делегацією; робота у складі організаційного комітету, суддівського корпусу; Студентський науковий гурток «Літературознавчі та мистецькі студії», керівник (2020-2024). Студентський науковий гурток «Scientific Hub», керівник (2024-2026 р.). Робота у складі журі Всеукраїнського конкурсу студентських наукових робіт з галузей знань і спеціальностей (Галузь: гуманітарні науки; Спеціальність: 023 Соціолінгвістика) (2024). Робота в складі оргкомітету Всеукраїнської олімпіади з

							англійської мови (2025-2026). Робота у складі журі Міжнародного конкурсу з української мови імені Петра Яцика (2024-2026 р.). Керівництво студентами, які зайняли 2 та 3 місця у І етапі Всеукраїнської олімпіади з англійської мови (2026 р.). 19) діяльність за спеціальністю у формі участі у професійних та / або громадських об'єднаннях; Член Української асоціації дослідників освіти.
143226	Гахов Сергій Олександрович	Доцент, Основне місце роботи	Навчально-науковий інститут Кібербезпеки та захисту інформації	Диплом спеціаліста, Харківським вищим військовим училищем радіозв'язку, рік закінчення: 1993, спеціальність: , Диплом магістра, Національна академія оборони України, рік закінчення: 2006, спеціальність: Організація бойового та оперативного забезпеченнгя військ (за видами та родами військ і сил), Диплом кандидата наук ДК 008375, виданий 26.10.2012, Атестат доцента АД 006511, виданий 09.02.2021	32	Проведення наукових досліджень в кібербезпеці	Види і результати професійної діяльності за спеціальністю відповідно до п.38 Ліцензійних умов провадження освітньої діяльності: п.п. 38.1), 38.3), 38.4), 38.8), 38.11), 38.12), 38.19), 38.20) наявність сертифіката відповідно до Загальноєвропейської рекомендації з мовної освіти В2 з англійської мови 1.наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection; 1. Bryhynets, A. Haidur, H. Gakhov, S.Marchenko, V. Quantitative WEB Application Vulnerability Assessment using SAST Methodology International Journal of Computing, 2025, 24(1), pp. 163–170 DOI: 10.1016/j.egyr.2025.04.056. (Scopus) 2. Sobchuk V., Gakhov S., Smoliev Y., Haidur H. Enhancing Intrusion Detection in Organizational Information Systems through AI-Powered Traffic Analysis (2024) CEUR Workshop Proceedings, 3933, pp. 190 - 203. https://www.scopus.com/inward/record.uri?

							eid=2-s2.0-86000713893&partnerID=40&md5=f59cab3a67f02a57321b8172f4b75ed6 . (Scopus) 3. Haidur, H., Gakhov, S., & Hamza, D. (2024). USING SUPPORT VECTORS TO BUILD A RULE-BASED SYSTEM FOR DETECTING MALICIOUS PROCESSES IN AN ORGANISATION'S NETWORK TRAFFIC. Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska, 14(4), 90–96. https://doi.org/10.35784/iapgos.6366. (Scopus) 4. Гайдур, Г. І., Гахов, С. О., Марченко, В. В., & Гайдур, К. В. (2024). Концептуальна модель виявлення фішингових атак на основі використання методів опорних векторів. Сучасний захист інформації, 2(58), 24–33. https://doi.org/10.31673/2409-7292.2024.020003 5. Гайдур Г. І. Гахов С. О, Сич М. В., Дмітрієв В. Є. Аналіз загроз мережевого трафіку рівнів моделі OSI для динамічного розрахунку RTO в контексті боротьби з DDOS атаками. Телекомунікаційні та інформаційні технології. № 3 (2023). С. 12-21. DOI: 10.31673/2412-4338.2023.031221. 6. Гайдур Г. І., Гахов С. О., Бригинець А. Виявлення мережевих аномалій з використанням алгоритмів нейронних мереж. Телекомунікаційні та інформаційні технології. № 1 (2023). С. 61-73. DOI: 10.31673/2412-4338.2023.016173. 3.наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора); 1. Козачок В.А., Гайдур Г.І., Гахов С.О.,

							Власенко В.О., Чумак Н.С. Політики безпеки. Навчальний посібник підготовлено для студентів вищих навчальних закладів – Київ: ДУТ ННІЗІ, 2020. – 167 с. 2. Haidur H. I., Gakhov S. O., Skybun O. Z. Cyber education in the context of the formation of ukraine's modern educational space: interdisciplinary approaches. Ukraine's capacity to implement the sustainable development program in the context of full-scale armed aggression: Scientific monograph. Riga, Latvia : "Baltija Publishing",Volume 1. 2025. p. 48-60. DOI https://doi.org/10.30525/978-9934-26-570-9-4 . 4.наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування; 1. Методичні рекомендації до виконання магістерських робіт на ступінь вищої освіти «Магістр» для здобувачів спеціальності 125 Кібербезпека / Гайдур Г.І., Гахов С.О., Марченко В.В. ,Чумак Н.С. /– К.: ДУІКТ, 2024. 44 с. 2. Методичні рекомендації до виконання кваліфікаційної роботи першого (бакалаврського) рівня вищої освіти спеціальності 125 Кібербезпека ОП Інформаційна та кібернетична безпека // Гайдур Г.І., Гахов С.О., Марченко В.В., Дмітрієв В.Є. / – К.: ДУІКТ, 2024. – 46 с. 3. Електроний курс «Проведення наукових досліджень в кібербезпеці».

							4. Електроний курс «Технології виявлення уразливостей мережевих ресурсів». 5. Електроний курс «SIEM системи». 6. Електроний курс «Цифрова криміналістика». 8.виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах; 1. Відповідальний виконавець ініціативної держбюджетної науково-дослідної роботи за темою: «Розробка методів та засобів підвищення живучості інформаційно-комунікаційнихсистем в умовах впливу кібернетичних атак» (реєстраційний номер НДР шифр «Живучість К14» РК №0114U000391) 2. Науковий керівник ініціативної держбюджетної науково-дослідної роботи за темою: «Методологія виявлення шкідливих процесів в інформаційних системах» (реєстраційний номер НДР 0121U113613). 11.наукове консультування підприємств, установ, організацій не менше трьох років, що здійснювалося на підставі договору із закладом вищої освіти (науковою установою); Консультація відповідно договору № 0203від 02 березня 2020 року з ТОВ « Центр інформаційної та технічної підтримки «Сапфоріс». 12.наявність апробаційних та/або науково-популярних,

							та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п’яти публікацій; 1. Гайдур Г. І., Гахов С. О., Скибун О. Ж. Кібербезпека у контексті формування міждисциплінарних підходів використання іт-технологій для відновлення України. Відновлення України: міжгалузевий теоретико-прикладний аналіз та потенціали розвитку : Міжнародний науково-практичний форум, 11 квітня 2025 року, м. Одеса. Львів – Торунь : Liha-Pres, 2025. – Ч. 2. – 81-83. 2. Gakhov S. Samoilenko V., Analysis of machine learning methods for detecting malicious processes in a corporate network. VII International Scientific and Practical Conference «GRUNDLAGEN DER MODERNEN WISSENSCHAFTLICHEN FORSCHUNG», December 13, 2024; Zurich, Switzerland, 244-246. DOI: 10.36074/logos-13.12.2024.050 3. Гайдур Г. І., Гахов С. О. Врахування тенденцій штучного інтелекту під час підготовки фахівців з кібербезпеки. Штучний інтелект у вищій освіті: ризики та перспективи інтеграції: матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, 1 липня – 11 серпня 2024 року. – Львів –Торунь : Liha-Pres, 2024. С. 50-53. ISBN 978-966-397-412-5 4. Haidur H., Gakhov S. Detection of malicious processes in the organization’s network traffic using synthetic data. Cybersecurity of energy, scientific-practical conference of the G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine: materials, May 31, 2023. Kyiv: PIMEE NAS of Ukraine, 2023.

							Р. 30–33. 5. Гайдур Г.І., Гахов С.О., Скибун О.Ж. Готові програмні продукти захисту персональних даних в рамках використання концепції BYOD. / Modern tools and methods of scientific investigations: collection of scientific papers «SCIENTIA» with Proceedings of the II International Scientific and Theoretical Conference, December 8, 2023. Antwerp, Kingdom of Belgium: International Center of Scientific Research. 347 p. pp.160-166. 6. Гайдур Г.І., Гахов С.О., Скибун О.Ж. Аналіз вимог нормативних документів щодо захисту персональних даних. / Scientific review of the actual events, achievements and problems: collection of scientific papers «SCIENTIA» with Proceedings of the I International Scientific and Theoretical Conference, December 1, 2023. Berlin, Federal Republic of Germany: International Center of Scientific Research. 347p. pp.167-173. 19.діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях; Учасник робочої групи з розробки професійних стандартів: «ФАХІВЕЦЬ З ПЛАНУВАННЯ ПОЛІТИКИ ТА СТРАТЕГІЇ КІБЕРБЕЗПЕКИ» «ФАХІВЕЦЬ З РЕАГУВАННЯ НА ІНЦИДЕНТИ КІБЕРБЕЗПЕКИ» «ФАХІВЕЦЬ ІЗ КІБЕРДОСЛІДЖЕНЬ ТА РОЗРОБОК СИСТЕМ БЕЗПЕКИ» «АНАЛІТИК ЗАГРОЗ БЕЗПЕКИ» 20. досвід практичної роботи за спеціальністю не менше п'яти років (крім педагогічної, науково-педагогічної, наукової діяльності). 1989-2013- Служба у Збройних Силах України за спеціальністю. 2013-2014 –

							начальник режимно-секретного відділу ТОВ «Прогноз Україна».
81112	Гайдур Галина Іванівна	Завідувач кафедри, Основне місце роботи	Навчально-науковий інститут Кібербезпеки та захисту інформації	Диплом спеціаліста, Київський інститут зв'язку Української державної академії зв'язку імені О.С. Попова, рік закінчення: 2001, спеціальність: 092401 Телекомунікаційні системи та мережі, Диплом доктора наук ДД 008401, виданий 05.03.2019, Диплом кандидата наук ДК 019172, виданий 17.01.2014, Атестат доцента 12ДЦ 043924, виданий 29.09.2015, Атестат професора АП 001534, виданий 26.02.2020	18	Прикладна загальна теорія систем кібербезпеки	Види і результати професійної діяльності за спеціальністю відповідно до п.38 Ліцензійних умов провадження освітньої діяльності: п.п. 38.1), 38.3), 38.4), 38.5), 38.6), 38.7), 38.8), 38.12,) 38.14), 38.19) наявність сертифіката відповідно до Загальноєвропейської рекомендації з мовної освіти B2 з англійської мови 1.наявність не менше п’яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection; 1. Sobchuk, V., Savchenko, V., Stepanchenko, B., & Haidur, H. (2026). Application of Impulsive SIRQ Models for the Development of Forecasting and Cyberattack Mitigation Scenarios. Preprints. https://doi.org/10.20944/preprints202602.1283.v1 (Web of Science) 2. Гайдур Г.І., Гахов С.О., Скибун О.Ж. (2025). Оцінка стану кібербезпеки критичної інфраструктури з використанням ШІ. Сучасний захист інформації, 2(62), 31–41.https://doi.org/10.31673/2409-7292.2025.020831. 3. Bryhynets, A. Haidur, H. Gakhov, S.Marchenko, V. Quantitative WEB Application Vulnerability Assessment using SAST Methodology International Journal of Computing, 2025, 24(1), pp. 163–170 DOI: 10.1016/j.egyr.2025.04.056. (Scopus) 4. Sobchuk V., Gakhov S., Smoliev Y., Haidur H. Enhancing Intrusion Detection in Organizational Information Systems through AI-Powered

							Traffic Analysis (2024) CEUR Workshop Proceedings, 3933, pp. 190 - 203. https://www.scopus.com/inward/record.uri?eid=2-s2.0-86000713893&partnerID=40&md5=f59cab3a67f02a57321b8172f4b75ed6 . (Scopus) 5. Vitalii Savchenko, Halyna Haidur, Svitlana Lehominova, Taras Dzyuba, and Oleksandr Laptiev. Modeling of media influence on personal information security 2024 IT&I. Information technology and implementation. November 20-21, 2024 Taras Shevchenko National University of Kyiv, 196-206. https://ceur-ws.org/Vol-3909/Paper_15.pdf 6. Haidur, H., Gakhov, S., & Hamza, D. (2024). USING SUPPORT VECTORS TO BUILD A RULE-BASED SYSTEM FOR DETECTING MALICIOUS PROCESSES IN AN ORGANISATION'S NETWORK TRAFFIC. Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska, 14(4), 90–96. https://doi.org/10.35784/iapgos.6366 (Scopus). 3.наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора); 1. Козачок В.А., Гайдур Г.І., Гахов С.О., Власенко В.О., Чумак Н.С. Політики безпеки. Навчальний посібник підготовлено для студентів вищих навчальних закладів – Київ: ДУТ ННІЗІ, 2020. – 167 с. 2. Кожухівський А.Д. Математичні методи криптології /А.Д. Кожухівського, І.Д. Горбенка, Г.І. Гайдур, О.А. Кожухівської, В.В. Марченка// Навчальний посібник К.: ДУТ, 2021. – 249 с. 3. Теорія інформації та кодування:

							Навчальний посібник для підготовки до практичних занять / Уклад. Гайдур Г.І, Бондаренко З.З. – К.: ДУІКТ, 2024 – 43 с. 4. Вступ до квантової криптології [Текст]: Навчальний посібник (Для студентів техн. спец. вищ. навч. закл.) / [А.Д. Кожухівський, І.Д. Горбенко, В.К. Задірака, О.М. Хіміч, Ю.І. Горбенко, Г.І. Гайдур, О.А. Кожухівська, В.В. Марченко.]; М-во освіти і науки України, Державний університет телекомунікацій.- К.: ДУІКТ, 2024. – 597 с. 5. Борсуковський Ю.В., Борсуковська В.Ю., Гайдур Г.І., Складанний П.М., Бурячок В.Л., Прикладні аспекти інформаційної та кібернетичної безпеки держави. Аналіз мережевого трафіку: навчальний посібник / ISBN 978-617-574-272-3 / УДК 32.973я73 р. / – Львів - Видавництво «Магнолія 2006», 2023, 222 с. 6. Haidur H. I., Gakhov S. O., Skybun O. Z. Cyber education in the context of the formation of ukraine's modern educational space: interdisciplinary approaches. Ukraine's capacity to implement the sustainable development program in the context of full-scale armed aggression: Scientific monograph. Riga, Latvia : "Baltija Publishing",Volume 1. 2025. p. 48-60. DOI https://doi.org/10.30525/978-9934-26-570-9-4. 4.наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю

							три найменування; 1. Електроний курс «Теорія інформації та кодування ». 2. Електроний курс «Прикладна теорія ІКБ». 3. Електронний курс «Науково-технічний переклад». 4.Електроний курс «Методологія наукових досліджень у кібербезпеці». 5. Методичні рекомендації до виконання магістерських робіт на ступінь вищої освіти «Магістр» для здобувачів спеціальності 125 Кібербезпека / Гайдур Г.І., Гахов С.О., Марченко В.В. ,Чумак Н.С. /– К.: ДУІКТ, 2024. 44 с. 6. Методичні рекомендації до виконання кваліфікаційної роботи першого (бакалаврського) рівня вищої освіти спеціальності 125 Кібербезпека ОП Інформаційна та кібернетична безпека // Гайдур Г.І., Гахов С.О., Марченко В.В., Дмітрієв В.Є. / – К.: ДУІКТ, 2024. – 46 с. 5.захист дисертації на здобуття наукового ступеня; Захист дисертації на здобуття наукового ступеню доктора технічних наук, диплом ДД № 008401, 2019 р., спеціальність 05.13.06 – «Інформаційні технології». 6.наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня; 1.Керівництво здобувача Бржевска Зореслава Михайлівна. Дисертація на здобуття наукового ступеня доктора філософії PhD за спеціальністю 125 Кібербезпека «Метод оцінки ресурсів достовірності інформації в умовах інформаційного протиборства.»; 2021, ДР № 001489, 26.04.2021, Державний університет

							телекомунікацій 2. Керівництво здобувача Сорокіна Дениса Володимировича. Дисертація на здобуття наукового ступеня доктора філософії PhD за спеціальністю 125 Кібербезпека «Методика створення захищених спеціалізованих мереж для підвищення ефективності надання промислових сервісів»; 2021, ДР 002117, 26 07.2021, Державний університет телекомунікацій. 3. Керівництво здобувача Прилєпов Євген Валерійович». Дисертація на здобуття наукового ступеню кандадата технічних наук за спеціальністю 05.13.06 – «Інформаційні технології». «Інформаційна технологія виявлення аномальних даних в інтернеті речей на основі кластерного аналізу». 2018. Державний університет телекомунікацій. 4. Керівництво здобувача Киричка Романа Васильовича. Дисертація на здобуття наукового ступеня доктора філософії PhD за спеціальністю 125 Кібербезпека «Методика забезпечення об'єктивного контролю захищеності корпоративних мереж шляхом проникнення»; 2021, ДР № 001490, 26.04.2021. Державний університет телекомунікацій. 5. Керівництво здобувача Марченко Віталія вікторович. Дисертація на здобуття наукового ступеня доктора філософії PhD за спеціальністю 125 Кібербезпека «Метод виявлення шкідливих процесів в інформаційній системі підприємства на основі ідентифікації та діагностування станів логічних об'єктів.»;

							2023, Диплом Н23 №000683 від 01.06. 2023 р., Державний університет телекомунікацій 7.участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад; 1. Спеціалізована вчена рада для проведення разового захисту дисертації на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека. ВЕТЛИЦЬКА Олена Сергіївна. Рецензент. Тема роботи: "Модель інформаційної захищеності особистості в умовах впливу результатів соціологічних досліджень". 2025 2. Спеціалізована вчена рада для проведення разового захисту дисертації на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека. Грищук Ольга Михайлівна. Рецензент. Тема роботи: " Симетрична криптографічна система на диференціальних перетвореннях". 2025 3. Спеціалізована вчена рада для проведення разового захисту дисертації на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека. Запорожченко Михайло Михайлович. Рецензент. Тема дисертаційної роботи: «Методи прогнозування соціоінженерних атак на корпоративні інформаційні системи на основі профілю захищеності користувача». 2025. 4. Спеціалізована вчена рада для проведення разового захисту дисертації на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека. Палко Дмитро Володимирович. Опонент. Тема дисертаційної роботи: «Адаптивний метод та моделі оцінювання

							ризиків кібербезпеки у розподілених інформаційних системах.». 2025. 8.виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах; 1. Науковий керівник ініціативної держбюджетної науково-дослідної роботи за темою: «Розробка методів та засобів підвищення живучості інформаційно-комунікаційних систем в умовах впливу кібернетичних атак» (реєстраційний номер НДР шифр «Живучість К14» РК №0114U000391); 2. Науковий керівник ініціативної держбюджетної науково-дослідної роботи за темою: «Методологія виявлення шкідливих процесів в інформаційних системах (реєстраційний номер НДР 0121U113613); 3. Науковий керівник науково-дослідної роботи за темою: «Розробка науково-методичних рекомендацій виявлення шкідливих процесів в інформаційній системі організації» (ТОВ «АЛЬФА-МЕТАЛ», м. Київ). 12.наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п'яти публікацій; 1. Гайдур Г., Собчук А., Степанченко Б. Аналіз стійкості та ефективності

							періодичних заходів кіберзахисту в епідемічних моделях // Математика. Інформаційні технології. Освіта. Тези доповідей XV Міжнар. наук.–практ. конф., 14 червня – 16 червня 2026 р. Луцьк–Світязь: СНУ імені Лесі Українки, 2026. С 132-134 2. Haydur, H., & Hamza, D. (2025, November 4–5). Hybrid method for malicious activity detection in information systems. In Digital Transformation: Strengthening the Cybersecurity Capacities in the Modern World (pp. 39–41). 3. Сич М., Бригинець А., Шулімова Д., Бойко А. (2024). ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ДЛЯ ЗБОРУ ДАНИХ НЕОБХІДНИХ ДЛЯ МАШИННОГО НАВЧАННЯ ДЛЯ ТРЕНУВАННЯ МОДЕЛЕЙ З МЕТОЮ АНАЛІЗУ DNS-ТРАФІКУ У СФЕРІ КІБЕРБЕЗПЕКИ. Матеріали конференцій МЦНД, (05.07.2024; Житомир, Україна), 157–163. https://doi.org/10.62731/mcnd-05.07.2024.006 4. Haidur H, Bryhynets A., Sych M. STRATEGIES OF ENHANCEMENT OF INTRUSION DETECTION AND PREVENTION CAPABILITIES THROUGH DECENTRALIZED MACHINE LEARNING. VII International Scientific and Theoretical Conference. 14.06.2024. Lisbon, Portuguese Republic https://doi.org/10.36074/scientia-14.06.2024. ISBN: 979-8-88955-776-0 5. Гайдур, Г. І., Сич, М. В., & Лазарєв, Є. Г. (2024). ШТУЧНИЙ ІНТЕЛЕКТ В БАЗАХ ДАНИХ: АВТОМАТИЗАЦІЯ ОПТИМІЗАЦІЇ ЗАПИТІВ ДЛЯ ПОКРАЩЕННЯ ПРОДУКТИВНОСТІ. InterConf Scientific Publishing Center, (204), 254-257. https://archive.intercon

							f.center/index.php/conference-proceeding/article/view/6501 6. Гайдур Г. І., Гахов С. О. Врахування тенденцій штучного інтелекту під час підготовки фахівців з кібербезпеки. Штучний інтелект у вищій освіті: ризики та перспективи інтеграції: матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, 1 липня – 11 серпня 2024 року. – Львів –Торунь : Liha-Pres, 2024. С. 50-53. ISBN 978-966-397-412-5. 7. Гайдур Г. І., Гахов С. О., Скибун О. Ж. Кібербезпека у контексті формування міждисциплінарних підходів використання іт-технологій для відновлення України. Відновлення України: міжгалузевий теоретико-прикладний аналіз та потенціали розвитку : Міжнародний науково-практичний форум, 11 квітня 2025 року, м. Одеса. Львів – Торунь : Liha-Pres, 2025. – Ч. 2. – 81-83. 8. Гайдур, Г. І., Дмітрієв, В. Є., & Лазарєв, Є. Г. (2025). Захист від соціальних атак: інтеграція безпеки з урахуванням людського фактору. Advanced top technology: електрон. наук. журн. – № 6. – Харків: СГ НТМ «Новий курс», 2025. – с.36. ISSN 3041-1998 (online) DOI: 10.61718/att https://www.newroute.org.ua/wp-content/uploads/ATT6.pdf . 14.керівництво студентом, який зайняв призове місце на І або ІІ етапі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт), або робота у складі організаційного комітету / журі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт), або

							керівництво постійно діючим студентським науковим гуртком / проблемною групою; керівництво студентом, який став призером або лауреатом Міжнародних, Всеукраїнських мистецьких конкурсів, фестивалів та проектів, робота у складі організаційного комітету або у складі журі міжнародних, всеукраїнських мистецьких конкурсів, інших культурно-мистецьких проектів (для забезпечення провадження освітньої діяльності на третьому (освітньо-творчому) рівні); керівництво здобувачем, який став призером або лауреатом міжнародних мистецьких конкурсів, фестивалів, віднесених до Європейської або Всесвітньої (Світової) асоціації мистецьких конкурсів, фестивалів, робота у складі організаційного комітету або у складі журі зазначених мистецьких конкурсів, фестивалів); керівництво студентом, який брав участь в Олімпійських, Паралімпійських іграх, Всесвітній та Всеукраїнській Універсіаді, чемпіонаті світу, Європи, Європейських іграх, етапах Кубка світу та Європи, чемпіонаті України; виконання обов'язків тренера, помічника тренера національної збірної команди України з видів спорту; виконання обов'язків головного секретаря, головного судді, судді міжнародних та всеукраїнських змагань; керівництво спортивною делегацією; робота у складі організаційного комітету, суддівського корпусу; Робота у складі журі Всеукраїнського конкурсу студентських наукових робіт з кібербезпеки (І етап) 2026 рік, ДУІКТ. 19.діяльність за

							спеціальністю у формі участі у професійних та/або громадських об'єднаннях; Учасник робочої групи з розробки професійного стандарту : «ФАХІВЕЦЬ З ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ» https://register.nqa.gov.ua/uploads/0/572-fahivec_z_tehnicnogo_zahistu_informacii_v_2.pdf «ФАХІВЕЦЬ З ОЦІНКИ ЗАХОДІВ ЗАХИСТУ ІНФОРМАЦІЇ (КІБЕРБЕЗПЕКИ)» https://register.nqa.gov.ua/uploads/0/579-fahivec_z_ocinki_zahodiv_zahistu_informacii_kiberbezpeki_v_2.pdf «ФАХІВЕЦЬ З КРИПТОГРАФІЧНОГО ЗАХИСТУ» https://register.nqa.gov.ua/uploads/0/569-fahivec_z_kriptograficnogo_zahistu_informacii_v_2.pdf .
356622	Кондратенко Наталія Юріївна	Доцент, Основне місце роботи	Навчально-науковий інститут Телекомунікацій	Диплом спеціаліста, Київський університет імені Тараса Шевченка, рік закінчення: 1998, спеціальність: Українська мова та література, Диплом кандидата наук ДК 050257, виданий 18.12.2018, Атестат доцента АД 010895, виданий 09.08.2022	13	Педагогіка та психологія у вищій школі	Види і результати професійної діяльності за спеціальністю відповідно до п.38 Ліцензійних умов провадження освітньої діяльності: п.п. 38.1), 38.3), 38.4), 38.12), 38.19), 38.20) 38.1) наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection. Stezhko S., Kondratenko N., Zabolotnia R., 1. Стежко С.О., Кондратенко Н.Ю., Ситник Л.І. Психологічні та лінгвістичні чинники ефективності професійно орієнтованого мовного навчання у вищій школі // Соціальна педагогіка: теорія та практика № 4, Полтава, 2025 С. 190-197. URL: DOI https://doi.org/10.12958/1817-3764-2025-4-190-197 http://socped.luguniv.e

							du.ua/index.php/socped/issue/view/10 2. Стежко С.О., Кондратенко Н.Ю., Заболотня Р.В. Формування професійної мовної особистості студента: психолінгвістичний, педагогічний і психологічний виміри, Збірника наукових праць Педагогіка формування творчої особистості у вищій і загальноосвітній школах, Журнал включено до міжнародної наукометричної бази Index Copernicus International (Республіка Польща). № 102, Запоріжжя, 2025, С. 58-63, DOI https://doi.org/10.32782/1992-5786.2025.102.10 .https://pedagogy-journal.kpu.zp.ua/102-2025. 3. Кондратенко Н., Кравченко В., Воропай І., Цифрова комунікація і штучний інтелект: методичний потенціал формування мовнокомунікативної компетентності Multidisciplinární mezinárodní vědecký magazín “Věda a perspektivy” je registrován v České republice. Státní registrační číslo u Ministerstva kultury ČR: E 24142. № 5(60) 2026, c. 95-107 DOI:10.52058/2708-7530-2026-5(60)-95-107. https://perspectives.pp.ua/index.php/vp/issue/archive 4. Стежко С.О., Колісниченко А.В., Кондратенко Н.Ю., Павлов В.О. Методика формування академічної мовної компетентності українською та англійською мовами засобами цифрових освітніх платформ. «Вісник науки та освіти»: журнал. 2026. № 3(45) 2026. С.1354-1368 .DOI: https://doi.org/10.52058/2786-6165-2026-3(45) .https://perspectives.pp.ua/index.php/vno/issue/view/461/564 5. Стежко С.О., Зозуля Н.Ю., Кондратенко Н.Ю. Переконувальне

							мовлення як результат взаємодії риторики та психолінгвістики. «Наукові інновації та передові технології» Державне управління, економіка, право, педагогіка, психологія: журнал. 2026. № 3(55) 2026, С. 1941-1953. https://doi.org/10.52058/2786-5274-2026-4(56)-1941-1953. https://perspectives.pp.ua/index.php/nauka/issue/view/463/566 . 6. Стежко С.О., Кондратенко Н.Ю., Аташкаде Р. В., Волкотруб Г. Й., Мелешко Т.В. Активізація критичного мислення студентів засобами інтерактивної мовної взаємодії у навчальному процесі ЗВО. «Вісник науки та освіти»: журнал. 2026. № 4(46) 2026. С 2122-2135. https://doi.org/10.52058/2786-6165-2026-4(46)-2122-2135 .https://perspectives.pp.ua/index.php/vno/issue/view/475/578 . 7. Стежко С. О., Зозуля Н. Ю., Павлов В. О., Кондратенко Н. Ю., Професійний дискурс майбутнього фахівця: порівняльний аналіз мовних засобів юридичної та іт-комунікації, «Вісник науки та освіти»: журнал. 2026. № 6(48) 2026. С. 796-809. DOI:10.52058/2786-6165-2026-6(48)-796-809. https://perspectives.pp.ua/index.php/vno/issue/archive 8. Stezhko Svitlana, Kondratenko Natalia, Zabolotnia Ruslana, Zabolotnii Bohdan, TEAMBUILDING AS A TOOL FOR EFFECTIVE IT-COMPANY MANAGEMENT // Danish scientific journal Published September 26, 2024 № 88. С.15-17. https://zenodo.org/records/13884401 38.3.наявність виданого підручника чи навчального посібника (включаючи електронні) або

							монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора) Стежко.С.О., Кондратенко Н.Ю., Заїка В.Ф. Сучасні методи викладання у вищій школі. Навчальний посібник. - Київ: ДУІКТ., 2025, 100с. https://duikt.edu.ua/ua/lib/1/category/516/view/2385 38.12. наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п'яти публікацій; 1. Стежко С.О, Кондратенко Н.Ю., Волкотруб Г.Й., Заболотня Р.В. Сучасний стан та перспективи розвитку штучного інтелекту у вищій школі./ Освіта як індикатор суспільного розвитку: теоретикопрактичний курс: матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, 2 жовтня – 12 листопада 2023 року. – Львів – Торунь: Liha-Pres, 2023. – С.37-41. 2. Стежко С.О., Кондратенко Н.Ю. Теоретичні аспекти формування комунікативної компетентності майбутніх юристів// «Часопис Київського університету права» №3, 2024, С.40-44 https://kup.edu.ua/vyyshov-drukom-iii-y-nomer-2024-roku-iurydychnoho-naukovo-teoretychnoho-shchokvartalnyka-chasopys-kyivskoho-universytetu-prava 3. Стежко С.О., Кондратенко Н.Ю., Волкотруб Г.Й., Заболотня Р.В. Лінгвоцид української мови як головної ознаки етносу. Збірник тез XVI Міжнародна конференція 5-6 травня 2025 р. Нові

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

							конференції з міжнародною участю (м. Київ, 28 листопада 2025 року) Київ: Київського інституту Національної гвардії України, 2025 С.240-243 https://kingu.edu.ua/naukovi-zahodi/ 38.14). Керівництво студентом, який зайняв призове місце на І або ІІ етапі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт), або робота у складі організаційного комітету / журі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт), або керівництво постійно діючим студентським науковим гуртком / проблемною групою; керівництво студентом, який став призером або лауреатом Міжнародних, Всеукраїнських мистецьких конкурсів, фестивалів та проектів, робота у складі організаційного комітету або у складі журі міжнародних, всеукраїнських мистецьких конкурсів, інших культурно-мистецьких проектів (для забезпечення провадження освітньої діяльності на третьому (освітньо-творчому) рівні); керівництво здобувачем, який став призером або лауреатом міжнародних мистецьких конкурсів, фестивалів, віднесених до Європейської або Всесвітньої (Світової) асоціації мистецьких конкурсів, фестивалів, робота у складі організаційного комітету або у складі журі зазначених мистецьких конкурсів, фестивалів); керівництво студентом, який брав участь в Олімпійських, Паралімпійських іграх, Всесвітній та Всеукраїнській Універсіаді, чемпіонаті світу,

							Європи, Європейських іграх, етапах Кубка світу та Європи, чемпіонаті України; виконання обов'язків тренера, помічника тренера національної збірної команди України з видів спорту; виконання обов'язків головного секретаря, головного судді, судді міжнародних та всеукраїнських змагань; керівництво спортивною делегацією; робота у складі організаційного комітету, суддівського корпусу 1.Керівництво постійно діючим студентським науковим гуртком «25 кроків до мовної впевненості» з 2022 р. по теперешній час. 38.19). Діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях; 1. Член громадської організації «Міжнародна асоціація сучасної освіти, науки та культури» (код ЄДРПОУ 44094570) №СЧ-360.12.23
81112	Гайдур Галина Іванівна	Завідувач кафедри, Основне місце роботи	Навчально-науковий інститут Кібербезпеки та захисту інформації	Диплом спеціаліста, Київський інститут зв'язку Української державної академії зв'язку імені О.С. Попова, рік закінчення: 2001, спеціальність: 092401 Телекомунікаційні системи та мережі, Диплом доктора наук ДД 008401, виданий 05.03.2019, Диплом кандидата наук ДК 019172, виданий 17.01.2014, Атестат доцента 12ДЦ 043924, виданий 29.09.2015, Атестат професора АП 001534, виданий 26.02.2020	18	Наукова комунікація та технічний переклад в кібербезпеці	Види і результати професійної діяльності за спеціальністю відповідно до п.38 Ліцензійних умов провадження освітньої діяльності: п.п. 38.1), 38.3), 38.4), 38.5), 38.6), 38.7), 38.8), 38.12,) 38.14), 38.19) наявність сертифіката відповідно до Загальноєвропейської рекомендації з мовної освіти B2 з англійської мови 1.наявність не менше п'яти публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України, до наукометричних баз, зокрема Scopus, Web of Science Core Collection; 1. Sobchuk, V., Savchenko, V., Stepanchenko, B., & Haidur, H. (2026). Application of Impulsive SIRQ Models

for the Development of Forecasting and Cyberattack Mitigation Scenarios. Preprints. https://doi.org/10.20944/preprints202602.1283.v1 (Web of Science)
2. Гайдур Г.І., Гахов С.О., Скибун О.Ж. (2025). Оцінка стану кібербезпеки критичної інфраструктури з використанням ШІ. Сучасний захист інформації, 2(62), 31–41.https://doi.org/10.31673/2409-7292.2025.020831.
3. Bryhynets, A. Haidur, H. Gakhov, S.Marchenko, V. Quantitative WEB Application Vulnerability Assessment using SAST Methodology International Journal of Computing, 2025, 24(1), pp. 163–170 DOI: 10.1016/j.egyr.2025.04.056. (Scopus)
4. Sobchuk V., Gakhov S., Smoliev Y., Haidur H. Enhancing Intrusion Detection in Organizational Information Systems through AI-Powered Traffic Analysis (2024) CEUR Workshop Proceedings, 3933, pp. 190 - 203. https://www.scopus.com/inward/record.uri?eid=2-s2.0-86000713893&partnerID=40&md5=f59cab3a67f02a57321b8172f4b75ed6 . (Scopus)
5. Vitalii Savchenko, Halyna Haidur, Svitlana Lehominova, Taras Dzyuba, and Oleksandr Laptiev. Modeling of media influence on personal information security 2024 IT&I. Information technology and implementation. November 20-21, 2024 Taras Shevchenko National University of Kyiv, 196-206. https://ceur-ws.org/Vol-3909/Paper_15.pdf
6. Haidur, H., Gakhov, S., & Hamza, D. (2024). USING SUPPORT VECTORS TO BUILD A RULE-BASED SYSTEM FOR DETECTING MALICIOUS PROCESSES IN AN ORGANISATION'S NETWORK TRAFFIC. Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska,

							14(4), 90–96. https://doi.org/10.35784/iapgos.6366 (Scopus). 3.наявність виданого підручника чи навчального посібника (включаючи електронні) або монографії (загальним обсягом не менше 5 авторських аркушів), в тому числі видані у співавторстві (обсягом не менше 1,5 авторського аркуша на кожного співавтора); 1. Козачок В.А., Гайдур Г.І., Гахов С.О., Власенко В.О., Чумак Н.С. Політики безпеки. Навчальний посібник підготовлено для студентів вищих навчальних закладів – Київ: ДУТ ННІЗІ, 2020. – 167 с. 2. Кожухівський А.Д. Математичні методи криптології /А.Д. Кожухівського, І.Д. Горбенка, Г.І. Гайдур, О.А. Кожухівської, В.В. Марченка// Навчальний посібник К.: ДУТ, 2021. – 249 с. 3. Теорія інформації та кодування: Навчальний посібник для підготовки до практичних занять / Уклад. Гайдур Г.І, Бондаренко З.З. – К.: ДУІКТ, 2024 – 43 с. 4. Вступ до квантової криптології [Текст]: Навчальний посібник (Для студентів техн. спец. вищ. навч. закл.) / [А.Д. Кожухівський, І.Д. Горбенко, В.К. Задірака, О.М. Хіміч, Ю.І. Горбенко, Г.І. Гайдур, О.А. Кожухівська, В.В. Марченко.]; М-во освіти і науки України, Державний університет телекомунікацій.- К.: ДУІКТ, 2024. – 597 с. 5. Борсуковський Ю.В., Борсуковська В.Ю., Гайдур Г.І., Складанний П.М., Бурячок В.Л., Прикладні аспекти інформаційної та кібернетичної безпеки держави. Аналіз мережевого трафіку: навчальний посібник / ISBN 978-617-574-272-3 / УДК 32.973я73 р. / – Львів - Видавництво «Магнолія 2006», 2023, 222 с. 6. Haidur H. I., Gakhov S. O., Skybun O. Z.

							Cyber education in the context of the formation of ukraine's modern educational space: interdisciplinary approaches. Ukraine's capacity to implement the sustainable development program in the context of full-scale armed aggression: Scientific monograph. Riga, Latvia : "Baltija Publishing",Volume 1. 2025. p. 48-60. DOI https://doi.org/10.30525/978-9934-26-570-9-4. 4.наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіатів, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/ робочих програм, інших друкованих навчально-методичних праць загальною кількістю три найменування; 1. Електроний курс «Теорія інформації та кодування ». 2. Електроний курс «Прикладна теорія ІКБ». 3. Електронний курс «Науково-технічний переклад». 4.Електроний курс «Методологія наукових досліджень у кібербезпеці». 5. Методичні рекомендації до виконання магістерських робіт на ступінь вищої освіти «Магістр» для здобувачів спеціальності 125 Кібербезпека / Гайдур Г.І., Гахов С.О., Марченко В.В. ,Чумак Н.С. /– К.: ДУІКТ, 2024. 44 с. 6. Методичні рекомендації до виконання кваліфікаційної роботи першого (бакалаврського) рівня вищої освіти спеціальності 125 Кібербезпека ОП Інформаційна та кібернетична безпека // Гайдур Г.І., Гахов С.О., Марченко В.В., Дмітрієв В.Є. / – К.: ДУІКТ, 2024. – 46 с.

							5.захист дисертації на здобуття наукового ступеня; Захист дисертації на здобуття наукового ступеню доктора технічних наук, диплом ДД № 008401, 2019 р., спеціальність 05.13.06 – «Інформаційні технології». 6.наукове керівництво (консультування) здобувача, який одержав документ про присудження наукового ступеня; 1.Керівництво здобувача Бржевска Зореслава Михайлівна. Дисертація на здобуття наукового ступеня доктора філософії PhD за спеціальністю 125 Кібербезпека «Метод оцінки ресурсів достовірності інформації в умовах інформаційного протиборства.»; 2021, ДР № 001489, 26.04.2021, Державний університет телекомунікацій 2. Керівництво здобувача Сорокіна Дениса Володимировича. Дисертація на здобуття наукового ступеня доктора філософії PhD за спеціальністю 125 Кібербезпека «Методика створення захищених спеціалізованих мереж для підвищення ефективності надання промислових сервісів»; 2021, ДР 002117, 26 07.2021, Державний університет телекомунікацій. 3. Керівництво здобувача Прилєпов Євген Валерійович». Дисертація на здобуття наукового ступеню кандадата технічних наук за спеціальністю 05.13.06 – «Інформаційні технології». «Інформаційна технологія виявлення аномальних даних в інтернеті речей на основі кластерного аналізу». 2018. Державний університет телекомунікацій.

							4. Керівництво здобувача Киричка Романа Васильовича. Дисертація на здобуття наукового ступеня доктора філософії PhD за спеціальністю 125 Кібербезпека «Методика забезпечення об'єктивного контролю захищеності корпоративних мереж шляхом проникнення»; 2021, ДР № 001490, 26.04.2021. Державний університет телекомунікацій. 5. Керівництво здобувача Марченко Віталія вікторович. Дисертація на здобуття наукового ступеня доктора філософії PhD за спеціальністю 125 Кібербезпека «Метод виявлення шкідливих процесів в інформаційній системі підприємства на основі ідентифікації та діагностування станів логічних об'єктів.»; 2023, Диплом Н23 №000683 від 01.06. 2023 р., Державний університет телекомунікацій 7.участь в атестації наукових кадрів як офіційного опонента або члена постійної спеціалізованої вченої ради, або члена не менше трьох разових спеціалізованих вчених рад; 1. Спеціалізована вчена рада для проведення разового захисту дисертації на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека. ВЕТЛИЦЬКА Олена Сергіївна. Рецензент. Тема роботи: "Модель інформаційної захищеності особистості в умовах впливу результатів соціологічних досліджень". 2025 2. Спеціалізована вчена рада для проведення разового захисту дисертації на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека. Грищук Ольга Михайлівна. Рецензент. Тема роботи: " Симетрична

							криптографічна система на диференціальних перетвореннях". 2025 3. Спеціалізована вчена рада для проведення разового захисту дисертації на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека. Запорожченко Михайло Михайлович. Рецензент. Тема дисертаційної роботи: «Методи прогнозування соціоінженерних атак на корпоративні інформаційні системи на основі профілю захищеності користувача». 2025. 4. Спеціалізована вчена рада для проведення разового захисту дисертації на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека. Палко Дмитро Володимирович. Опонент. Тема дисертаційної роботи: «Адаптивний метод та моделі оцінювання ризиків кібербезпеки у розподілених інформаційних системах.». 2025. 8.виконання функцій (повноважень, обов'язків) наукового керівника або відповідального виконавця наукової теми (проекту), або головного редактора/члена редакційної колегії/експерта (рецензента) наукового видання, включеного до переліку фахових видань України, або іноземного наукового видання, що індексується в бібліографічних базах; 1. Науковий керівник ініціативної держбюджетної науково-дослідної роботи за темою: «Розробка методів та засобів підвищення живучості інформаційно-комунікаційних систем в умовах впливу кібернетичних атак» (реєстраційний номер НДР шифр «Живучість К14» РК №0114U000391); 2. Науковий керівник

							ініціативної держбюджетної науково-дослідної роботи за темою: «Методологія виявлення шкідливих процесів в інформаційних системах (реєстраційний номер НДР 0121U113613); 3. Науковий керівник науково-дослідної роботи за темою: «Розробка науково-методичних рекомендацій виявлення шкідливих процесів в інформаційній системі організації» (ТОВ «АЛЬФА-МЕТАЛ», м. Київ). 12.наявність апробаційних та/або науково-популярних, та/або консультаційних (дорадчих), та/або науково-експертних публікацій з наукової або професійної тематики загальною кількістю не менше п'яти публікацій; 1. Гайдур Г., Собчук А., Степанченко Б. Аналіз стійкості та ефективності періодичних заходів кіберзахисту в епідемічних моделях // Математика. Інформаційні технології. Освіта. Тези доповідей XV Міжнар. наук.–практ. конф., 14 червня – 16 червня 2026 р. Луцьк–Світязь: СНУ імені Лесі Українки, 2026. С 132-134 2. Haydur, H., & Hamza, D. (2025, November 4–5). Hybrid method for malicious activity detection in information systems. In Digital Transformation: Strengthening the Cybersecurity Capacities in the Modern World (pp. 39–41). 3. Сич М., Бригинець А., Шулімова Д., Бойко А. (2024). ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ДЛЯ ЗБОРУ ДАНИХ НЕОБХІДНИХ ДЛЯ МАШИННОГО НАВЧАННЯ ДЛЯ ТРЕНУВАННЯ МОДЕЛЕЙ З МЕТОЮ АНАЛІЗУ DNS-ТРАФІКУ У СФЕРІ КІБЕРБЕЗПЕКИ. Матеріали конференцій МЦНД, (05.07.2024;

Житомир, Україна), 157–163. https://doi.org/10.62731/mcnd-05.07.2024.006
4. Haidur H, Bryhynets A., Sych M. STRATEGIES OF ENHANCEMENT OF INTRUSION DETECTION AND PREVENTION CAPABILITIES THROUGH DECENTRALIZED MACHINE LEARNING. VII International Scientific and Theoretical Conference. 14.06.2024. Lisbon, Portuguese Republic https://doi.org/10.36074/scientia-14.06.2024. ISBN: 979-8-88955-776-0
5. Гайдур, Г. І., Сич, М. В., & Лазарєв, Є. Г. (2024). ШТУЧНИЙ ІНТЕЛЕКТ В БАЗАХ ДАНИХ: АВТОМАТИЗАЦІЯ ОПТИМІЗАЦІЇ ЗАПИТІВ ДЛЯ ПОКРАЩЕННЯ ПРОДУКТИВНОСТІ. InterConf Scientific Publishing Center, (204), 254-257. https://archive.interconf.center/index.php/conference-proceeding/article/view/6501
6. Гайдур Г. І., Гахов С. О. Врахування тенденцій штучного інтелекту під час підготовки фахівців з кібербезпеки. Штучний інтелект у вищій освіті: ризики та перспективи інтеграції: матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, 1 липня – 11 серпня 2024 року. – Львів –Торунь : Liha-Pres, 2024. С. 50-53. ISBN 978-966-397-412-5.
7. Гайдур Г. І., Гахов С. О., Скибун О. Ж. Кібербезпека у контексті формування міждисциплінарних підходів використання іт-технологій для відновлення України. Відновлення України: міжгалузевий теоретико-прикладний аналіз та потенціали розвитку : Міжнародний науково-практичний форум, 11 квітня 2025 року, м. Одеса. Львів – Торунь : Liha-Pres, 2025. – Ч. 2. – 81-83.

							8. Гайдур, Г. І., Дмітрієв, В. Є., & Лазарєв, Є. Г. (2025). Захист від соціальних атак: інтеграція безпеки з урахуванням людського фактору. Advanced top technology: електрон. наук. журн. – № 6. – Харків: СГ НТМ «Новий курс», 2025. – с.36. ISSN 3041-1998 (online) DOI: 10.61718/att https://www.newroute.org.ua/wp-content/uploads/ATT6.pdf . 14.керівництво студентом, який зайняв призове місце на І або ІІ етапі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт), або робота у складі організаційного комітету / журі Всеукраїнської студентської олімпіади (Всеукраїнського конкурсу студентських наукових робіт), або керівництво постійно діючим студентським науковим гуртком / проблемною групою; керівництво студентом, який став призером або лауреатом Міжнародних, Всеукраїнських мистецьких конкурсів, фестивалів та проектів, робота у складі організаційного комітету або у складі журі міжнародних, всеукраїнських мистецьких конкурсів, інших культурно-мистецьких проектів (для забезпечення провадження освітньої діяльності на третьому (освітньо-творчому) рівні); керівництво здобувачем, який став призером або лауреатом міжнародних мистецьких конкурсів, фестивалів, віднесених до Європейської або Всесвітньої (Світової) асоціації мистецьких конкурсів, фестивалів, робота у складі організаційного комітету або у складі журі зазначених

							мистецьких конкурсів, фестивалів); керівництво студентом, який брав участь в Олімпійських, Паралімпійських іграх, Всесвітній та Всеукраїнській Універсіаді, чемпіонаті світу, Європи, Європейських іграх, етапах Кубка світу та Європи, чемпіонаті України; виконання обов'язків тренера, помічника тренера національної збірної команди України з видів спорту; виконання обов'язків головного секретаря, головного судді, судді міжнародних та всеукраїнських змагань; керівництво спортивною делегацією; робота у складі організаційного комітету, суддівського корпусу; Робота у складі журі Всеукраїнського конкурсу студентських наукових робіт з кібербезпеки (І етап) 2026 рік, ДУІКТ. 19.діяльність за спеціальністю у формі участі у професійних та/або громадських об'єднаннях; Учасник робочої групи з розробки професійного стандарту : «ФАХІВЕЦЬ З ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ» https://register.nqa.gov.ua/uploads/0/572-fahivec_z_tehnicnogo_zahistu_informacii_v_2.pdf «ФАХІВЕЦЬ З ОЦІНКИ ЗАХОДІВ ЗАХИСТУ ІНФОРМАЦІЇ (КІБЕРБЕЗПЕКИ)» https://register.nqa.gov.ua/uploads/0/579-fahivec_z_ocinki_zahodiv_zahistu_informacii_kiberbezpeki_v_2.pdf «ФАХІВЕЦЬ З КРИПТОГРАФІЧНОГО ЗАХИСТУ» https://register.nqa.gov.ua/uploads/0/569-fahivec_z_kriptograficnogo_zahistu_informacii_v_2.pdf .

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