НАЦІОНАЛЬНЕ АГЕНТСТВО ІЗ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	**Чернівецький національний університет імені Юрія Федьковича**
Освітня програма	**58038 Кібербезпека**
Рівень вищої освіти	**Магістр**
Спеціальність	**125 Кібербезпека та захист інформації**

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

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

Використані скорочення:

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

Загальні відомості

1. Інформація про ЗВО (ВСП ЗВО)

Реєстраційний номер ЗВО у ЄДЕБО	**61**
Повна назва ЗВО	**Чернівецький національний університет імені Юрія Федьковича**
Ідентифікаційний код ЗВО	**02071240**
ПІБ керівника ЗВО	**Білоскурський Руслан Романович**
Посилання на офіційний веб-сайт ЗВО	**www.chnu.edu.ua**

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

https://registry.edbo.gov.ua/university/61

3. Загальна інформація про ОП, яка подається на акредитацію

ID освітньої програми в ЄДЕБО	**58038**
Назва ОП	**Кібербезпека**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека та захист інформації**
Спеціалізація (за наявності)	*відсутня*
Рівень вищої освіти	**Магістр**
Тип освітньої програми	**Освітньо-професійна**
Вступ на освітню програму здійснюється на основі ступеня (рівня)	**Бакалавр, Магістр (ОКР «спеціаліст»)**
Структурний підрозділ (кафедра або інший підрозділ), відповідальний за реалізацію ОП	**НН ІФТКН, кафедра радіотехніки та інформаційної безпеки**
Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП	**Економічний факультет, факультет педагогіки, психології та соціальної роботи, факультет іноземних мов, Навчально-науковий інститут фізико-технічних та комп'ютерних наук**
Місце (адреса) провадження освітньої діяльності за ОП	**Навчально-науковий ІФТКН, 58002, м. Чернівці, вул. Сторожинецька, 101**
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	**107190**
ПІБ гаранта ОП	**Шпатар Петро Михайлович**
Посада гаранта ОП	**завідувач кафедри**
Корпоративна електронна адреса гаранта ОП	**p.shpatar@chnu.edu.ua**
Контактний телефон гаранта ОП	**+38(050)-978-50-14**
Додатковий телефон гаранта ОП	**+38(037)-250-94-89**

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

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

Освітньо-професійна програма «Кібербезпека» підготовки здобувачів другого (магістерського) рівня вищої освіти започаткована у Чернівецькому національному університеті імені Юрія Федьковича у 2017 році (прот. №6 засід. Вченої ради від 6.06.2017 р., наказ №162а/4 від 3.07.2017 р.). За підготовку магістрів за ОПП «Кібербезпека» за спеціальністю 125 – Кібербезпека та захист інформації відповідає кафедра радіотехніки та інформаційної безпеки Навчально-наукового інституту фізико-технічних та комп'ютерних наук ЧНУ. Остання чинна редакція ОП затверджена Вченою радою ЧНУ 26.06.2024 р. (прот. №9) і введена в дію наказом №248 від 28.06.2024 р.
У ЧНУ підготовку фахівців за напрямом «Інформаційна безпека» розпочато у 2002 році. Плідна співпраця тодішніх кафедри радіотехніки, фізичного факультету ЧНУ з держструктурами та промисловими підприємствами створила можливості підготовки висококваліфікованих фахівців, які мають глибокі теоретичні знання та необхідну практичну підготовку у сфері систем технічного захисту інформації. Пізніше, враховуючи зміни нормативного характеру та ґрунтуючись на результатах аналізу ринку праці та працевлаштування випускників, у ЧНУ було започатковано ОПП «Кібербезпека». В основу цієї ОП покладено ідею ґрунтовної базової підготовки у сфері кібербезпеки та захисту інформації, а також формування індивідуальної освітньої траєкторії здобувача завдяки гнучкій системі, що поєднує вибіркові дисципліни, практику, тематику індивідуальних завдань та дипломного проєктування і орієнтується на подальше працевлаштування випускника. Досвід діяльності ЧНУ та інших регіональних ЗВО підтверджують справедливість такого підходу.
У 2018 році ОПП «Кібербезпека» підготовки здобувачів другого (магістерського) рівня вищої освіти у Чернівецькому національному університеті імені Юрія Федьковича успішно пройшла акредитацію.
Зміст ОПП регулярно оновлюється. Робоча група проводить зустрічі та опитування в різних форматах усіх зацікавлених в ОПП, регулярно збирає зауваження та пропозиції для її оновлення. Блок вибіркових дисциплін доповнюється дисциплінами, що ґрунтуються на досягненнях випускової кафедри у практичній та науковій сферах і враховують побажання здобувачів освіти та стейкхолдерів. Зокрема, під час останнього оновлення ОП була зорієнтована на здобуття студентами професійних знань, умінь, навичок, загальних та фахових компетентностей для успішного здійснення професійної діяльності, розв'язання задач дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки, зокрема, в напрямку професійного стандарту «Фахівець сфери захисту інформації».

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

Рік навчання	Навчальний рік, у якому відбувся набір здобувачів відповідного року навчання	Обсяг набору на ОП у відповідному навчальному році	Контингент студентів на відповідному році навчання станом на 1 жовтня поточного навчального року		У тому числі іноземців	
			ОД	*З*	*ОД*	*З*
1 курс	2024 - 2025	50	11	1	0	0
2 курс	2023 - 2024	50	22	0	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	**58036 Кібербезпека**
другий (магістерський) рівень	**58038 Кібербезпека**
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	123622	32909

Власні приміщення ЗВО (на праві власності, господарського відання або оперативного управління)	116304	30535
Приміщення, які використовуються на іншому праві, аніж право власності, господарського відання або оперативного управління (оренда, безоплатне користування тощо)	7318	2374
Приміщення, здані в оренду	1284	0

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

8. Документи щодо ОП

Документ	Назва файла	Хеш файла
Освітня програма	*ОПП_(ЧНУ)_125_Кб_та_ЗІ__Маг_2024.pdf*	wzGDESKvZ+WRX8d/MLGu3nMqG4EozOMn6N5A+WW6ci0=
Освітня програма	*ОПП_(ЧНУ)_125_Кб_та_ЗІ__Маг_2023.pdf*	ZsIbR5jErSIAKSiQIZXuQoxiVRZwEQrlhF83ZHlPDEE=
Навчальний план за ОП	*План_2023.pdf*	94bWQnx990to2+Ka+toTvFj4yG9sJMoBMiIHdTY1G2k=
Навчальний план за ОП	*План_2024.pdf*	n00UendrO+92+hpXw6IjiuOjanwbsKYDWdoxGaKC2X8=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Рецензія_ВНТУ.pdf*	37awNZEiPR401/KKPoengrpaAjsJZb7PCiNQvWOfJyI=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Рецензія_Департ_кіберполіції.pdf*	kRoPuuv8PClBc5bPrEn6Tud5+hVWN1snbcvLR1a5kDs=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Рецензія_Румунія_USV.pdf*	iipgVYiJUwSpjkvQolYxm6hkq+HusAh4WNHMNpzPF9Y=

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?

ОПП «Кібербезпека» підготовки здобувачів другого (магістерського) рівня вищої освіти затверджена у 2017 році. Розробка відбувалась за відсутності відповідного Стандарту освіти. Після затвердження Стандарту ОПП була приведена у відповідність йому, а саме: уточнено цілі ОП, усі загальні компетентності, фахові компетентності та РН; в ОП сформовано перелік обов'язкових компонент, які сприяють набуттю цих компетентностей; згідно Стандарту вищої освіти в ОП передбачено можливість вільного вибору дисциплін для реалізації індивідуальної освітньої траєкторії здобувачів вищої освіти.
В подальшому ОП регулярно оновлювалась.
З врахуванням підсумків акредитаційної експертизи під час оновлення ОП у 2024 році здійснено кроки в напрямку підготовки здобувачів до проходження сертифікації за професійним стандартом у сфері кібербезпеки (фахівець сфери захисту інформації). Під час роботи над розвитком ОП узгоджено фахові (професійні) компетентності та РН (з

урахуванням трудових функцій фахівця), переглянуто зміст ОК. Так, в ОП додано КФ12, РН25 та ППО8, скориговано наповнення ЗПО2 та ППО1, ППО2, ППО6, ППО7, змінено ППО5, розширено перелік вибіркових дисциплін курсами, які можуть допомогти здобувачам підготуватись до сертифікації.
Загалом, ОК ОП забезпечують відповідні компетентності та РН освітнього Стандарту, що відображено у матрицях відповідності програмних компетентностей та результатів навчання компонентам ОП.

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

ОП не передбачає присвоєння професійної кваліфікації, проте під час її оновлення враховувалися вимоги професійного стандарту «Фахівець сфери захисту інформації» (https://register.nqa.gov.ua/uploads/0/439-profesijnij_standart_fahivec_sferi_zahistu_informacii.pdf).
Загалом, можливості випускників за ОП не обмежуються зазначеною професією, тому для визначення складових ОПП «Кібербезпека» ЧНУ орієнтується на вимоги Національного класифікатора професій та видів економічної діяльності, затверджених професійних стандартів для професій у галузі кібербезпеки, постанови та інші нормативні документи Кабінету Міністрів України, вимоги «Положення про систему внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти в ЧНУ», ухваленого Вченою радою ЧНУ (прот. № 7 від 31.08.2020 р.) (https://drive.google.com/file/d/14UAVRHptFJkoS4NW5h35lDhfpsqOsyrp/view).

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

Результати моніторингу відгуків та пропозицій здобувачів ВО щодо змісту ОП показують, що студенти прагнуть розвивати навички критичного мислення, комунікації та співпраці, що допоможе їм успішно інтегруватися в сучасне суспільство та ринок праці; поглиблено вивчати передові технології кіберзахисту, зокрема використання штучного інтелекту та машинного навчання у створенні захищених інфоком. систем, застосовувати інноваційні технології навчання, розширити свої можливості в міжнародних програмах академ. мобільності студентів, що дозволить їм відчути себе активним суб'єктом навчальної та майбутньої професійної діяльності, спроможним визначати особистісні цілі й засоби їх досягнення (http://surl.li/zdntbq , http://surl.li/rplhie, https://bit.ly/3PAWOLn).
Ці пропозиції розглядаються на зустрічах членів проектної групи, на підставі чого проводиться аналіз їх кореляції з метою та РН ОП та можуть вноситись зміни.
Зокрема, враховано пропозицію здобувача Пархоменка Є. відносно розширення переліку вибіркових ОК дисципліною «Технології та кібербезпека засобів штучного інтелекту». Також за результатами опитування здобувачів освіти щодо введення дисципліни (теми), в якій розглядається оцінка фінансових показників ризиків інформаційної безпеки, в ОП додано ППО8. Ці та інші пропозиції підтримані проектною групою для підсилення РН 2, 3, 5, 13, 20, 24, 25 чинної на момент пропозиції редакції ОП, затверджені на засіданнях кафедри (прот. №16, 16.02.2022; №16, 21.04.2023; №17, 02.05.2024).

- роботодавці

Випусковою кафедрою проводяться зустрічі з роботодавцями та обговорення вимог до фахівця на ринку праці (http://surl.li/nfzura, http://surl.li/pzgoxl), члени проектної групи беруть участь у різноманітних заходах, присвячених цій проблематиці (http://surl.li/fangmq). В результаті такої взаємодії з урахуванням специфіки та пропозицій роботодавців (державних установ, Держспецзв'язку, Департаменту кіберполіції Національної поліції України, НАБУ, представників Чернівецького ІТ Кластера тощо) здійснюється формування та коригування мети та програмних результатів навчання за ОП. Так, за пропозицією представників відділу інформаційної безпеки Управління СБУ в Чернівецькій області та відділу протидії кіберзлочинам Департаменту кіберполіції в Чернівецькій області Національної поліції України (http://surl.li/fgvsox) були запроваджені визначені освітньою програмою компетентність КФ11 та РН24.
Аналіз цих зустрічей дозволив зробити висновок, що їх вимоги до потенційних випускників-кандидатів на працевлаштування корелюють з метою, змістом та РН чинної редакції ОП (https://radiotech.chnu.edu.ua/novyny/kafedra/formuvannia-praktychnykh-navychok-u-fakhivtsiv-z-kiberbezpeky-kliuchovyi-napriamok-rozvytku-osvity-u-sferi-informatsiinoi-bezpeky/).

- академічна спільнота

Співпраця з представниками українських та закордонних ЗВО дозволяє враховувати інтереси академічної спільноти у формуванні мети та РН ОП через обмін досвідом та обговорення під час науково-методичних секцій міжвузівських та міжнародних наукових конференцій, семінарів, круглих столів тощо (https://bit.ly/4dYdVA1, https://bit.ly/3yQJ8q0, https://bit.ly/4g2hDu8, https://bit.ly/4dZgVvU, https://bit.ly/3MmJNma, http://surl.li/fangmq, https://bit.ly/3T5EDyz, https://bit.ly/3XhcKpW, https://bit.ly/4cFf6Dh).
В роботі Екзаменаційної комісії з атестації здобувачів випускова кафедра запрошує для головування представників інших ЗВО, зокрема НУ «Львівська політехніка», КНУ ім. Тараса Шевченка. У звітах ЕК вони висловлюють свої побажання та рекомендації щодо підготовки фахівців, які в подальшому використовуються для коригування мети та програмних результатів ОП. Зокрема, за рекомендаціями представників академічної спільноти (рецензент Яремчук Ю.Є., голови ЕК Стахіра П.Й. та Толюпа С.В.), що враховують сучасні тенденції розвитку ринку праці, запроваджено ЗПО1, ЗПО2, ППО3, ППО5, які у свою чергу дозволяють повною мірою впровадити в освітній процес компетентності та РН, передбачені затвердженим стандартом освіти.
Ефективність такої співпраці підсилюється залученням здобувачів освіти та викладачів випускової до міжнародних освітніх проектів за участі ЗВО України (грант G-202206-68835 http://surl.li/rsmzgs, проект USAID https://bit.ly/3MmJNma).

- інші стейкхолдери

Реалізація студентоцентрованого підходу до організації освітнього простору характеризується тим, що саме роботодавці й інші заінтересовані сторони вибудовують концепцію підготовки майбутніх випускників, тому під час формулювання мети та РН ОП зацікавлені сторони надавали свої пропозиції, враховані при оновленні ОП. Більшість з наданих пропозицій ґрунтувались на результатах дослідження ринку праці, законодавчих документах МОН України, можливостях працевлаштування магістрів (https://radiotech.chnu.edu.ua/novyny/kafedra/memorandum-pro-spivpratsiu-z-derzhavnoiu-sluzhboiu-spetsialnoho-zv-iazku-ta-zakhystu-informatsii-ukrainy/ , https://www.chnu.edu.ua/novyny/aktualni-novyny/memorandum-pro-spivpratsiu-z-derzhavnoiu-sluzhboiu-spetsialnoho-zviazku-ta-zakhystu-informatsii-ukrainy/).
Водночас випусковою кафедрою проводиться активна робота й з іншими зацікавленими сторонами (http://doncv.gov.ua/?p=2925, https://radiotech.chnu.edu.ua/novyny/kafedra/pidpysano-memorandum-pro-spivpratsyu-mizh-chernivetskym-natsionalnym-universytetom-imeni-yuriya-fedkovycha-ta-hromadskoyu-orhanizatsiyeyu-ayti-kor/).
Також налагоджена співпраця з установами, що відповідають за забезпечення комплексного вирішення питань регулювання зайнятості населення, профорієнтації та працевлаштування громадян (https://bit.ly/3r3BDVg, https://cutt.ly/kVmhxHd).

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

Згідно Стратегічного плану розвитку (http://surl.li/afflo), Статуту ЧНУ (https://bit.ly/3vQ58vY) та Концепції розвитку (https://www.chnu.edu.ua/media/fwmjte4r/kontseptsiia-rozvytku-universytetu_2023-2026.pdf) мета ОПП «Кібербезпека» відповідає місії ЧНУ, яка передбачає інноватівність, збалансованість, успіх і реалізується через розвиток системи освіти та наукової діяльності шляхом підготовки високопрофесійних, конкурентоспроможних фахівців, здатних активно діяти в умовах ринкової економіки та соціального партнерства; розвиток наукових пріоритетів, наукових шкіл, інноваційної складової.
Випускова кафедра бере участь у низці міжнародних проектів та програм (ERASMUS+, CRDF Global, Intel® FPGA Academic Program, USAID «Кібербезпека критично важливої інфраструктури України», http://radiotech.chnu.edu.ua/projects/), укладені меморандуми та угоди про співпрацю із провідними вітчизняними та міжнародними організаціями та підприємствами (http://surl.li/fgvsox, https://www.chnu.edu.ua/novyny/aktualni-novyny/memorandum-pro-spivpratsiu-z-derzhavnoiu-sluzhboiu-spetsialnoho-zviazku-ta-zakhystu-informatsii-ukrainy/), завдяки чому забезпечується актуальність мети ОП, формуються підстави до постійних системних змін у змісті та організації підготовки фахівців з вищою освітою. У свою чергу, така комунікація між стейкхолдерами та ЧНУ впливає на перспективи подальшого розвитку ЗВО в цілому.

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

Впродовж останніх років відзначається широке впровадження різноманітних інформаційних і телекомунікаційних технологій, які у свою чергу стимулюють дослідження науково-прикладного характеру, розроблення і застосування високоефективних засобів захисту інформації. Це зумовлює потребу у висококваліфікованих фахівцях спеціальності 125 – Кібербезпека та захист інформації, яка особливо загострилася у зв'язку з військовими діями в Україні (зокрема, https://radiotech.chnu.edu.ua/novyny/kafedra/mizhnarodna-konferentsiia-pid-ehidoiu-nato-ta-suchavskoho-universytetu-imeni-shtefana-chel-mare/). Зазначені тенденції враховані під час формулювання мети та програмних результатів навчання ОПП «Кібербезпека».
Тісна співпраця з роботодавцями, участь у міжнародних програмах (зокрема, USAID, CRDF Global тощо) та систематична робота над розвитком ОП створюють передумови для забезпечення узгодження мети і РН ОП з розвитком спеціальності.

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

Стрімкий розвиток інфокомунікацій стимулює розвиток і застосування новітніх інструментів захисту інформації. Це зумовлює потребу у висококваліфікованих фахівцях спеціальності 125 – Кібербезпека та захист інформації (https://bit.ly/44H6ic3). Такі тенденції та галузевий контекст враховані під час формулювання мети та РН ОП. Компетентності випускників, здатних забезпечувати захист об'єктів критичної інфраструктури, бізнесу, працювати у компаніях фахового профілю та споріднених галузей, у повній мірі узгоджуються з РН ОП, сформульованими відповідно до чинного стандарту освіти. Також конкурентна перевага на ринку праці підсилюється РН24, РН25, набуття яких готує здобувачів до роботи в умовах реального бізнесу та вимог до їх проф. кваліфікації.
КРТтаІБ та ЧНУ загалом укладено низку договорів про співпрацю з держустановами, комерційними компаніями (http://surl.li/nhluou), згідно з якими студенти проходять практику та працевлаштовуються, що надає їм можливість адаптуватися до реальних вимог ринку праці.
На регіональному рівні тенденції розвитку ОП враховують програми і плани розвитку Чернівецької обл. на період до 2027 р.(http://surl.li/zffnpj). В цьому аспекті випускники за ОП затребувані у держструктурах та їх підрозділах, на промислових підприємствах та в ІТ-компаніях м. Чернівці та Західного регіону.
Формування інд. освітньої траєкторії здобувачів освіти з врахуванням регіон. контексту забезпечується постійним оновленням переліку вибіркових ОК.

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

Під час формулювання мети та програмних результатів навчання ОП враховано досвід провідних ЗВО України, зокрема: Національного університету «Львівська політехніка», Харківського національного університету внутрішніх справ, Київського національного університету імені Тараса Шевченка, Національного технічного університету «Дніпровська політехніка», а також ОПП «Кібербезпека» Тернопільського національного університету імені Івана Пулюя та ОПП «Кібербезпека інформаційних технологій та систем» Вінницького національного технічного університету та інших. Аналіз цих ОП сприяв удосконаленню структурно-логічної схеми ОП та дозволив сформувати підходи до організації практичної підготовки здобувачів. Під час останнього оновлення ОП і узгодження її з вимогами професійного стандарту при формуванні ППО8 був врахований досвід ОП «Кібербезпека» (другий, магістерський рівень вищої освіти) ХНУВС та КНУ імені Тараса Шевченка.
На зустрічах та методичних семінарах в рамках науково-практичних конференцій (https://radiotech.chnu.edu.ua/novyny/kafedra/ix-mizhnarodna-naukovo-praktychna-konferentsiia-physical-and-technological-problems-of-transmission-processing-and-storage-of-information-in-infocommunication-systems/, https://radiotech.chnu.edu.ua/novyny/kafedra/ii-den-ix-mizhnarodnoi-naukovo-praktychnoi-konferentsii-physical-and-technological-problems-of-transmission-processing-and-storage-of-information-in-infocommunication-systems-predt-2021/) за участі представників ЗВО України, розробники ОПП «Кібербезпека» ЧНУ обговорювали ключові питання формування і оновлення ОП.

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

У формулюванні мети та програмних результатів навчання ОП враховано досвід іноземних освітніх програм у сфері інформаційної безпеки, зокрема, Сучавського університету Штефана чел Маре (https://fiesc.usv.ro/masterat-educatie/), а саме впорядковано блоки обов'язкових та вибіркових дисциплін.
У рамках міжнародного стажування представники робочої групи мають можливість ознайомлюватися з подібними ОП підготовки магістрів у іноземних ЗВО. Наприклад, представники кафедри радіотехніки та інформаційної безпеки Шпатар П.М., Ластівка Г.І. та Гресь О.В. під час стажування на факультеті електронної інженерії та інформаційних технологій університету «Люблінська політехніка» (Польща) вивчали досвід освітніх програм за спорідненими спеціальностями та брали участь у дослідженнях щодо розроблення новітніх технологій безпеки та застосування машинного навчання. Результати цієї роботи відображені у змісті ЗПО2, ППО3, ППО5, ППО7 та підкріплюють РН 4, 13, 16, 22, 24.

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)?

67

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

23

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

Зміст та ОК ОП являють собою логічно взаємопов'язану систему та відповідають предметній області спеціальності 125 – Кібербезпека та захист інформації згідно Стандарту вищої освіти. Цілі ОП відповідають Стандарту; програма має прикладне спрямування і орієнтована на здобуття студентами професійних знань, умінь, навичок, загальних та фахових компетентностей для успішного здійснення професійної діяльності, розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки, зокрема, в напрямку проф. стандарту «Фахівець сфери захисту інформації».
Об'єктами проф. діяльності в ОП, згідно Стандарту, є: сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформ. систем і технологій, інших бізнес-операційних процесів на об'єктах інформ. діяльності; інформ. системи та технології; системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформ. потоків); тощо. Цим об'єктам відповідає вивчення ОК професійної підготовки ОП.
Кожний ОК ОП враховує складові теоретичного змісту предметної області, що передбачає: теоретичні засади наукоємних технологій, фізичні і математичні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем (переважно забезпечується ОК: ППО1, ППО3); моделювання та оптимізації процесів, теорія математичної статистики (переважно ППО2); криптографічного та технічного захисту інформації (переважно ППО5, ППО7); теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформ. безпеки та/або кібербезпеки (переважно ППО4, ППО7-ППО11).
При формуванні ОП враховані надані в описі предметної області Стандарту методи, методики та технології

створення, обробки, передачі, приймання, знищення, відображення, захисту інформ. ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформ. безпеки та/або кібербезпеки, на що спрямовані ППО1, ППО3, ППО5, ППО7. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформ. ресурсів у кіберпросторі розглядаються в ППО1, ППО2, ППО4, ППО6-ППО11.
Інструменти та обладнання предметної області включають засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване ПЗ (ППО1, ППО5, ППО7); автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформ. потоків) (ППО1, ППО2, ППО7), методи і моделі теорії ризиків та управління інформ. ресурсами при дослідженні і супроводженні об'єктів інформ. діяльності у галузі інформ. безпеки та/або кібербезпеки (ППО6-ППО8). ОП містить також практичну складову (ППО9-ППО11), спрямовану на закріплення набутих навичок використання інструментів та обладнання предметної області.

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

Формування індивідуальної освітньої траєкторії забезпечується шляхом:
- складання індивідуального навчального плану, який є робочим документом магістра, що формується на підставі робочого навчального плану і містить інформацію про перелік та послідовність вивчення навчальних дисциплін, обсяг навчального навантаження здобувача (усі види навчальної діяльності), типи індивідуальних завдань, форму підсумкового оцінювання та атестацію здобувача;
- вибору дисциплін з блоку вибіркових компонент ОП за власним бажанням;
- самостійної роботи здобувачів з кожної дисципліни навчального плану на підставі відповідних методичних рекомендацій.
Результати опитування здобувачів показують, що, попри певну суперечливість відповідей, магістрам забезпечена можливість формування індивідуальної освітньої траєкторії. Вони можуть обирати вибіркові дисципліни із запропонованого блоку, розширювати базу практик відповідно до свого подальшого працевлаштування, а також здійснювати дослідницьку діяльність не тільки в межах базової кафедральної тематики, а й узгоджувати тему дипломної роботи/проекту з індивідуальними потребами професійної діяльності (https://bit.ly/3PAWOLn). Результативність такого підходу підтверджується наявністю патентів (наприклад, https://iprop-ua.com/inv/7ccvpfhi), актів впровадження у виробництво та освітній процес розробок магістрів (https://radiotech.chnu.edu.ua/diploma_design/).

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

Можливість реалізувати своє право на вибір навчальних дисциплін регламентується «Положенням про порядок реалізації студентами ЧНУ права на вибір навчальних дисциплін» (надалі Положення) (http://surl.li/affog).
Навчальні дисципліни за вибором здобувача вищої освіти вводяться в ОП з метою задоволення індивідуальних освітніх потреб студентів, посилення їх конкурентоспроможності на ринку праці, сприяють академічній мобільності магістра, а їх частка в ОПП «Кібербезпека» складає 25,6 % кредитів ЄКТС від загального обсягу.
Перелік вибіркових дисциплін підготовки магістра за ОПП «Кібербезпека» визначається випусковою кафедрою (https://radiotech.chnu.edu.ua/educationprograms/).
Терміни проведення процедур вибору студентами навчальних дисциплін визначаються з необхідності своєчасного (для планування та організації освітнього процесу, його методичного і кадрового забезпечення) формування контингенту студентів у групах і потоках. Студенти реалізовують своє право вибору навчальних дисциплін у семестрі, що передує семестру їх вивчення. Процедура вибору включає шість етапів:
- ознайомлення студентів із порядком, термінами та особливостями запису та формування груп для вивчення навчальних дисциплін вільного вибору в ЧНУ, а також із особливостями присвоєння професійних кваліфікацій за освітньою програмою, на якій навчається студент;
- ознайомлення студентів із переліками дисциплін вибору, які пропонуються як за програмою, за якою вони навчаються, так і за іншими програмами (зустрічі з представниками кафедр, деканатів, кураторами та презентації силабусів дисциплін, розміщених на сайті кафедр);
- запис студентів на вивчення навчальних дисциплін здійснюється за затвердженим графіком в ЧНУ з чітко визначеним терміном, але тривалість етапу не може перевищувати два тижні;
- опрацювання заяв студентів факультетом, проектними групами освітніх програм, перевірка контингенту студентів і попереднє формування груп на спеціалізації (профілі), а також мобільних груп на вивчення вибіркових дисциплін. За результатами етапу студентам, вибір яких не може бути задоволений з причин, перелічених у пп. 2.3 Положення, повідомляється про відмову (із зазначенням причини) і пропонується зробити вибір із скоригованого переліку (тривалість етапу не більше 5 робочих днів);
- повторний запис студентів на вивчення навчальних дисциплін (здійснюється за правилами, наведеними вище, тривалість – не більше 5 робочих днів);
- остаточне опрацювання заяв студентів факультетом, проектними групами освітніх програм, прийняття рішень щодо студентів, які не скористалися правом вільного вибору, перевірка контингенту студентів і формування груп на спеціалізації (профілі), а також мобільних груп на вивчення вибіркових дисциплін (тривалість етапу не більше тижня). Копії затверджених списків груп подаються до навчального відділу.
У ЧНУ починаючи з 2020-2021 н.р. запроваджено формування загальноуніверситетського каталогу вибіркових дисциплін (https://www.chnu.edu.ua/navchannia/dlia-studentiv/kataloh-kursiv/)

Опишіть, яким чином ОП та навчальний план передбачають практичну підготовку здобувачів вищої

освіти, яка дозволяє здобути компетентності, необхідні для подальшої професійної діяльності

В освітній програмі та навчальному плані ОПП «Кібербезпека» передбачається практична підготовка здобувачів у вигляді лабораторних, практичних занять, курсового та дипломного проектування, виробничої та переддипломної практик, які регламентуються «Положенням про проведення практики», (https://drive.google.com/file/d/1EMTd09rzwmD6gmLzuThArr1uKS6U2Bj6/view) та відповідним методичним забезпеченням (http://radiotech.chnu.edu.ua/syllabuses_krtib/). Практики завершуються захистом на випусковій кафедрі у відповідності до затвердженого порядку. На основі багаторічного досвіду проведення практик визначене коло підприємств, які здатні організовувати цей вид підготовки фахівців на належному рівні (https://radiotech.chnu.edu.ua/agreements/). Виходячи з потреб роботодавців та моніторингу ринку праці і розвитку спеціальності, формулюються цілі і завдання практичної діяльності студентів, визначається її зміст, який переглядається щорічно при оновленні робочих програм.
З метою поглиблення практичного спрямування підготовки здобувачів при кафедрі радіотехніки та інформаційної безпеки ЧНУ створене студентське конструкторське бюро «Алеф» (наказ №15 від 14.02.2003, керівник – к.т.н. Верига А.Д.) (http://radiotech.chnu.edu.ua/alef/), до складу якого входить підрозділ «Системи захисту інформації».

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

В ОП передбачена сукупність ОК, що сприяють набуттю соціальних навичок (soft skills), зокрема: здатність до ефективної комунікаційної взаємодії, вміння публічно виступати, працювати в команді, приймати обґрунтовані рішення, навички тайм-менеджменту тощо, відображені у ЗПО1, ЗПО2, ППО3, ППО4. Дисципліни, що передбачають групову форму виконання лабораторних робіт (ППО5, ППО7), практики (ППО9, ППО10) та інші також забезпечують формування soft skills. Важливе місце у набутті студентами вміння вільно спілкуватись, доносити свою думку колегам чи клієнтам зрозуміло і ввічливо, використовуючи проф. термінологію, займають консультації перед захистом дипломних робіт, що регулярно проводяться викладачами КРТІБ протягом місяця, що передує фінальному захисту (ППО11) в ЕК. На цих зустрічах (в т.ч. онлайн) магістри роблять доповіді за темою проекту чи дослідження, отримують конструктивні зауваження щодо доповіді та її представлення, навчаються відстоювати одержані результати.
Здобувачі освіти беруть активну участь у діяльності органів студентського самоврядування, де в тому числі розвиваються їх soft skills.
Під час оновлення ОП проведений аналіз та відбулося обговорення рекомендацій експертів НАЗЯВО щодо розширення переліку ЗК та РН такими, що відображають додаткові соціальні навички випускників. Оскільки спектр soft skills, про які згадували стейкхолдери, доволі широкий, було прийняте рішення обмежитись передбаченими Стандартом ЗК (протокол засідання каф. №17 від 02.05.2024 р.).

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 ОП має чітку структуру, ОК утворюють логічну взаємопов'язану систему, що відображено наведеною в ОП структурно-логічною схемою. Це допомагає здобувачеві освіти осягнути зміст і взаємозв'язок ОК та сформувати свою індивідуальну освітню траєкторію на основі запропонованих вибіркових дисциплін (http://radiotech.chnu.edu.ua/syllabuses_krtib/).
Успішне виконання здобувачем освіти передбачених ОП ОК забезпечує досягнення заявленої мети та програмних результатів навчання та слугують передумовою успішного проходження професійної сертифікації.

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

Відповідно до «Положення про організацію освітнього процесу в ЧНУ» (https://bit.ly/3Zb1Ot3) розроблено вимоги щодо обсягу окремих ОК (у кредитах ЄКТС) із фактичним навантаженням здобувачів, а саме: кількість контактних годин на 1 кредит для здобувачів другого (магістерського) рівня вищої освіти становить від 8 до 10 год. Решта часу відводиться на самостійну роботу. При цьому максимальне тижневе аудиторне навантаження не повинно перевищувати 18 год.
Для ОПП «Кібербезпека:
обсяг підготовки магістрів становить 90 кредитів, з них
- загальна підготовка – 8 кредитів (8,9 %);
- професійна підготовка – 59 кредитів (65,5 %);
- вибіркові освітні компоненти – 23 кредити (25,6 %).
Середній обсяг однієї обов'язкової навчальної дисципліни ОП становить 5,6 кредитів, а мінімальний – 4 кредити.
Середній показник кількості контактних годин на 1 кредит – 8,8 год.
При складанні розкладу занять враховуються норми навантаження здобувачів, відведена кількість аудиторних годин забезпечує достатній обсяг годин для виконання самостійної роботи.
Завантаженість здобувачів за ОП визначається опитуванням студентів (бесіди під час занять або індивідуальних консультацій), спостереженням з боку викладачів та наукових керівників з подальшим обговоренням результатів на засіданнях випускової кафедри (наприклад, прот. засідання кафедри № 16 від 20.03.2024).

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

Відповідно до Стандарту освіти, 16 кредитів ОП відведено на проходження здобувачами практики (ППО9, ППО10), яка може проводитись на реальних підприємствах та на базі держустанов сфери кібербезпеки (http://surl.li/nhluou). Також практична підготовка в рамках ОП передбачає виконання завдань на практичних та лабораторних заняттях, які мають конкретизований практико орієнтований характер. Зокрема, в дисципліні ППО6 студенти можуть прослідкувати процес ліцензування та атестації об'єктів інформаційної діяльності, а також саму процедуру отримання ліцензії на прикладі створення відповідного підрозділу ЧНУ (https://radiotech.chnu.edu.ua/novyny/kafedra/).
Перелік вибіркових ОК містить навчальні дисципліни, розроблені із залученням фахівців-практиків і враховують їх рекомендації та практичний досвід (наприклад, «Цифрова криміналістика»).
З метою провадження освітнього процесу за дуальною формою відповідно до Розпорядження Кабінету Міністрів України від 19.09.2018 № 660-р «Про схвалення Концепції підготовки фахівців за дуальною формою здобуття освіти» в ЧНУ прийнято «Положення про дуальну форму здобуття вищої освіти у ЧНУ» (http://surl.li/panozu). Підготовка здобувачів за дуальною формою освіти в рамках ОПП «Кібербезпека» не здійснюється, проте запроваджуються заходи щодо подолання розриву між теорією і практикою, освітою й виробництвом, підвищення якості підготовки з урахуванням вимог роботодавців.

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

Досягнення цілей сталого розвитку (ЦСР) задекларовано у Концепції розвитку ЧНУ на 2023-2026 р. (https://bit.ly/3Xawmed), зокрема, у розділах II - Завдання Університету (п. 5-7) та III - Принципи розвитку.
ЧНУ постійно, послідовно і відкрито здійснює політику та проводить заходи з метою досягнення ЦСР: впродовж тривалого часу реалізуються проекти енергоефективності, кліматичних інновацій та підприємництва (наприклад, Енерго-інноваційний хаб ЧНУ (https://bit.ly/3X1TlIa), Innovation Laboratories for Climate Actions (https://bit.ly/3XpNmhF тощо); проводяться заходи, що сприяють гендерній рівності та розширенню прав і можливостей жінок і дівчат (https://cutt.ly/cVJi1Ma).
На рівні ОП також створені умови для набуття здобувачами компетентностей, пов'язаних із забезпеченням сталого розвитку:
ОК ОПП «Кібербезпека» містять окремі теми щодо досягнення ЦСР (ЗПО2 та ППО4 формують навички роботи в команді, міжкульт. розуміння, терпимості, взаємної поваги та спільної відповідальності, навчання впродовж життя; ППО9-ППО11 включають розгляд питань впровадження «зелених технологій» у проф. діяльності майбутніх фахівців).
Питання формування свідомих громадян, відповідальних за майбутнє дітей, власної країни та людства загалом, розкривається під час виховної роботи. Освітня програма також включає вибіркові ОК, зміст яких присвячений ЦСР, та через неформальну та інформальну освіту, зокрема, завдяки можливості опанування курсів NA Cisco (Exploring Sustainability, A Framework for Sustainability in IT).

3. Доступ до освітньої програми та визнання результатів навчання

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

Правила прийому на навчання до ЧНУ знаходяться за посиланням: https://bit.ly/3sQxqIo

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

Прийом на навчання здійснюється на підставі Правил прийому до ЧНУ (https://bit.ly/3sQxqIo), розроблених відповідно до Порядку прийому на навчання до закладів вищої освіти України в 2024 році. Правила прийому розміщені на вебсайті ЗВО, чіткі, не містять дискримінаційних положень (приймаються громадяни України; іноземці; особи без громадянства, які проживають на території України на законних підставах, мають відповідний ступінь, освітній (освітньо-кваліфікаційний) рівень та виявили бажання здобути вищу освіту). Програма фахових вступних випробувань (https://www.chnu.edu.ua/abituriientu/vstup-do-mahistratury/pidhotovka-do-vstupu/fakhovyi-ispyt-mahistratura/) для осіб, які здобули попередній рівень вищої освіти, передбачає перевірку набуття вступником компетентностей та результатів навчання, визначених стандартом вищої освіти за спеціальністю 125 – Кібербезпека для першого (бакалаврського) рівня вищої освіти. У 2024 році таких абітурієнтів не було.
Згідно Правил прийому у 2024 році для абітурієнтів вступ до ОП здійснюється за результатами ЄДКІ (ЄФВВ) на конкурсній основі за відповідними джерелами фінансування та в межах ліцензованого обсягу за спеціальністю.

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?

Згідно «Положення про порядок реалізації права на акад. мобільність учасників осв. процесу ЧНУ» (https://bit.ly/3Z5z1YU), «Положення про організацію осв. процесу в ЧНУ», «Положення про порядок відрахування, переривання навч., поновлення, переведення, надання акад. відпустки у ЧНУ» (http://surl.li/loeevs) ЧНУ визнає еквівал. і перезараховує РН здобувача, отримані у ЗВО-партнері. Визнання РН здійснюється з використанням ECTS або системи оцінювання, прийнятої у країні ЗВО-партнера. Порядок перезарах. визначається угодою, яка підписується перед поїздкою на навчання і доводиться до відома здобувача. Перезарах. вивчених ОК здійснюється на підставі представленого здобувачем документа з переліком здобутків та РН з навч. курсів, кількістю кредитів та інформацією про систему оцінювання навч. здобутків, завіреного ЗВО-партнером. Перезарахування оцінок за шкалою оцін. ЧНУ здійснюють за середнім показником отриманої оцінки в ЗВО-партнері деканати, навч. і міжнар. відділи.
Визнання результатів попереднього навчання, кредитів ЄКТС, перезарах. ОК здійснюється так:
обов'язкові ОК або їх складники – за умови, що під час попереднього навч. особа здобула передбачені ОП або аналогічні РН;
вибіркові ОК – зараховуються, зокрема, ОК попереднього навчання, не зараховані як обов'язкові.
При прийнятті на навч. осіб, які подають документ про здобутий за кордоном ступінь освіти, обов'язковою є процедура визнання і встановлення еквівалентності документа (наказ МОНУ №504, 5.05.2015 р).

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

В ЧНУ визнання результатів навчання та кваліфікацій, отриманих на інших освітніх програмах залежно від випадків визнання регламентується: «Положенням про організацію освітнього процесу в ЧНУ» (http://surl.li/utojrr), «Правилами прийому до ЧНУ» (https://bit.ly/3sQxqIo), «Про порядок реалізації права на академічну мобільність учасників освітнього процесу ЧНУ» (https://bit.ly/3Z5z1YU).
Академічна мобільність передбачає участь здобувачів вищої освіти в освітньому процесі ЗВО (в Україні або за кордоном), проходження навчальної або виробничої практики, проведення наукових досліджень з можливістю перезарахування в установленому порядку освоєних навчальних дисциплін, практик тощо. Право на академічну мобільність здобувачів вищої освіти ЧНУ реалізується на підставі міжнародних договорів про співробітництво в галузі освіти та науки, міжнародних програм і проектів, договорів про співробітництво між ЧНУ та іноземними або вітчизняними ЗВО, а також може бути реалізоване здобувачами ВО з власної ініціативи, підтриманої адміністрацією ЧНУ на основі індивідуальних запрошень та інших механізмів.
Прикладів визнання результатів навчання та кваліфікацій, отриманих на інших освітніх програмах, на ОПП «Кібербезпека» магістерського рівня підготовки здобувачів вищої освіти не було. Проте проводиться робота щодо підготовки і реалізації зазначених можливостей: між ЧНУ та ЗВО України активно розвивається співпраця у напрямку внутрішньої академічної мобільності, укладаються відповідні договори та розроблений план заходів на 2024-2025 н.р.

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 отриманих у неформальній освіті результатів навчання регулюється «Положенням про взаємодію формальної та неформальної освіти, визнання результатів навчання (здобутих шляхом неформальної та/або інформальної, в системі формальної освіти) у Чернівецькому національному університеті імені Юрія Федьковича» (прот. №4 від 28.03.2022 р.) (https://www.chnu.edu.ua/media/3aykf41y/polozhennia-pro-vzaiemodiiu-formalnoi-ta-neformalnoi-osvity.pdf), в якому визначені критерії визнання результатів навчання, отриманих у неформальній освіті. Інформація про можливості неформальної освіти доступна на сайті ЧНУ. Текст згаданих Положень для учасників освітнього процесу розміщений на офіційному сайті ЧНУ у вільному доступі (розділ Університет > Нормативні документи > Пошук нормативних документів, https://www.chnu.edu.ua/universytet/normatyvni-dokumenty/).
Також про можливості неформальної освіти в контексті конкретних дисциплін здобувачів повідомляють гарант ОП та викладачі, які забезпечують проведення занять. Таку інформацію студентам надають на перших заняттях навчального року.

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

Випадків зарахування результатів навчання, отриманих у неформальній освіті, за ОПП «Кібербезпека» як окремих предметів чи модулів освітніх компонент не було. У вибірковій дисципліні «Захист і моніторинг комп'ютерних мереж» (Перелік на 2024-2025 н.р., https://radiotech.chnu.edu.ua/elective_subjects/) передбачена можливість вивчення здобувачем курсу «CyberOps Associate» Мережної Академії CISCO, успішне проходження якого може бути зараховане магістру як Змістовий модуль 2 даної дисципліни із додаванням відповідних 24 балів до загальної підсумкової оцінки.
На ОПП «Кібербезпека» магістерського рівня підготовки здобувачів ВО проводиться робота щодо підготовки і реалізації зазначених можливостей. Зокрема, у 2023-2024 н.р. студенту Дундичу Є. був зарахований 1 кредит (10 балів) в межах дисципліни «ТЗІ в комп'ютерних системах» на підставі сертифікату про участь у програмі внутр. акад. мобільності у ЛНТУ (угода про співпрацю від 09.04.2024, прот. засід. каф. № 17, 02.05.2024). Є й інші приклади визнання результатів навчання: Братівник А. («ТЗІ в комп'ютерних системах», прот. засід. каф. №17, 10.05.2023 р.), Обжелянський Г. («ТЗІ в телекомунікаційних системах», прот. №5, 13.10.2023 р.), Панівський Р. («Захист і моніторинг комп. мереж», прот. №17, 02.05.2024 р.). Відповідні рішення внесені до протоколів засідань КРТІБ.

Між ЧНУ та ЗВО України активно розвивається співпраця у напрямку внутр. акад. мобільності, укладаються відповідні договори та розроблений план заходів на 2024-2025 н.р.

4. Навчання і викладання за освітньою програмою

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

Освітній процес на ОПП «Кібербезпека» відповідає вимогам нормативних документів, оскільки на їх основі розробляються положення та процедури освітньої діяльності, а також реалізуються освітні програми в ЧНУ (https://www.chnu.edu.ua/universytet/normatyvni-dokumenty).
Форми й методи навчання регламентуються «Положенням про організацію освітнього процесу в ЧНУ» (http://surl.li/utojrr).
Методи, засоби та технології навчання і викладання на ОП відображені в робочих програмах ОК. Розробка РНП та силабусів регламентується відповідними положеннями і рекомендаціями: «Положення про порядок проведення внутрішнього моніторингу якості освітньої діяльності та якості вищої освіти в ЧНУ» (http://surl.li/aetyy), «Положення про систему внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти в ЧНУ» (https://cutt.ly/5CBgLrI). Кожна РНП ОК розробляється викладачами, які забезпечуються даним ОК, узгоджується з гарантом та затверджується на засіданнях випускової кафедри та методичної ради ННІФТКН. РНП містить: освітні технології, методи навчання і викладання навчальної дисципліни, засоби оцінювання (форми поточного та підсумкового контролю), які добираються розробниками РНП відповідно до Стандарту освіти, специфіки ОК і забезпечують досягнення мети та програмних результатів навчання за ОП.
Вагому роль відіграють електронні ресурси, зокрема система електронного навчання ЧНУ (https://moodle.chnu.edu.ua).

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

Впровадження технології студентоцентрованого навчання регламентується «Положенням про систему внутр. забезпечення якості освітньої діяльності та якості ВО в ЧНУ» (https://cutt.ly/5CBgLrI), що передбачає спрямованість освітнього процесу на набуття компетентностей, активне включення здобувачів в освітню діяльність на засадах рівноправних партнерських стосунків, з метою формування позитивної мотивації та особистісно-професійного саморозвитку. Такий підхід вимагає посилення ролі студента як учасника процесу навчання – від пасивного слухача до активного, який може впливати на процес отримання знань: можливість вибору дисциплін, місця проходження практики, навчання за індивідуальним графіком, формування завдань дослідницької та професійної діяльності з врахуванням індивідуальних інтересів. Зворотний зв'язок зі студентами реалізується через корпорат. email або ін. засоби комунікації. Навчально-методичне забезпечення ОК доступне на сайті кафедри (https://bit.ly/3SjxnwQ, https://cutt.ly/8VHPa7S) та у Moodle.
Задоволеність студентів формами і методами навчання і викладання відслідковується через соцопитування і анкетування (https://bit.ly/3RisI0k, http://surl.li/zdntbq, https://bit.ly/3LgmPgx). Загалом, отримані результати показують задоволеність здобувачів навчанням за ОП, яке відповідає їх уявленню про сучасну вищу освіту; респонденти відзначають відкритість та доступність інформаційно-консультаційної допомоги, цікаве наповнення і зрозуміле викладання навчальних дисциплін тощо.

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

Відповідно до Закону України «Про вищу освіту» та Статуту ЧНУ (https://bit.ly/3LARC6y), викладання навчальних дисциплін ОП передбачає академічну свободу, творчість, поширення знань та інформації. Одним з основоположних принципів діяльності університету є гарантування академічних свобод учасників освітнього та науково-інноваційного процесів. Відповідно до «Положення про організацію освітнього процесу в ЧНУ» (http://surl.li/utojrr) науково-педагогічним працівникам надається можливість вільно викладати, проводити наукові дослідження та поширювати отримані результати та виражати власну фахову думку; їм забезпечена свобода від втручання в професійну діяльність, свобода вибору й використання педагогічно обґрунтованих форм, методів, способів і засобів навчання, виховання. Академічна свобода охоплює й інтереси здобувачів, котрі враховуються викладачем в організації освітнього процесу (https://cutt.ly/8VHPa7S). Гнучке застосування різних форм і методів навчання і викладання з урахуванням специфіки окремої ОК сприяють досягненню програмних результатів ОП. З іншого боку, здобувачі завдяки можливості вибору дисциплін отримують знання з урахуванням своїх здібностей та потреб (особливих і інклюзивних). Крім того, вони мають право вільно висловлювати свої думки на заняттях, під час захисту курсових та магістерських робіт тощо; можуть використовувати дистанційну освітню платформу Coursera, яка надала безкоштовний доступ для ЧНУ до курсів дисциплін відомих університетів усього світу.

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

Цілі, зміст та очікувані результати навчання, порядок та критерії оцінювання регламентуються нормативними документами, розміщеними на сайті ЧНУ: https://www.chnu.edu.ua/universytet/normatyvni-dokumenty/. Ця ж інформація у розрізі окремих освітніх компонентів висвітлена в робочих програмах та силабусах, які розробляються за затвердженою в ЧНУ формою, регулярно оновлюються та розміщуються на сайті випускової кафедри. На першому занятті з навчальної дисципліни викладач доводить до відома здобувачів її зміст, послідовність, організаційні форми вивчення та їхній обсяг, визначає форми та засоби поточного й підсумкового контролю, результати навчання та необхідне навчально-методичне забезпечення. Здобувачі вищої освіти можуть ознайомитися з силабусом та робочою програмою навчальної дисципліни на сайті кафедри (http://radiotech.chnu.edu.ua/syllabuses_krtib/) та у системі Moodle, в рамках якої студенти мають доступ до електронних сторінок навчальних дисциплін. В електронному курсі зазвичай розміщені силабус, наповнення окремих навчальних елементів, перелік завдань та методичних вказівок з лабораторних та практичних робіт, очікувані форми звітності, критерії оцінювання, електронні тести та завдання для самоконтролю та підсумкової звітності, перелік літератури до навчальної дисципліни тощо. На сьогодні така форма надання інформації щодо ОК задовольняє всіх учасників освітнього процесу.

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

В рамках ОПП «Кібербезпека» передбачені такі форми та методи участі магістрів у дослідницькій діяльності: виконання завдань з науково-дослідною складовою у процесі вивчення фахових дисциплін (курсова робота з ППО1 «Технології комплексного захисту інформації», семінари з ППО3 «Перспективні напрямки розвитку систем кіберзахисту» та ін.), а також доповіді за результатами досліджень в рамках тематики дипломного проектування на наукових конференціях різного рівня. Щорічно в ЧНУ проводиться студентська наукова конференція, на якій здобувачі даної ОП представляють свої роботи (https://www.chnu.edu.ua/nauka/studentu/studentska-naukova-konferentsiia/arkhiv-studentskykh-konferentsii-chnu/). Під час виконання зазначених завдань здобувачі опановують вміння та навички аналізувати, верифікувати, оцінювати повноту інформації в ході професійної діяльності, при необхідності доповнювати й синтезувати відсутню інформацію та працювати в умовах невизначеності тощо. Викладачі, які забезпечують освітній процес за ОП, не обмежуються ознайомленням здобувачів із новітніми технологіями та науково-технічною інформацією в рамках викладу матеріалу навчальних предметів на заняттях, а й залучають студентів до досліджень за науковою тематикою випускової кафедри (https://radiotech.chnu.edu.ua/diploma_design , https://radiotech.chnu.edu.ua/projects /).
Здобувачі ОП успішно виступають на Всеукраїнських конкурсах студентських наукових робіт та конференціях різного рівня, інших заходах з кібербезпеки, де вони здобувають призові місця та відзнаки (https://bit.ly/3XqGNvu, https://bit.ly/3MrUjIR).
Крім того, результати досліджень прикладного характеру, виконаних в рамках дипломного проектування, відображаються у патентах на корисну модель, співавторами яких є студенти (наприклад, Влодарчик Д., №143362, https://iprop-ua.com/inv/7ccvpfhi/).
При кафедрі радіотехніки та інформаційної безпеки ЧНУ під керівництвом доцента Вериги А.Д. функціонує студентське конструкторське бюро «Алеф» (http://radiotech.chnu.edu.ua/alef/), яке забезпечує розвиток науково-дослідної, проектної та виробничої діяльності здобувачів. Учасники КБ мають можливість розробляти сучасні пристрої та системи захисту інформації, а успішні розробки представляються на конкурсах студентських наукових робіт та пропонуються до впровадження в освітній процес та виробництво.
Для заохочення студентів у представленні наукових здобутків у ЧНУ діє система матеріальних винагород. Наукова робота враховується в стипендіальному рейтингу (https://drive.google.com/file/d/18DJGM-5txAr4cJMixpf5SvbQFcSvrSej/view).

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

Порядок моніторингу та удосконалення ОК у ЧНУ регламентується «Положенням про розроблення та реалізацію освітніх програм ЧНУ» (https://bit.ly/3ddiGMl). Оновлення змісту навчальних дисциплін у ЧНУ відбувається щорічно або за необхідності з урахуванням поточних змін у законодавстві, розвитку технологій (навчальних та фахових) та наукових досліджень у профільній галузі. РП навчальних дисциплін ОПП «Кібербезпека» та інше навчально-методичне забезпечення, в якому відображено зміст ОК, затверджуються випусковою кафедрою перед початком нового навчального року. На КРТІБ проводяться засідання наукового семінару, регулярно відбуваються обговорення результатів стажування та підвищення кваліфікації професорсько-викладацького складу, аналіз результатів роботи Екзаменаційної комісії по захисту кваліфікаційних робіт/проектів. На основі пропозицій, висловлених під час цих заходів, викладачі, які забезпечують освітні компоненти ОП, формують нові елементи робочих навчальних програм дисциплін та коригують програми практик. Так, наприклад, у формуванні переліку тем семінарських занять ППО3 («Перспективні напрямки розвитку систем кіберзахисту») враховано тематичний напрям наукових досліджень і науково-технічних розробок (https://radiotech.chnu.edu.ua/projects/), а також відображені тенденції розвитку технологій забезпечення захисту інформації в інфокомунікаційних системах, які розглядались на міжнародній науково-практичній конференції (http://radiotech.chnu.edu.ua/predt/), що регулярно проводиться кафедрою радіотехніки та інформаційної безпеки ЧНУ.
За результатами стажування доц. кафедри Шпатаря П.М. в університеті «Люблінська політехніка» у ППО5 («Криптографічний захист інформації») запроваджено тему «Застосування штучного інтелекту в асиметричному шифруванні», матеріали якої використовуватимуться магістрами у дипломних роботах. Доцент Верига А.Д. використав досвід, набутий під час стажування у Сучавському університеті Штефана чел Маре (Румунія) за проблематикою формування освітньої програми з кібербезпеки, що враховано під час впорядкування блоків обов'язкових та вибіркових дисциплін ОПП «Кібербезпека».
Загалом, на випусковій кафедрі публікується значний обсяг наукових статей у рейтингових фахових виданнях, видаються підручники, навчальні посібники, монографії, матеріали яких включаються до ОК та використовуються у

дипломному проектуванні.
Викладачі кафедри регулярно беруть активну участь у тренінгах, буткампах, вебінарах та інших заходах, які організовуються для освітян та студентів провідними компаніями та професійними спільнотами у сфері кібербезпеки (наприклад, https://bit.ly/3Mq5ilU, https://bit.ly/3Mr8rC8, https://bit.ly/4dZgVvU). Результати таких зустрічей знаходять відображення у розвитку як самої ОП, так і в наповненні ОК в її складі.
Викладачі кафедри Ластівка Г.І. та Рождественська М.Г. є інструкторами Програми мережних академій Cisco, курси якої розширюють можливості здобувачів у формуванні індивідуальної освітньої траєкторії.

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

Завдання інтернаціоналізації належить до пріоритетних напрямків розвитку ЧНУ, які реалізуються за допомогою розробленого плану дій і заходів (https://www.chnu.edu.ua/media/uexmj1eg/internationalization-strategy_ukr.pdf).
Діяльність випускової кафедри спрямовується на забезпечення активної участі в міжнародних освітніх та наукових програмах і проектах (Erasmus+, Horizon 2020, CRDF та ін.), міжнародних наукових конференціях, семінарах тощо.
ОП передбачає ознайомлення здобувачів зі світовими науковими здобутками у сфері інформаційної безпеки. У локальній мережі ЧНУ є доступ до баз даних Cambridge University Press, Web of Science, Scopus та ін. Викладачі, залучені до реалізації ОП, проходять міжнародне стажування та беруть участь у програмах академічної мобільності (доц. Ластівка Г.І. та Шпатар П.М. – у технологічному університеті «Люблінська політехніка» (Польща), проф. Політанський Р.Л. – в Університеті Штефана чел Маре (Румунія), доц. Венкель Т.В. – в Університеті Коньянг (Konyang, Республіка Корея) та ін.).
Впродовж 2020-2023 викладачі випускової кафедри брали участь у локалізації англомовних курсів Програми мережних академій Cisco для українських студентів (доц. Ластівка Г.І. та Рождественська М.Г. перекладали курси IT Essentials, DevNet Associate, CyberOps Associate).
Магістри також можуть реалізувати своє право на міжнародну академічну мобільність («Положення про порядок реалізації права на академічну мобільність учасників освітнього процесу ЧНУ» (https://bit.ly/3Z5z1YU).

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?

Види, форми та особливості проведення контрольних заходів регламентовано «Положенням про контроль і систему оцінювання результатів навчання здобувачів вищої освіти у ЧНУ» (https://drive.google.com/file/d/1aDDzrMzuZ7OA1CervuLzeYLONEosLySV/view), а також відображено у Положенні про організацію освітнього процесу у ЧНУ (http://surl.li/utojrr). Для оцінювання навчальних досягнень здобувачів ВО в рамках навчальних дисциплін здійснюється поточний та підсумковий контроль.
Згідно з Положенням, передбачені такі форми контролю: усний, письмовий, різновидом його є тестовий контроль у письмовій або електронній формах. Різновиди контрольних заходів, що використовуються: усне та письмове опитування; поточне тестування; представлення доповідей та мультимедійних презентацій; захист лабораторних робіт; захист звітів за результатами практик; онлайн-тестування із застосуванням платформи Moodle (Додаток до «Положення про організацію освітнього процесу у ЧНУ», https://drive.google.com/file/d/1ChIo3Qnw3jsPcFZsbS-7gGv4m3hJ6HbA/view); модульні контрольні роботи, підсумковий тестовий контроль, самооцінка та самоаналіз.
Поточний контроль дозволяє здійснювати перевірку розуміння і засвоєння матеріалу дисципліни, набутих навичок виконання завдань курсового проектування, умінь самостійно опрацьовувати літературні джерела, здатності визначати ключові моменти теми чи розділу, умінь публічно чи письмово представити опрацьований матеріал (презентації).
Поточний контроль проводиться впродовж семестру і здійснюється на семінарських, практичних, лабораторних заняттях та під час виконання завдань модульних контрольних робіт та тестів. За організацію поточного контролю та його методичне забезпечення відповідає викладач, який проводить ці види занять.
Підсумковий контроль проводиться для оцінки результатів навчання на певному рівні вищої освіти або на його окремих завершених етапах і включає екзамен, залік й атестацію. Підсумкова атестація випускників за даною ОП проводиться у формі публічного захисту кваліфікаційної роботи на засіданні ЕК з атестації здобувачів вищої освіти, затвердженої Вченою радою університету.
Всі зазначені заходи повною мірою дозволяють перевірити досягнення студентами програмних результатів навчання.
З формами контрольних заходів певної навчальної дисципліни ОП здобувач може ознайомитися, переглянувши освітню програму, навчальний план, силабус та робочу програму цього ОК, які розміщуються на сайті кафедри та в рамках платформи Moodle.
При проведенні навчання у дистанційному форматі контроль здійснюється відповідно до Додатку до «Положення про організацію освітнього процесу в ЧНУ» за 100-бальною шкалою шляхом сумування балів, отриманих під час оцінювання рівня оволодіння теоретичним матеріалом та виконання практичної частини курсу.
Інструментом стимулювання до покращення якості навчання є рейтингове оцінювання успішності здобувачів вищої освіти, що регламентується «Положенням про рейтинг студентів ЧНУ» (http://surl.li/vyijan, http://surl.li/rblezj).

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

Відомості про форми контрольних заходів та критерії оцінювання навчальних досягнень здобувачів ВО чітко та зрозуміло сформульовані у робочих програмах навчальних дисциплін, оприлюднених на сайті кафедри, а також у відповідних курсах на платформі Moodle (згідно з «Положенням про контроль і систему оцінювання результатів навчання здобувачів ВО у ЧНУ», https://drive.google.com/file/d/1aDDzrMzuZ7OA1CervuLzeYLONEosLySV/view).
На першому занятті кожної навчальної дисципліни викладач зобов'язаний чітко і зрозуміло ознайомити студентів з механізмами проведення контрольних заходів та критеріями їх оцінювання, зокрема, повідомити про розподіл балів за навчальні елементи ОК, а також поінформувати щодо наявного методичного забезпечення. Після проведення контрольного заходу викладач роз'яснює студентам допущені помилки та аргументує оцінку. Здійснення тих чи інших контрольних заходів викладачем контролюється завідувачем кафедри, дирекцією, навчальним відділом, ректоратом ЧНУ у вигляді контрольних зрізів та оцінки рівня залишкових знань.
Оцінювання навчальних досягнень здобувачів за кількісними критеріями здійснюється за національною шкалою (відмінно, добре, задовільно, незадовільно; зараховано, не зараховано); 100-бальною шкалою та шкалою ECTS (A, B, C, D, E, FX, F).

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

Відомості щодо форм контрольних заходів та критеріїв оцінювання доводяться здобувачам вищої освіти через оприлюднені на сайті випускової кафедри ОП, робочий навчальний план, силабуси, робочі програми дисциплін та матеріали на платформі Moodle. На перших заняттях з навчальної дисципліни (лекційному, лабораторному, практичному) викладач знайомить студентів із тематикою всіх видів занять, у т.ч. контрольних заходів, розподілом часу, запланованого на засвоєння матеріалу, а також тем, відведених на самостійне опрацювання. Також здобувачі ВО інформуються про терміни і процедуру проведення контрольних заходів, критерії оцінювання дисципліни в цілому та за окремими видами робіт.
Після завершення практики, оформлення студентом звітних документів впродовж 3 днів проводиться захист.
З метою забезпечення організації освітнього процесу і проведення підсумкового контролю в НН ІФТКН за погодженням з кафедрами складається розклад заліків та екзаменів, який доводиться до відома студентів і викладачів не пізніше, ніж за місяць до проведення контролю. Графік заліково-екзаменаційної сесії оприлюднюється на дошці оголошень та на сайті НН ІФТКН.
Організація та проведення атестації здобувачів здійснюється відповідно до «Положення про атестацію здобувачів вищої освіти та організацію роботи Екзаменаційної комісії в ЧНУ» (https://drive.google.com/file/d/1-JYnU5bt8e_KIz4-AlQPDuSOLFGd6mN8/view). Графік роботи ЕК оприлюднюється не пізніше, ніж за місяць до початку її діяльності.

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

Відповідно до стандарту вищої освіти за другим (магістерським) рівнем спеціальності 125 – Кібербезпека атестація випускників ОПП «Кібербезпека» проводиться у формі захисту кваліфікаційної магістерської роботи/проекту та завершується видачею документу встановленого зразка про присудження здобувачу ступеня магістра із присвоєнням кваліфікації: магістр з кібербезпеки та захисту інформації.
Атестація здійснюється відкрито і публічно. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації.
Кваліфікаційна робота має бути розміщена на офіційному сайті (або у репозитарії) ЧНУ або випускової кафедри.
Строк і тривалість проведення атестації здобувачів визначається графіком освітнього процесу та регулюються пунктами «Положення про атестацію здобувачів вищої освіти та організацію роботи Екзаменаційної комісії в ЧНУ» (https://drive.google.com/file/d/1-JYnU5bt8e_KIz4-AlQPDuSOLFGd6mN8/view).
Згідно стандарту вищої освіти другого (магістерського) рівня спеціальності 125 – Кібербезпека, проведення атестації здобувачів у формі ЄДКІ не передбачене.

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

Процедура проведення контрольних заходів визначена «Положенням про контроль і систему оцінювання результатів навчання здобувачів вищої освіти у ЧНУ» (https://drive.google.com/file/d/1aDDzrMzuZ7OA1CervuLzeYLONEosLySV/view).
Процедура проведення захисту практик регламентується «Положенням про проведення практики здобувачів вищої освіти ЧНУ» (https://drive.google.com/file/d/1EMTd09rzwmD6gmLzuThArr1uKS6U2Bj6/view).
Атестація здобувачів регулюється «Положенням про атестацію здобувачів вищої освіти та організацію роботи Екзаменаційної комісії в ЧНУ» (https://drive.google.com/file/d/1-JYnU5bt8e_KIz4-AlQPDuSOLFGd6mN8/view).
Текст згаданих Положень для учасників освітнього процесу розміщений на офіційному сайті ЧНУ у вільному доступі (розділ Університет > Нормативні документи > Пошук нормативних документів, https://www.chnu.edu.ua/universytet/normatyvni-dokumenty/).
Інформацію про процедуру проведення контрольних заходів також можна знайти в робочих програмах та силабусах навчальних дисциплін на сайті випускової кафедри (http://radiotech.chnu.edu.ua/syllabuses_krtib/), а також вона доступна для здобувачів ВО через систему дистанційного навчання Moodle.

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

Згідно «Положення про контроль і систему оцінювання результатів навчання здобувачів ВО у ЧНУ» (https://drive.google.com/file/d/1aDDzrMzuZ7OA1CervuLzeYLONEosLySV/view) визначені процедури забезпечення об'єктивності оцінювання через дотримання прозорості, створення рівних можливостей і упередження несправедливих пільг, відкритість інформації щодо умов оцінювання, єдині критерії оцінювання, оприлюднення строків здачі контрольних заходів; встановлення єдиних правил перескладання контрольних заходів.
Оскарження результатів семестрового контролю регламентується «Положенням про апеляцію на результати підсумкового семестрового контролю знань студентів» (https://drive.google.com/file/d/16FPnHMJXd2al362HvDwmvoZ5uEih42ks/view)
Процедури запобігання конфлікту інтересів регулюють «Правила академічної доброчесності ЧНУ» (https://drive.google.com/file/d/1EzBsehqERCEzxJwWe-rz6_eTUFUBGv40/view) та «Етичний кодекс ЧНУ» (http://surl.li/fmidcs).
Для об'єктивності проведення захисту курсових проектів складається комісія з трьох викладачів кафедри. Захист магістерських робіт проводиться на відкритому засіданні ЕК за обов'язкової присутності голови комісії. Здобувачі та інші особи можуть вільно здійснювати аудіо-, відеозапис процесу захисту атестаційної роботи. Всі курсові і магістерські роботи випускників зберігаються в архіві кафедри протягом 3 років.
Випадків оскарження результатів контрольних заходів та атестації здобувачами, а також конфліктів інтересів не було.

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

Відповідно до «Положення про контроль і систему оцінювання результатів навчання здобувачів ВО у ЧНУ» (http://surl.li/affxu), система оцінювання в ЧНУ передбачає накопичення балів під час теоретичного та практичного навчання і здійснюється за 100-бальною шкалою. Студенти, які одержали під час семестрового контролю незадовільні оцінки і навчаються на контрактній основі, можуть ліквідувати заборгованість до кінця навчального року. Здобувач не допускається до перескладання іспиту з дисципліни, доки не виконає всі види робіт, передбачені програмою. Повторне складання іспитів допускається не більше двох разів з кожної дисципліни: один раз – викладачу, другий – комісії, яка створюється директором НН ІФТКН.
Згідно «Положення про порядок відрахування, переривання навчання, поновлення, переведення, надання академвідпустки здобувачам вищої освіти ЧНУ» (https://cutt.ly/RC7if0u), здобувач, який під час складання екзамену комісії отримав незадовільну оцінку, відраховується з ЧНУ або залишається на повторний курс; рішення комісії – остаточне. Повторний захист дипломної роботи можливий через рік після неуспішного захисту. Так, наприклад, на ОПП «Кібербезпека» мали місце випадки повторного складання іспиту з ППО6 (2021-2022 н.р. - Губчак А., Юрков Д.); повторного захисту дипломних робіт впродовж 2019-2024 н.р. не було.

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

Процедури розгляду звернень здобувачів щодо оцінювання (незгоди, конфлікту тощо) регулюються «Положенням про апеляцію на результати підсумкового семестрового контролю знань студентів ЧНУ» (https://drive.google.com/file/d/16FPnHMJXd2al362HvDwmvoZ5uEih42ks/view), а також п.5 «Положення про атестацію здобувачів вищої освіти та організацію роботи Екзаменаційної комісії в ЧНУ» (https://drive.google.com/file/d/1-JYnU5bt8e_KIz4-AlQPDuSOLFGd6mN8/view).
У разі надходження від здобувача апеляції розпорядженням ректора створюється комісія для розгляду апеляції. Головою комісії призначається проректор, директор НН ІФТКН, їх заступники або начальник навчального відділу. Комісія розглядає апеляції здобувачів щодо порушення процедури захисту кваліфікаційних робіт, що могло негативно вплинути на оцінку ЕК. Апеляція розглядається протягом трьох календарних днів після її подання. У випадку встановлення комісією порушення процедури проведення атестації, яке влипнуло на результати оцінювання, комісія пропонує ректору ЧНУ скасувати відповідне рішення ЕК та провести повторне засідання ЕК з обов'язковою присутністю представників комісії з розгляду апеляції.
Випадків апеляцій на результати проведення семестрових контрольних заходів та порушення процедури захисту кваліфікаційних робіт на ОПП «Кібербезпека» не було.

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

Задля дотримання академічної доброчесності в ЧНУ розроблено низку нормативних документів: «Правила академічної доброчесності у ЧНУ» (https://drive.google.com/file/d/1EzBsehqERCEzxJwWe-rz6_eTUFUBGv40/view); «Положення про постійну комісію з питань академічної доброчесності, правових засад діяльності та регламенту Вченої ради ЧНУ» (https://drive.google.com/file/d/1auN6M5FzyvaglVi3HW16N01TT1IjuD7q/view); «Етичний кодекс ЧНУ» (http://surl.li/fmidcs); «Положення про виявлення та запобігання академічному плагіату в ЧНУ» (https://cutt.ly/mVH8mqi). Дотримання канонів академічної доброчесності членами університетської спільноти задекларованe у Статуті ЧНУ та є атрибутивною частиною Контракту кожного працівника, студента. Дотримання академічної доброчесності здобувачами освіти передбачає: самостійне виконання індивідуальних завдань, завдань поточного та підсумкового контролю; посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей; дотримання норм законодавства про авторське право і суміжні права тощо. Ставлення здобувачів ЗВО до реалізації положень і процедури дотримання академічної доброчесності можна з'ясувати через періодичні анонімні опитування. За ОПП «Кібербезпека» кваліфікаційні роботи здобувачів проходять обов'язкову перевірку на наявність академічного плагіату, а також з метою підвищення якості навчального процесу рекомендовано перевіряти й інші письмові роботи (реферати, курсові роботи/проекти тощо).

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

У «Положенні про виявлення та запобігання академічному плагіату в ЧНУ» (https://cutt.ly/mVH8mqi) регламентовано порядок перевірки й умови подання навчально-методичних та кваліфікаційних робіт на перевірку та відповідальність за плагіат. Для виявлення фактів академічного плагіату ЧНУ укладаються угоди з компаніями відповідного профілю (Unicheck, Turnitin). Антиплагіатна програма визначає ступінь ідентичності тексту. Всі кваліф. роботи студентів ОПП «Кібербезпека» проходять обов'язкову перевірку на наявність академічного плагіату. Текст вважається оригінальним, якщо схожість не перевищує 30%, в такому випадку кваліфікаційна робота допускається до захисту.
За потреби можуть перевірятись й інші письмові роботи (курсові, реферати тощо). За підтримки компанії Tutnitin всі роботи, подані у системі Електронного навчання, автоматично перевіряються на оригінальність.
Питання академічної доброчесності обговорюються і на засіданнях випускової кафедри, зокрема, під час уточнення вимог до виконання магістерських робіт/проектів за ОПП «Кібербезпека» (прот. №6, 24.11.2020; №17, 10.05.2023; №16, 20.03.2024).
У ННІ ІФТКН створена Етична комісія, до якої можуть звернутися учасники освітнього процесу у разі порушення академічної доброчесності. До складу комісії входять представники підрозділів ННІФТКН та студентського самоврядування (https://bit.ly/3qENXeg).
Кваліфікаційні роботи здобувачів вищої освіти ОП оприлюднюються на сайті випускової кафедри (https://radiotech.chnu.edu.ua/diploma_design/).

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

У ЧНУ функціонує постійна комісія з академічної доброчесності, правових засад діяльності та регламенту Вченої ради ЧНУ (http://surl.li/affzs), яка популяризує академічну доброчесність. Відповідні комісії створені в усіх структурних підрозділах, в тому числі в ННІФТКН. ЧНУ є учасником проєкту AcademIQ «Ініціатива академічної доброчесності та якості освіти» (http://surl.li/icdviu). Повідомлення про заходи з популяризації академічної доброчесності представлені на сайті ЧНУ (http://surl.li/bvguow) та на сайті ННІ ІФТКН (https://cutt.ly/oC5vTjS). У ЧНУ регулярно проходять семінари з питань наукової етики та недопущення академічного плагіату в освітньому процесі та наукових роботах. Питання популяризації академічної доброчесності серед здобувачів ВО кожного року розглядається на науково-методичній та науково-технічній радах, кафедрах за участі представників бібліотеки. Поширенню досвіду академічної доброчесності серед здобувачів ВО сприяє перевірка на академічний плагіат курсових, кваліфікаційних та наукових робіт (https://moodle.chnu.edu.ua/).
На випусковій кафедрі призначено відповідального за перевірку текстів на предмет їх унікальності, який стимулює здобувачів та науково-педагогічний колектив до дотримання вимог академічної доброчесності. Зокрема, здобувачі ВО кафедри радіотехніки та інформаційної безпеки неодноразово брали участь у вебінарах за тематикою академічної доброчесності (http://surl.li/mavydp, http://surl.li/qqopfj тощо).

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

Питання відповідальності за порушення академічної доброчесності, як-от академічний плагіат, фальсифікація, списування, обман, хабарництво тощо, регламентуються «Положенням про організацію освітнього процесу» (http://surl.li/utojrr). Положенням передбачено, що здобувачі ВО можуть притягатися до таких видів академічної відповідальності: повторне проходження оцінювання; повторне проходження відповідного освітнього компонента освітньої програми; позбавлення академічної стипендії; позбавлення наданих університетом пільг з оплати навчання; відрахування з університету.
В ЧНУ створена комісія з академічної доброчесності. Її склад та регламент діяльності передбачені «Правилами ЧНУ з академічної доброчесності» (http://surl.li/affyt). Комісія розглядає випадки порушення правил академічної доброчесності та приймає рішення щодо підтвердження чи спростування факту порушення членом університетської спільноти правил академічної доброчесності. Формою роботи комісії є відкриті засідання; рішення ухвалюються простою більшістю присутніх. Рішення Комісії вручається особі, щодо якої воно виносилося, та адміністрації університету для вжиття необхідних заходів і оприлюднюється на веб-сайті університету.
Випадків порушення академічної доброчесності здобувачами ОПП «Кібербезпека» не зафіксовано.

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

Для забезпечення необхідного рівня професіоналізму викладачів їх обрання відбувається на конкурсній основі («Положення про проведення конкурсу на заміщення вакантних посад науково-педагогічних працівників у ЧНУ» (https://drive.google.com/file/d/1hm-0n4WmOXuAn4Q_oiz1b4GuR9-77J53/view).
На посади науково-педагогічних працівників обираються особи, які мають наукові ступені або вчені звання відповідно до профілю кафедри, а також особи, які мають ступінь магістра. Конкурсний відбір проводиться на

засадах відкритості, гласності, законності, об'єктивності, неупередженого ставлення до кандидатів на зайняття вакантних посад. Конкурс на заміщення вакантної посади оголошується ректором, про що видається відповідний наказ. Оголошення про проведення конкурсу, терміни та умови його проведення публікуються на офіційному сайті університету. Кандидатури претендентів обговорюються на засіданні кафедри в їх присутності. Обрання на посади асистентів, доцентів, професорів проводиться таємним голосуванням на засіданні Вченої ради. Рівень професіоналізму науково-педагогічних працівників ОПП «Кібербезпека» відповідає п. 37, 38 Ліцензійних умов провадження освітньої діяльності. Викладачі випускової кафедри мають наукові публікації, методичні розробки, сертифікати тощо, що підтверджують їхню фаховість у тому освітньому компоненті, який вони забезпечують. Зведена інформація про викладачів наведена в Таблиці 2 звіту СО.
Якщо ОК має міждисциплінарний характер, до її забезпечення залучаються викладачі відповідних спеціальностей, що відображено в робочих програмах ОК та іншому навчально-методичному забезпеченні (наприклад, ППО4, ППО5 та інші).
Враховуючи рекомендації, надані експертами НАЗЯВО під час акредитаційної експертизи ОПП «Кібербезпека» у 2023-2024 н.р., випусковою кафедрою вжито ряд заходів (https://www.chnu.edu.ua/media/w4mlmtwo/pyt-212plan_zakhodiv_125_kiberbezpekapptx.pdf):
- до освітнього процесу даної ОП залучено викладачів (професорів, д. т. н.) за спеціальністю 125 – Кібербезпека;
- 5 викладачів кафедри наразі здобувають ступінь магістра за спеціальністю 125 – Кібербезпека та захист інформації;
- прийняте рішення про присудження асистенту КРТІБ к.т.н. за спеціальністю 05.13.21 – системи технічного захисту інформації Гресь О.В. вченого звання доцента (рішення Вченої ради ЧНУ, прот. №9 від 26.06.2024 р., https://www.chnu.edu.ua/media/h44fpxnz/protokol-9-vid-26062024.pdf);
- активізована робота з професіоналами- практиками (https://radiotech.chnu.edu.ua/novyny/kafedra/korotki-pidsumky-spivpratsi-kolektyvu-kafedry-radiotekhniky-ta-informatsiinoi-bezpeky-chnu-zi-steikkholderamy-u-2023-2024-navchalnomu-rotsi/).

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

Відповідно до Положення про проведення конкурсу на заміщення вакантних посад науково-педагогічних працівників у ЧНУ (https://bit.ly/3Z9qxAj) п. 6, 7 оцінка рівня професійної кваліфікації претендента на посаду перш за все здійснюється випусковою кафедрою. Участь у процедурі розгляду кандидатури беруть гаранти та члени проектної групи ОП, які реалізуються на кафедрі.
В п. 4 Положення про гаранта освітньої програми Чернівецького національного університету імені Юрія Федьковича (https://www.chnu.edu.ua/media/qmapwn1b/polozhennia-pro-haranta-osvitnoi-prohramy.pdf) гарант ОП за своїми функціональними обов'язками відповідає за реалізацію ОП на всіх етапах та під час проведення акредитації. Серед завдань гаранта ОП є контроль якості та відповідності вимогам кадрового забезпечення ОП. Таким чином, добір НПП для успішної реалізації конкретної ОП, досягнення її ПРН, спроможність забезпечити викладання відповідно до цілей освітньої програми, необхідний рівень професіоналізму кандидата на посаду на першому етапі процедури проведення конкурсу забезпечується гарантом та випусковою кафедрою. Подальша оцінка відповідності кваліфікації (академічної, професійної) претендента відбувається згідно процедури, визначеної Положенням.
На кафедрі радіотехніки та інформаційної безпеки ЧНУ, на якій реалізується дана ОП, аналізується відповідність претендентів ліцумовам (http://surl.li/wciboj), подібна практика має місце й на інших кафедрах 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

ЧНУ активно залучає роботодавців до реалізації осв. процесу. Взаємодія в рамках укладених меморандумів та угод про співпрацю із вітчизняними та міжнар. організаціями та підпр. (http://surl.li/nhluou) дає можливість удосконалювати РП та зміст ОК, оновлювати перелік вибір. курсів, оперативно реагувати на потреби ринку праці у регіоні. Стейкхолдери беруть участь у розробленні метод. матеріалів вибір. дисциплін (http://surl.li/gqyjyo), формуванні лаб. бази (Компанія Tektelic, ТОВ «ІнТех», http://surl.li/fdxwm, https://bit.ly/3SdUCbg), практик та дипл. проектування, що дозволить їм в перспективі поповнити свій кадровий потенціал. Наприклад, здобувачі в рамках курсу «Радіомоніторинг і радіопротидія на об'єктах інформ. діяльності» брали участь в екскурсіях до КП «Міжнар. аеропорт «Чернівці», Чернівецького обл. відділу КФ ДП «Укр. держ. центр радіочастот» (2019-2022 н.р.) з метою ознайомлення з роботою цих підприємств, обладнанням та методиками проведення РЧ моніторингу.
Здобувачі освіти брали участь у низці вебінарів, організованих в рамках проекту USAID "Кібербезпека критично важливої інфр. України".
До підготовки здобувачів за даною ОП залучаються проф.-практики та провідні фахівці галузі. Зокрема, восени 2022 р. в рамках вивчення ППО5 професором ХНУ ім. Каразіна, д.т.н. І.Д. Горбенком була прочитана серія лекцій з питань прикладної криптології. Професор, д.т.н. М.І. Прокофьєв впродовж 2023-2024 н.р. проводив заняття з ППО1 та керував дипломним проектуванням (http://surl.li/zwywdk).

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

ЧНУ сприяє проф. розвиткові викладачів як складової системи забезпечення якості освітньої діяльності, згідно «Положення про підвищення кваліфікації науково-педагог. працівників ЧНУ» (http://surl.li/cflafo).
В період карантину ЧНУ перейшов на дистанційне навчання й провів для співробітників курси внутрішнього підвищення кваліфікації «Основи користування Moodle» (3 кред.), організував надання викладачам безоплатного доступу до платформи дистанц. навчання Coursera. Викладачами факультету іноземних мов проводилась серія

науково-метод. семінарів-практикумів «Алгоритм підготовки до викладання фахових дисциплін англ. мовою» (Ластівка Г.І., Рождественська М.Г.). Для підвищення педмайстерності викладачів у ЧНУ створені курси «Педагогічно-дослідницька компетентність молодого науковця та викладача вищої школи: актуальні виклики і перспективи», http://surl.li/skgvwd (Косован Г.В., свід. ПК-РМВ, № 52/2024 від 19. 04.2024 р.)
Безперервний проф. розвиток викладачів забезпечується системою постійно діючих наукових та методичних заходів. У ЧНУ створено умови для здійснення програм академ. мобільності за Еразмус+ та отримання міжнар. сертифікації для викладачів (http://surl.li/cqawwv). Зокрема, пройшли стажування у Сучавському університеті Штефана чел Маре (Румунія) – проф. Політанський Р.Л.; «Люблінська політехніка» (Польща) – доц. Шпатар П.М. та ін.
Усі викладачі ОП пройшли підвищення кваліфікації та стажування фахового спрямування у провідних ЗВО України та за її межами, що відображено в таб.2.

Наведіть конкретні приклади заохочення розвитку викладацької майстерності

В університеті працює система матеріального, морального та професійного заохочення викладачів за досягнення, що регулюється Статутом (https://bit.ly/3LARC6y), Колективним договором ЧНУ на 2022-2025 роки (https://drive.google.com/file/d/1Yc7snvzBdvcoPDi10JDBz2LYbwWLS65z/view). Якість освітньої діяльності науково-педагогічних працівників визначається за результатами рейтингового оцінювання наукової, навчально-методичної та гуманітарно-виховної діяльності викладачів університету, яким передбачено стимулювання переможців рейтингу (http://surl.li/kxyia). Таке рейтингове оцінювання в ЧНУ здійснюється щорічно. Крім рейтингу науково-педагогічних працівників ЧНУ формує рейтинг кафедр. Кафедра радіотехніки та інформаційної безпеки займає 27 місце серед 80 кафедр ЧНУ (http://surl.li/kxyim).
На основі аналізу рекомендацій експертів НАЗЯВО представниками КРТІБ сформовані пропозиції до оновлення Положення про рейтингове оцінювання НПП ЧНУ у розрізі критеріїв активності НПП, що оцінюють викладацьку майстерність.
Підвищення викладацької майстерності відбувається також через відкриті заняття для здобувачів.
Щорічно проводиться конкурс на кращі підручники, переможці отримують грошові винагороди для їх видання.
У 2021 р. кращі молоді асистенти ЧНУ були нагороджені стипендіями в криптовалюті від компанії Orca finance (асистент кафедри радіотехніки та інформаційної безпеки, к.т.н. Вовчук Д.А.) (http://surl.li/pfvcpa).

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

Навч.-методичне забезпечення (роб. програми, силабуси, метод. посібники тощо) з обов'язкових та вибіркових ОК ОП представлене на сайті КРТІБ (https://radiotech.chnu.edu.ua/) та платформі електронного навчання ЧНУ (https://moodle.chnu.edu.ua/).
Фінансування ОП здійснюється в рамках фін.-екон. діяльності ЧНУ та грантових програм (http://surl.li/lbybq).
Для підготовки здобувачів за ОП використовується мат.-тех. база ЧНУ, яка відповідає Ліц. вимогам провадження освітньої діяльності. ОП забезпечена усіма необхідними ресурсами для досягнення мети і РН. Для виконання лаб. і практичних робіт створено комп'ютерний клас та низку спецлабораторій: ТЗЗІ в радіотехнічних пристроях і телеком. системах, Вбудованих систем тощо (http://radiotech.chnu.edu.ua/labs/). В освітньому процесі використовується Колективна радіостанція ЧНУ (http://radiotech.chnu.edu.ua/ur4yww/) та професійне обладнання партнерів (ППО1, ППО7). Детальна інформація про мат.-тех. ресурси та ПЗ, що використовується в освітньому процесі за кожним ОК, наведена у Таблиці 1. В усіх навч. корпусах ЧНУ функціонує мережа eduroam.
Наукова бібліотека ЧНУ (з фондом біля 3 млн. книг) надає доступ до баз даних Scopus, Web of Science тощо (http://www.library.chnu.edu.ua). На КРТІБ створено бібліотеку з фах. літературою та навч. посібниками.
На території ЧНУ працюють їдальні та інша інфраструктура; студенти забезпечуються гуртожитками.

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

ЧНУ забезпечує безперешкодний доступ викладачів і здобувачів вищої освіти до відповідної інфраструктури та інформаційних ресурсів, потрібних для навчання, викладацької та/або наукової діяльності.
Для викладання дисциплін за ОП та дипломного проектування задіюються аудиторії та лабораторії з мультимедійним устаткуванням, доступом до Інтернету та комп'ютерними системами необхідної конфігурації; в усіх навчальних корпусах ЧНУ функціонує мережа eduroam.
Наукова бібліотека ЧНУ (з фондом біля 3 млн. книг) надає доступ до баз даних Scopus, Web of Science тощо (http://www.library.chnu.edu.ua). На випусковій кафедрі створено бібліотеку з фаховою літературою та навчальними посібниками. Для доступу магістрів до матеріалів ОК, проведення контрольних заходів та навчання в дистанційній формі використовується система Moodle.
На території ЧНУ працюють їдальні та інші необхідні для організації освіт. процесу елементи інфраструктури; студенти забезпечуються гуртожитками, списки на поселення оприлюднюються на сайті ННІФТКН (https://docs.google.com/document/d/1xF3YcQEkj3jfqKFZ7IFoE_36fGkj8cNsTaBpr33sznw/edit).
Інформація, оприлюднення якої регламентоване законодавством, розміщується на сайтах університету та його підрозділів (https://www.chnu.edu.ua/, http://ptcsi.chnu.edu.ua/, https://radiotech.chnu.edu.ua/).

Усі викладачі та здобувачі ЧНУ мають корпоративні електронні адреси, які використовуються для комунікації та реєстрації на освітніх платформах та інформаційних ресурсах тощо.

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

Згідно Статуту ЧНУ (https://bit.ly/3LARC6y), здобувачам ВО забезпечується право на: безпечні й нешкідливі умови навчання, праці та побуту; трудову діяльність у позанавчальний час; безоплатне користування бібліотеками, інформаційними фондами, навчальною, науковою та спортивною базами університету; користування виробничою, культурно-освітньою, побутовою базами ЗВО у порядку, передбаченому Статутом ЧНУ; забезпечення гуртожитком на термін навчання у порядку, встановленому законодавством; участь у науково-дослідних, дослідно-конструкторських роботах, конференціях, виставках, конкурсах, представлення робіт для публікації; участь у заходах з освітньої, наукової, науково-дослідної, спортивної, мистецької, громадської діяльності, що проводяться в Україні та за кордоном, у встановленому законодавством порядку; участь в обговоренні та вирішенні питань удосконалення освітнього процесу, науково-дослідної роботи, організації дозвілля, побуту, оздоровлення тощо.
Створена в ЧНУ соціологічна лабораторія періодично проводить опитування студентів щодо потреб та інтересів студентства та рівня їх задоволеності (https://cutt.ly/6CU2V71, http://surl.li/kxynu, https://bit.ly/3RisIok).
Між викладачами та студентами стосунки будуються на основі взаємоповаги. Куратори спілкуються зі студентами, допомагають консультаціями та порадами, передають життєві настанови, залучають до волонтерства. Крім цього, потребами та інтересами здобувачів вищої освіти займається профспілка студентів та студпарламент ЧНУ.

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.

У ЧНУ забезпечується освітня, організаційна, інформаційна, консультативна та соціальна підтримка здобувачів відповідно до ЗУ «Про вищу освіту», Статуту ЧНУ, рішень Вченої ради, наказів і розпоряджень ректора та реалізується в спільній діяльності студентів, викладачів та кураторів. Планування підтримки в ЧНУ здійснюють: випускова кафедра, навч. відділ, профспілкова організація, органи студ. самоврядування та передбачає:
-освітня підтримка – застосування студентоцентрованого підходу у навчанні; покращення мотивації до здобуття освіти та готовності до навчання впродовж життя; моделювання реальних проф. умов спілкування; створення сприятливого психоемоційного клімату у студ. групі; якісне навч.-метод. забезп. освіт. процесу; використання інновац. пед. технологій;
-організаційна – створення належних умов навчання студентів; забезпечення вільного вибору навч. дисциплін, принципів академ. доброчесності, моніторингу якості освіти;
-консультативна – організацію групових та інд. консультацій для оперативного задоволення освітніх, організаційних та соц. потреб здобувачів;
-інформаційна – забезпечення вільного доступу до інформації щодо розкладів навч. занять і консультацій тощо; це реалізується за допомогою офіційних веб-сайтів ЧНУ, ННІФТКН, випускової кафедри, персон. сторінок викладачів, інф. стендів;
-соціальна – її отримують напівсироти, сироти та діти, позбавлені батьк. піклування, малозабезпечені, інваліди, діти учасників бойових дій тощо. Студенти з дітьми отримують подарунки від профспілки ЗВО на день Св. Миколая. Спілкування кураторів зі студентами дозволяє виявляти тих, хто потребує допомоги.
Для надання псих. допомоги студентам та співробітникам створений соціально-псих. центр (http://bit.ly/3Mt41uw), який регулярно проводить опитування (http://surl.li/grbxs, http://surl.li/kxypt). Більшість студентів задоволені рівнем підтримки в ЧНУ (результати анкетування студентів за ОП).
ЧНУ забезпечує безпечні умови навчання, праці та побуту, а студенти повинні виконувати вимоги щодо порядку дій під час тривоги (https://bit.ly/4cSlSpv), охорони праці, ТБ тощо. Регулярно студенти проходять інструктаж з ТБ у навч. лабораторіях із записами у відповідних журналах. У приміщеннях підтримуються необхідні сан. норми щодо площі, освітлення, темпер. режиму тощо; здійснюється технагляд, проводиться ремонт. У корпусах діє цілодобова охорона; у 8 та 9 корпусах, де проходять заняття здобувачів за ОП, функціонують запасні виходи та укриття. Під час пандемії в ЧНУ було повною мірою забезпечено дотримання сан. норм.
Медпослуги надаються у медпункті студмістечка та міській студполіклініці. Проводяться профілак. медогляд студентів, акції «Тиждень здоров'я», «Кидай палити!» тощо.
Одним з критеріїв оцінювання НПП в анкетуванні студентів є педагогічний такт викладача, що безпосередньо впливає на псих. здоров'я здобувачів.
Право на захист від будь-яких форм експлуатації, фіз. та псих. насильства регламентоване у «Правилах внутр. трудового розпорядку ЧНУ» (http://surl.li/anouj).

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)

Відповідно до Статуту (https://bit.ly/3LARC6y), у ЧНУ створюються необхідні умови для навчання особам з особливими освітніми потребами (ООП).
Згідно з «Положенням про організацію освітнього процесу в ЧНУ» (http://surl.li/utojrr) особи з ООП мають право на безоплатне забезпечення інформацією для навчання у доступних форматах з використанням технологій, що враховують обмеження життєдіяльності; на спеціальний навчально-реабілітаційний супровід та вільний доступ до інфраструктури ЗВО.
У ЧНУ затверджений «Порядок супроводу (надання допомоги) осіб з інвалідністю та інших маломобільних груп

населення у ЧНУ» (http://surl.li/aeuix). Він установлює порядок безперешкодного доступу інвалідів та інших маломобільних громадян в приміщення, визначає дії відповідальних осіб щодо забезпечення комфортності перебування таких осіб у ЧНУ. Порядок забезпечується технічними рекомендаціями щодо пристосування середовища життєдіяльності закладів до потреб маломобільних груп (http://surl.li/aeuiz). Для осіб з ООП у «Правилах прийому до ЧНУ у 2024 р.» прописані спеціальні умови вступу (https://bit.ly/3sQxqIo).
В ЧНУ функціонує електронна дистанційна система навчання (Moodle), створено корпоративні облікові записи (email) викладачів і здобувачів для комунікації.
Навчання осіб з ООП за ОПП «Кібербезпека» не було. У разі появи таких здобувачів, окрім зазначених умов, їм можуть бути запропоновані вибіркові дисципліни за курсами Мережної Академії CISCO з відтворенням матеріалів для осіб з порушеннями зору.

Продемонструйте наявність унормованих антикорупційних політик, процедур реагування на випадки цькування, дискримінації, сексуального домагання, інших конфліктних ситуацій, які є доступними для всіх учасників освітнього процесу та яких послідовно дотримуються під час реалізації освітньої програми

Відповідно до законодавства України, у ЧНУ значна увага приділяється процедурам запобігання і врегулювання конфлікту інтересів серед учасників освіт. процесу.
У випадку виникнення конфліктних ситуацій здобувач має право звернутися до керівництва ЧНУ та профспілки студентів з метою захисту своїх прав. Розгляд скарг і звернень відбувається на особистому прийомі керівництвом ЧНУ.
Принципи політики попередження і врегулювання конфліктних ситуацій в ЧНУ регулюються «Положенням про засади безконфліктних ситуацій та врегулювання спорів учасників освіт. процесу» (http://surl.li/bdmzw). Основні стратегії їх розв'язання: пошук компромісу, налагодження співпраці, взаємне пристосування сторін, запобігання відновленню конфлікту. Як засоби розв'язання конфлікту визначені: усунення причин конфлікту, зміна вимог іншої сторони, якщо опонент іде на певні поступки, консенсус. У ЧНУ працює соц.-психологічний центр щодо запобігання, вирішення і профілактики конфліктів в освіт. просторі. Скарг, пов'язаних із конфліктними ситуаціями, в межах ОПП «Кібербезпека» не було.
Для врегулювання конфліктних ситуацій у гуртожитку в ННІФТКН створена комісія з соц. питань. До її складу входять голова (заст. директора з виховної роботи), представники студ. самоврядування, завідувач гуртожитку, студенти-активісти, а діяльність регламентується документами (https://bit.ly/3ZduNwm).
Несумісними зі званням члена спільноти ЧНУ є: хабарництво чи будь-які інші форми корупції, створення умов з боку адмінпрацівників ЧНУ та факультетів для появи хабарництва чи проявів корупції, шахрайство, хуліганство, сексуальні домагання, інші кримінальні діяння, свідоме порушення законодавства України, проходження академ. процедур контролю знань підставними особами, плагіату, списування при складанні будь-якого виду підсумкового або поточного академ. контролю. Дотримання академ. доброчесності регулюється «Етичним кодексом ЧНУ».
У ЗВО здійснюється систематичний моніторинг корупційних проявів шляхом опитування студентів (анкета «Викладач очима студента» https://bit.ly/3PzDbmJ). Одним з питань є: «Чи доводилось Вам на сесії «віддячувати» викладачеві за оцінку знань?». Згідно останнього опитування здобувачів ННІФТКН відповіді такі: «ні» - 97,03%, «так» - 0,99%, «не хочу відповідати» - решта. У процесі реалізації ОП не виникало потреб застосування антикорупційних процедур. Скарг, пов'язаних із сексуальними домаганнями та дискримінацією, в межах ОПП «Кібербезпека» також не було.
Підсумки опитування здобувачів за ОП свідчать, що ЗВО завжди реагує на прояви неприпустимої поведінки, дискримінації, корупції; викладачі враховують індивід. особливості, освіт. потреби та здібності студентів; поведінка й висловлювання викладачів є професійними та недискримінаційними (https://bit.ly/3PAWOLn).
Семінари до Дня дівчат у ІКТ, що проводились у ННІФТКН, не виявили проявів гендерної дискримінації у ЧНУ та ОПП «Кібербезпека» зокрема (https://cutt.ly/cVJi1Ma).

8. Внутрішнє забезпечення якості освітньої програми

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

Процедури розроблення, затвердження, моніторингу та періодичного перегляду ОП в ЧНУ регулюються такими документами:
«Положенням про розроблення та реалізацію освітніх програм Чернівецького національного університету імені Юрія Федьковича» від 27 квітня 2020 року, протокол №4 (https://bit.ly/3T98s1i);
«Положенням про порядок проведення внутрішнього моніторингу якості освітньої діяльності та якості вищої освіти в Чернівецькому національному університеті імені Юрія Федьковича» (прот. №7 від 31.08.2020 р.) (https://bit.ly/3Tei5f5);
«Положенням про систему внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти в Чернівецькому національному університеті імені Юрія Федьковича» (прот. №7 від 31.08.2020 р.) https://bit.ly/3MtwAYU).
Деякі аспекти роботи з реалізації та удосконалення ОП регламентується «Положенням про організацію освітнього процесу в ЧНУ» (http://surl.li/utojrr) (прот. №12 від 02.09.2024) та «Положенням про гаранта освітньої програми ЧНУ» (https://bit.ly/4dQUTfh) (прот. №7 від 30.06.2021).
Розроблення і затвердження ОП контролюються Сектором ліцензування, акредитації та нострифікації навчального відділу ЧНУ (https://bit.ly/477aTHz).

Проведення різних видів моніторингу: періодичного перегляду освітніх програм, навчальних планів та інших навчально-методичних документів з метою забезпечення відповідності стандартам вищої освіти здійснюється Центром забезпечення якості вищої освіти у ЧНУ (https://bit.ly/3Zb3a9A).

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

Систематичний моніторинг та удосконалення ОП згідно «Положення про розроблення та реалізацію освітніх програм ЧНУ» (https://bit.ly/3T98s1i) організовує керівник проектної групи з метою забезпечення належного рівня освітніх послуг і створення сприятливого й ефективного освітнього середовища для студентів. ОП удосконалюється робочою групою із залученням студентів та інших стейкхолдерів. У процесі реалізації ОП під час обговорень з НПП, здобувачами, випускниками та роботодавцями з'ясовується необхідність внесення змін до окремих її ОК. Відповідно до «Положення про організацію освітнього процесу в ЧНУ» (http://surl.li/utojrr) (прот. №12 від 02.09.2024) ОП переглядаються щорічно, а внесення змін відбувається за потреби, але не рідше одного разу на 2 роки для другого (магістерського) рівня ВО. Оновлення ОП є складовою внутрішньої системи забезпечення якості освітньої діяльності та якості ВО в системі управління якістю ЧНУ, результати чого постійно оприлюднюються на офіційному сайті ЧНУ. Проєкт оновленої ОП не менш як за місяць до затвердження оприлюднюється на сайті КРТІБ для громадського обговорення. Оновлена ОП погоджується завідувачем випускової кафедри, навчальним відділом ЧНУ, затверджується Вченою радою ЧНУ, до складу якої входять представники студентського самоврядування, та вводиться в дію наказом ректора.
Зміни, внесені до ОП за результатами останнього перегляду (оновлена ОП затв. Вченою радою ЧНУ 26.06.2024 р., прот. №6; наказ №248, 28.06.2024 р.), представлені на сайті випускової кафедри (https://bit.ly/3zHu4LU).
Серед ключових змін слід відзначити наступні:
1) враховуючи прикладне спрямування ОП і орієнтацію на здобуття студентами фахових знань, умінь та навичок для здійснення подальшої професійної діяльності, за рекомендацією НПП випускової кафедри та роботодавців, а також враховуючи рекомендації, висловлені під час акредитаційної експертизи, прийняте рішення розвивати ОП в напрямку проф. стандарту «фахівець сфери захисту інформації»;
2) на основі аналізу компетентностей та РН Стандарту освіти за спеціальністю та професійного стандарту введено КФ12 та РН25;
3) проведено перерозподіл кредитів між складовими ОП: вилучено вибірковий ОК ЗПВ3, введено новий ОК ППО8, скориговано назву та зміст ППО5;
4) загалом, скориговано матрицю відповідності програмних компетентностей та РН компонентам ОП з урахуванням вимог Стандарту освіти, проф. стандарту та керуючись рекомендаціями експертів НАЗЯВО;
5) за пропозиціями студентів, стейкхолдерів та моніторингової групи ЦЗЯВО ЧНУ для розширення можливостей щодо формування індивідуальної освітньої траєкторії здобувачів ВО до Переліку вибіркових освітніх компонент ОП додано курс «Цифрова криміналістика», а також в цьому напрямку доповнено тематику дипломного проектування.
Аналіз отриманих на оновлену редакцію ОПП «Кібербезпека» рецензій та відгуків стейкхолдерів, показав, що внесені зміни сприяють покращенню фахової підготовки випускників та підвищенню їх конкурентоспроможності на ринку праці.

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

Соціологічною лабораторією ЧНУ та випусковою кафедрою проводяться опитування студентів щодо покращення якості та організації освітнього процесу відповідно до «Положення про систему внутр. забезпечення якості освітньої діяльності та якості ВО в ЧНУ». Результати опитувань здобувачів, що враховують пропозиції змін до ОП, аналізуються та узагальнюються членами робочої групи, зіставляються з пропозиціями роботодавців і викладачів, обговорюються та затверджуються на засіданні КРТІБ.
Зокрема, враховано пропозицію студ. Рижакової В.І. відносно розширення переліку вибіркових освітніх компонент дисципліною, пов'язаною з захистом персональних даних та соціальною інженерією; студ. Мочернюком Т.М. запропоновано ввести дисципліну, присвячену поглибленому вивченню криптографічного захисту в інформаційних системах; студ. Пархоменком Є.В. висловлено побажання щодо розроблення і впровадження курсу з основ нейромереж, що зумовило доповнення переліку вибір. дисциплін курсами «Захист персон. даних та соціальна інженерія», «Математичні основи нейромереж», а також враховано під час впровадження обов'язкової дисципліни ППО5. Зазначені пропозиції були підтримані проектною групою для підсилення РН 2, 3, 5, 13, 20 та РН 24 чинної на той момент редакції ОПП та затверджені на засіданнях випускової каф. (прот. №16, 16.02.2022; №16, 21.04.2023). Висловлені в опитуваннях здобувачів пропозиції щодо збільшення практичної підготовки сприяли вибору проф. стандарту, на який зорієнтована оновлена у 2024 р. ОП.

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

Провідною технологією навчання здобувачів вищої освіти в ЧНУ є студентоцентрований підхід, що передбачає спрямованість освітнього процесу на набуття компетентностей та активне включення здобувачів у освітню діяльність на засадах рівноправних партнерських стосунків, з метою розвитку їх здатності до критичного мислення, формування позитивної мотивації та особистісно-професійного саморозвитку.
Ядром студентства є органи студентського самоврядування, які включені до складу колегіальних органів управління Вченої ради ЧНУ, Вченої ради НН ІФТКН, Науково-методичної ради ЧНУ, громадського самоврядування, тому беруть участь у процедурах внутрішнього забезпечення якості: під час обговорення, затвердження, перегляду ОП, обговорення нормативних документів, створення нових ОП, обговорення подальшої стратегії та розвитку якості

освіти. Здобувачі вищої освіти, в тому числі представники студентського самоврядування, можуть брати участь у перегляді ОПП «Кібербезпека», висловлюючи конструктивні пропозиції, зауваження та рекомендації, а також вирішувати питання організації навчання (https://www.chnu.edu.ua/universytet/studentske-zhyttia/studentskyi-parlament/).

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

КРТІБ проводяться зустрічі з роботодавцями та обговорення вимог до фахівця на ринку праці. Як результат, переважна більшість випускників за ОПП «Кібербезпека» працевлаштовуються на підприємствах, в організаціях та комерційних компаніях у сфері ІБ та ЗІ Західного регіону.
З метою залучення роботодавців до процедур забезпечення якості освіт. процесу КРТІБ організовуються зустрічі, на які вони запрошуються і де обговорюються питання підвищення ефективності підготовки фахівців та внесення змін до ОП. В результаті такої взаємодії з урахуванням специфіки та пропозицій роботодавців (держустанов, Держспецзв'язку, Департаменту кіберполіції Нацполіції України, представників Чернівецького ІТ Кластера тощо) здійснюється оновлення ОП. Так, за пропозицією представників відділу ІБ Управління СБУ в Чернівецькій області та відділу протидії кіберзлочинам Департаменту кіберполіції (https://bit.ly/482sgt4, https://bit.ly/3R6A7Qk) запроваджені визначені ОП КФ11 та РН24. До компонент ОПП введено ППО7, що відповідає РН 1, 5-8, 10-14, 16, 20, 22, 24 (пропозиції Datami та SoftServe); це відображено у прот. засідання КРТІБ №16 від 16.02.2022 р. та затв. Вч. радою ЧНУ (пр. №4, 28.03.2022) в оновленій редакції ОПП «Кібербезпека» (https://bit.ly/4660hHd).
Зміни, внесені до ОП у 2024 н.р., ґрунтувалися на результатах аналізу зустрічей зі стейкхолдерами (http://surl.li/fangmq, http://surl.li/jjiqtk, https://bit.ly/3MmJNma). Представники роботодавців залучаються до рецензування кваліф. проектів/робіт тощо.

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

Відслідковування траєкторій працевлаштування випускників ЧНУ та кафедри радіотехніки та інформаційної безпеки здійснюється через неформальний зв'язок (Facebook, Viber тощо) та індивідуально. Випускникам розсилаються запрошення на дні відкритих дверей кафедри, визначні дати, благодійні заходи та інші. На цих заходах випускники розповідають про свій кар'єрний шлях, наводять приклади практичного застосування знань і умінь, здобутих в університеті, у своїй професійній діяльності, а також висловлюють своє бачення спеціальності з урахуванням практичного досвіду. Слід зауважити, що частина викладачів КРТІБ – її випускники за спеціальностями «Системи технічного захисту інформації» або «Кібербезпека», які неперервно комунікують з однокурсниками фахівцями-практиками, тому їх пропозиції та зауваження також важливі і враховуються під час перегляду ОП.
Через кураторів випускників та керівників магістерських робіт в соціальних мережах, електронною поштою тощо поширюється інформація про наявні вакансії потенційних роботодавців.
У ЧНУ створена асоціація випускників (https://www.chnu.edu.ua/universytet/pry-universyteti/asotsiatsiia-vypusknykiv/), що також сприяє підтримці зворотного зв'язку з випускниками та відслідковуванню траєкторій їх працевлаштування (http://radiotech.chnu.edu.ua/graduates/).

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

Створена у ЧНУ система забезпечення якості є багатоплановою і передбачає застосування моніторингу як базового інструмента системи внутрішнього забезпечення якості вищої освіти та управлінської діяльності (https://bit.ly/3Zb3a9A). Організація й проведення моніторингів здійснюється відповідно до Положення «Про порядок проведення внутрішнього моніторингу якості освітньої діяльності та якості вищої освіти в Чернівецькому національному університеті імені Юрія Федьковича».
Основними напрямами моніторингу в ЧНУ є:
• реалізація державної політики у сфері вищої освіти, контроль за дотриманням кафедрами, факультетами, навчально-науковими інститутами, Університетом законодавчих актів і нормативно-правових документів про вищу освіту;
• аналіз якості розроблення освітніх програм спеціальності (освітньо-професійної та освітньо-наукової) відповідно рівня вищої освіти;
• вивчення й узагальнення якості навчально-методичного забезпечення підготовки фахівців на кафедрах, факультетах, у навчально-наукових інститутах;
• рівень навчальних досягнень здобувачів вищої освіти у розрізі: студент-група-курс- факультет / навчально-науковий тощо.
Основні напрями моніторингу змінюються й доповнюються з урахуванням результатів акредитації освітніх програм, пропозицій гарантів, суб'єктів освітнього процесу, роботодавців тощо.
Для організації зворотного зв'язку зі стейкхолдерами та вчасного реагування на результати моніторингу освітньої програми та/або освітньої діяльності з реалізації освітньої програми на засіданнях науково-методичної ради (НМР) ЧНУ, методичних рад підрозділів та кафедр проводиться аналіз, розробляються заходи щодо усунення виявлених проблем та в подальшому обговорюється ефективність цих заходів. Результати опитувань, звіти з матеріалами моніторингу та їх обговоренням оприлюднюються на сайтах ЧНУ та підрозділів (https://www.chnu.edu.ua/navchannia/posluhy-dlia-zdobuttia-osvity/zabezpechennia-iakosti-vyshchoi-osvity/rezultaty-monitorynhu-iakosti-pidhotovky-fakhivtsiv/ , https://docs.google.com/forms/d/1HD3UkdKYA-4rW-c1z3baG-3O6dh7cvDa4927_xZ0sUs/viewanalytics,

https://docs.google.com/forms/d/1mF2StP5K7XQOgF7fAJu7z6Z3GRgU1UTYjMlq7yJe1tg/viewanalytics , https://www.chnu.edu.ua/media/xv1olwka/op-kiberbezpeka_mahistr_2023.pdf тощо). Зокрема, підсумки акредитаційної експертизи ОПП «Кібербезпека» були проаналізовані на засіданні НМР ЧНУ (прот. засід. №5 від 28.12.2023, https://www.chnu.edu.ua/media/vbjpo3bc/protokol-5-vid-28122023-r-2.pdf), а результати впровадження вжитих кафедрою заходів обговорені наприкінці навчального року на засіданнях НМР ЧНУ (прот. № 11, 27.06.2024 р.) та метод. ради ННІФТКН (прот. №10, 28.06.2024 р.) (https://bit.ly/3Mz99gC, https://bit.ly/4ganoro).

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?

Враховуючи зміни у технології проведення процесу акредитації, в ЧНУ розроблено процедури реагування на зауваження і пропозиції, які виникають в результаті роботи ЕГ з ОП різних спеціальностей. Висновки ЕГ та ГЕР розглядаються і аналізуються на Вченій і методичній радах ЧНУ і його підрозділів (http://surl.li/kybkr, http://surl.li/kybmh). Приймаються відповідні рішення і вживаються заходи щодо їх усунення.
Акредитація ОПП «Кібербезпека» за технологією НАЗЯВО проводилася у 2023 р. Під час роботи над оновленою редакцією ОПП «Кібербезпека» враховано її результати, відгуки здобувачів та стейкхолдерів (https://bit.ly/3zHu4LU), а також рекомендації з акред. матеріалів інших ОП.
Щодо вжитих заходів по ключових зауваженнях та рекомендаціях, зазначимо:
Критерій 2. Проаналізовано практичну підготовку фахівців за ОП та внесено зміни щодо орієнтації ОП на проф. стандарт у сфері кібербезпеки. Внесено зміни щодо перерозподілу РН у ППО1, ППО7, введено ППО8.
Критерій 5. Для висвітлення критеріїв оцінювання досягнень здобувачів при розробці силабусів вирішено включити посилання на робочу програму навчальної дисципліни з детальною інформацією щодо вивчення курсу, оприлюднену на сайті випускової кафедри. Також здійснюється оприлюднення кваліф. робіт на вебсторінці кафедри.
Критерій 6. Для підсилення НПП ОК ОП залучено до освітнього процесу за сумісництвом фахівців сфери ЗІ, д.т.н. Прокофьєва М.І. та Яремчука Ю.Є. Також залучено к.т.н. за спец. 125-Кібербезпека, які мають відповідну базову освіту і виконали всі вимоги щодо присвоєння вчених звань доцента. Проведений аналіз публік. активності НПП, задіяного в реалізації ОП. Проведено гостьові лекції представниками ІТ-галузі та викладачами інших ЗВО України, зокрема ХНУ, Харк. НУ ім. Каразіна (інформація на вебсторінці кафедри).
Критерій 7. В освітньому процесі залучені:
автоматиз. комплекс виявлення і вимірювання радіовипромінювань АКОР-3 (СН 0011803, спец. ПЗ для комплексу «Система АКОР-М»; базова версія 7.9.3459 та оновлення для неї версія 8.3.3499. Свідоцтво про приймання АКОР-3 АСЧА 411168.003, дата випуску 30.05.2018),
спец. комплекс акустичного захисту мовної інформації КАЗМІ,
детектор поля PROTECT,
акустичний защумлювач PIAC2BA,
генератори шуму PIAC-1M, DNG-2000,
виявники GPS-трекерів, прихованих відеокамер та жучків GPS SIGNAL DETEKTOR K18 тощо.
Для реалізації ОП використовується:
ПЗ з відкритим вихідним кодом: Kali Linux 2022.3, Nmap 7.94, Metasploit, Aircrack-ng 1.7, Wireshark, SQLMap, CyberChef v10.5.2 (https://github.com/gchq/CyberChef), Python3.10;
пропрієтарне ПЗ: Burp Suite Community Edition (https://portswigger.net/), Microsoft Visual Studio Community 2022 (JavaScript, C/C++), PyCharm v2022.3 (https://www.jetbrains.com/pycharm/).
Критерій 8. Враховуючи воєнний стан, реалізувати розміщення на стендах кафедри інформацію про випускників щодо їх кар'єрного шляху.
Критерій 9. Проаналізовано сайт кафедри з приводу розміщення актуальної інформації щодо проектів ОП та терміни її оприлюднення.

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

Політика ЧНУ щодо забезпечення якості освітньої діяльності реалізується через внутрішні процеси забезпечення якості із залученням усіх учасників освітнього процесу. Вона передбачає: перегляд змісту та внесення змін до ОП, участь викладачів у програмах моніторингу якості викладання навчальних дисциплін ОП; практичну реалізацію інноваційних педагогічних та віртуальних технологій навчання (вебінари, електронні курси); пропагування академічної доброчесності і свободи (комісія з академічної доброчесності, семінари із запрошеними спікерами); запобігання нетолерантності чи дискримінації (Центр психологічної підтримки для членів академічної спільноти). До цих процесів залучаються й представники інших ЗВО: під час конференцій, семінарів (вебінарів) та стажування вони беруть участь у обговоренні ОПП «Кібербезпека», надають рецензії, де висловлюють свої пропозиції щодо поліпшення підготовки випускників. Студенти також залучаються до обговорення питань, пов'язаних зі структурою та змістом даної ОП. Представники студентського активу є членами Вченої ради ННІФТКН, беруть участь у її засіданнях, виступають з пропозиціями щодо процедур внутрішнього забезпечення якості різних ОП. В ЧНУ функціонує ЦЗЯВО, його основні напрями діяльності: аналіз змісту ОП; забезпечення якості організації навчального процесу; проведення форм контролю; впровадження новітніх інформаційних технологій тощо. В ННІФТКН забезпечення якості ОП контролюється випусковими кафедрами, методичною радою, адміністрацією.

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

В ЧНУ відповідно до чинного законодавства створена і функціонує система внутрішнього забезпечення якості

освітньої діяльності та якості ВО (https://bit.ly/3Zb3a9A), що базується на стійкій довірі до ЧНУ з боку суспільства та роботодавців як надавача послуг з підготовки високоосвічених, конкурентоспроможних фахівців для потреб суспільства, які відповідають міжнар. вимогам та володіють високим рівнем якості отриманих знань. Це сприяє формуванню культури якості освіти за усіма напрямками діяльності учасників освітнього процесу та спонукає їх до свідомого дотримання належного рівня якості.
Елементами формування культури якості ВО є те, що починаючи з 2017 року в ЧНУ проводяться тренінги для гарантів ОП; викладачі КРТІБ беруть участь у конференціях, що проводяться ЗВО України і присвячені тематиці якості освіти (КНУ http://surl.li/khptvr, ОНТУ http://surl.li/fzqsky, https://bit.ly/3MyvICf).
21.08.2024 р. представники ЧНУ взяли участь у регіон. семінарі «Сучасний стан системи забезпечення якості ВО в Україні: виклики та перспективи», https://bit.ly/3ZeA9JU.
Також у ЧНУ відбулася зустріч із головою НАЗЯВО А. Бутенком, під час якої обговорювалися питання вдосконалення якості ВО, акад. доброчесності тощо. https://bit.ly/4e6vON4.
Обговорення результатів акредитації ОП з відповідними рекомендаціями щодо усунення недоліків відбулося на засіданні наук.-метод. ради ЧНУ (прот. № 11, 27.06.2024 р.) та метод. ради ННІФТКН (прот. №10, 28.06.2024 р.) (https://bit.ly/3Mz99gC, https://bit.ly/4gan0ro).

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?

http://radiotech.chnu.edu.ua/educationprograms/

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

http://radiotech.chnu.edu.ua/syllabuses_krtib/
http://radiotech.chnu.edu.ua/educationprograms/

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

Правила і процедури, що регулюють права та обов'язки всіх учасників освітнього процесу, зазначено у Статуті університету (Розділ 7. Права й обов'язки науково-педагогічних, наукових, педагогічних та інших працівників, а також осіб, які навчаються в Університеті; Розділ 8. Організація освітнього процесу та ін.) (https://drive.google.com/file/d/1mZ7ZsfEzixci6w4sPbGRfVTzBcPyCXms/view), «Колективному договорі ЧНУ на 2022-2025 роки» (https://www.chnu.edu.ua/universytet/normatyvni-dokumenty/kolektyvnyi-dohovir/). Їх визначено та конкретизовано відповідно до чинних нормативно-правових актів у «Правилах внутрішнього трудового розпорядку ЧНУ» (https://bit.ly/3xsYJrH).
Окремі аспекти прав та обов'язків регулюються в ЧНУ нормативною документацією з організації освітньої діяльності, розробки і затвердження освітніх програм, зарахування досягнень та атестації здобувачів вищої освіти, студентоцентрованого навчання, академічної мобільності і доброчесності, внутрішнього забезпечення якості освіти в ЧНУ. Усі зазначені документи є у вільному доступі, що досягається через їх оприлюднення на офіційному сайті ЧНУ, і можуть бути знайдені у розділі «Університет > Нормативні документи > Пошук нормативних документів»: (https://www.chnu.edu.ua/universytet/normatyvni-dokumenty/).
Також усі матеріали опубліковано у збірнику нормативних документів ЧНУ, наявному на кожній кафедрі та в деканаті (https://drive.google.com/file/d/1oiZdkjt-0XmhqMaLm-3o6zRg4LRK3pEq/view).
Здобувачі вищої освіти при вступі оформлюють договори.

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП?

Сильні сторони ОПП:
- значний і тривалий досвід КРТІБ ЧНУ у підготовці фахівців у сфері ІБ;
- компетентність, досвідченість та висока фаховість НПП, що відповідає ліц. вимогам; відкритість НПП, готовність до співпраці та взаємодоповнюваність у навч. та наук. діяльності, відкрите та приязне спілкування зі студентами і готовність надати консультацію за необхідності як в аудиторії, так і онлайн чи через електронні ресурси;
- залучення професіоналів-практиків до підготовки здобувачів;
- врахування специфіки регіону та потреб ринку праці у фахівцях для підприємств і установ галузі;
- налагоджені надійні партнерські відносини з профільними підприємствами та установами;
- методи навчання та оцінювання результатів були переглянуті, розширені з урахуванням сучасних реалій (інд.,

дистанційне навчання); реалізується студентоцентроване навчання;
- навч.-методичне, інформаційне та мат.-технічне забезпечення випускової кафедри за номенклатурою, якісними та кількісними показниками забезпечує всі дисципліни навчального плану та відповідає чинним нормативам;
- технічні засоби навчання та наявні навчальні площі забезпечують проведення всіх видів занять за навчальним планом на сучасному рівні;
в оновленій ОП сформований блок дисциплін загальної підготовки, який надає можливість набуття soft skills, що закріплюються ще і вибірковими компонентами;
- дотримання етики та політики академ. доброчесності, зокрема забезпечення можливості здобувачам самостійно перевіряти власні авторські навч. та наукові роботи на текстові запозичення за допомогою системи Turnitin Similarity;
- ОП забезпечує повноцінну підготовку магістрів до проф., практичної та науково-дослідної діяльності, про що свідчать регулярні звернення роботодавців щодо рекомендації їх до працевлаштування;
- успішна участь здобувачів за ОПП «Кібербезпека» у конкурсах студентських наук. робіт та студентських наук. конференціях за напрямком ІБ та суміжних галузей;
- тісна співпраця із Сучавським університетом Штефана чел Маре та налагоджена діяльність з обміну досвідом, зокрема організація та проведення Міжнародної наук.-практ. конференції «Physical and Technological Problems of Transmission, Processing and Storage of Information in Infocommunication Systems»;
- здобувачі мають можливість безкоштовної публікації результатів наук. досліджень у фаховому наук. журналі «Security of Infocommunication Systems and Internet of Things», який започатковано та видається кафедрою та має категорію «Б» за вісьмома спеціальностями, зокрема за 125;
- можливість долучатись до наук. досліджень з оплатою праці шляхом працевлаштування на посади фахівців наук. проєктів, які виконуються на кафедрі.
Слабкі сторони:
- відсутність програми подвійних дипломів (процес укладання угод розпочато);
- слабка активність у підготовці та захисті дисертацій докторів філософії;
- модернізація мат.-тех. забезпечення навчання осіб з особливими потребами у разі появи таких здобувачів;
- повільний темп впровадження в освітній процес англомовних ОК.

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

Згідно з Стратегічним планом розвитку ЧНУ на 2019-2026 р.р., з метою розвитку ОП упродовж найближчих 3 років планується здійснити такі заходи:
- оновлення наявної ОПП «Кібербезпека» з урахуванням вимог професійного стандарту «фахівець сфери кібербезпеки»;
- розширення можливостей щодо забезпечення здобувачам, які навчаються за даною ОП, формування індивідуальної освітньої траєкторії через вибір освітніх компонентів варіативної складової з освітніх програм інших спеціальностей ЧНУ та інших ЗВО України;
- постійне осучаснення матеріально-технічної бази для забезпечення фахових дисциплін та інших ОК, зокрема обладнання навчально-наукових лабораторій;
- поєднання теоретичного та прикладного аспектів навчання, підвищення якості та ефективності виробничих практик здобувачів вищої освіти;
- впровадження підвищення кваліфікації викладачів шляхом тренінгів щодо професійного розвитку, сучасних технологій навчання, в тому числі іноземною мовою;
- сприяння обміну студентами на основі двосторонніх угод між ЧНУ та закладами вищої освіти зарубіжних країн-партнерів, розширення можливостей міжнародного стажування для викладачів випускової кафедри;
- розширення партнерських відносин із закордонними підприємствами та компаніями в галузі інформаційної безпеки;
- активізація роботи щодо участі студентів та викладачів в міжнародних та всеукраїнських наукових конференціях, а також науково-педагогічного персоналу кафедри радіотехніки та інформаційної безпеки щодо наукових публікацій у періодичних виданнях, що входять до міжнародних наукометричних баз;
- впровадження в освітній процес англомовних навчальних дисциплін та зацікавленість НПП в їх підготовці;
- подання наукового журналу «Security of Infocommunication Systems and Internet of Things», який є фаховим за спеціальністю 125, до міжнародних наукометричних баз;
- створення на кафедрі радіотехніки та інформаційної безпеки сучасного навчально-наукового центру «Кіберполігон»;
- створення секції IEEE для активнішого залучення здобувачів до міжнародних наукових програм та індексування матеріалів конференції «Physical and Technological Problems of Transmission, Processing and Storage of Information in Infocommunication Systems» міжнародними наукометричними базами.

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: БІЛОСКУРСЬКИЙ РУСЛАН РОМАНОВИЧ

Дата: 14.10.2024 р.

Таблиця 1. Інформація про освітні компоненти ОП

Назва освітнього компонента	**Вид освітнього компонента**	**Силабус або інші навчально-методичні матеріали**		**Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього***
		Назва файла	**Хеш файла**	
Наукова та професійна комунікація іноземною мовою	навчальна дисципліна	*Роб_прогр_ЗПО1_2024.pdf*	nTvGiFv0b08u/R7QZqMF3BOnD0VBxBdJ1X/qTjOovYE=	*Для проведення очного/дистанційного навчання: аудиторний фонд; бібліотеки ЧНУ та кафедр; доступ до мережі Інтернет, системи дистанційної комунікації GoogleMeet; офісний пакет LibreOffice; внутрішня корпоративна пошта та система електронного навчання Moodle (https://moodle.chnu.edu.ua). Аудиторія "МУЛЬТИМЕДІЙНИЙ КЛАС КАФЕДРИ ІНОЗЕМНИХ МОВ ДЛЯ ПРИРОДНИЧИХ ФАКУЛЬТЕТІВ": 1. Комп'ютер Intel Core i3-10325/3.9GHz/DDR4 8GB 2400 MHz/SSD 256 GB з монітором 22" Acer (2021, 10 шт.). 2. Проектор мультимедійний Acer X1123H (2021, 1 шт.). 3. БФП EPSON L3151 (2021, 1 шт.). 4. Веб-камера Logitech c270HD (2019, 1 шт.). 5. Акустична система Sven312 (1 шт.). Наявне матеріально-технічне та інформаційне забезпечення достатнє для реалізації ОП.*
Науково-педагогічна діяльність та навчання персоналу в галузі ІБ	навчальна дисципліна	*Роб_прогр_ЗПО2_2024.pdf*	bQ9V297odSpglGrAdlXQsdzr40659XNSl9EB5GeSlLk=	*Аудиторний фонд; бібліотеки ЧНУ та кафедри радіотехніки та інформаційної безпеки; наявність каналів доступу до Інтернету, в тому числі точки доступу Eduroam Ubiquiti UniFi AC LR AP (2021 р., 3 шт.) на КРТтаІБ; система дистанційної комунікації GoogleMeet; офісний пакет LibreOffice; внутрішня корпоративна пошта та система електронного навчання Moodle (https://moodle.chnu.edu.ua). Обладнання аудиторії: проектор мультимедійний Epson EB-X04 (2019 р., 1 шт.), екран (1 шт.). Для проведення дистанційного навчання: 1. Комп'ютер Intel Core i3-10325/3.9GHz/DDR4 8GB 2400 MHz/SSD 256 GB з монітором 22" Acer (2021 р., 1 шт.). 2. Веб-камера Logitech c170 (2019, 1 шт.). 3. Акустична система Sven312 (1 шт.). https://drive.google.com/file/d/115jr1gxMFBwopa5HgDrXRh5Oee1MJTRT/view Наявне матеріально-технічне та інформаційне забезпечення достатнє для реалізації ОП.*
Технології комплексного захисту інформації	навчальна дисципліна	*Роб_прогр_ППО1_2024.pdf*	7BCW8YZli/sdyAxeScdHT3zSZ/BV+b7/lDh20rIewgA=	*Аудиторний фонд; бібліотеки ЧНУ та кафедри радіотехніки та інформаційної безпеки; система дистанційної комунікації*

				GoogleMeet; офісний пакет LibreOffice; внутрішня корпоративна пошта та система електронного навчання Moodle (https://moodle.chnu.edu.ua); наявність каналів доступу до Інтернету, в тому числі точки доступу Eduroam Ubiquiti UniFi AC LR AP (2021 р., 3 шт.) на КРТтаІБ. *Обладнання для проведення лекційних та практичних занять (в т.ч. захист курсових робіт) в очному/дистанційному форматах:* *1. Комп'ютер AMD Athlon II X245 2.9 GHz/DDR3 2GB/HDD 512 GB з монітором 20" Acer (2018 р., 1 шт.).* *2. Проектор мультимедійний Acer X128HP (1 шт.) з екраном.* *3. Веб-камера Logitech c170 (2019, 1 шт.).* *4. Акустична система Sven312 (1 шт.).* *https://drive.google.com/file/d/12agp4j405uhdmL1XAfcAgDtCxEg3kA6h/view* *Наявне матеріально-технічне та інформаційне забезпечення достатнє для реалізації ОП.*
Перспективні напрямки розвитку систем кіберзахисту	навчальна дисципліна	*Роб_прогр_ППО3_2024.pdf*	qd5vMzXkgv5Kq0EkldHi1XpIn9cG6CwAP+dcKaR8ED8=	*Аудиторний фонд; бібліотеки ЧНУ та кафедри радіотехніки та інформаційної безпеки; наявність каналів доступу до Інтернету, в тому числі точки доступу Eduroam Ubiquiti UniFi AC LR AP (2021 р., 3 шт.) на КРТтаІБ; система дистанційної комунікації GoogleMeet; офісний пакет LibreOffice; внутрішня корпоративна пошта та система електронного навчання Moodle (https://moodle.chnu.edu.ua).* *Обладнання для проведення лекційних та практичних занять в очному/дистанційному форматах:* *1. Комп'ютер Intel Core i3-10325/3.9GHz/DDR4 8GB 2400 MHz/SSD 256 GB з монітором 22" Acer (2021 р., 1 шт.).* *2. Проектор мультимедійний Epson X04 (2019, 1 шт.) з екраном.* *3. Веб-камера Logitech c170 (2019, 1 шт.).* *4. Акустична система Sven312 (1 шт.).* *Проведення лабораторних та наочно-демонстраційних занять: Лабораторія "Моделювання і синтезу радіоелектронних засобів радіоспектроскопічних та медіаінформаційних систем".* *Обладнання:* *1. Комп'ютер: IntelCore i3 3.9GHz, 8GB, 256GB з монітором PHILIPS 23.8 (2021 р., 4 шт.).* *2. Комп'ютер Intel Core i5 3.0GHz, 32GB, 500GB M.2, HDD 4TB RAID, GTX 1060 (2021 р., 1 шт.).* *3. Проектор мультимедійний Acer X1123H (2021 р., 1 шт.).* *4. Інтерактивна дошка Intech RD82A (2021 р., 1 шт.), екран (1 шт.).* *Для проведення лабораторних*

				занять застосовується обладнання: *1. Комп'ютер: IntelCore i3 3.9GHz, 8GB, 256GB з монітором PHILIPS 23.8 (2021 р., 4 шт.).* *2. Плата розробника Intel DE1-SoC (FPGA Cyclone V) виробництва Terasic Technologies (2021 р.).* *3. Плата розробника Intel DE10 Lite (CPLD MAX10) виробництва Terasic Technologies (2021 р.).* *4. Керований комутатор Mikrotik Cloud Smart Switch CSS326-24G 2S+RM (2021 р., 1 шт.).* *5. Одноплатний міні-комп'ютер Raspberry Pi 4 Model B 2GB з LCD HDMI Waveshare, (2021 р., 4 шт.).* *6. Плата розробника Cypress CY8CKIT-044 PSoC® 4 M-Series Pioneer Kit, (2021 р.).* *7. Шлюз LoRaWAN IoT Tektelic Kona Micro Lite Gateway з набором Smart Room Sensor (3шт.).* *8. Аналізатор спектру Siglent SSA3032X (2021 р., 1 шт.).* *9. Осцилограф цифровий HANTEK DSO5072P (2021 р., 2 шт.).* *10. Осцилограф цифровий SIGLENT SDS1202CNL+ (2021 р., 1шт.).* *11. Генератор сигналів FeelTech FY6600 (2 шт.).* *12. Цифровий двоканальний генератор довільних форм сигналів з функціями частотоміра OWON AG2052F (1 шт.).* *13. Мультиметр UNI-T UT801 (2 шт.).* *14. Блок живлення регульований Baku BK-305D 30V 5A (2 шт.).* *Програмне забезпечення:* *1. MATLAB & Simulink (Student Version).* *2. Altium Designer - PCB Design Software (Student Version).* *3. Quartus Prime Standard.* *https://drive.google.com/file/d/115jr1gxMFBwopa5HgDrXRh5Oee1MJTRT/view* *https://drive.google.com/file/d/1GYMHA6Ue3xvddQJLPgr3KbCk3JxthbIu/view* *Наявне матеріально-технічне та інформаційне забезпечення достатнє для реалізації ОП.*
Моделювання та оптимізація процесів у ІБ	навчальна дисципліна	*Роб_прогр_ППО2_2024.pdf*	FVNjLgnkDp+7fmgWxk9VBz+PGrqcz8jIF6uHd5YDe4A=	*Аудиторний фонд; бібліотеки ЧНУ та кафедри радіотехніки та інформаційної безпеки; система дистанційної комунікації GoogleMeet; офісний пакет LibreOffice; внутрішня корпоративна пошта та система електронного навчання Moodle (https://moodle.chnu.edu.ua); наявність каналів доступу до Інтернету, в тому числі точки доступу Eduroam Ubiquiti UniFi AC LR AP (2021 р., 3 шт.) на КРТmaІБ.* *Проведення лекційних та практичних занять:* *аудиторія В10:* *1. Комп'ютер AMD A4-6300-/3.7GHz/DDR4 8GB 2400 MHz/SSD 256 GB з монітором 22" LG (2018, 10 шт.).*

				2. Проектор мультимедійний Epson EB-X31 (1 шт.). *3. Екран (1 шт.).* *4. Веб-камера Logitech c170 (2019, 1 шт.).* *5. Акустична система Sven312 (1 шт.).* *Програмне забезпечення:* *1. Wolfram Mathematica https://www.wolfram.com/mathematica/* *https://drive.google.com/file/d/1W8eDMDKMsb4cCNRIWM6OzKL5eA-yfq5f/view* *Наявне матеріально-технічне та інформаційне забезпечення достатнє для реалізації ОП.*
Ризик-орієнтований аналіз в кібербезпеці	навчальна дисципліна	*Роб_прогр_ППО8_2024.pdf*	lWAsD7g11CnSJcW+usQZYvZpV5PRvmrIozuFMaUdtlM=	*Аудиторний фонд; бібліотеки ЧНУ та кафедри радіотехніки та інформаційної безпеки; система дистанційної комунікації GoogleMeet; внутрішня корпоративна пошта та система електронного навчання Moodle (https://moodle.chnu.edu.ua); наявність каналів доступу до Інтернету, в тому числі точки доступу Eduroam Ubiquiti UniFi AC LR AP (2021 р., 3 шт.) на КРТтаІБ.* *Проведення лекційних та практичних занять:* *аудиторія В10:* *1. Комп'ютер AMD A4-6300-/3.7GHz/DDR4 8GB 2400 MHz/SSD 256 GB з монітором 22" LG (2018, 10 шт.).* *2. Проектор мультимедійний Epson EB-X31 (1 шт.).* *3. Екран (1 шт.).* *4. Веб-камера Logitech c170 (2019, 1 шт.).* *5. Акустична система Sven312 (1 шт.).* *Програмне забезпечення:* *1. https://coras.tools/#/* *2. Пакет ПЗ LibreOffice 24.8.1* *https://drive.google.com/file/d/1W8eDMDKMsb4cCNRIWM6OzKL5eA-yfq5f/view* *Наявне матеріально-технічне та інформаційне забезпечення достатнє для реалізації ОП.*
Ліцензування, атестація і сертифікація у сфері безпеки об'єктів інформаційної діяльності	навчальна дисципліна	*Роб_прогр_ППО6_2024.pdf*	8snkTgB3wdoM0XqUoRCt2ns9QBndGEjeKS6CGb4fwJ4=	*Аудиторний фонд; бібліотеки ЧНУ та кафедри радіотехніки та інформаційної безпеки; система дистанційної комунікації GoogleMeet; офісний пакет LibreOffice; внутрішня корпоративна пошта та система електронного навчання Moodle (https://moodle.chnu.edu.ua); наявність каналів доступу до Інтернету, в тому числі точки доступу Eduroam Ubiquiti UniFi AC LR AP (2021 р., 3 шт.) на КРТтаІБ.* *Обладнання для проведення лекційних та практичних занять (в т.ч. захист курсових робіт) в очному/дистанційному форматах:* *1. Комп'ютер AMD Athlon II X245 2.9 GHz/DDR3 2GB/HDD 512 GB з монітором 20" Acer (2018 р., 1 шт.).* *2. Проектор мультимедійний*

				Acer X128HP (1 шт.) з екраном. *3. Веб-камера Logitech c170 (2019, 1 шт.).* *4. Акустична система Sven312 (1 шт.).* *https://drive.google.com/file/d/12agp4j405uhdmL1XAfcAgDtCxEg3kA6h/view* *Наявне матеріально-технічне та інформаційне забезпечення достатнє для реалізації ОП.*
Особливості проектної діяльності в кібербезпеці	навчальна дисципліна	*Роб_прогр_ППО4_2024.pdf*	Gyr7KJ/VpSZOxMgLv5pSNxRwd8OOlWihgeh1/TOUdo4=	*Аудиторний фонд; бібліотеки ЧНУ та кафедри радіотехніки та інформаційної безпеки; наявність каналів доступу до Інтернету, в тому числі точки доступу Eduroam Ubiquiti UniFi AC LR AP (2021 р., 3 шт.) на КРТmaІБ; система дистанційної комунікації GoogleMeet; офісний пакет LibreOffice; внутрішня корпоративна пошта та система електронного навчання Moodle (https://moodle.chnu.edu.ua).* *Обладнання аудиторії: проектор мультимедійний Epson EB-X04 (2019 р., 1 шт.), екран (1 шт.).* *Для проведення дистанційного навчання:* *1. Комп'ютер Intel Core i3-10325/3.9GHz/DDR4 8GB 2400 MHz/SSD 256 GB з монітором 22" Acer (2021 р., 1 шт.).* *2. Веб-камера Logitech c170 (2019, 1 шт.).* *3. Акустична система Sven312 (1 шт.).* *https://drive.google.com/file/d/115jr1gxMFBwopa5HgDrXRh5Oee1MJTRT/view* *Наявне матеріально-технічне та інформаційне забезпечення достатнє для реалізації ОП.*
Безпека інфокомунікацій та безперервність бізнес-процесів	навчальна дисципліна	*Роб_прогр_ППО7_2024.pdf*	pCjitatR1PATpu2DQ4GwULKTmvE/56KhWb1agkRb/G0=	*Аудиторний фонд; бібліотеки ЧНУ та кафедри радіотехніки та інформаційної безпеки; система дистанційної комунікації GoogleMeet; офісний пакет LibreOffice; внутрішня корпоративна пошта та система електронного навчання Moodle (https://moodle.chnu.edu.ua); наявність каналів доступу до Інтернету, в тому числі точки доступу Eduroam Ubiquiti UniFi AC LR AP (2021 р., 3 шт.) на КРТmaІБ.* *Проведення практичних, лабораторних та наочно-демонстраційних занять: Лабораторія ТЕХНІЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ* *Обладнання:* *1. Комплекс АКОР-3 (1 шт.).* *2. Вимірювач Р5-10 (1 шт.).* *3. Спеціалізований комплекс акустичного захисту мовної інформації КАЗМІ (1 шт.).* *4. Генератор сигналів ALTG(2018 р., 1 шт.).* *5. Осцилограф OWON DS5032E (2018 р., 2 шт.).* *6. Детектор поля PROTECT 1206i (2018 р., 2 шт.).* *7. Акустичний зашумлювач PIAC2BA (2019 р., 1 шт.).* *8. Генератор радіошуму PIAC-1M*

				(2019 р., 1 шт.). *9. Генератор акустичного шуму DNG-2000 (2022 р., 1 шт.).* *10. Віброметр BENETECH GM 63B (2018 р., 1 шт).* *11. Шумомір BENETECH GM1356 (2022 р., 1 шт.).* *12. Генератор зашумлення телефонних ліній STEALTH SEC model 2003 (2022 р., 2 шт.).* *13. Виявник GPS-трекерів, прихованих відеокамер та жучків GPS SIGNAL DETEKTOR K18 (2022 р., 1 шт.).* *14. Зразки акустичних та вібровипромінювачів.* *15. Мережевий фільтр PIAC - 4ФМ/1 (2018 р., 1 шт.).* *16. Розділовий трансформатор PIAC-4TP/1 (2018 р., 1 шт.).* *17. Інше обладнання лабораторії ТЗЗІ.* *Лабораторія ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ* *Обладнання:* *1. Комп'ютери AMD X2 240/N68S/3.0GHz/DDR2 2GB 800 MHz/HDD 500 GB/DWD-RW з монітором 22" Acer 20" TFT (6 шт.).* *Програмне забезпечення для проведення лабораторних та практичних робіт:* *1. Спеціалізоване програмне (математичне) забезпечення для комплекса "Система АКОР-М" базова версія 7.9.3459, входить в комплект поставки, та оновлення для неї версія 8.3.3499.* *2. NetIQ Chariot 5.0 (free triall).* *3. Internet Information Services 10.0* *Для проведення дистанційного навчання:* *1. Ноутбук Lenovo V580c/ i5-3230M CPU, 2.60GHz, 6GB RAM, HDD 500 GB з дисплеєм 15.6".* *2. Гарнітура Sven AP-860MV (2019 р., 1 шт.).* *https://drive.google.com/file/d/1kBOjxU27rEtyyBFKwvFa6kKclABS9zrH/view* *https://drive.google.com/file/d/1L6eBgRfMvjf79VF56W7Da0LN6nChwnkV/view* *Наявне матеріально-технічне та інформаційне забезпечення достатнє для реалізації ОП.*
Виробнича практика	практика	*Роб_прогр_ППО9_2024+.pdf*	ZzmjkI2nMRjrp9LbN1s9x+Z+6aOYagIB950L1yDl+EU=	*Матеріально-технічне забезпечення баз практик відповідно до укладених договорів. Бібліотеки ЧНУ та кафедри радіотехніки та інформаційної безпеки; система дистанційної комунікації GoogleMeet; офісний пакет LibreOffice; внутрішня корпоративна пошта та система електронного навчання Moodle (https://moodle.chnu.edu.ua); наявність каналів доступу до Інтернету, в тому числі точки доступу Eduroam Ubiquiti UniFi AC LR AP (2021 р., 3 шт.) на КРТmaIБ.* *Для проведення захистів:* *1. Комп'ютер Intel Core i3-10325/3.9GHz/DDR4 8GB 2400 MHz/SSD 256 GB з монітором 22"*

				Acer (2021 р., 1 шт.). *2. Проектор мультимедійний Epson EB-X04 (2019 р., 1 шт.).* *3. Веб-камера Logitech c270HD (2019 р., 1 шт.).* *4. Акустична система Sven312 (1 шт.).* *https://drive.google.com/file/d/115jr1gxMFBwopa5HgDrXRh5Oee1MJTRT/view* *Наявне матеріально-технічне та інформаційне забезпечення достатнє для реалізації ОП.*
Переддипломна практика	практика	*Роб_прогр_ППО10_2024+.pdf*	2W2kG2JSNs+py16PMR79Qhnp23WByjuEB78+rfkoPnA=	*Аудиторний фонд; бібліотеки ЧНУ та кафедри радіотехніки та інформаційної безпеки; система дистанційної комунікації GoogleMeet; офісний пакет LibreOffice; внутрішня корпоративна пошта та система електронного навчання Moodle (https://moodle.chnu.edu.ua); наявність каналів доступу до Інтернету, в тому числі точки доступу Eduroam Ubiquiti UniFi AC LR AP (2021 р., 3 шт.) на КРТтаІБ.* *Для проведення захистів:* *1. Комп'ютер Intel Core i3-10325/3.9GHz/DDR4 8GB 2400 MHz/SSD 256 GB з монітором 22" Acer (2021 р., 1 шт.).* *2. Проектор мультимедійний Epson EB-X04 (2019 р., 1 шт.).* *3. Веб-камера Logitech c270HD (2019 р., 1 шт.).* *4. Акустична система Sven312 (1 шт.).* *https://drive.google.com/file/d/115jr1gxMFBwopa5HgDrXRh5Oee1MJTRT/view* *Наявне матеріально-технічне та інформаційне забезпечення достатнє для реалізації ОП.*
Дипломне проектування (кваліфікаційна робота)	підсумкова атестація	*Metod_diplom_2024_.pdf*	pcveCaAg+p6Wox+B5/FjVkT8vu509FD42/nVDIFcNAI=	*Лабораторії кафедри радіотехніки та інформаційної безпеки, інших структурних підрозділів Чернівецького національного університету імені Юрія Федьковича (http://radiotech.chnu.edu.ua/labs/) та бази практик.* *Бібліотеки ЧНУ та кафедри радіотехніки та інформаційної безпеки; система дистанційної комунікації GoogleMeet; офісний пакет LibreOffice; внутрішня корпоративна пошта та система електронного навчання Moodle (https://moodle.chnu.edu.ua); наявність каналів доступу до Інтернету, в тому числі точки доступу Eduroam Ubiquiti UniFi AC LR AP (2021 р., 3 шт.) на КРТтаІБ.* *Для проведення захистів:* *1. Комп'ютер Intel Core i3-10325/3.9GHz/DDR4 8GB 2400 MHz/SSD 256 GB з монітором 22" Acer (2021 р., 1 шт.).* *2. Проектор мультимедійний Epson EB-X04 (2019 р., 1 шт.).* *3. Веб-камера Logitech c270HD (2019 р., 1 шт.).* *4. Акустична система Sven312 (1 шт.).* *https://drive.google.com/file/d/115j*

				r1gxMFBwopa5HgDrXRh5Oee1MJTRT/view *Наявне матеріально-технічне та інформаційне забезпечення достатнє для реалізації ОП.*
Криптографічний захист інформації	навчальна дисципліна	*Роб_прогр_ППО5_2024_.pdf*	608RZiE+GKasIbaD6Nmc+2K4RGo/XEgUZfygRZ3By6U=	*Аудиторний фонд; бібліотеки ЧНУ та кафедри радіотехніки та інформаційної безпеки; система дистанційної комунікації GoogleMeet; внутрішня корпоративна пошта та система електронного навчання Moodle (https://moodle.chnu.edu.ua); наявність каналів доступу до Інтернету, в тому числі точки доступу Eduroam Ubiquiti UniFi AC LR AP (2021 р., 3 шт.) на КРТmaIБ.* *Проведення лекційних та лабораторних занять: аудиторія В10:* *1. Комп'ютер AMD A4-6300-/3.7GHz/DDR4 8GB 2400 MHz/SSD 256 GB з монітором 22" LG (2018, 10 шт.).* *2. Проектор мультимедійний Epson EB-X31 (1 шт.).* *3. Екран (1 шт.).* *4. Веб-камера Logitech c170 (2019, 1 шт.).* *5. Акустична система Sven312 (1 шт.).* *Програмне забезпечення:* *1. Пакет ПЗ LibreOffice 24.8.1* *2. ОС Windows 10 PRO FOR OEM SOFTWARE* *3. Пакет математичних обчислень Maple 9.0* *4. Віртуальна машина робочої станції CyberOps* *5. Програмне забезпечення Visual Studio 2019* *6. Інтегроване середовище розробки для мов програмування: Python 3.8, PyCharm, NetBeans, Eclipce, Idea Studio, C++, C#, Java, Notepad++, GoogleDocsRedactors* *7. Збірка комп'ютерних програм «Система криптографічного захисту інформації «Шифр-X.509» Версія 2» (без обмеження на кількість сертифікатів (ліцензія для використання в освітньому процесі НЛ №: СП-0922-01)* *8. Adobe Acrobat Reader.* *https://drive.google.com/file/d/1W8eDMDKMsb4cCNRIWM6OzKL5eA-yfq5f/view* *Наявне матеріально-технічне та інформаційне забезпечення достатнє для реалізації ОП.*

* 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)
77220	Венкель Тетяна Василівна	доцент, Основне місце роботи	Факультет іноземних мов	Диплом спеціаліста, Чернівецький ордена Трудового Червоного Прапора державний університет, рік закінчення: 1985, спеціальність: , Диплом кандидата наук ДК 030073, виданий 30.06.2005, Атестат доцента 12ДЦ 019997, виданий 30.10.2008	35	Наукова та професійна комунікація іноземною мовою	Кандидат філологічних наук 10.02.04 – германські мови, 2005 р., (диплом ДК № 030073) «Синтагматичні, парадигматичні та епідигматичні характеристики прикметників на позначення кольору в англійській мові»; доцент кафедри іноземних мов (12 ДЦ № 019997). Стажування та підвищення кваліфікації: Університет Коньянг (Konyang), Нонсан, Республіка Корея. Курс лекцій з основ Академічної англійської мови для аспірантів та наукових співробітників кафедри біомедичної інженерії університету Коньянг, Корея. З 22.09.2020 по 29.09.2020, 180 годин, 6 кредитів. 1. Jung-Young Son, Tetiana Venkel, Aleksei Chernyshov, Hyoung Lee and Hyun-Woo Kim, Characterization of Distortions in Electro-Holographic Image by A Shack-Hartmann Wavefront Sensor – Proc. Of SPIE, Vol. 11369, 113690U, 2020, SPIE CCC code: 0277-786X/20/$21 doi 10.1117/12.2556446, – 10 pp. https://www.spiedigitallibrary.org/conference-proceedings-of-spie/11369/2556446/Characterization-of-distortions-in-electro-holographic-image-by-A-Shack/10.1117/12.2556446.short IF 0.42, SNIP 0.39) ISSN:0277-786X E-ISSN:1996-756X CiteScore 02.2019 – 0.42 2. Vashpanov, Y.; Heo, G.; Kim, Y.; Venkel, T.; Son, J.-Y. Detecting Green Mold Pathogens on Lemons Using Hyperspectral Images. – Appl. Sci. 2020, 10, 1209; doi:10.3390/app10041209. – www.mdpi.com/journal/applsci. – 15 pp. ISSN 2076-3417;

							CODEN: ASPCC7 IMPACT FACTOR: 2.474 (2019) ; 5-Year Impact Factor: 2.458 (2019) Citations Scopus 3 Web of Science 3 Crossref 3 CiteScore Q2 3. Jung-Young Son, Hyoung Lee, Jung Kim, Beom-Ryeol Lee, Wook-Ho Son, Tetiana Venkel [3D8/3DSA8-2] A HMD for users with any interocular distance.– Proceedings of the International Display Workshops Volume 26 (IDW '19) – https://doi.org/10.36463/idw.2019.0995 https://confit.atlas.jp/guide/organizer/idw/idw2019/subject/3D8_3DSA8-2/search;jsessionid=1B948D3818ECA2E553DDD8EE025A3602?eventCode=idw2019&subjectCode=3D8_3DSA8-2 – P. 995-998 (Міжнародна конференція, 27-29 листопада 2019 р., Саппоро, Японія) ISSN-L 1883-249/26/0995©2019 ITE and SID ISBN 9781713806301 http://www.proceedings.com/53345.html 4. Венкель О.В., Венкель Т.В., Манютіна О.І. Англійська мова за професійним спрямуванням для студентів відділу комп'ютерних технологій : навч. посіб. для студентів комп'ютерних спеціальностей вищих навчальних закладів у 2 ч. Чернівці : ПВКФ Технодрук, 2020. Ч. 1. 160 с. (рекомендований Вченою радою ЧНУ протокол № 10 від 02 листопада 2020 р.) 5. Венкель О.В., Венкель Т.В., Манютіна О.І. Англійська мова за професійним спрямуванням для студентів відділу комп'ютерних технологій : навч. посіб. для студентів комп'ютерних спеціальностей вищих навчальних закладів у 2 ч. Чернівці : ПВКФ Технодрук, 2020. Ч. 2. 140 с. (рекомендований Вченою радою ЧНУ протокол № 10 від 02 листопада 2020 р.)

							6. Венкель Т.В. Англійська мова професійного спрямування. Кібербезпека: Загрози, проблеми, захист / уклад.: Венкель Т.В. – Вид. 2-ге, перероблене, доповнене. – Чернівці, 2020. – 102 с. (посібник в електронній формі). 7. Венкель Т.В. Методична розробка з аналітичного фахового читання англійською мовою до монографії: "CYBERSECURITY FOR BEGINNERS" Raef Meeuwisse "Кібербезпека для початківців" Raef Meeuwisse, Cybersecurity for Beginners, для студентів 2 курсу спеціальність – 125 "Кібербезпека". – Укл.: Венкель Т.В. – Чернівці, 2020. – 95 с. (посібник в електронній формі) Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 1, 2 п. 37 та 1, 3, 4, 10, 12, 19, 20 п. 38 чинних Ліцензійних умов.
485596	Яремчук Юрій Євгенович	професор, Сумісництво	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	Диплом магістра, Вінницький державний технічний університет, рік закінчення: 1996, спеціальність: 8.091101 Комп'ютерні науки, Диплом доктора наук ДД 003857, виданий 22.12.2014, Атестат професора 12ПР 010166, виданий 26.02.2015	0	Безпека інфокомунікацій та безперервність бізнес-процесів	Доктор наук за спеціальнстю 05.13.21 «Системи захисту інформації». Дисертаційна робота на тему «Моделі, методи та засоби асиметричного криптографічного захисту інформації на основі рекурентних послідовностей». Стажування та підвищення кваліфікації: 1. Вінницький національний технічний університет, Центр інформаційних технологій і захисту інформації, курс «Захист інформації в інформаційно-комунікаційних системах та на об'єктах інформаційної діяльності», свідоцтво про підвищення кваліфікації СПК

							№306536 від 03.06.2024 р. (78 год.) 2. Department of Electronic and Information Technologies, Faculty Electrical Engineering and Computer Science of Lublin University of Technology to Poland, дистанційна, стажування за кордоном, Development of information technologies through the use of new technologies in the field of research of image processing, machine learning, deep learning, artificial intelligence, intelligent data analysis, neural networks, security technologies, development of information-measuring systems diagnostic monitoring, з 06.03.2023 р. по 06.05.2023 р. Сертифікат №7-2023-VNTU, 2023-05-06. (180 год.) 3. Вінницький національний технічний університет, Центр інформаційних технологій і захисту інформації, курс «Захист інформації в інформаційно-комунікаційних системах та на об'єктах інформаційної діяльності», свідоцтво про підвищення кваліфікації СПК №306518 від 10.10.2022 р. (78 год.) 4. Тренінг для розробників і рецензентів тестових завдань зі спеціальності 125 «Кібербезпека», Науково-методичний центр вищої та фахової передвищої освіти Міністерства освіти і науки України, 29.10-26.11.2021 р. (15 год.) 5. Вінницький національний технічний університет, Центр інформаційних технологій і захисту інформації, курс «Захист інформації в інформаційно-комунікаційних системах та на об'єктах інформаційної діяльності», свідоцтво про підвищення кваліфікації СПК №301847 від

							29.06.2021 р. (78 год.) 6. Національне агентство із забезпечення якості вищої освіти, Експерт з акредитації освітніх програм, сертифікат 06.10.2019 р. (5 год.) 1. Методичні вказівки до виконання курсових робіт з дисципліни «Основи криптографічного захисту інформації» для студентів спеціальності 125 «Кібербезпека» (освітні програми «Управління інформаційною безпекою» та «Кібербезпека інформаційних технологій та систем») / уклад. Ю. Є. Яремчук, О. В. Салієва. – Вінниця : ВНТУ, 2023. – 41 с. 2. Key generation method based on Genitor Genetic Algorithm model / Andrii Pryimak, Yurii Yaremchuk, Nataliia Kunanets // Proceedings of the 2nd International Conference on Conflict Management in Global Information Networks (CMiGiN 2022). – Kyiv, Ukraine, November 30, 2022, P. 51-60. (Scopus). 3. Яремчук Ю.Є. Підвищення стійкості цифрових водяних знаків у потокових відеозаписах на основі диференціального вбудовування енергії (DEW) / Ю. Є. Яремчук, В. В. Карпінець, І. С. Зоря, Д. О. Козак // Вісник Вінницького політехнічного інституту. 2023. – № 1. – С. 55–64. 4. Method of user authentication by keyboard handwriting based on neural networks and genetic algorithm / Andrii Pryimak, Yurii Yaremchuk, Olha Salieva, Vasyl Karpinets, Nataliia Kunanets // Proceedings of the International Workshop of IT-professionals on Artificial Intelligence (ProfIT AI 2021). – Kharkiv, Ukraine, September 20-21, 2021, P. 141-149. (Scopus). 5. Салієва О.В. Визначення рівня

							захищеності системи захисту інформації на основі когнітивного моделювання / О.В. Салієва, Ю.Є. Яремчук // Безпека інформації. – Т. 26, №1, 2020. – С. 42–49. 6. Яремчук Ю.Є. Вдосконалення стеганографічного методу PVD захисту цифрових зображень / Ю. Є. Яремчук, В. В. Карпінець, І. С. Зоря // Тези науково-практичної конференції «Проблеми експлуатації та захисту інформаційно-комунікаційних систем», м. Київ, 7–9 червня 2023 р., Національний авіаційний університет. – К.: Вид-во НАУ, 2023. – С. 49–51. 7. Яремчук Ю.Є., Грицак А.В. Удосконалений метод криптографічного захисту інформації // Тези науково-практичної конференції «Проблеми експлуатації та захисту інформаційно-комунікаційних систем». – м. Київ: Національний авіаційний університет, 2022. – С. 122–123. Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 1-5 п. 37 та 1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 19, 20 п. 38 чинних Ліцензійних умов.
485596	Яремчук Юрій Євгенович	професор, Сумісництво	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	Диплом магістра, Вінницький державний технічний університет, рік закінчення: 1996, спеціальність: 8.091101 Комп'ютерні науки, Диплом доктора наук ДД 003857, виданий 22.12.2014, Атестат професора	0	Криптографічний захист інформації	Доктор наук за спеціальнстю 05.13.21 «Системи захисту інформації». Дисертаційна робота на тему «Моделі, методи та засоби асиметричного криптографічного захисту інформації на основі рекурентних послідовностей». Стажування та підвищення кваліфікації: 1. Вінницький національний

				12ПР 010166, виданий 26.02.2015			технічний університет, Центр інформаційних технологій і захисту інформації, курс «Захист інформації в інформаційно-комунікаційних системах та на об'єктах інформаційної діяльності», свідоцтво про підвищення кваліфікації СПК №306536 від 03.06.2024 р. (78 год.) 2. Department of Electronic and Information Technologies, Faculty Electrical Engineering and Computer Science of Lublin University of Technology to Poland, дистанційна, стажування за кордоном, Development of information technologies through the use of new technologies in the field of research of image processing, machine learning, deep learning, artificial intelligence, intelligent data analysis, neural networks, security technologies, development of information-measuring systems diagnostic monitoring, з 06.03.2023 р. по 06.05.2023 р. Сертифікат №7-2023-VNTU, 2023-05-06. (180 год.) 3. Вінницький національний технічний університет, Центр інформаційних технологій і захисту інформації, курс «Захист інформації в інформаційно-комунікаційних системах та на об'єктах інформаційної діяльності», свідоцтво про підвищення кваліфікації СПК №306518 від 10.10.2022 р. (78 год.) 4. Тренінг для розробників і рецензентів тестових завдань зі спеціальності 125 «Кібербезпека», Науково-методичний центр вищої та фахової передвищої освіти Міністерства освіти і науки України, 29.10-26.11.2021 р. (15 год.) 5. Вінницький національний технічний університет,

							Центр інформаційних технологій і захисту інформації, курс «Захист інформації в інформаційно-комунікаційних системах та на об'єктах інформаційної діяльності», свідоцтво про підвищення кваліфікації СПК №301847 від 29.06.2021 р. (78 год.) 6. Національне агентство із забезпечення якості вищої освіти, Експерт з акредитації освітніх програм, сертифікат 06.10.2019 р. (5 год.) 1. Методичні вказівки до виконання курсових робіт з дисципліни «Основи криптографічного захисту інформації» для студентів спеціальності 125 «Кібербезпека» (освітні програми «Управління інформаційною безпекою» та «Кібербезпека інформаційних технологій та систем») / уклад. Ю. Є. Яремчук, О. В. Салієва. – Вінниця : ВНТУ, 2023. – 41 с. 2. Key generation method based on Genitor Genetic Algorithm model / Andrii Pryimak, Yurii Yaremchuk, Nataliia Kunanets // Proceedings of the 2nd International Conference on Conflict Management in Global Information Networks (CMiGiN 2022). – Kyiv, Ukraine, November 30, 2022, P. 51-60. (Scopus). 3. Яремчук Ю.Є. Підвищення стійкості цифрових водяних знаків у потокових відеозаписах на основі диференціального вбудовування енергії (DEW) / Ю. Є. Яремчук, В. В. Карпінець, І. С. Зоря, Д. О. Козак // Вісник Вінницького політехнічного інституту. 2023. – № 1. – С. 55–64. 4. Method of user authentication by keyboard handwriting based on neural networks and genetic algorithm / Andrii Pryimak, Yurii Yaremchuk, Olha

							Salieva, Vasyl Karpinets, Nataliia Kunanets // Proceedings of the International Workshop of IT-professionals on Artificial Intelligence (ProfIT AI 2021). – Kharkiv, Ukraine, September 20-21, 2021, P. 141-149. (Scopus). 5. Салієва О.В. Визначення рівня захищеності системи захисту інформації на основі когнітивного моделювання / О.В. Салієва, Ю.Є. Яремчук // Безпека інформації. – Т. 26, №1, 2020. – С. 42–49. 6. Яремчук Ю.Є. Вдосконалення стеганографічного методу PVD захисту цифрових зображень / Ю. Є. Яремчук, В. В. Карпінець, І. С. Зоря // Тези науково-практичної конференції «Проблеми експлуатації та захисту інформаційно-комунікаційних систем», м. Київ, 7–9 червня 2023 р., Національний авіаційний університет. – К.: Вид-во НАУ, 2023. – С. 49–51. 7. Яремчук Ю.Є., Грицак А.В. Удосконалений метод криптографічного захисту інформації // Тези науково-практичної конференції «Проблеми експлуатації та захисту інформаційно-комунікаційних систем». – м. Київ: Національний авіаційний університет, 2022. – С. 122–123. Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 1-5 п. 37 та 1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 19, 20 п. 38 чинних Ліцензійних умов.
60708	Кушнір Микола	доцент, Основне	Навчально-науковий	Диплом спеціаліста,	36	Ліцензування, атестація і	Стажування та підвищення

	Ярославович	місце роботи	інститут фізико-технічних та комп'ютерних наук	Чернівецький ордена Трудового Червоного Прапора державний університет, рік закінчення: 1978, спеціальність: Фізика, Диплом кандидата наук ФМ 026676, виданий 25.06.1986, Атестат доцента 02ДЦ 000432, виданий 24.12.2003		сертифікація у сфері безпеки об'єктів інформаційної діяльності	кваліфікації: Стажування в Тернопільському національному технічному ун-ті імені Івана Пулюя, з 24.05.2021 по 18.06.2021. Свідоцтво ПК № 05408102/001739-21 від 18.06.2021. Тема: «Наукові основи та програмно-апаратні засоби запровадження технології електронного навчання в освітній процес з метрології, телекомунікацій, електричної інженерії та поліграфії». 1. Kushnir, M., and K. Tokarieva. "A Generalization of the Arima Model to the Nonlinear and Continuous Cases." //Cybernetics and Systems Analysis, 2023. Vol. 59, pp. 900-909. https://link.springer.com/article/10.1007/s10559-023-00625-8. 2. Kushnir, M., Kosovan, H., & Kroialo, P. (2022). METHOD OF ENCRYPTING IMAGES BASED ON TWO MULTIDIMENSIONAL CHAOTIC SYSTEMS USING FUZZY LOGIC. [МЕТОД ШИФРУВАННЯ ЗОБРАЖЕНЬ НА ОСНОВІ ДВОХ БАГАТОВИМІРНИХ ХАОТИЧНИХ СИСТЕМ ІЗ ЗАСТОСУВАННЯМ НЕЧІТКОЇ ЛОГІКИ] Radioelectronic and Computer Systems, 2022(4), 117-128. doi:10.32620/reks.2022.4.09. ISSN: 1814-4225, EISSN: 2663-2012. Q = 4. https://www.scopus.com/record/display.uri?eid=2-s2.0-85146827813&origin=resultslist&sort=plf-f 3. Kushnir, M. Y., Kosovan, H. V., & Kroyalo, P. M. (2022). PROPERTIES OF GENERATORS OF PSEUDO-RANDOM SEQUENCES CONSTRUCTED USING FUZZY LOGIC AND TWO-DIMENSIONAL CHAOTIC SYSTEMS . Radio Electronics, Computer Science, Control, (1), 39. https://doi.org/10.15588/1607-3274-2022-1-5.

							ISSN: 1607-3274 eISSN: 2313-688X Q = 4 4. Dubrouski V., Semenko A., Kushnir M., Steita M.M. (2022) Parametric Analysis of Statistical and Correlation Characteristics of Discrete Processes in Dynamic Systems with Non-stationary Nonlinearities in Time for the Secure Intent-Based Networks. In: Klymash M., Beshley M., Luntovskyy A. (eds) Future Intent-Based Networking. Lecture Notes in Electrical Engineering, vol 831. Springer, Cham. https://doi.org/10.1007/978-3-030-92435-5_14 ISSN 18761100 Q = 4 https://www.scopus.com/sourceid/19700186822 https://www.scopus.com/record/display.uri?eid=2-s2.0-85121385059&origin=resultslist&sort=plf-f 5. Кушнір, М., Галюк, С., Семенко, А., & Крояло, П. (2022). ОСОБЛИВОСТІ СТВОРЕННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ З ВИКОРИСТАННЯМ ХАОТИЧНОГО СИГНАЛУ. Інфокомунікаційні та комп'ютерні технології, 1(03), 28-42. https://doi.org/10.36994/2788-5518-2022-01-03-02 6. Kushnir M., Vovchuk D., Haliuk S., Ivaniuk P., Politanskyi R. (2021) Approaches to Building a Chaotic Communication System. In: Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. https://doi.org/10.1007/978-3-030-43070-2_11. ISSN:2367-4512E-ISSN:2367-4520; Q = 4 https://www.scopus.com/record/display.uri?eid=2-s2.0-85087206316&origin=resultslist https://www.scopus.com/sourceid/21100975545?origin=recordpage Член редколегії

							вісника університету «Україна», Серія ІНФОКОМУНІКАЦІЙНІ ТА КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ (Категорія Б) https://visn-icct.uu.edu.ua/index.php/icct/about/editorialTeam Керівництво дисертації на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації (Косован Г.В.) Науковий керівник міжнародних грантів: 1. CRDF Global Grant Agreement G-202206-68835, Integration of new Cybersecurity course into the Curriculum of the Yuriy Fedkovych Chernivtsi National University, Mykola Kushnir, 1,500 USD, 3.5 months, till 09.26, 2022. https://docs.google.com/document/d/16eXTjjLWItrbh-MAoDAmOUCql2xkDTVn/edit 2. CRDF Global Grant Agreement G-202301-69802, Promotion of the Cyber Hygiene E-Learning course at the Yuriy Fedkovych Chernivtsi National University, Mykola Kushnir, 5,000 USD, 27.01. -27.08. 2023. https://docs.google.com/document/d/1R9nrF94mLZtC0z0b-nFhWU696PCeSHd_/edit Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 4, 5 п. 37 та 1, 6, 8, 10, 19 п. 38 чинних Ліцензійних умов.
96194	Гресь Олександр Володимирович	асистент, Основне місце роботи	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	Диплом бакалавра, Чернівецький національний університет імені Юрія Федьковича, рік закінчення: 2007, спеціальність: 1601	12	Ризик-орієнтований аналіз в кібербезпеці	Доцент по кафедрі радіотехніки та інформаційної безпеки (рішення Вченої ради ЧНУ, прот. №9 від 26.06.2024 р., https://www.chnu.edu.ua/media/h44fpxnz/protokol-9-vid-26062024.pdf); наказ

				Інформаційна безпека, Диплом спеціаліста, Чернівецький національний університет імені Юрія Федьковича, рік закінчення: 2008, спеціальність: Захист інформації з обмеженим доступом та автоматизація її обробки, Диплом кандидата наук ДК 056646, виданий 14.05.2020			№1415 від 02.10.2024 р. МОНУ "Про затвердження рішень Атестаційної колегії Міністерства освіти і науки України" про присвоєння вченого звання доцента, https://mon.gov.ua/npa/pro-zatverdzhennia-rishen-atestatsiinoi-kolehii-ministerstva-02-10-2024). Стажування та підвищення кваліфікації: 1. Lublin University of Technology, “Lubelska Politechnica”, Poland. Traineeship: “New knowledge in the development of information technologies through the use of new technologies in the field of research of image processing, machine learning, deep learning, artificial intelligence, intelligent data analysis, neural networks, security technologies, development of information-measuring systems diagnostic monitoring”, during 06.03.2023-06.05.2023, 180 hours / 6 credits ECTS, Sertificate № 3-2023-ChNU, 06-05-2023. 2. Підвищення кваліфікації на тему: “Оцінювання захищеності інформації. Експертні оцінювання у сфері технічного захисту інформації”, (“Information protection assessment. Expert evaluation in the technical protection of information”, Харківський нац. університет радіоелектроніки, 2020 р. Свідоцтво про підв. квал. №АА 02071197/000002-20 від 19 лютого 2020 року. 3. Підвищення кваліфікації на тему: “Виявлення закладних пристроїв”, (“Development of pocket devices”, Харківський нац. університет радіоелектроніки, 2020 р. Свідоцтво про підв. квал. №АА 02071197/000008-20 від 21 лютого 2020 року. 4. Захист кандидатської

							дисертації, 2020 р. 1. Larin V., Rozorinov H., Hres O., Rusyn V., Subbotin S., Chichikalo N., Larina K. (2022) Decision-making Algorithm in Case of Failure of the Electric Motor of a Multi-rotor Unmanned Aerial Vehicle. CEUR Workshop Proceedings, 3137, 154-163, ISSN 1613-0073. https://ceur-ws.org/Vol-3137/paper13.pdf 2. Rozorinov, H., Hres, O., Rusyn, V. (2022) GENERALIZED MODEL OF INFORMATION PROTECTION PROCESS IN AUDIOVISUAL CONTENT DISTRIBUTION NETWORKS. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska, 12(4), pp. 21–25, ISSN 2083-0157. https://ph.pollub.pl/index.php/iapgos/article/view/3317 3. Rozorinov H., Hres O., Rusyn V., Shpatar P. Environment of electromagnetic compatibility of radio-electronic communication means. IAPGOŚ. 2020. №1. Pp. 16-19. https://ph.pollub.pl/index.php/iapgos/article/view/917/1281 4. Гресь О. В., Розорінов Г. М., Пількевич Ю. Г., Костяк М. Ю., Пархуць Л. Т. Програмна реалізація системи потокового шифрування інформації на основі дискретних відображень. Вимірювальна та обчислювальна техніка в технологічних процесах. 2020. №1. С.60-66. https://journals.khnu.km.ua/index.php/MeasComp/article/view/2021/2480 5. Шпатар П.М., Гресь О.В., Качур В.В., Томулець А.Я. Детектування поодиноких фотонів в квантових криптографічних системах. Вісник ХНУ, Серія: технічні науки. 2020. №6. С. 28-32.

							ISSN 2307-5732 http://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/03/VKNU-TS-2020-N6-291-1.pdf. 6. Rozorinov H. Generalized model of the process of information protection in audiovisual content networks / Rozorinov H., Sirchenko I., Shpatar P., Hres O., Nichyy B. // Proccedings of IX International Scientific and Practical Conference “Physical and technical problems of information transmission, processing and storage of information communication systems”. – 21-23 October, 2021, Chernivtsi Suceava (Ukraine-Romania). – Pp. 78-80. 7. Гресь О.В., Косован В.М. Програмні засоби для дослідження властивостей генератора псевдовипадкових послідовностей на основі дискретного відображення /О.В. Гресь, В.М. Косован // Міжнародна наукова інтернет конференція “Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення”, 6-7 липня 2023. – Тернопіль, Україна – Переворськ, Польща. Випуск 79, С. 12-15. http://www.konferenciaonline.org.ua/ua/article/id-1243/ 8. Методи і засоби ТЗІ: методичні вказівки до курс. проектування/ укл.: Ластівка Г. І., Гресь О. В. [Навч. ел. видання] – Чернівці: Чернівецький нац. університет, 2022. – 90 с. https://drive.google.com/file/d/19gvHSMhwKACWvo6UnW1NH4QWgtAvDvn4/view Виконання функцій члена редакційної колегії наукового видання, включеного до переліку фахових видань України (з жовтня 2022 року): наукове фахове видання України (Категорія Б), науково-технічний

							журнал: “Вимірювальна та обчислювальна техніка в технологічних процесах”. https://vottp.khmnu.edu.ua/index.php/vottp/about/editorialTeam Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 1, 2 п. 37 та 1, 4, 5, 8, 12, 14 п. 38 чинних Ліцензійних умов.
60708	Кушнір Микола Ярославович	доцент, Основне місце роботи	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	Диплом спеціаліста, Чернівецький ордена Трудового Червоного Прапора державний університет, рік закінчення: 1978, спеціальність: Фізика, Диплом кандидата наук ФМ 026676, виданий 25.06.1986, Атестат доцента 02ДЦ 000432, виданий 24.12.2003	36	Перспективні напрямки розвитку систем кіберзахисту	Стажування та підвищення кваліфікації: Стажування в Тернопільському національному технічному ун-ті імені Івана Пулюя, з 24.05.2021 по 18.06.2021. Свідоцтво ПК № 05408102/001739-21 від 18.06.2021. Тема: «Наукові основи та програмно-апаратні засоби запровадження технології електронного навчання в освітній процес з метрології, телекомунікацій, електричної інженерії та поліграфії». 1. Kushnir, M., and K. Tokarieva. "A Generalization of the Arima Model to the Nonlinear and Continuous Cases." //Cybernetics and Systems Analysis, 2023. Vol. 59, pp. 900-909. https://link.springer.com/article/10.1007/s10559-023-00625-8. 2. Kushnir, M., Kosovan, H., & Kroialo, P. (2022). METHOD OF ENCRYPTING IMAGES BASED ON TWO MULTIDIMENSIONAL CHAOTIC SYSTEMS USING FUZZY LOGIC. [МЕТОД ШИФРУВАННЯ ЗОБРАЖЕНЬ НА ОСНОВІ ДВОХ БАГАТОВИМІРНИХ ХАОТИЧНИХ СИСТЕМ ІЗ ЗАСТОСУВАННЯМ НЕЧІТКОЇ ЛОГІКИ] Radioelectronic and Computer Systems,

							2022(4), 117-128. doi:10.32620/reks.2022.4.09. ISSN: 1814-4225, EISSN: 2663-2012. Q = 4. https://www.scopus.com/record/display.uri?eid=2-s2.0-85146827813&origin=resultslist&sort=plf-f 3. Kushnir, M. Y., Kosovan, H. V., & Kroyalo, P. M. (2022). PROPERTIES OF GENERATORS OF PSEUDO-RANDOM SEQUENCES CONSTRUCTED USING FUZZY LOGIC AND TWO-DIMENSIONAL CHAOTIC SYSTEMS . Radio Electronics, Computer Science, Control, (1), 39. https://doi.org/10.15588/1607-3274-2022-1-5. ISSN: 1607-3274 eISSN: 2313-688X Q = 4 4. Dubrouski V., Semenko A., Kushnir M., Steita M.M. (2022) Parametric Analysis of Statistical and Correlation Characteristics of Discrete Processes in Dynamic Systems with Non-stationary Nonlinearities in Time for the Secure Intent-Based Networks. In: Klymash M., Beshley M., Luntovskyy A. (eds) Future Intent-Based Networking. Lecture Notes in Electrical Engineering, vol 831. Springer, Cham. https://doi.org/10.1007/978-3-030-92435-5_14 ISSN 18761100 Q = 4 https://www.scopus.com/sourceid/19700186822 https://www.scopus.com/record/display.uri?eid=2-s2.0-85121385059&origin=resultslist&sort=plf-f 5. Кушнір, М., Галюк, С., Семенко, А., & Крояло, П. (2022). ОСОБЛИВОСТІ СТВОРЕННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ З ВИКОРИСТАННЯМ ХАОТИЧНОГО СИГНАЛУ. Інфокомунікаційні та комп'ютерні технології, 1(03), 28-42. https://doi.org/10.36994/2788-5518-2022-01-03-02 6. Kushnir M., Vovchuk D., Haliuk S., Ivaniuk

							P., Politanskyi R. (2021) Approaches to Building a Chaotic Communication System. In: Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. https://doi.org/10.1007/978-3-030-43070-2_11. ISSN:2367-4512E-ISSN:2367-4520; Q = 4 https://www.scopus.com/record/display.uri?eid=2-s2.0-85087206316&origin=resultslist https://www.scopus.com/sourceid/21100975545?origin=recordpage Член редколегії вісника університету «Україна», Серія ІНФОКОМУНІКАЦІЙНІ ТА КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ (Категорія Б) https://visn-icct.uu.edu.ua/index.php/icct/about/editorialTeam Керівництво дисертації на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації (Косован Г.В.) Науковий керівник міжнародних грантів: 1. CRDF Global Grant Agreement G-202206-68835, Integration of new Cybersecurity course into the Curriculum of the Yuriy Fedkovych Chernivtsi National University, Mykola Kushnir, 1,500 USD, 3.5 months, till 09.26, 2022. https://docs.google.com/document/d/16eXTjjLWItrbh-MAoDAmOUCql2xkDTVn/edit 2. CRDF Global Grant Agreement G-202301-69802, Promotion of the Cyber Hygiene E-Learning course at the Yuriy Fedkovych Chernivtsi National University, Mykola Kushnir, 5,000 USD, 27.01. -27.08. 2023. https://docs.google.com/document/d/1R9nrF94mLZtCozob-nFhWU696PCeSHd_/edit

							Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 4, 5 п. 37 та 1, 6, 8, 10, 19 п. 38 чинних Ліцензійних умов.
86449	Політанський Руслан Леонідович	професор, Основне місце роботи	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	Диплом магістра, Московський фізико-технічний інститут, рік закінчення: 1994, спеціальність: Прикладна математика і фізика, Диплом доктора наук ДД 005179, виданий 25.02.2016, Диплом кандидата наук ДК 014144, виданий 10.04.2002, Атестат доцента 12ДЦ 031513, виданий 29.03.2012, Атестат професора АП 002287, виданий 02.11.2020	15	Моделювання та оптимізація процесів у ІБ	Стажування та підвищення кваліфікації: 1. Стажування в Київському національному університеті імені Тараса Шевченко з 10.01.2024 по 21.02.2024; кількість кредитів – 6 /180 год. ECTS (сертифікат № 056/0229 від 27.02.2024 р.). Тема: «Методи та засоби розробки комплексних систем захисту інформації». 2. Стажування в Сучавському університеті «Штефан чел Маре» (Румунія) (міжнародний сертифікат «Certificat De Participare» № 01/14.02.2020 від 14.02.2020 р., тема «Кібербезпека, інформаційні технології, засоби телекомунікацій та радіотехніки та інструменти і методи дослідження у європейських університетах» (наказ по університету № 13- від 14.01.2019). 3. Навчальний курс «Approximation Methods» на платформі Coursera (розробник University of Colorado Boulder). Сертифікат від 19.01.2023. https://coursera.org/verif y/YLJ2XQ4Q5LCM. 1. Politanskyi, R., Vistak, M., Veryga, A. and Ruda, T. Modelling of spintronic devices for application in random access memory / Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska. 2020, 10(1), pp. 62-65. DOI: 10.35784/iapgos.915. 2. A. Veryga, R. Politanskyi. Time interval switching device / IAPGOŚ /

							Editor-in-Chief prof. P. Comoda, Lublin, Poland: Politechnika Lubelska. 2020. №1, p.12-15. (ISSN 2083-015,7 Index Copernicus). DOI: https://doi.org/10.35784/iapgos.908. 3. Політанський Р.Л. Дослідження періодичності псевдовипадкових послідовностей методом булевого гіперкубу / Вчені записки ТНУ ім. В.І. Вернадського. Технічні науки / Гол. ред. проф. В.П. Казарін. Херсон, Україна: Таврійський національний університет ім. Вернадського. 2020, Том 31 (70), № 2, С. 145-152 (фахове видання). 4. Kushnir M., Vovchuk D., Haliuk S., Ivaniuk P., Politanskyi R. (2021) Approaches to Building a Chaotic Communication System. In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer. DOI: 10.1007/978-3-030-43070-2_11. 5. Politanskyi R. et al. Entropy calculation for networks with determined values of flows in nodes. Mathematical Modeling and Computing, Vol. 9, No. 4, pp. 936–944 (2022). https://doi.org/10.23939/mmc2022.04.936. 6. Politanskyi R. et al. Investigation of High-Speed Methods for Determining the Equilibrium State of a Network Based on the Principle of Maximum Entropy. In: Klymash, M., Luntovskyy, A., Beshley, M., Melnyk, I., Schill, A. (eds) Emerging Networking in the Digital Transformation Age. Lecture Notes in Electrical Enginering, vol 965 (2023). Springer, Cham. https://doi.org/10.1007/978-3-031-24963-1_35. Керівництво дисертації на здобуття

							наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації (Гресь О.В.). Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 4, 5 п. 37 та 1, 3, 4, 6, 7, 8 п. 38 чинних Ліцензійних умов.
454724	Прокофьєв Михайло Іванович	професор, Сумісництво	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	Диплом спеціаліста, Київський ордена Леніна політехнічний інститут, рік закінчення: 1972, спеціальність: Конструювання виробництва радіоапаратури, Диплом доктора наук ДД 009872, виданий 14.05.2020, Диплом кандидата наук ДК 026418, виданий 26.02.2015, Атестат доцента АД 014986, виданий 24.04.2024	0	Технології комплексного захисту інформації	Фахівець - практик. 1997 р. – 2021 р. – директор НДЦ «ТЕЗІС» КПІ ім. Ігоря Сікорського. 1. M. Prokofiev, A. Yanenko, S. Peregudov. K. Shevchenko. Perspectives of the using mm-range radiometry in telecommunication systems of information transmission" // Adv. InfCommun. Technol., vol. 59, 2019. 2. Konstantyn Shevchenko, Oleksiy Yanenko, Mikhail Prokofiev, Sergey Peregudov , Vasyl Kuz, Stanislav Ustenko. Measurement Of The Reflection Coefficient Of Moist Materials At Ultrahigh Frequencies // Journal of the Technical University of Gabrovo. 2019. 3. Konstantyn Shevchenko, Oleksiy Yanenko, Mikhail Prokofiev, Sergey Peregudov, Vasyl Kuz. Microwave Food Fat Meter // Proceedings of the international scientific conference “UNITECH 2020" 4. Konstantyn Shevchenko, Oleksiy Yanenko, Mikhail Prokofiev, Sergey Peregudov, Vasyl Kuz. Commutation-modulation method and means of determining acupuncture points // Proceedings of the international scientific conference “UNITECH 2021” 5. Прокофьєв М. І. Методичні рекомендації до самостійної роботи з дисципліни «Основи

							кібербезпеки та національної безпеки» для здобувачів освіти спеціальності 125 Кібербезпека та захист інформації СО «Бакалавр» / укладачі М. І. Прокофьєв, Л. П. Половенко, О. В. Гресь. Вінниця: ДонНУ імені Василя Стуса, 2024 – 88 с.
118310	Ластівка Галина Іванівна	доцент, Основне місце роботи	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	Диплом бакалавра, Чернівецький державний університет ім. Ю.Федьковича, рік закінчення: 1998, спеціальність: 090701 Радіотехніка, Диплом магістра, Чернівецький державний університет імені Юрія Федьковича, рік закінчення: 1999, спеціальність: Радіотехніка, Диплом кандидата наук ДК 064434, виданий 22.12.2010, Атестат доцента 12ДЦ 035476, виданий 31.05.2013	21	Науково-педагогічна діяльність та навчання персоналу в галузі ІБ	Стажування та підвищення кваліфікації: 1. Програма підвищення кваліфікації SoftServe Academy “CLOUD ENVIRONMENT CONFIGURATION AND SECURITY (Налаштування та безпека хмарних середовищ)” . З 07.03.2024 по 02.04. 2024, 120 год. / 4 кредити ECTS, сертифікат Series DG № 17539/2024. 2. Курс-стажування «Менеджмент у продуктовому IT», сертифікат від 15.04.2024 , 1dd186f5dc6c9d5b8585e69a001b5864. 3. Lublin University of Technology, “Lubelska Politechnica”, Poland. Traineeship: “New knowledge in the development of information technologies through the use of new technologies in the field of research of image processing, machine learning, deep learning, artificial intelligence, intelligent data analysis, neural networks, security technologies, development of information-measuring systems diagnostic monitoring”, during 15.05.2023-15.07.2023, 180 hours / 6 credits ECTS, Sertificate № 5-2023-ChNU, 15-07-2023. 4. Стажування в Тернопільському національному технічному ун-ті імені Івана Пулюя, з 24.05.2021 по 18.06.2021. Свідоцтво ПК № 05408102/001740-21 від 18.06.2021. Тема: «Наукові основи та програмно-апаратні

							засоби запровадження технології електронного навчання в освітній процес з метрології, телекомунікацій, електричної інженерії та поліграфії». 5. Програма підвищення каліф. з серії наук.-метод. семінарів-практикумів «Алгоритм підготовки до викладання фахових дисциплін англійською мовою» (ЧНУ). З 29.01.2020 по 25.06.2020. Сертифікат, наказ №190 від 17.07.2020. 6. Підвищення кваліфікації у Центрі підтримки академій Cisco Нац. технічного університету «Харківський політехнічний інститут» в рамках Програми Академій Cisco (курс «Основи апаратного та програмного забезпечення ПК» та СТЕМ-практика з Інтернету речей та кібербезпеки). З 1.09.2020 по 25.10.2020. Сертифікат від 25.10.2020 р. 1. Методи і засоби ТЗІ: методичні вказівки до курс. проектування/ укл.: Ластівка Г. І., Гресь О. В. [Навч. ел. видання] – Чернівці: Чернівецький нац. університет, 2022. – 90 с. https://drive.google.com/file/d/19gvHSMhwKACWvo6UnW1NH4QWgtAvDvn4/view 2. Косован Г.В. Безпека інфокомунікацій та безперервність бізнеспроцесів / укл.: Г.В. Косован, Г.І. Ластівка, П.М. Шпатар. Чернівці: Чернівецький національний університет, 2023. – 152 с. https://radiotech.chnu.edu.ua/educationbooks/ 3. Міждисциплінарна курсова робота: методичні вказівки до курсового проектування/ укл. : Ластівка Г. І., Рождественська М. Г. [Навчальне електронне видання] – Чернівці : Чернівецький

							національний університет, 2023.– 57 с. https://radiotech.chnu.edu.ua/educationbooks/ 4. Oleksandr Dubyniak, Halyna Lastivka, Oleksandr Lastivka Study of methods of artificially generated voice information detection // IX International Scientific-Practical Conference Physical and Technological Problems of Transmission, Processing and Storage of Information in Infocommunication Systems 21-23 October 2021, Chernivtsi-Suceava (Ukraine-Romania). 5. Samila, A., Khandozhko, A., Lastivka, G., Khandozhko, V. Evaluation of the contribution of higher-order electron-nuclear interactions to the NQR frequencies using 115In spectra in InSe. Proceedings of SPIE - The International Society for Optical Engineering, 2021, Vol. 12126, 121260H-129–134 https://www.spiedigitallibrary.org/conference-proceedings-of-spie/12126/2615420/Evaluation-of-the-contribution-of-higher-order-electron-nuclear-interactions/10.1117/12.2615420.full 6. Samila, A.P., Lastivka, G.I., Tanasyuk, Y.V. Actual problems of computer parametric identification of the NMR and NQR spectra: A review. J. Nano-Electron. Phys. 2019. Vol. 11, No 5. P. 05036-1–10. https://www.scopus.com/record/display.uri?eid=2-s2.0-85075778494&origin=resultslist https://www.scopus.com/sourceid/21100210917?origin=resultslist 7. A. Veryha, R. Politansky, M. Rozhdestvenska and H. Lastivka. Analysis of Self-Similar Binary Sequences // Security of Infocommunication Systems and Internet of Things. – 2023. Vol 1, №1. P. 01003-1-5. https://doi.org/10.31861/sisiot2023.1.01003

							8. Дубиняк О., Ластівка Г., Ластівка О. Вивчення та дослідження методів виявлення штучно згенерованої мовної інформації // VI Всеукр. науково-практична конф. «Перспективні напрямки сучасної електроніки, інформаційних і комп'ютерних систем» (MEICS-2021). Дніпро, 24-26 листопада 2021 р. http://meics.dnure.dp.ua/program 9. В. В. Браїловський, Г. І. Ластівка, І. С. Паюк, М. Г. Рождественська, П. М. Шпатар. Використання засобів платформи MOODLE для підготовки здобувачів вищої освіти з кібербезпеки до ЄДКІ. XI Міжнар. науково-практична конференція "Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій", 12–14 грудня 2022 р., м. Запоріжжя.- С. 89-91. URL: https://scholar.google.com/scholar?oi=bibs&cluster=18208501513419092697&btnI=1&hl=uk Відповідальний секретар редакційної колегії журналу «Безпека інфокомунікаційних систем та Інтернету речей», сформованого відповідно до наказу № 239 від 1.09.2022 р. Мережна Академія Cisco (Cisco Networking Academy in Ukraine), інструктор. Участь в роботі міжнародного освітнього гранту G-202206-68835 «Integration of new Cybersecurity courses into the Curriculum of the Yuriy Fedkovych Chernivtsi National University» під егідою CRDF Global в Україні (Меморандум про взаєморозуміння між Чернівецьким нац. ун-том ім. Юрія Федьковича та Представництвом Фонду цивільних досліджень та

							розвитку США від 17.06.2022 р.). Член ГО «Східноєвропейське наукове товариство», посвідчення № ES 164 від 8.01.2024 р. Сертифікат LangSkill B2 Reference number 19Y138G019DQ1 15/07/2023. Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 3, 5 п. 37 та 1, 3, 4, 7, 8, 10, 12, 13, 14, 19, 20 п. 38 чинних Ліцензійних умов.
104068	Галушка Зоя Іванівна	завідувач кафедри, Основне місце роботи	Економічний факультет	Диплом спеціаліста, Київський ордена Леніна державного університету імені Т.Г. Шевченка, рік закінчення: 1980, спеціальність: Політична економія, Диплом доктора наук ДД 000142, виданий 10.11.2011, Диплом кандидата наук ЭК 021623, виданий 23.07.1986, Атестат доцента ДЦ 022419, виданий 17.04.1990, Атестат професора 12ПР 008309, виданий 30.11.2012	38	Особливості проектної діяльності в кібербезпеці	Стажування та підвищення кваліфікації: 1. Кафедра економічної теорії ДВНЗ «Київський національний економічний університет імені Вадима Гетьмана» (2020 р.) 2. «Фандрейзинг та основи проєктної діяльності у закладах освіти: європейський досвід» (м. Краків, Польща); з 22.04.2023 року по 28.05.2023 р. Наказ №100 від 09.03.2023 р. Сертифікат SZFL-002406 від 28.05.2023 р. 1. Економічний та управлінський потенціал соціалізації економіки : монографія / за заг. ред. З.І. Галушки. Чернівці : Чернівец. нац. ун-т. ім. Ю. Федьковича, 2020. - 408 с. 2. Галушка З. І., Лусте О.О. Стратегії розвитку бізнесу: теорія і практика. Навчальний посібник. Чернівці. ЧНУ, 2021. 290 с. 3. Менеджмент: збірник тестових завдань. Укл.: Антохов А.А., Галушка З.І., Запухляк В.М., Поченчук Г.М. та ін. / За ред. Галушки З.І., Поченчук Г.М. Чернівці. Чернівец. нац. ун-т. 2021. 203 с.

							4. Менеджмент і адміністрування : підручник для магістрів / Колектив авторів: д.е.н., проф. Галушка З.І., д.е.н., доц. Антохов А.А., к.е.н., доц. Запухляк В.М та ін. Чернівці : ЧНУ. 2021. 437 с. 5. Галушка З.І. Невизначеність як економічна категорія та як середовище функціонування бізнесу. Економіка: реалії часу. Науковий журнал. 2023. No1 (65). С.26-32. URL: https://economics.net.ua/files/archive/2023/N01/26.pdf. DOI: 10.15276/ETR.01.2023.3. DOI: 10.5281/zenodo.7834244. 6. Zoia Halushka, Ruslan Biloskurskyy, Viacheslav Kravets, Volodymyr Gruntkovskyi, Karina Stromilova. Managing the development of microeconomic systems in the face of global challenges. Ad alta: Journal of Interdisciplinary Research. Special Issue12/01-XXV. Pp.48-52. ISSN 1804-7890 ISSN 2464-6733 (Online) Чехія / Czech Republic. Web of Science (ESCI), ERIH PLUS, CrossRef, EBSCO, Index Copernicus http://www.magnanimitas.cz/12-01-xxv 7. Галушка З.І. Гнучкі методи управління проєктами: роль проєктного менеджера. Проблеми системного підходу в економіці. Випуск 4(84). 2021. С. 37-43. DOI: https://doi.org/10.32782/2520-2200/2021-4-5 8. Галушка З.І. Соціальний цикл розвитку організації: стратегії виживання в умовах невизначеності. Науковий вісник Чернівецького університету: Економіка: Випуск 830. 2021. С.71-77 http://econom.chnu.edu.ua/journal/index.php/ecovis/article/view/151 Академічна та професійна кваліфікація

							забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 1, 2 п. 37 та 1, 3, 4, 6, 7, 8, 9, 10, 12, 19 п. 38 чинних Ліцензійних умов. Для досягнення цілей та програмних результатів навчання за ОК "Особливості проектної діяльності в кібербезпеці" до забезпечення даної дисципліни залучений доцент кафедри радіотехніки та інформаційної безпеки, к.т.н. Лесінський В.В. (диплом кандидата наук ДК 011681, виданий 25.01.2013; атестат доцента АД 005427, виданий 24.09.2020), який має такі досягнення: Стажування та підвищення кваліфікації: 1. 04-28.11.2019 р. Сучавський університет імені Штефана чел Маре, м. Сучава, Румунія, тема: «Система викладання предметів у галузі комп'ютерних наук, засобів телекомунікації та електронної техніки; дослідницька робота у європейських університетах», (Наказ № 739 від 4.11.2019 р.), міжнародний сертифікат № 35/29.11.2019 11-21.02.20. 2. Харківський національний університет радіоелектроніки; теми: «Оцінювання захищеності інформації», свідоцтво: 001132 (19.02.2020); «Виявлення закладних пристроїв», свідоцтво: 001138 (21.02.2020). Навчально-методичні посібники: 1. Управління інформаційною безпекою / Лесінський В.В., Толюпа С.В., Політанський Л.Ф., Політанський Р.Л. Чернівці: ЧНУ «Рута»,

							2021. - 540 с. 2. Системи захисту інформації / С. В. Толюпа, С. С. Бучик, О. А. Лаптєв, В. В. Лесінський. К. : Міленіум. 2022. - 390 с. Статті у наукових виданнях: 1. TWO-DIMENSIONAL HYPERCHAOTIC MAP FOR CHAOTIC OSCILLATIONS // O. Krulikovskyi, S. Haliuk, I. Safronov, V. Lesinskyi // Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska, 14(3), 29–34. DOI: https://doi.org/10.35784/iapgos.6165. Scopus, ISSN: 2391-6761. 2. DEVELOPMENT OF TOOLS FOR ASSESSING AND REALIZING THE POTENTIAL OF ENERGY-SAVING ECONOMIC DEVELOPMENT OF ENTERPRISES // V. Lesinskyi, O. Yemelyanov, O. Zarytska, T. Petrushka, N. Myroschenko / Eastern-European Journal of Enterprise Technologies. 2024, 4(13(130)). DOI: https://doi.org/10.15587/1729-4061.2024.308986, Scopus, ISSN: 1729-3774. 3. DEVELOPMENT OF A TOOLKIT FOR ASSESSING AND OVERCOMING BARRIERS TO THE IMPLEMENTATION OF ENERGY SAVING PROJECTS // V Lesinskyi, O. Yemelyanov, O.Zarytska, A Symak. T. Petrushka / Eastern-European Journal of Enterprise Technologies. Vol. 5 No. 3 (107) (2020), pp. 24–38: Control processes. http://journals.uran.ua/eejet/article/view/214997 DOI: https://doi.org/10.15587/1729-4061.2020.214997. Scopus, ISSN: 1729-3774. 4. Devising a toolset for assessing the potential of loan financing of projects aimed at implementing energy-saving technologies // V.Lesinskyi,

							O.Yemelyanov, O.Zarytska, A.Symak, T.Petrushka / Eastern-European Journal of Enterprise Technologies. Vol. 4 No. 13(112) (2021) p. 15–33: Transfer of technologies: industry, energy, nanotechnology, http://journals.uran.ua/eejet/article/view/238795/237878, DOI: https://doi.org/10.15587/1729-4061.2021.238795, Scopus, ISSN: 1729-3774. 5. Designing a Tool-Set for Assessing the Organizational and Technological Inertia of Energy Consumption Processes at Enterprises // V. Lesinskyi, O. Zarytska, O. Yemelyanov, T. Petrushka, N. Myroshchenko // Eastern-European Journal of Enterprise Technologies. Vol. 6 No. 13(120) (2022) p. 29–40. https://journals.uran.ua/eejet/article/view/267231, DOI: https://doi.org/10.15587/1729-4061.2022.267231, Scopus, ISSN: 1729-3774. Участь у міжнародних конференціях: 1. AWARENESS OF CYBERSECURITY. RISKS POSED BY UNTRAINED EMPLOYEES // V. Lesinskyi, V. Zaitseva / Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах: IX Міжнародна науково-практична конференція. 21-23 жовтня 2021р., Чернівці, Україна. https://easychair.org/conferences/submission_download?upload=116788;submission=5722938;a=27584444. 2. Using elements of machine learning, artificial intelligence, and nonlinear dynamics to transmit secure information in communication systems // V. Lesinskyi, M. Kushnir // Cybersecurity and military artificial intelligence. New legal

							challenges and resilience perspectives. 26 January 2024. Suceava, Romania "Ștefan cel Mare" University from Suceava, Romania. Режим доступу: https://cmai.ro/. 3. Analysis of Using of Fractal Signals for Noise Immune Information Transmission Systems // V. Lesinskyi, A.Veryga, R.Politanskyi, T.Ruda // 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, (TCSET). 2020. P.162-165, https://ieeexplore.ieee.org/abstract/document/9088532, DOI: 10.1109/TCSET49122.2020, Scopus, ISBN: 978-172815566-1; 4. Аналіз параметрів фрактальних сигналів побудованих на основі послідовностей Кантора // A. Veryha, R. Politansky, M. Vistak, V. Lesinskyi / Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах: IX Міжнародна науково-практична конференція. 21-23 жовтня 2021 р., Чернівці, Україна. https://easychair.org/conferences/submission_download?submission=5682061;upload=116788;a=27584444. Академічна та професійна кваліфікація Лесінського В.В. забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням пп. 1, 3, 4, 7, 10 п. 38 чинних Ліцензійних умов.

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
РН24. Організовувати процес навчання персоналу компанії у відповідності до сучасних норм та вимог, проводити спільно з представниками державних та комерційних структур тренінги щодо протидії проявам соціальної інженерії.	☐	Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		Безпека інфокомунікацій та безперервність бізнес-процесів	Лекції: пояснювально-ілюстративний метод, презентації; робота з книгою: з навчально-методичною, науковою та нормативною літературою; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; лабораторні заняття: метод проблемного підходу, дослідницький метод; самостійна робота: підготовка презентацій, рефератів, а також формуванням напрацювань для виконання і захисту лабораторних робіт.	Поточний контроль – усні та письмові (тестування, захист лабораторних робіт, захист завдань практичного характеру) відповіді здобувача освіти. Підсумковий контроль (екзамен) – усне або письмове опитування, тестовий контроль.
		Науково-педагогічна діяльність та навчання персоналу в галузі ІБ	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); робота з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); інтерактивні методи навчання: робота в малих групах та тренінги, методи проектів, кейс-метод, метод «мозкового штурму», ділова гра, рольова гра та інші освітні технології; самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни (реферат, доповідь тощо).	Поточний контроль – тести, опитування (усне та письмове), представлення презентації, доповідь та аргументований захист у процесі командної роботи. Підсумковий контроль (екзамен) – усне, письмове опитування, тестовий контроль.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на	☒	Дипломне проектування (кваліфікаційна робота)	Дослідницький метод; словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота	Захист кваліфікаційної (дипломної) роботи.

основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.			над індивідуальним завданням або за програмою навчальної дисципліни.	
		Переддипломна практика	Дослідницький метод; пояснення; бесіда; дискусія, робота з навчально-методичною та фаховою літературою, самостійна робота, проведення досліджень за обраною темою.	Поточний контроль - презентація результатів виконання завдань. Підсумковий контроль (залік) – доповідь за отриманими під час проходження переддипломної практики результатами на випусковій кафедрі.
		Перспективні напрямки розвитку систем кіберзахисту	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; семінарські заняття: підготовка презентацій, рефератів; методи інтерактивного навчання: робота в малих групах, тренінги, метод проектів, кейс-метод, метод «мозкового штурму», ділова гра, рольова гра та інші освітні технології; лабораторні заняття: евристичний метод, метод проблемного викладу; самостійна робота: репродуктивний метод, дослідницький метод; робота з науковою та літературою професійного спрямування.	Поточний контроль: усні та письмові (тестування, захист лабораторних робіт, представлення доповідей та захист рефератів) відповіді здобувача освіти. Підсумковий контроль – екзамен (усне або письмове опитування; тестовий контроль, в тому числі засобами платформ електронного навчання).
		Технології комплексного захисту інформації	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; самостійна робота: підготовка презентацій, рефератів; робота з навчально-методичною, науковою, нормативною літературою. Дисципліною передбачене виконання курсової роботи.	Поточний контроль: усні та письмові (контрольна робота, тестування, захист завдань практичного характеру) відповіді студента, захист курсових робіт. Підсумковий контроль: екзамен (усне, письмове опитування, тестовий контроль).
РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.	☒	Переддипломна практика	Дослідницький метод; пояснення; бесіда; дискусія, робота з навчально-методичною та фаховою літературою, самостійна робота, проведення досліджень за обраною темою.	Поточний контроль - презентація результатів виконання завдань. Підсумковий контроль (залік) – доповідь за отриманими під час проходження переддипломної практики результатами на випусковій кафедрі.
		Моделювання та оптимізація процесів у ІБ	Лекції: пояснювально-ілюстративний метод, презентації; робота з навчально-методичною, науковою літературою; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи	Поточний контроль – усні та письмові (тестування) відповіді здобувача освіти, доповіді та аргументований захист під час проведення підсумкового оцінювання. Підсумковий контроль – залік.

			навчання: підключення до освітніх порталів (Coursera); самостійна робота: підготовка презентацій, рефератів, а також формуванням напрацювань для виконання і захисту практичних робіт.	
		Дипломне проектування (кваліфікаційна робота)	Дослідницький метод; словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Захист кваліфікаційної (дипломної) роботи.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.	☒	Дипломне проектування (кваліфікаційна робота)	Дослідницький метод; словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Захист кваліфікаційної (дипломної) роботи.
		Переддипломна практика	Дослідницький метод; пояснення; бесіда; дискусія, робота з навчально-методичною та фаховою літературою, самостійна робота, проведення досліджень за обраною темою.	Поточний контроль - презентація результатів виконання завдань. Підсумковий контроль (залік) – доповідь за отриманими під час проходження переддипломної практики результатами на випусковій кафедрі.
		Моделювання та оптимізація процесів у ІБ	Лекції: пояснювально-ілюстративний метод, презентації; робота з навчально-методичною, науковою літературою; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: підключення до освітніх порталів (Coursera); самостійна робота: підготовка презентацій, рефератів, а також формуванням напрацювань для виконання і захисту практичних робіт.	Поточний контроль – усні та письмові (тестування) відповіді здобувача освіти, доповіді та аргументований захист під час проведення підсумкового оцінювання. Підсумковий контроль – залік.
РН20. Ставити та вирішувати складні інженерно-прикладні та	☒	Ліцензування, атестація і сертифікація у сфері безпеки об'єктів	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); практичні заняття: наочні	Поточний контроль – усні та письмові (тестування) відповіді студента; представлення презентації,

наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.		інформаційної діяльності	інформаційної діяльності методи (презентації, ілюстрації, тощо); інтерактивні методи навчання: робота в малих групах та тренінги; робота з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни (реферат, доповідь тощо). здобувача освіти.	доповідь та аргументований захист у процесі командної роботи. Підсумковий контроль (екзамен) – усне, письмове опитування, тестовий контроль.
		Перспективні напрямки розвитку систем кіберзахисту	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; семінарські заняття: підготовка презентацій, рефератів; методи інтерактивного навчання: робота в малих групах, тренінги, метод проектів, кейс-метод, метод «мозкового штурму», ділова гра, рольова гра та інші освітні технології; лабораторні заняття: евристичний метод, метод проблемного викладу; самостійна робота: репродуктивний метод, дослідницький метод; робота з науковою та літературою професійного спрямування.	Поточний контроль: усні та письмові (тестування, захист лабораторних робіт, представлення доповідей та захист рефератів) відповіді здобувача освіти. Підсумковий контроль – екзамен (усне або письмове опитування; тестовий контроль, в тому числі засобами платформ електронного навчання).
		Дипломне проектування (кваліфікаційна робота)	Дослідницький метод; словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Захист кваліфікаційної (дипломної) роботи.
		Переддипломна практика	Дослідницький метод; пояснення; бесіда; дискусія, робота з навчально-методичною та фаховою літературою, самостійна робота, проведення досліджень за обраною темою.	Поточний контроль - презентація результатів виконання завдань. Підсумковий контроль (залік) – доповідь за отриманими під час проходження переддипломної практики результатами на випусковій кафедрі.
РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи	☒	Особливості проектної діяльності в кібербезпеці	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); практичні заняття:	Поточний контроль: усні та письмові (опитування під час занять, тестування, обговорення завдань практичного характеру, доповідь за індивідуальною темою) відповіді студента. Підсумковий контроль –

кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.			репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги, методи проектів, кейс-метод, метод «мозкового штурму», ділова гра, рольова гра та інші освітні технології; самостійна робота: підготовка презентацій, рефератів; опрацювання літературних джерел та інформаційних ресурсів.	екзамен (усне або письмове опитування; тестовий контроль).
		Переддипломна практика	Дослідницький метод; пояснення; бесіда; дискусія, робота з навчально-методичною та фаховою літературою, самостійна робота, проведення досліджень за обраною темою.	Поточний контроль - презентація результатів виконання завдань. Підсумковий контроль (залік) – доповідь за отриманими під час проходження переддипломної практики результатами на випусковій кафедрі.
		Дипломне проектування (кваліфікаційна робота)	Дослідницький метод; словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Захист кваліфікаційної (дипломної) роботи.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.	☒	Дипломне проектування (кваліфікаційна робота)	Дослідницький метод; словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Захист кваліфікаційної (дипломної) роботи.
		Переддипломна практика	Дослідницький метод; пояснення; бесіда; дискусія, робота з навчально-методичною та фаховою літературою, самостійна робота, проведення досліджень за обраною темою.	Поточний контроль - презентація результатів виконання завдань. Підсумковий контроль (залік) – доповідь за отриманими під час проходження переддипломної практики результатами на випусковій кафедрі.
		Науково-педагогічна діяльність та навчання персоналу в галузі ІБ	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); робота з навчально-методичною, науковою, нормативною літературою; комп'ютерні	Поточний контроль – тести, опитування (усне та письмове), представлення презентації, доповідь та аргументований захист у процесі командної роботи.

			засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); інтерактивні методи навчання: робота в малих групах та тренінги, методи проектів, кейс-метод, метод «мозкового штурму», ділова гра, рольова гра та інші освітні технології; самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни (реферат, доповідь тощо).	Підсумковий контроль (екзамен) – усне, письмове опитування, тестовий контроль.
РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.	☒	Переддипломна практика	Дослідницький метод; пояснення; бесіда; дискусія, робота з навчально-методичною та фаховою літературою, самостійна робота, проведення досліджень за обраною темою.	Поточний контроль - презентація результатів виконання завдань. Підсумковий контроль (залік) – доповідь за отриманими під час проходження переддипломної практики результатами на випусковій кафедрі.
		Перспективні напрямки розвитку систем кіберзахисту	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; семінарські заняття: підготовка презентацій, рефератів; методи інтерактивного навчання: робота в малих групах, тренінги, метод проектів, кейс-метод, метод «мозкового штурму», ділова гра, рольова гра та інші освітні технології; лабораторні заняття: евристичний метод, метод проблемного викладу; самостійна робота: репродуктивний метод, дослідницький метод; робота з науковою та літературою професійного спрямування.	Поточний контроль: усні та письмові (тестування, захист лабораторних робіт, представлення доповідей та захист рефератів) відповіді здобувача освіти. Підсумковий контроль – екзамен (усне або письмове опитування; тестовий контроль, в тому числі засобами платформ електронного навчання).
		Науково-педагогічна діяльність та навчання персоналу в галузі ІБ	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); робота з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); інтерактивні методи навчання: робота в малих групах та тренінги, методи проектів, кейс-метод, метод «мозкового штурму», ділова гра, рольова гра та інші освітні технології; самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни (реферат, доповідь тощо).	Поточний контроль – тести, опитування (усне та письмове), представлення презентації, доповідь та аргументований захист у процесі командної роботи. Підсумковий контроль (екзамен) – усне, письмове опитування, тестовий контроль.
		Наукова та професійна комунікація іноземною мовою	Комунікативно-діяльнісний підхід, метод комунікативних завдань, система навчання CLIL та інші у традиційних формах навчального процесу (практичне заняття, консультація, самостійна робота) з використанням	Поточний контроль – усна (доповідь, презентація) чи письмова (тестування; анотація / реферат наукової статті) відповідь студента. Підсумковий контроль (залік) – усне та письмове опитування, тестовий контроль.

			наочних засобів (презентації, ілюстрації, відеоматеріали, аудіювання тощо) або у змішаній формі із застосуванням електронних курсів та платформ для дистанційного навчання.	
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.	☒	Ризик-орієнтований аналіз в кібербезпеці	Під час проведення лекційних занять використовуються пояснювально-ілюстративний метод та підхід проблемного навчання; для проведення практичних занять використовуються інтуїтивно-пошуковий та дослідницький методи, при яких викладач ставить перед студентами задачу, і вони розв'язують її самостійно або під керівництвом викладача, висуваючи ідеї, перевіряючи їх, знаходячи для цього необхідні дані, методи, підходи тощо; самостійна робота: опрацювання матеріалів лекцій та літературних джерел за відповідною тематикою, підготовка виступів-презентацій, рефератів; інтерактивні методи навчання: робота в малих групах та тренінги.	Поточний контроль: усні та письмові (тестування, доповіді за індивідуальними темами, захист завдань практичного характеру) відповіді здобувача освіти. Підсумковий контроль – екзамен; передбачає усне або письмове опитування, зокрема, тестовий контроль.
		Моделювання та оптимізація процесів у ІБ	Лекції: пояснювально-ілюстративний метод, презентації; робота з навчально-методичною, науковою літературою; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: підключення до освітніх порталів (Coursera); самостійна робота: підготовка презентацій, рефератів, а також формуванням напрацювань для виконання і захисту практичних робіт.	Поточний контроль – усні та письмові (тестування) відповіді здобувача освіти, доповіді та аргументований захист під час проведення підсумкового оцінювання. Підсумковий контроль – залік.
		Особливості проектної діяльності в кібербезпеці	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги, методи проектів, кейс-метод, метод «мозкового штурму», ділова гра, рольова гра та інші освітні технології; самостійна робота: підготовка презентацій, рефератів; опрацювання літературних джерел та інформаційних ресурсів.	Поточний контроль: усні та письмові (опитування під час занять, тестування, обговорення завдань практичного характеру, доповідь за індивідуальною темою) відповіді студента. Підсумковий контроль – екзамен (усне або письмове опитування; тестовий контроль).
РН15. Зрозуміло і	☒	Дипломне	Дослідницький метод;	Захист кваліфікаційної

недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.		проектування (кваліфікаційна робота)	словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	(дипломної) роботи.
		Перспективні напрямки розвитку систем кіберзахисту	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; семінарські заняття: підготовка презентацій, рефератів; методи інтерактивного навчання: робота в малих групах, тренінги, метод проектів, кейс-метод, метод «мозкового штурму», ділова гра, рольова гра та інші освітні технології; лабораторні заняття: евристичний метод, метод проблемного викладу; самостійна робота: репродуктивний метод, дослідницький метод; робота з науковою та літературою професійного спрямування.	Поточний контроль: усні та письмові (тестування, захист лабораторних робіт, представлення доповідей та захист рефератів) відповіді здобувача освіти. Підсумковий контроль – екзамен (усне або письмове опитування; тестовий контроль, в тому числі засобами платформ електронного навчання).
		Науково-педагогічна діяльність та навчання персоналу в галузі ІБ	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); робота з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); інтерактивні методи навчання: робота в малих групах та тренінги, методи проектів, кейс-метод, метод «мозкового штурму», ділова гра, рольова гра та інші освітні технології; самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни (реферат, доповідь тощо).	Поточний контроль – тести, опитування (усне та письмове), представлення презентації, доповідь та аргументований захист у процесі командної роботи. Підсумковий контроль (екзамен) – усне, письмове опитування, тестовий контроль.
		Наукова та професійна комунікація іноземною мовою	Комунікативно-діяльнісний підхід, метод комунікативних завдань, система навчання CLIL та інші у традиційних формах навчального процесу (практичне заняття, консультація, самостійна робота) з використанням наочних засобів (презентації, ілюстрації, відеоматеріали, аудіювання тощо) або у змішаній формі із застосуванням електронних курсів та платформ для дистанційного навчання.	Поточний контроль – усна (доповідь, презентація) чи письмова (тестування; анотація / реферат наукової статті) відповідь студента. Підсумковий контроль (залік) – усне та письмове опитування, тестовий контроль.

РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.	☒	Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		Безпека інфокомунікацій та безперервність бізнес-процесів	Лекції: пояснювально-ілюстративний метод, презентації; робота з книгою: з навчально-методичною, науковою та нормативною літературою; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; лабораторні заняття: метод проблемного підходу, дослідницький метод; самостійна робота: підготовка презентацій, рефератів, а також формуванням напрацювань для виконання і захисту лабораторних робіт.	Поточний контроль – усні та письмові (тестування, захист лабораторних робіт, захист завдань практичного характеру) відповіді здобувача освіти. Підсумковий контроль (екзамен) – усне або письмове опитування, тестовий контроль.
РН25. Консультувати керівництво або уповноважених представників щодо рівня ризику та стану безпеки, аналізу витрат/вигоди програм, політик, процесів, систем та елементів інформаційної безпеки; надавати консультативні послуги з питань технічного та криптографічного захисту інформації.	☐	Криптографічний захист інформації	Лекції: пояснювально-ілюстративний метод; лабораторні заняття: евристичний метод, метод проблемного викладу, робота в малих групах та тренінги, методи проектів, кейс-метод, метод «мозкового штурму», ділова гра, рольова гра та інші освітні технології; самостійна робота: репродуктивний метод, дослідницький метод; опрацювання літературних джерел та інформаційних ресурсів.	Поточний контроль – виконання та захист завдань лабораторних робіт, усне та фронтальне опитування. Підсумковий контроль – залік (письмове опитування, тестовий контроль).
		Особливості проектної діяльності в кібербезпеці	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги, методи проектів, кейс-метод, метод «мозкового штурму», ділова гра, рольова гра та інші освітні технології; самостійна робота: підготовка презентацій, рефератів; опрацювання літературних джерел та інформаційних ресурсів.	Поточний контроль: усні та письмові (опитування під час занять, тестування, обговорення завдань практичного характеру, доповідь за індивідуальною темою) відповіді студента. Підсумковий контроль – екзамен (усне або письмове опитування; тестовий контроль).
		Ризик-орієнтований аналіз в кібербезпеці	Під час проведення лекційних занять використовуються пояснювально-ілюстративний метод та підхід проблемного навчання; для проведення	Поточний контроль: усні та письмові (тестування, доповіді за індивідуальними темами, захист завдань практичного характеру) відповіді здобувача освіти. Підсумковий контроль –

			практичних занять використовуються інтуїтивно-пошуковий та дослідницький методи, при яких викладач ставить перед студентами задачу, і вони розв'язують її самостійно або під керівництвом викладача, висуваючи ідеї, перевіряючи їх, знаходячи для цього необхідні дані, методи, підходи тощо; самостійна робота: опрацювання матеріалів лекцій та літературних джерел за відповідною тематикою, підготовка виступів-презентацій, рефератів; інтерактивні методи навчання: робота в малих групах та тренінги.	екзамен; передбачає усне або письмове опитування, зокрема, тестовий контроль.
		Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.	☒	Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		Безпека інфокомунікацій та безперервність бізнес-процесів	Лекції: пояснювально-ілюстративний метод, презентації; робота з книгою: з навчально-методичною, науковою та нормативною літературою; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; лабораторні заняття: метод проблемного підходу, дослідницький метод; самостійна робота: підготовка презентацій, рефератів, а також формуванням напрацювань для виконання і захисту лабораторних робіт.	Поточний контроль – усні та письмові (тестування, захист лабораторних робіт, захист завдань практичного характеру) відповіді здобувача освіти. Підсумковий контроль (екзамен) – усне або письмове опитування, тестовий контроль.
		Криптографічний захист інформації	Лекції: пояснювально-ілюстративний метод; лабораторні заняття: евристичний метод, метод проблемного викладу, робота в малих групах та тренінги, методи проектів, кейс-метод, метод «мозкового штурму», ділова гра, рольова гра та інші освітні технології; самостійна робота: репродуктивний метод, дослідницький метод;	Поточний контроль – виконання та захист завдань лабораторних робіт, усне та фронтальне опитування. Підсумковий контроль – залік (письмове опитування, тестовий контроль).

			опрацювання літературних джерел та інформаційних ресурсів.	
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	☒	Безпека інфокомунікацій та безперервність бізнес-процесів	Лекції: пояснювально-ілюстративний метод, презентації; робота з книгою: з навчально-методичною, науковою та нормативною літературою; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; лабораторні заняття: метод проблемного підходу, дослідницький метод; самостійна робота: підготовка презентацій, рефератів, а також формуванням напрацювань для виконання і захисту лабораторних робіт.	Поточний контроль – усні та письмові (тестування, захист лабораторних робіт, захист завдань практичного характеру) відповіді здобувача освіти. Підсумковий контроль (екзамен) – усне або письмове опитування, тестовий контроль.
		Технології комплексного захисту інформації	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; самостійна робота: підготовка презентацій, рефератів; робота з навчально-методичною, науковою, нормативною літературою. Дисципліною передбачене виконання курсової роботи.	Поточний контроль: усні та письмові (контрольна робота, тестування, захист завдань практичного характеру) відповіді студента, захист курсових робіт. Підсумковий контроль: екзамен (усне, письмове опитування, тестовий контроль).
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	☒	Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		Ризик-орієнтований аналіз в кібербезпеці	Під час проведення лекційних занять використовуються пояснювально-ілюстративний метод та підхід проблемного навчання; для проведення практичних занять використовуються інтуїтивно-пошуковий та дослідницький методи, при яких викладач ставить перед студентами задачу, і вони розв'язують її самостійно або під керівництвом викладача, висуваючи ідеї, перевіряючи їх, знаходячи для цього необхідні дані, методи, підходи тощо; самостійна робота: опрацювання матеріалів лекцій та літературних	Поточний контроль: усні та письмові (тестування, доповіді за індивідуальними темами, захист завдань практичного характеру) відповіді здобувача освіти. Підсумковий контроль – екзамен; передбачає усне або письмове опитування, зокрема, тестовий контроль.

			джерел за відповідною тематикою, підготовка виступів-презентацій, рефератів; інтерактивні методи навчання: робота в малих групах та тренінги.	
		Безпека інфокомунікацій та безперервність бізнес-процесів	Лекції: пояснювально-ілюстративний метод, презентації; робота з книгою: з навчально-методичною, науковою та нормативною літературою; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; лабораторні заняття: метод проблемного підходу, дослідницький метод; самостійна робота: підготовка презентацій, рефератів, а також формуванням напрацювань для виконання і захисту лабораторних робіт.	Поточний контроль – усні та письмові (тестування, захист лабораторних робіт, захист завдань практичного характеру) відповіді здобувача освіти. Підсумковий контроль (екзамен) – усне або письмове опитування, тестовий контроль.
РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.	☒	Безпека інфокомунікацій та безперервність бізнес-процесів	Лекції: пояснювально-ілюстративний метод, презентації; робота з книгою: з навчально-методичною, науковою та нормативною літературою; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; лабораторні заняття: метод проблемного підходу, дослідницький метод; самостійна робота: підготовка презентацій, рефератів, а також формуванням напрацювань для виконання і захисту лабораторних робіт.	Поточний контроль – усні та письмові (тестування, захист лабораторних робіт, захист завдань практичного характеру) відповіді здобувача освіти. Підсумковий контроль (екзамен) – усне або письмове опитування, тестовий контроль.
		Технології комплексного захисту інформації	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; самостійна робота: підготовка презентацій, рефератів; робота з навчально-методичною, науковою, нормативною літературою. Дисципліною передбачене виконання курсової роботи.	Поточний контроль: усні та письмові (контрольна робота, тестування, захист завдань практичного характеру) відповіді студента, захист курсових робіт. Підсумковий контроль: екзамен (усне, письмове опитування, тестовий контроль).
		Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з літературою професійного спрямування; самостійна	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.

			робота: репродуктивний метод, дослідницький метод.	
РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	☒	Дипломне проектування (кваліфікаційна робота)	Дослідницький метод; словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Захист кваліфікаційної (дипломної) роботи.
		Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		Наукова та професійна комунікація іноземною мовою	Комунікативно-діяльнісний підхід, метод комунікативних завдань, система навчання CLIL та інші у традиційних формах навчального процесу (практичне заняття, консультація, самостійна робота) з використанням наочних засобів (презентації, ілюстрації, відеоматеріали, аудіювання тощо) або у змішаній формі із застосуванням електронних курсів та платформ для дистанційного навчання.	Поточний контроль – усна (доповідь, презентація) чи письмова (тестування; анотація / реферат наукової статті) відповідь студента. Підсумковий контроль (залік) – усне та письмове опитування, тестовий контроль.
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.	☒	Дипломне проектування (кваліфікаційна робота)	Дослідницький метод; словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Захист кваліфікаційної (дипломної) роботи.
		Переддипломна практика	Дослідницький метод; пояснення; бесіда; дискусія, робота з навчально-методичною та фаховою літературою, самостійна робота, проведення досліджень за обраною темою.	Поточний контроль - презентація результатів виконання завдань. Підсумковий контроль (залік) – доповідь за отриманими під час проходження переддипломної практики результатами на випусковій кафедрі.

		Особливості проектної діяльності в кібербезпеці	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги, методи проектів, кейс-метод, метод «мозкового штурму», ділова гра, рольова гра та інші освітні технології; самостійна робота: підготовка презентацій, рефератів; опрацювання літературних джерел та інформаційних ресурсів.	Поточний контроль: усні та письмові (опитування під час занять, тестування, обговорення завдань практичного характеру, доповідь за індивідуальною темою) відповіді студента. Підсумковий контроль – екзамен (усне або письмове опитування; тестовий контроль).
		Перспективні напрямки розвитку систем кіберзахисту	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; семінарські заняття: підготовка презентацій, рефератів; методи інтерактивного навчання: робота в малих групах, тренінги, метод проектів, кейс-метод, метод «мозкового штурму», ділова гра, рольова гра та інші освітні технології; лабораторні заняття: евристичний метод, метод проблемного викладу; самостійна робота: репродуктивний метод, дослідницький метод; робота з науковою та літературою професійного спрямування.	Поточний контроль: усні та письмові (тестування, захист лабораторних робіт, представлення доповідей та захист рефератів) відповіді здобувача освіти. Підсумковий контроль – екзамен (усне або письмове опитування; тестовий контроль, в тому числі засобами платформ електронного навчання).
		Наукова та професійна комунікація іноземною мовою	Комунікативно-діяльнісний підхід, метод комунікативних завдань, система навчання CLIL та інші у традиційних формах навчального процесу (практичне заняття, консультація, самостійна робота) з використанням наочних засобів (презентації, ілюстрації, відеоматеріали, аудіювання тощо) або у змішаній формі із застосуванням електронних курсів та платформ для дистанційного навчання.	Поточний контроль – усна (доповідь, презентація) чи письмова (тестування; анотація / реферат наукової статті) відповідь студента. Підсумковий контроль (залік) – усне та письмове опитування, тестовий контроль.
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.	☒	Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		Перспективні напрямки розвитку систем кіберзахисту	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; семінарські заняття: підготовка презентацій,	Поточний контроль: усні та письмові (тестування, захист лабораторних робіт, представлення доповідей та захист рефератів) відповіді

			рефератів; методи інтерактивного навчання: робота в малих групах, тренінги, метод проектів, кейс-метод, метод «мозкового штурму», ділова гра, рольова гра та інші освітні технології; лабораторні заняття: евристичний метод, метод проблемного викладу; самостійна робота: репродуктивний метод, дослідницький метод; робота з науковою та літературою професійного спрямування.	здобувача освіти. Підсумковий контроль – екзамен (усне або письмове опитування; тестовий контроль, в тому числі засобами платформ електронного навчання).
		Моделювання та оптимізація процесів у ІБ	Лекції: пояснювально-ілюстративний метод, презентації; робота з навчально-методичною, науковою літературою; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: підключення до освітніх порталів (Coursera); самостійна робота: підготовка презентацій, рефератів, а також формуванням напрацювань для виконання і захисту практичних робіт.	Поточний контроль – усні та письмові (тестування) відповіді здобувача освіти, доповіді та аргументований захист під час проведення підсумкового оцінювання. Підсумковий контроль – залік.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	☒	Дипломне проектування (кваліфікаційна робота)	Дослідницький метод; словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Захист кваліфікаційної (дипломної) роботи.
		Переддипломна практика	Дослідницький метод; пояснення; бесіда; дискусія, робота з навчально-методичною та фаховою літературою, самостійна робота, проведення досліджень за обраною темою.	Поточний контроль - презентація результатів виконання завдань. Підсумковий контроль (залік) – доповідь за отриманими під час проходження переддипломної практики результатами на випусковій кафедрі.
		Криптографічний захист інформації	Лекції: пояснювально-ілюстративний метод; лабораторні заняття: евристичний метод, метод проблемного викладу, робота в малих групах та тренінги, методи проектів, кейс-метод, метод «мозкового штурму», ділова гра, рольова гра та інші освітні технології; самостійна робота: репродуктивний метод, дослідницький метод; опрацювання літературних	Поточний контроль – виконання та захист завдань лабораторних робіт, усне та фронтальне опитування. Підсумковий контроль – залік (письмове опитування, тестовий контроль).

			джерел та інформаційних ресурсів.	
		Перспективні напрямки розвитку систем кіберзахисту	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; семінарські заняття: підготовка презентацій, рефератів; методи інтерактивного навчання: робота в малих групах, тренінги, метод проектів, кейс-метод, метод «мозкового штурму», ділова гра, рольова гра та інші освітні технології; лабораторні заняття: евристичний метод, метод проблемного викладу; самостійна робота: репродуктивний метод, дослідницький метод; робота з науковою та літературою професійного спрямування.	Поточний контроль: усні та письмові (тестування, захист лабораторних робіт, представлення доповідей та захист рефератів) відповіді здобувача освіти. Підсумковий контроль – екзамен (усне або письмове опитування; тестовий контроль, в тому числі засобами платформ електронного навчання).
		Технології комплексного захисту інформації	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; самостійна робота: підготовка презентацій, рефератів; робота з навчально-методичною, науковою, нормативною літературою. Дисципліною передбачене виконання курсової роботи.	Поточний контроль: усні та письмові (контрольна робота, тестування, захист завдань практичного характеру) відповіді студента, захист курсових робіт. Підсумковий контроль: екзамен (усне, письмове опитування, тестовий контроль).
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	☒	Технології комплексного захисту інформації	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; самостійна робота: підготовка презентацій, рефератів; робота з навчально-методичною, науковою, нормативною літературою. Дисципліною передбачене виконання курсової роботи.	Поточний контроль: усні та письмові (контрольна робота, тестування, захист завдань практичного характеру) відповіді студента, захист курсових робіт. Підсумковий контроль: екзамен (усне, письмове опитування, тестовий контроль).
		Ризик-орієнтований аналіз в кібербезпеці	Під час проведення лекційних занять використовуються пояснювально-ілюстративний метод та підхід проблемного навчання; для проведення практичних занять використовуються інтуїтивно-пошуковий та дослідницький методи, при	Поточний контроль: усні та письмові (тестування, доповіді за індивідуальними темами, захист завдань практичного характеру) відповіді здобувача освіти. Підсумковий контроль – екзамен; передбачає усне або письмове опитування, зокрема, тестовий контроль.

			яких викладач ставить перед студентами задачу, і вони розв'язують її самостійно або під керівництвом викладача, висуваючи ідеї, перевіряючи їх, знаходячи для цього необхідні дані, методи, підходи тощо; самостійна робота: опрацювання матеріалів лекцій та літературних джерел за відповідною тематикою, підготовка виступів-презентацій, рефератів; інтерактивні методи навчання: робота в малих групах та тренінги.	
		Безпека інфокомунікацій та безперервність бізнес-процесів	Лекції: пояснювально-ілюстративний метод, презентації; робота з книгою: з навчально-методичною, науковою та нормативною літературою; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; лабораторні заняття: метод проблемного підходу, дослідницький метод; самостійна робота: підготовка презентацій, рефератів, а також формуванням напрацювань для виконання і захисту лабораторних робіт.	Поточний контроль – усні та письмові (тестування, захист лабораторних робіт, захист завдань практичного характеру) відповіді здобувача освіти. Підсумковий контроль (екзамен) – усне або письмове опитування, тестовий контроль.
РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.	☒	Технології комплексного захисту інформації	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; самостійна робота: підготовка презентацій, рефератів; робота з навчально-методичною, науковою, нормативною літературою. Дисципліною передбачене виконання курсової роботи.	Поточний контроль: усні та письмові (контрольна робота, тестування, захист завдань практичного характеру) відповіді студента, захист курсових робіт. Підсумковий контроль: екзамен (усне, письмове опитування, тестовий контроль).
		Перспективні напрямки розвитку систем кіберзахисту	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; семінарські заняття: підготовка презентацій, рефератів; методи інтерактивного навчання: робота в малих групах, тренінги, метод проектів, кейс-метод, метод «мозкового штурму», ділова гра, рольова гра та інші освітні технології; лабораторні заняття: евристичний метод, метод проблемного викладу; самостійна робота: репродуктивний метод,	Поточний контроль: усні та письмові (тестування, захист лабораторних робіт, представлення доповідей та захист рефератів) відповіді здобувача освіти. Підсумковий контроль – екзамен (усне або письмове опитування; тестовий контроль, в тому числі засобами платформ електронного навчання).

			дослідницький метод; робота з науковою та літературою професійного спрямування.	
		Переддипломна практика	Дослідницький метод; пояснення; бесіда; дискусія, робота з навчально-методичною та фаховою літературою, самостійна робота, проведення досліджень за обраною темою.	Поточний контроль - презентація результатів виконання завдань. Підсумковий контроль (залік) – доповідь за отриманими під час проходження переддипломної практики результатами на випусковій кафедрі.
		Дипломне проектування (кваліфікаційна робота)	Дослідницький метод; словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Захист кваліфікаційної (дипломної) роботи.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	☒	Дипломне проектування (кваліфікаційна робота)	Дослідницький метод; словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Захист кваліфікаційної (дипломної) роботи.
		Переддипломна практика	Дослідницький метод; пояснення; бесіда; дискусія, робота з навчально-методичною та фаховою літературою, самостійна робота, проведення досліджень за обраною темою.	Поточний контроль - презентація результатів виконання завдань. Підсумковий контроль (залік) – доповідь за отриманими під час проходження переддипломної практики результатами на випусковій кафедрі.
		Ліцензування, атестація і сертифікація у сфері безпеки об'єктів інформаційної діяльності	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); практичні заняття: наочні інформаційної діяльності методи (презентації, ілюстрації, тощо); інтерактивні методи навчання: робота в малих групах та тренінги; робота з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари	Поточний контроль – усні та письмові (тестування) відповіді студента; представлення презентації, доповідь та аргументований захист у процесі командної роботи. Підсумковий контроль (екзамен) – усне, письмове опитування, тестовий контроль.

			тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни (реферат, доповідь тощо). здобувача освіти.	
		Технології комплексного захисту інформації	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; самостійна робота: підготовка презентацій, рефератів; робота з навчально-методичною, науковою, нормативною літературою. Дисципліною передбачене виконання курсової роботи.	Поточний контроль: усні та письмові (контрольна робота, тестування, захист завдань практичного характеру) відповіді студента, захист курсових робіт. Підсумковий контроль: екзамен (усне, письмове опитування, тестовий контроль).
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	☒	Безпека інфокомунікацій та безперервність бізнес-процесів	Лекції: пояснювально-ілюстративний метод, презентації; робота з книгою: з навчально-методичною, науковою та нормативною літературою; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; лабораторні заняття: метод проблемного підходу, дослідницький метод; самостійна робота: підготовка презентацій, рефератів, а також формуванням напрацювань для виконання і захисту лабораторних робіт.	Поточний контроль – усні та письмові (тестування, захист лабораторних робіт, захист завдань практичного характеру) відповіді здобувача освіти. Підсумковий контроль (екзамен) – усне або письмове опитування, тестовий контроль.
		Технології комплексного захисту інформації	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; самостійна робота: підготовка презентацій, рефератів; робота з навчально-методичною, науковою, нормативною літературою. Дисципліною передбачене виконання курсової роботи.	Поточний контроль: усні та письмові (контрольна робота, тестування, захист завдань практичного характеру) відповіді студента, захист курсових робіт. Підсумковий контроль: екзамен (усне, письмове опитування, тестовий контроль).
		Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з літературою професійного спрямування; самостійна	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.

			робота: репродуктивний метод, дослідницький метод.	
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	☒	Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		Безпека інфокомунікацій та безперервність бізнес-процесів	Лекції: пояснювально-ілюстративний метод, презентації; робота з книгою: з навчально-методичною, науковою та нормативною літературою; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; лабораторні заняття: метод проблемного підходу, дослідницький метод; самостійна робота: підготовка презентацій, рефератів, а також формуванням напрацювань для виконання і захисту лабораторних робіт.	Поточний контроль – усні та письмові (тестування, захист лабораторних робіт, захист завдань практичного характеру) відповіді здобувача освіти. Підсумковий контроль (екзамен) – усне або письмове опитування, тестовий контроль.
		Технології комплексного захисту інформації	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; самостійна робота: підготовка презентацій, рефератів; робота з навчально-методичною, науковою, нормативною літературою. Дисципліною передбачене виконання курсової роботи.	Поточний контроль: усні та письмові (контрольна робота, тестування, захист завдань практичного характеру) відповіді студента, захист курсових робіт. Підсумковий контроль: екзамен (усне, письмове опитування, тестовий контроль).