НАЦІОНАЛЬНЕ АГЕНТСТВО ІЗ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	**Чернівецький національний університет імені Юрія Федьковича**
Освітня програма	**2402 Кібербезпека**
Рівень вищої освіти	**Магістр**
Спеціальність	**125 Кібербезпека**

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	**Петришин Роман Іванович**
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	**2402**
Назва ОП	**Кібербезпека**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека**
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	**Факультет педагогіки, психології та соціальної роботи, кафедра педагогіки та методики початкової освіти; Факультет іноземних мов, кафедра іноземних мов для природничих факультетів; 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(037)-250-94-89**
Додатковий телефон гаранта ОП	**+38(050)-978-50-14**

Форми здобуття освіти на ОП	Термін навчання
очна денна	1 р. 4 міс.
заочна	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 відповідає кафедра радіотехніки та інформаційної безпеки Навчально-наукового інституту фізико-технічних та комп'ютерних наук ЧНУ. Остання чинна редакція ОП затверджена Вченою радою ЧНУ 3.04.2023 р. (прот. №3) і введена в дію наказом №118 від 3.04.2023 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. З того часу науковцями кафедри захищена низка кандидатських дисертацій (Косован Г.В. (2019 р.) за спеціальністю 05.13.21 – Системи захисту інформації під керівництвом доцента кафедри Кушніра М.Я.; Гресь О.В. (2020 р.) за спеціальністю 05.13.21 – Системи захисту інформації під керівництвом професора кафедри Політанського Р.Л.) та опубліковано значна кількість наукових праць у рейтингових міжнародних журналах.
Зміст ОПП регулярно оновлюється. Усі зміни були пов'язані із актуалізацією освітньої програми по відношенню до Законодавства України, внутрішніх положень ЧНУ та вимог стейкголдерів. Робоча група проводить зустрічі та опитування 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.

5. Інформація про контингент здобувачів вищої освіти на ОП станом на 1 жовтня поточного навчального року у розрізі форм здобуття освіти та набір на ОП (кількість здобувачів, зарахованих на навчання у відповідному навчальному році сумарно за усіма формами здобуття освіти)

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	2023 - 2024	22	22	0	0	0
2 курс	2022 - 2023	63	58	5	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	**22992 Лінгвістичне забезпечення кібербезпеки** **22991 Кібербезпека**
другий (магістерський) рівень	**2402 Кібербезпека** **3250 Системи технічного захисту інформації**
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	32509
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_Mag_2022.pdf*	MZJc4TIe+ufeqiuZxZPC3PRXylFWt6r53v6kcmZhRT4=
Освітня програма	*ОПП_(ЧНУ)_125_Mag_2023.pdf*	c68jPmtc5lKWyk7rngZBQ9hwsT9SQIe9x1Ft2hakpuw=
Навчальний план за ОП	*План_маг_125_2023.pdf*	g1b85d2EEgsvP/6WGH6+R+e17iqV2PlQ0ofO7oPvt7Y=
Навчальний план за ОП	*План_маг_125_2022.pdf*	b5d1FX1mdD1qYNwU/Tokzg2mQcjX9EBk1dj10QRXVds=
Рецензії та відгуки роботодавців	*Рец_ВНТУ_2022.pdf*	pYIfZI6XN3GJLMjYcb730FoFeEbc6k1Hv16kXERxfBk=
Рецензії та відгуки роботодавців	*Рец_кіберполіція_2022.pdf*	ed46xCJuPwMYOShYkpy6XvtZrglgMMZiQgqGdMbNLmI=
Рецензії та відгуки роботодавців	*Рецензія_Datami_2023.pdf*	LhSuBfKerH8uLozYZ54SMNCLGrFh/QzLd/t5Ka1v+gc=

1. Проектування та цілі освітньої програми

Якими є цілі ОП? У чому полягають особливості (унікальність) цієї програми?

Основною ціллю освітньо-професійної програми є підготовка висококваліфікованих фахівців у галузі інформаційних технологій зі спеціальності 125 – Кібербезпека, здатних вирішувати складні спеціалізовані задачі та практичні проблеми інформаційної безпеки, захищеності інформаційного і кіберпросторів окремих суб'єктів або держави в цілому від ризику стороннього кібернетичного впливу.
Унікальністю освітньо-професійної програми є те, що в ній реалізований студентоцентрований підхід і передбачена підготовка високопрофесійних, конкурентоспроможних фахівців у сфері інформаційної безпеки та кіберзахисту на основі співпраці з підприємствами, комерційними компаніями, організаціями та державними установами Західного регіону (зокрема, Держспецзв'язку, Національна поліція України, СБУ, ІТ-компанії Datami, SoftServe тощо), науково-дослідними та освітніми закладами України та інших країн, з урахуванням індивідуальних запитів здобувачів.

Продемонструйте, із посиланням на конкретні документи ЗВО, що цілі ОП відповідають місії та стратегії ЗВО

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) ОПП «Кібербезпека» відповідає місії ЧНУ, яка передбачає інноваційність, 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 (https://bit.ly/3D95Qta; https://bit.ly/3QnyOIw), в результаті чого коригуються цілі 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.

Опишіть, яким чином інтереси та пропозиції таких груп заінтересованих сторін (стейкхолдерів) були враховані під час формулювання цілей та програмних результатів навчання ОП:
- здобувачі вищої освіти та випускники програми

Результати моніторингу відгуків та пропозицій здобувачів ВО щодо змісту та організації освітнього процесу показують, що студенти прагнуть 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/dcozh; https://bit.ly/3PAWOLn).
Ці пропозиції аналізуються на засіданнях випускової кафедри та Вченої ради ННІФТКН, на підставі чого вносяться зміни та доповнюється наповнення обов'язкових ОК, перелік вибіркових ОК, а також коригуються форми й методи організації освітнього процесу тощо. Зокрема, враховано пропозицію здобувача Пархоменка Є. відносно розширення переліку вибіркових ОК дисципліною «Математичні основи нейромереж», а здоб. Рижаковою В. запропоновано приділити більше уваги проблемам захисту персональних даних та протидії соціальній інженерії, що відображено у введенні відповідної теми в ЗПО2 та доповненні переліку вибіркових дисциплін курсом «Захист персональних даних та соціальна інженерія». Ці пропозиції підтримані проектною групою для підсилення РН 2, 3, 5, 13, 20, 24 чинної на момент пропозиції редакції ОП, затверджені на засіданнях кафедри (прот. №16, 16.02.2022; №16, 21.04.2023).

- роботодавці

Випусковою кафедрою проводяться зустрічі з роботодавцями та обговорення вимог до фахівця на ринку праці (зокрема, https://bit.ly/3R6NZKp). В результаті такої взаємодії з урахуванням специфіки та пропозицій роботодавців (державних установ, Держспецзв'язку, Департаменту кіберполіції Національної поліції України, представників Чернівецького IT Кластера тощо) здійснюється формування та коригування цілей та програмних результатів навчання 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 (https://bit.ly/482sgt4, https://bit.ly/3R6A7Qk) були запроваджені визначені освітньою програмою компетентність КФ11 та РН24. До компонент освітньо-професійної програми було введено дисципліну ППО7 «Безпека інфокомунікацій та безперервність бізнес-процесів», що відповідає РН 1, 5-8, 10-14, 16, 20, 22, 24 (пропозиція представників компаній Datami та SoftServe); це відображено у протоколі засідання випускової кафедри №16 від 16.02.2022 р. та затверджено Вченою радою ЧНУ (протокол №4 від 28.03.2022) в оновленій редакції ОПП «Кібербезпека» (http://radiotech.chnu.edu.ua/opp_125_master/). Також представники роботодавців залучаються до проведення занять, планування тематики кваліфікаційних проектів і робіт, рецензування та їх подальшого впровадження.

- академічна спільнота

Співпраця з представниками українських та закордонних ЗВО дозволяє враховувати інтереси академічної спільноти у формуванні цілей та програмних результатів ОПП «Кібербезпека» через обмін досвідом та обговорення під час науково-методичних секцій міжвузівських та міжнародних наукових конференцій, семінарів, круглих столів (https://cutt.ly/CVaPFYb, http://surl.li/dbhtf, https://bit.ly/3Ex4cB7).
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 цілей 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 у 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 «Integration of new Cybersecurity courses into the Curriculum of the Yuriy Fedkovych Chernivtsi National University», https://bit.ly/3Z6jTIS, проект USAID "Кібербезпека критично важливої інфраструктури України").

- 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 цілей та РН ОП кожна із зацікавлених сторін надавала свої пропозиції щодо її наповнення, враховані при регулярному оновленні ОП. Більшість з наданих пропозицій ґрунтувались на результатах дослідження ринку праці, законодавчих документах МОН України, можливостях працевлаштування магістрів (https://bit.ly/3r2uBn8, https://bit.ly/3QnyOIw).
Водночас випусковою кафедрою проводиться активна робота й з іншими зацікавленими сторонами (http://doncv.gov.ua/?p=2925). Також налагоджена співпраця з установами, що відповідають за забезпечення комплексного вирішення питань регулювання зайнятості населення, профорієнтації та працевлаштування громадян. У 2020 р. спільно з фахівцями підрозділів Чернівецького обласного центру зайнятості для учасників АТО/ООС та безробітних організовані зустрічі, на яких було презентовано спеціальності, які можна здобути в ННІФТКН ЧНУ та надано інформацію щодо професійного навчання (https://bit.ly/3r3BDVg, https://cutt.ly/kVmhxHd). За підсумками обговорень освітніх компонент ОП внесено корективи, спрямовані на

адаптацію потенційних здобувачів до вивчення дисциплін. Зокрема, у ЗПО1, ППО1, ППО2 ОПП «Кібербезпека» розширено коло питань вступних тем, доповнено перелік завдань самостійного опрацювання.

Продемонструйте, яким чином цілі та програмні результати навчання ОП відбивають тенденції розвитку спеціальності та ринку праці

Впродовж останніх років відзначається стрімкий розвиток різноманітних інформаційних і телекомунікаційних технологій, які у свою чергу стимулюють розвиток і застосування новітніх інструментів захисту інформації. Це зумовлює потребу у висококваліфікованих фахівцях спеціальності 125 – Кібербезпека, яка особливо загострилася у зв'язку з військовими діями в Україні (https://bit.ly/44H6ic3). Зазначені тенденції враховані під час формулювання цілей та програмних результатів навчання ОПП «Кібербезпека». Компетентності випускників, здатних забезпечувати захист об'єктів критичної інфраструктури, великих бізнес-корпорацій та малого бізнесу, працювати у компаніях фахового профілю та споріднених галузей, у повній мірі узгоджуються з програмними результатами ОП, сформульованими у відповідності до чинного стандарту освіти. Також конкурентна перевага на ринку праці підсилюється програмним результатом РН 24, набуття якого готує здобувачів до роботи в умовах реального бізнесу, розвиває навички організації навчання персоналу і протидії проявам соціальної інженерії.
Кафедрою радіотехніки та інформаційної безпеки та ЧНУ загалом укладено низку договорів про співпрацю з держустановами, комерційними компаніями (https://bit.ly/44Hnmic, https://bit.ly/3D95Qta), згідно з якими студенти проходять практику та працевлаштовуються. В такий спосіб здобувачі освіти мають можливість адаптуватися до тенденцій розвитку спеціальності та реальних вимог ринку праці.

Продемонструйте, яким чином під час формулювання цілей та програмних результатів навчання ОП було враховано галузевий та регіональний контекст

Під час формулювання цілей та РН, що передбачає врахування галузевого та регіонального контекстів, у процес розробки освітньої програми залучається широке коло стейкхолдерів, переважно регіонального рівня.
Галузевий контекст ОП у повній мірі відбиває особливості та вимоги галузі інформаційних технологій у розвитку економіки України, що знаходить підтвердження у питаннях змісту, форми та методів теоретичної та практичної підготовки з максимальним наближенням до реальних умов праці. Оволодіння випускником програмними результатами навчання та компонентами ОП, що їх реалізують, забезпечує йому досягнення високого професійного рівня та дозволяє ефективно конкурувати на ринку праці.
На регіональному рівні тенденції розвитку ОПП «Кібербезпека» враховують відповідні програми і плани розвитку Чернівецької області на період до 2027 року (https://bukoda.gov.ua/documents/strategiya-rovzitku-oblasti). В цьому аспекті фахівці, здатні вирішувати складні спеціалізовані задачі та практичні проблеми інформаційної безпеки, захищеності інформаційного і кіберпросторів окремих суб'єктів або держави в цілому від ризику стороннього кібернетичного впливу, затребувані у багатьох держустановах, держструктурах та їх підрозділах, на промислових підприємствах та в ІТ-компаніях м. Чернівці та Західного регіону.
Формування індивідуальної освітньої траєкторії здобувачів освіти з врахуванням регіонального контексту забезпечується створенням і постійним оновленням відповідного набору вибіркових ОК.

Продемонструйте, яким чином під час формулювання цілей та програмних результатів навчання ОП було враховано досвід аналогічних вітчизняних та іноземних програм

Під час формулювання цілей та РН ОП враховано досвід провідних ЗВО України, зокрема: НУ «Львівська політехніка», ХНУРЕ, КНУ ім. Тараса Шевченка, НТУ «Дніпровська політехніка», а також ОПП «Кібербезпека» ТНТУ та ОПП «Кібербезпека інформаційних технологій та систем» ВНТУ. Аналіз програм цих та інших ЗВО сприяв удосконаленню структурно-логічної схеми ОП та дозволив сформувати підходи до організації практичної підготовки здобувачів. На зустрічах та методичних семінарах в рамках науково-практичних конференцій (https://cutt.ly/CVaPFYb) за участі представників зазначених ЗВО, розробники ОПП «Кібербезпека» ЧНУ обговорювали ключові питання формування і оновлення ОП. Викладачі цих ЗВО залучаються до проведення окремих лекцій.
У формулюванні цілей та РН ОП враховано досвід іноземних 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 ознайомлюються з подібними ОП підготовки магістрів у іноземних ЗВО. Наприклад, Шпатар П.М., Ластівка Г.І., Гресь О.В. стажувалися на факультеті електронної інженерії та інформаційних технологій університету «Люблінська політехніка» (Польща) 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.

Продемонструйте, яким чином ОП дозволяє досягти результатів навчання, визначених стандартом вищої освіти за відповідною спеціальністю та рівнем вищої освіти

ОПП «Кібербезпека» підготовки здобувачів другого (магістерського) рівня вищої освіти розроблялась у 2017 році за відсутності стандарту освіти. У 2018 році вона успішно пройшла акредитацію, а після затвердження Стандарту освіти (https://mon.gov.ua/storage/app/media/vyshcha/standarty/2021/03/19/125%20Kiberbezpeka_mahistr_18_03_21_332.docx) була приведена у відповідність йому.
Для досягнення результатів навчання:
– цілі ОП визначено із урахуванням нормативних вимог Стандарту вищої освіти до компетентностей та програмних результатів підготовки здобувачів ВО за спеціальністю 125 – Кібербезпека другого (магістерського) рівня вищої освіти;

– згідно Стандарту вищої освіти, теоретичний зміст ОП включає теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки;
– в ОП введено перелік обов'язкових компонент, які сприяють формуванню усіх компетентностей (інтегральної, загальних та фахових), визначених Стандартом вищої освіти;
– створено можливості для використання методів, моделей, методик та технологій створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методів та моделей розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки; технологій, методів та моделей дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі;
– в ОП передбачене застосування засобів, пристроїв, мережного устаткування та середовища, прикладного та спеціалізованого програмного забезпечення, автоматизованих систем та комплексів проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методів і моделей теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки;
– згідно Стандарту вищої освіти в ОП передбачено можливість вільного вибору дисциплін (27,8 %) для формування індивідуальної освітньої траєкторії здобувачів вищої освіти;
– ОП передбачає використання в освітньому процесі платформ Moodle, Google Meet, Zoom для формування компетентностей та контролю програмних результатів навчання

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?

РН ОПП «Кібербезпека» відповідають Стандарту вищої освіти за спеціальністю 125 - Кібербезпека за другим (магістерським) рівнем.

2. Структура та зміст освітньої програми

Яким є обсяг ОП (у кредитах ЄКТС)?

90

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

65

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

25

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

Зміст та освітні компоненти ОП являють собою логічно взаємопов'язану систему та в сукупності дають можливість досягти заявлених цілей та РН, що відповідають предметній галузі спеціальності 125 – Кібербезпека. Програма має прикладне спрямування і орієнтована на здобуття студентами професійних знань, умінь, навичок, загальних та фахових компетентностей для успішного здійснення професійної діяльності. Основний фокус освітньої програми спрямовано на спеціальну освіту та професійну підготовку в галузі знань 12 – Інформаційні технології за спеціальністю 125 – Кібербезпека. Акцент робиться на підготовку фахівців, здатних розробляти, організовувати й підтримувати комплекс заходів щодо забезпечення інформаційної безпеки з урахуванням їхньої адміністративно-управлінської й технічної реалізації, економічної доцільності, можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації, у тому числі криптографічних та програмно-апаратних засобів.
Досягнення цілей та програмних результатів навчання забезпечується обов'язковими компонентами, що відображено у матриці відповідності ОП.
Під час засвоєння освітніх компонент здобувачі оволодівають сучасними методами та технологіями, що необхідні для вирішення фахових та дослідницьких завдань з розроблення нових чи удосконалення існуючих технологій і засобів захисту інформації. Реалізація освітніх компонент передбачає поєднання лекційних занять з виконанням практичних робіт, лабораторного практикуму, курсового проектування, підготовкою матеріалів та доповідей наукового та практичного характеру. ОП містить також практичну складову, до якої входять в тому числі виробнича (ППО8) та переддипломна практики (ППО9), які спрямовані на закріплення теоретичних знань, отриманих в період навчання, набуття нових фахових практичних навичок та умінь самостійно вирішувати професійні завдання в умовах, наближених до умов реального підприємства чи організації. Виконання та захист випускової

кваліфікаційної роботи/проекту (ППО10) дозволяє здобувачу продемонструвати рівень засвоєння освітніх компонент, що враховують усі програмні результати навчання ОП.
До освітніх компонент вибіркового блоку ОП можливе залучення інших кафедр НН ІФТКН та університету, стейкхолдерів та роботодавців.

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://cutt.ly/oVO1vSt). Результативність такого підходу підтверджується наявністю патентів (наприклад, https://iprop-ua.com/inv/7ccvpfhi), актів впровадження у виробництво та освітній процес розробок магістрів (http://radiotech.chnu.edu.ua/or_master_125/).

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 27,8% кредитів ЄКТС від загального обсягу.
Перелік вибіркових дисциплін підготовки магістра за ОПП «Кібербезпека» визначається випусковою кафедрою (http://radiotech.chnu.edu.ua/opp_125_master/).
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 ОП «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://bit.ly/3D95Qta). 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, які відповідають цілям та результатам навчання ОП результатам навчання ОП

В ОП передбачена сукупність навчальних дисциплін, що сприяють не лише набуттю професійних, але і 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 освітніх компонентах «Проф. комунікація іноземною мовою» (ЗПО1), «Наук.-пед. діяльність та навчання персоналу в галузі ІБ» (ЗПО2), «Перспективні напрямки розвитку систем кіберзахисту» (ППО3), «Особливості проектної діяльності в кібербезпеці» (ППО4). Дисципліни, що передбачають групову форму виконання лабораторних робіт («Вибрані розділи криптології» (ППО5), «Безпека інфоком. та безперервність бізнес-процесів» (ППО7)), практики (ППО8, ППО9) 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 професійну термінологію, займають консультації перед захистом дипломних робіт, що регулярно проводяться викладачами випускової кафедри протягом місяця, що передує фінальному захисту (ППО10) в ЕК. На цих зустрічах (останнім часом 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.

Яким чином зміст ОП ураховує вимоги відповідного професійного стандарту?

Професійний стандарт за спеціальністю відсутній.
Загалом, 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 (протокол № 7 від 31.08.2020 р.)
(https://drive.google.com/file/d/14UAVRHptFJkoS4NW5h35lDhfpsqOsyrp/view).
Фахівці з кібербезпеки можуть працювати, згідно з чинною редакцією Національного класифікатора України: Класифікатор професій (Зміна № 10 до ДК 003:2010):
2139.2 Розробник систем захисту інформації;
2139.2 Аналітик загроз безпеки;
2139.2 Аналітик систем захисту інформації та оцінки вразливостей;
2139.2 Аналітик з безпеки інформаційно-телекомунікаційних систем;
2139.2 Фахівець з криптографічного захисту інформації;
2139.2 Фахівець з питань безпеки у сфері інформаційно-комунікаційних технологій;
2139.2 Фахівець з реагування на інциденти кібербезпеки;
2139.2 Фахівець з підтримки інфраструктури кіберзахисту;
2139.2 Фахівець з технічного захисту інформації;
2139.2 Фахівець з тестування систем захисту інформації;
2139.2 Фахівець сфери захисту інформації;
2359.2 Інструктор-методист інформаційної безпеки та кібербезпеки.

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

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. Обсяг освітніх компонентів ОПП «Кібербезпека» відповідає фактичному навантаженню здобувачів, досягненню цілей та програмних результатів навчання. Обсяг підготовки магістрів становить 90 кредитів, з них
- загальна підготовка – 8 кредитів (8,9 %);
- професійна підготовка – 57 кредитів (63,3 %);
- вибіркові освітні компоненти – 25 кредитів (27,8 %).
Для самостійного та дистанційного навчання використовується система електронного навчання Moodle.
При складанні розкладу занять враховуються норми навантаження здобувачів, відведена кількість аудиторних годин достатня для виконання самостійної роботи. Середній обсяг одного обов'язкового компонента ОП становить 5,4 кредитів, а мінімальний – 3 кредити. Співвідношення між обсягом аудиторних та самостійних годин для ОК цього блоку коливається від 1/1,8 до 1/3.
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. Ефективність самостійної роботи оцінюється на проміжному та підсумковому контролі. У робочих програмах наводиться визначений перелік матеріалу та контрольні питання для самостійного опрацювання.

Якщо за ОП здійснюється підготовка здобувачів вищої освіти за дуальною формою освіти, продемонструйте, яким чином структура освітньої програми та навчальний план зумовлюються завданнями та особливостями цієї форми здобуття освіти

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 впровадження елементів дуальної форми навчання в освітній процес ЧНУ» (https://drive.google.com/file/d/1_cEMtri8-6HmaoEaQTfQXpRtz_gCgxa2/view).
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.

3. Доступ до освітньої програми та визнання результатів навчання

Наведіть посилання на веб-сторінку, 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 Умов прийому на навчання до закладів вищої освіти України в 2023 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. Вступ до ОП здійснюється на конкурсній основі за відповідними джерелами фінансування та в межах ліцензованого обсягу за спеціальністю.

Яким документом ЗВО регулюється питання визнання результатів навчання, отриманих в інших ЗВО? Яким чином забезпечується його доступність для учасників освітнього процесу?

Згідно з «Положенням про порядок реалізації права на академічну мобільність здобувачів вищої освіти ЧНУ» (протокол №6 від 30.06.2020 р.) (https://bit.ly/3SxJFkT) та «Положенням про порядок відрахування, переривання навчання, поновлення, переведення, надання академічної відпустки здобувачам вищої освіти ЧНУ» (протокол №2 від 27.02.2020 р.) (https://cutt.ly/3VAUgda), 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 вищої освіти з власної ініціативи, підтриманої адміністрацією ЧНУ на основі індивідуальних запрошень та інших механізмів.
При прийнятті на навчання осіб, які подають документ про здобутий за кордоном ступінь (рівень) освіти, обов'язковою є процедура визнання і встановлення еквівалентності Документа, що здійснюється відповідно до наказу МОН України №504 від 5.05.2015 р. «Деякі питання визнання в Україні іноземних документів про освіту».

Опишіть на конкретних прикладах практику застосування вказаних правил на відповідній ОП (якщо такі були)?

ЧНУ визнає еквівалентними та перезараховує результати навчання здобувача вищої освіти у ЗВО-партнері. Визнання результатів навчання в рамках академічного співробітництва із ЗВО-партнерами здійснюється з використанням європейської системи трансферу та накопичення кредитів ECTS або з використанням системи оцінювання навчальних здобутків здобувачів вищої освіти, прийнятої у країні ЗВО-партнера, якщо в ній не передбачено застосування ECTS. Порядок перезарахування визначається угодою, яка підписується перед поїздкою на навчання. Перезарахування вивчених навчальних дисциплін здійснюється на підставі представленого здобувачем вищої освіти документа з переліком та результатами навчальних здобутків з навчальних дисциплін, кількістю кредитів та інформацією про систему оцінювання навчальних здобутків здобувача вищої освіти, завіреного в установленому порядку ЗВО-партнері. До основних проблем під час визнання результатів навчання, отриманих в інших ЗВО, можна віднести розбіжність у змісті освітніх програм, практичної підготовки та технічному забезпеченні. Практики застосування вказаних правил на ОПП «Кібербезпека» не було.

Яким документом ЗВО регулюється питання визнання результатів навчання, отриманих у неформальній освіті? Яким чином забезпечується його доступність 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» (протокол №10 від 28.10.2019 р.) (https://drive.google.com/file/d/100CFtXHLrgqS-T43aFun6blUvZO7Z0z1/view), в якому визначені критерії визнання результатів навчання, отриманих у неформальній освіті. Інформація про можливості неформальної освіти доступна на сайті ЧНУ. Також про можливості неформальної освіти в контексті конкретних дисциплін здобувачів повідомляють викладачі, які забезпечують проведення занять.

Опишіть на конкретних прикладах практику застосування вказаних правил на відповідній ОП (якщо такі були)

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 2022-2023 н. р., https://drive.google.com/file/d/1W_tCH5S_99HR7d1eeaIEV93bBktGap9r/view) 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.

4. Навчання і викладання за освітньою програмою

Продемонструйте, яким чином форми та методи навчання і викладання на ОП сприяють досягненню програмних результатів навчання? Наведіть посилання на відповідні документи

Форми й методи навчання регламентуються «Положенням про організацію освітнього процесу в ЧНУ» (https://bit.ly/3Zb1Ot3). Основними формами навчання є аудиторні (лекції, лабораторні, практичні, семінарські тощо), позааудиторні заняття (самостійна робота, виконання індивідуального завдання), практики, конструкторська або науково-дослідна робота, поєднання яких забезпечує досягнення програмних результатів навчання у пізнавальній, дослідницькій та професійній сферах. При викладанні освітніх компонент ОП застосовуються методи навчання: практичний (експерименти, задачі, вправи), наочний (спостереження, ілюстрації, демонстрації), словесний (лекція, семінар, пояснення, дискусія), робота з книгою (читання, конспектування), аудіо-відео-метод (перегляд слайдів, електронні засоби). Вагому роль відіграють електронні ресурси, зокрема система електронного навчання ЧНУ (https://moodle.chnu.edu.ua/).
Розробка навчальних програм 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).
На випусковій кафедрі запроваджена практика проведення відкритих занять з подальшим обговоренням застосованих викладачем форм та методів навчання, що сприяє вдосконаленню освітнього процесу.

Продемонструйте, яким чином форми і методи 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 корпоративну електронну пошту або інші 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, https://bit.ly/3LgmPgx). Загалом, результати проведеного опитування 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 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» (https://bit.ly/3Zb1Ot3) 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://cutt.ly/JC0c4Sp, http://radiotech.chnu.edu.ua/projects).
Здобувачі ОП успішно виступають на Всеукраїнських конкурсах студентських наукових робіт та конференціях різного рівня, де здобувають призові місця та відзнаки (http://radiotech.chnu.edu.ua/page/4/).
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 навчальних дисциплін 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. Робочі програми навчальних дисциплін ОПП «Кібербезпека» та інше навчально-методичне забезпечення, в якому відображено зміст ОК, затверджуються випусковою кафедрою перед початком нового навчального року. На кафедрі радіотехніки та інформаційної безпеки 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://cutt.ly/JC0c4Sp), 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 в ППО5 («Вибрані розділи криптології») 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, http://surl.li/kzhaf, http://surl.li/kzhaq). 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 у межах ОП пов'язані із інтернаціоналізацією діяльності ЗВО

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 здобувачів вищої освіти ЧНУ» (http://surl.li/aeudh).

5. Контрольні заходи, оцінювання здобувачів вищої освіти та академічна доброчесність

Опишіть, яким чином форми контрольних заходів у межах навчальних дисциплін ОП дозволяють перевірити досягнення програмних результатів навчання?

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). 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» (https://drive.google.com/file/d/1DG2_aEX5y5gkZMdVi6qry4NwztXw0-3h/view, http://surl.li/kxxhs).

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 силабусах, 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 проінформувати 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)?

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.
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. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.
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).

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 доступна для здобувачів ВО через систему дистанційного навчання Moodle.

Яким чином ці процедури 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_eTUFUBGv4o/view) та «Етичний кодекс ЧНУ» (https://bit.ly/3Lflw03).
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. Кількість балів при оцінюванні знань студента з дисципліни, яка завершується екзаменом чи заліком, визначається Вченою радою НН ІФТКН, але кількість балів для поточного оцінювання повинна бути не менша 35. Студенти, які одержали під час семестр. контролю незадов. 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/RC7ifou), здобувач, який під час складання екзамену комісії отримав незадов. 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 (Губчак А., Юрков Д.); повторного захисту дипломних робіт впродовж 2019-2023 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_eTUFUBGv4o/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» (https://bit.ly/3Lflw03); «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?

У «Положенні про виявлення та запобігання академічному плагіату в ЧНУ» (https://www.chnu.edu.ua/media/ozmforih/polozennia-pro-vyiavlennia-ta-zapobihannia-plahiatu.pdf) регламентовано порядок перевірки й умови подання навчально-методичних та кваліфікаційних робіт на перевірку та відповідальність за плагіат. Для виявлення фактів академічного плагіату ЧНУ щорічно укладає угоду з компанією Unicheck. Антиплагіатна програма визначає ступінь ідентичності тексту. Всі кваліфікаційні роботи студентів ОПП «Кібербезпека» проходять обов'язкову перевірку на наявність академічного плагіату. Текст вважається оригінальним, якщо схожість не перевищує 20%, в такому випадку кваліфікаційна робота допускається до захисту. Питання академічної доброчесності обговорюються і на засіданнях випускової кафедри, зокрема, під час уточнення вимог до виконання магістерських робіт/проектів (прот. №6, 24.11.2020; №17, 10.05.2023).
За потреби можуть перевірятись й інші письмові роботи (курсові, реферати тощо).
У НН ІФТКН створена Етична комісія, до якої можуть звернутися учасники освітнього процесу у разі порушення академічної доброчесності. До складу комісії входять представники підрозділів НН ІФТКН та студентського самоврядування (https://bit.ly/3qENXeg).

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 НН ІФТКН. ЧНУ є учасником проєкту AcademIQ «Ініціатива академічної доброчесності та якості освіти» (https://www.chnu.edu.ua/universytet/vazhlyvo/akademichna-dobrochesnist/). Повідомлення про заходи з популяризації академічної доброчесності представлені на сайті ЧНУ (https://bit.ly/3Re9mtp) та на сайті НН 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.
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, для здобувачів ВО кафедри радіотехніки та інформаційної безпеки був проведений вебінар на тему «Академічна доброчесність» (http://surl.li/dalzr).

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» (https://drive.google.com/file/d/14PoxHnt_u7rPqGbGu3cccWyTRXbI5-Gg). 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

Яким чином під час конкурсного добору викладачів ОП забезпечується необхідний рівень їх професіоналізму?

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. 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.

Опишіть, із посиланням на конкретні приклади, яким чином ЗВО залучає роботодавців до організації та реалізації освітнього процесу

ЧНУ активно залучає роботодавців до організації і реалізації освітнього процесу. Взаємодія в рамках укладених меморандумів та угод про співпрацю із провідними вітчизняними та міжнародними організаціями та підприємствами (https://bit.ly/3D95Qta) дає можливість удосконалювати робочі програми та зміст освітніх компонент, оновлювати перелік вибіркових дисциплін, оперативно реагувати на потреби ринку праці у регіоні. Стейкхолдери беруть участь у обговоренні наповнення ОК, розробленні методичних матеріалів вибіркових дисциплін (http://radiotech.chnu.edu.ua/opp_125_master/), формуванні лаб. бази (Компанія Tektelic, ТОВ «ІнТех», http://surl.li/fdxwm, https://bit.ly/3SdUCbg), практик та дипломного проектування, вносять пропозиції до оновлення змісту ОП (http://radiotech.chnu.edu.ua/opp_125_master/), що дозволить їм в перспективі поповнювати свій кадровий потенціал. Наприклад, здобувачі ВО в рамках дисципліни «Радіомоніторинг і радіопротидія на об'єктах інформаційної діяльності» брали участь в екскурсіях до КП «Міжнародний аеропорт «Чернівці», Чернівецького обласного відділу КФ ДП «Укр. держ. центр радіочастот» (2019-2022 н.р.) з метою ознайомлення з роботою цих підприємств, обладнанням та методиками проведення радіочастотного моніторингу.
Також здобувачі освіти брали участь у низці вебінарів, організованих в рамках проекту USAID "Кібербезпека критично важливої інфраструктури України".
Такі заходи спрямовані на посилення практичної підготовки здобувачів у майбутній професійній діяльності

Опишіть, із посиланням на конкретні приклади, яким чином ЗВО залучає до аудиторних занять на ОП професіоналів-практиків, експертів галузі, представників роботодавців

До підготовки здобувачів за даною ОП залучаються професіонали-практики та провідні фахівці галузі. Зокрема, восени 2022 року в рамках вивчення курсу ППО5 професором кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В. Н. Каразіна, д.т.н. І. Д. Горбенком була прочитана серія лекцій, присвячених питанням прикладної криптології. В умовах вимушеного дистанційного навчання значно розширились можливості залучення до освітнього процесу професіоналів та представників стейкхолдерів. Зокрема, за допомогою платформи Google Meet було організовано низку зустрічей зі студентами кафедри, присвячених питанням інформаційної безпеки, що є предметом вивчення ППО1 (http://surl.li/lafew). Представники відділів кібербезпеки та технічної підтримки СБУ, кіберполіції та ІТ-компаній під час своїх виступів окрім доповідей за запропонованою темою, звернули увагу здобувачів на необхідні навички та вміння, якими має володіти їхній працівник. У жовтні 2020 р. відбулася лекція на тему «Як ефективно керувати персоналом», яку провів бізнес-аналітик Калинюк В.В. Лекція та її обговорення викликали значний інтерес з боку здобувачів. Інформація про ці заходи подана на сайті кафедри (http://radiotech.chnu.edu.ua/).

Опишіть, яким чином ЗВО сприяє професійному розвиткові викладачів ОП? Наведіть конкретні приклади такого сприяння

ЧНУ сприяє професійному розвиткові викладачів як складової системи забезпечення якості освітньої діяльності, згідно «Положення про підвищення кваліфікації науково-педагогічних працівників ЧНУ» (https://drive.google.com/file/d/1opL_rGqQxGOytwv1IkoQUAKdjKInQeK6/view).
В період карантину ЧНУ одним з перших перейшов на дистанційне навчання й провів для співробітників курси внутрішнього підвищення кваліфікації «Основи користування Moodle» (3 кред.), організував надання викладачам безоплатного доступу до платформи дистанційного навчання Coursera. Викладачами факультету іноземних мов проводилась серія науково-методичних семінарів-практикумів «Алгоритм підготовки до викладання фахових дисциплін англійською мовою» (взяли участь доценти Ластівка Г.І., Рождественська М.Г.).
Безперервний професійний розвиток викладачів забезпечується системою постійно діючих наукових та методичних заходів. У ЧНУ створено умови для здійснення програм академічної мобільності за Еразмус+ та отримання міжнародної сертифікації для викладачів (https://www.chnu.edu.ua/mizhnarodna-diialnist/zakordonni-partnery/erazmusplus/). 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 табл. 2.

Продемонструйте, що ЗВО стимулює розвиток 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/1Yc7snvzBdvcoPDi1oJDBz2LYbwWLS65z/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 складає рейтинг кафедр. Кафедра радіотехніки та інформаційної безпеки займає 27 місце серед 80 кафедр ЧНУ (http://surl.li/kxyim).
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/lkhrn).

7. Освітнє середовище та матеріальні ресурси

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

Фінансування ОП здійснюється в рамках фінансово-економічної діяльності ЧНУ та грантових програм (http://surl.li/lbybq).
Для підготовки здобувачів за ОПП «Кібербезпека» використовується матеріально-технічна база ЧНУ, яка відповідає Ліцензійним вимогам провадження освітньої діяльності. ОП забезпечена усіма необхідними ресурсами для досягнення цілей і програмних РН. Для виконання лабораторних і практичних робіт створено комп'ютерний клас та низку спецлабораторій: ТЗЗІ в радіотехнічних пристроях і телекомунікаційних системах, Вбудованих систем та ін. (http://radiotech.chnu.edu.ua/labs/). В освітньому процесі використовується Колективна радіостанція ЧНУ (http://radiotech.chnu.edu.ua/ur4yww/) та професійне обладнання партнерів (ОК8, ОК5 редакції ОП 2019-2021 н.р.).
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 інша інфраструктура; студенти забезпечуються гуртожитками.

Продемонструйте, яким чином освітнє середовище, створене у ЗВО, дозволяє задовольнити потреби та інтереси здобувачів вищої освіти ОП? Які заходи вживаються ЗВО задля виявлення і врахування цих потреб та інтересів?

Згідно зі Статутом 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 студентський парламент ЧНУ.

Опишіть, яким чином ЗВО забезпечує безпечність освітнього середовища для життя та здоров'я здобувачів вищої освіти (включаючи психічне здоров'я)?

Відповідно до Статуту, університет забезпечує здобувачам ВО безпечні та нешкідливі умови навчання, праці та побуту. Водночас, студенти повинні виконувати вимоги з охорони праці, техніки безпеки, виробничої санітарії, протипожежної безпеки, щодо порядку дій під час тривоги (https://www.chnu.edu.ua/universytet/vazhlyvo/bezpeka/). Кожного семестру студенти проходять інструктаж з ТБ у навчальних лабораторіях із записами у відповідних журналах. В аудиторіях і лабораторіях підтримуються необхідні санітарні норми щодо площі приміщень, освітлення, температурного режиму тощо. За приміщеннями ЧНУ постійно здійснюється технічний нагляд, проводяться поточний та капітальний ремонти. У корпусах діє цілодобова охорона; у 8 та 9 корпусах, де проводяться заняття здобувачів за ОПП «Кібербезпека», функціонують запасні виходи та укриття. Під час пандемії в ЧНУ було

повною мірою забезпечено дотримання санітарних норм.
Медичні послуги надаються у медпункті студмістечка та міській студентській поліклініці. Проводяться профілактичний медогляд студентів, акції «Тиждень здоров'я», «Кидай палити!» тощо.
Одним з критеріїв оцінювання викладацького складу в анкетуванні студентів є педагогічний такт викладача, що безпосередньо впливає на психічне здоров'я здобувачів.
Право на захист від будь-яких форм експлуатації, фізичного та психічного насильства регламентоване у «Правилах внутрішнього трудового розпорядку ЧНУ» (http://surl.li/anouj). В ЧНУ функціонує соціально-психологічний центр (http://surl.li/grbxs).

Опишіть механізми освітньої, організаційної, інформаційної, консультативної та соціальної підтримки здобувачів вищої освіти? Яким є рівень задоволеності здобувачів вищої освіти цією підтримкою відповідно до результатів опитувань?

У ЧНУ забезпечується освітня, організаційна, інформаційна, консультативна та соціальна підтримка здобувачів ВО 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 зазначеної підтримки в ЧНУ здійснюють: випускова кафедра, навчальний відділ, профспілкова організація, органи студентського самоврядування.
Освітня підтримка передбачає: застосування студентоцентрованого підходу у навчанні; покращення мотивації до здобуття освіти та готовності до навчання впродовж життя; моделювання реальних професійних умов спілкування; створення сприятливого психоемоційного клімату у студентській групі; якісне навчально-методичне забезпечення освітнього процесу; використання інноваційних педагогічних технологій.
Організаційна підтримка передбачає: забезпечення розуміння, врахування та узгодження потреб студентів щодо надання освітніх послуг; створення належних умов їх навчання; забезпечення вільного вибору студентами навчальних дисциплін; реалізацію принципів академічної доброчесності; організацію і здійснення моніторингу якості освіти.
Консультативна підтримка передбачає: організацію групових та індивідуальних консультацій для оперативного задоволення освітніх, організаційних та соціальних потреб здобувачів.
Інформаційна підтримка передбачає забезпечення вільного доступу до інформації, необхідної для організації освітнього процесу (зокрема щодо розкладів навчальних занять і консультацій; масових заходів ЧНУ та роботи його структурних підрозділів; нормативних документів тощо). Інформування студентів з освітніх і позаосвітніх питань відбувається за допомогою розміщення інформації на офіційних веб-сайтах ЧНУ, НН ІФТКН, випускової кафедри, персональних сторінках викладачів, інформаційних стендах.
Соціальну підтримку отримують студенти таких категорій: напівсироти, сироти та діти, позбавлені батьківського піклування, малозабезпечені, ті, що мають дітей або проживають у гірських районах, інваліди, чорнобильці, діти учасників бойових дій. Студенти з дітьми отримують подарунки від профспілки ЗВО на день Св. Миколая. Для студентів-сиріт та осіб, позбавлених батьківського піклування, організовуються виплати, компенсації на продукти харчування, вони звільняються від оплати за проживання в гуртожитку, отримують щорічну матеріальну допомогу. Спілкування кураторів зі студентами дозволяє виявляти соціально незахищених та тих, хто потребує допомоги.
Для надання психологічної допомоги студентам та співробітникам створений соціально-психологічний центр (https://drive.google.com/file/d/1KQUVI-1EiHFL4vBiU5AjTrGYN_6Dp7ia/view), який регулярно проводить опитування студентів (http://surl.li/grbxs, http://surl.li/kxypt).
Більшість студентів задоволені рівнем освітньої, організаційної, інформаційної, консультативної та соціальної підтримки в ЧНУ, про що свідчать результати анкетування студентів, які навчаються за даною ОП.

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» (https://bit.ly/3BBa2Ra) 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 2023 р.» прописані спеціальні умови вступу (http://surl.li/khwvu).
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.

Яким чином у ЗВО визначено політику та процедури врегулювання конфліктних ситуацій (включаючи пов'язаних із сексуальними домаганнями, дискримінацією та корупцією)? Яким чином забезпечується їх доступність політики та процедур врегулювання для учасників освітнього процесу?

Якою є практика їх застосування під час реалізації ОП?

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 «Правилами внутрішнього розпорядку в студентських гуртожитках ЧНУ» та іншими 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 ІФТКН 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 (http://surl.li/lbyel).
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 в мережі Інтернет

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://drive.google.com/file/d/1rFVXb_JZ0VNab4J2x8tHTz2vfVmH4JOP/view);
«Положенням про порядок проведення внутрішнього моніторингу якості освітньої діяльності та якості вищої освіти в Чернівецькому національному університеті імені Юрія Федьковича» (прот. №7 від 31 серпня 2020 року)
(https://drive.google.com/file/d/1BGtjpMStV35WLKnGjo0zOwZMjofsBwnK/view);
«Положенням про систему внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти в Чернівецькому національному університеті імені Юрія Федьковича» (прот. №7 від 31 серпня 2020 року)
https://drive.google.com/file/d/14UAVRHptFJkoS4NW5h35lDhfpsqOsyrp/view).
Деякі аспекти роботи з реалізації та удосконалення освітніх програм регламентується «Положенням про організацію освітнього процесу в ЧНУ»
(https://drive.google.com/file/d/1x419wQ3yhhBi0azmcm_xUod7zrSsdCVN/view) (прот. №9 від 30.09.2019) та «Положенням про гаранта освітньої програми ЧНУ» (https://www.chnu.edu.ua/media/qmapwn1b/polozhennia-pro-haranta-osvitnoi-prohramy.pdf) (прот. №7 від 30.06.2021).
Розроблення і затвердження ОП контролюються Сектором ліцензування, акредитації та нострифікації навчального відділу ЧНУ (https://www.chnu.edu.ua/navchannia/navchalnyi-viddil/diialnist/).

Опишіть, 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 є важливими умовами її реалізації та розвитку. Цей процес у ЧНУ (згідно «Положення про розроблення та реалізацію освітніх програм ЧНУ»,
https://drive.google.com/file/d/1rFVXb_JZ0VNab4J2x8tHTz2vfVmH4JOP/view) 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 науково-педагогічними працівниками, здобувачами ВО, випускниками та роботодавцями з'ясовується необхідність внесення змін до окремих її ОК. Суть та обсяги цих змін визначаються мірою задоволеності здобувачів ВО, що можуть бути визначеними за результатами анкетування, показниками їх працевлаштування, участю у міжнародних програмах академічної мобільності, оцінками з боку роботодавців тощо.

Оновлені ОП узгоджуються з представниками студентського самоврядування, завідувачем випускової кафедри, навчальним відділом ЧНУ, затверджуються Вченою радою ЧНУ та вводяться в дію наказом ректора. Крім того, оновлені ОП – складова компонента внутрішньої системи забезпечення якості освітньої діяльності ЗВО, які оприлюднюються на сайті випускової кафедри.
Зміни, внесені до ОП за результатами останнього перегляду (оновлена ОП затверджена Вченою радою ЧНУ 3.04.2023, прот. №3), представлені на сайті кафедри радіотехніки та інформаційної безпеки ЧНУ (http://radiotech.chnu.edu.ua/opp_125_master/). Серед ключових змін слід відзначити наступні:
1) на основі пропозицій та їх обговорення з зацікавленими сторонами освітнього процесу ОПП «Кібербезпека», а також враховуючи зауваження моніторингової групи Центру забезпечення якості вищої освіти ЧНУ, уточнено формулювання характеристик ОП, зазначений зв'язок ОП з місією та стратегічним планом розвитку ЧНУ на 2019-2026 р.;
2) за пропозиціями здобувачів та представників академічної спільноти (рецензент Яремчук Ю.Є., голови ЕК Стахіра П.Й., Толюпа С.В.), що враховують сучасні тенденції розвитку ринку праці, запроваджено ЗПО1, ЗПО2, ППО3, ППО5;
3) за пропозиціями студентів, стейкхолдерів та моніторингової групи ЦЗЯВО ЧНУ для розширення можливостей щодо формування індивідуальної освітньої траєкторії здобувачів ВО змінений формат Переліку вибіркових освітніх компонент ОП;
4) враховуючи прикладне спрямування ОП і орієнтацію на здобуття студентами фахових знань, умінь та навичок для здійснення подальшої професійної діяльності, за рекомендацією професорсько-викладацького складу випускової кафедри та роботодавців прийняте рішення передбачити курсову роботу в обов'язковій дисципліні циклу професійної підготовки «Технології комплексного захисту інформації» (ППО1).
Судячи з аналізу отриманих на оновлену редакцію ОПП «Кібербезпека» рецензій та відгуків стейкхолдерів, 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 позиція береться до уваги під час перегляду ОП

Соціологічною лабораторією ЧНУ та випусковою кафедрою проводиться опитування студентів щодо покращення якості та організації освітнього процесу відповідно до «Положення про систему внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти в ЧНУ». Результати опитувань здобувачів, що враховують висловлені пропозиції щодо змін ОП, аналізуються та узагальнюються членами робочої групи, зіставляються з пропозиціями роботодавців і викладачів, обговорюється та затверджується на засіданні випускової кафедри.
Зокрема, було враховано пропозицію студентки Рижакової В.І. відносно розширення переліку вибіркових освітніх компонент дисципліною, пов'язаною з захистом персональних даних та соціальною інженерією; студентом Мочернюком Т.М. запропоновано ввести дисципліну, присвячену поглибленому вивченню криптографічного захисту в інформаційних системах; магістром Пархоменком Є.В. висловлено побажання щодо розроблення і впровадження курсу з основ нейромереж, що зумовило доповнення переліку вибіркових дисциплін курсами «Захист персональних даних та соціальна інженерія», «Математичні основи нейромереж», а також враховано під час впровадження обов'язкової дисципліни ППО5 («Вибрані розділи криптології»). Зазначені пропозиції були підтримані проектною групою для підсилення програмних результатів навчання (відповідно, РН 2, 3, 5, 13, 20 та РН 24 чинної на момент пропозиції редакції ОПП) та затверджені на засіданнях випускової кафедри (прот. №16, 16.02.2022 та №16, 21.04.2023).

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 процесу періодичного перегляду ОП та інших процедур забезпечення її якості

Випусковою кафедрою проводяться зустрічі з роботодавцями та обговорення вимог до фахівця на ринку праці. Як результат, переважна більшість випускників магістратури за ОПП «Кібербезпека» працевлаштовуються на підприємствах, в організаціях та комерційних компаніях у сфері ІБ та захисту інформації Західного регіону.
З метою залучення роботодавців до процедур забезпечення якості освіт. процесу випусковою кафедрою 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 формування та коригування цілей та програмних РН 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 випускової кафедри №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). Представники роботодавців залучаються до проведення занять, планування тематик кваліф. проектів/ робіт, рецензування та їх подальшого впровадження.

Опишіть практику збирання та врахування інформації щодо кар'єрного шляху та траєкторій працевлаштування випускників ОП

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 КРТтаІБ – 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.
Багато студентів працевлаштовані вже під час навчання та навчаються за індивідуальним графіком.
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/).

Які недоліки в ОП та/або освітній діяльності з реалізації ОП були виявлені у ході здійснення процедур внутрішнього забезпечення якості за час її реалізації? Яким чином система забезпечення якості ЗВО відреагувала на ці недоліки?

Внутрішнє забезпечення якості ОП у ЧНУ регламентується «Положенням про систему внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти в ЧНУ(https://drive.google.com/file/d/1Ti3xngUzuP-nIcWMsQhijff4G4-x9nux/view). Порядок моніторингу та удосконалення ОП в університеті деталізований «Положенням про порядок проведення внутрішнього моніторингу якості освітньої діяльності та якості вищої освіти в Чернівецькому національному університеті імені Юрія Федьковича» (https://drive.google.com/file/d/1BGtjpMStV35WLKnGjoozOwZMjofsBwnK/view) та «Положенням про розроблення та реалізацію освітніх програм ЧНУ» (https://drive.google.com/file/d/13O1K-SnZkg7h4vlNS8Nhp4uqaDjg_BHY/view). Моніторинг та удосконалення освітніх програм ЧНУ в процесі їх реалізації включають визначення: змісту освітніх програм за результатами останніх досліджень у відповідній галузі знань з метою забезпечення їх відповідності сучасним вимогам; змін потреб суспільства; очікувань, потреб та ступеня задоволення студентів стосовно ОП. Зауваження та недоліки щодо освітнього процесу за ОПП «Кібербезпека», виявлені внутрішньою системою забезпечення якості, постійно аналізуються та обговорюються робочою групою із залученням стейкхолдерів; вносяться пропозиції до змін у змісті ОП та організації освітнього процесу. Зокрема, було впроваджено такі заходи:
- зміст освітніх компонент ОП (робочі програми, силабуси, методичне забезпечення) переглядається і оновлюється перед початком нового навчального року;
- розширений перелік вибіркових дисциплін, які можуть обирати студенти;
- для кращого інформування здобувачів ВО щодо змісту ОП та організації освітнього процесу розширений спектр відомостей, які відображаються на сайті випускової кафедри (посібники, інформація про співпрацю зі стейкхолдерами, академічною спільнотою, динаміку змін ОП тощо);
- за відгуками провідних спеціалістів галузі запроваджуються нові варіативні дисципліни та формується їхнє навчально-методичне забезпечення;
- на основі відгуків вступників за ОПП «Кібербезпека» через недостатній рівень їх результатів ЕВІ з іноземної мови, центр забезпечення якості вищої освіти організував проведення моніторингу якості викладання іноземних мов у ЧНУ із залученням викладачів відповідних ОП першого (бакалаврського) рівня ВО. Прийнято рішення інтенсифікувати викладання іноземної мови на всіх ОП та організовано безкоштовні курси для студентів 4 курсу (https://docs.google.com/presentation/d/1xNy5frPnTzq7VDZzt-1Fwzpcnd7BE2PE/edit#slide=id.p22);
- здійснюються заходи щодо оновлення лабораторної бази, комп'ютерної техніки і програмного забезпечення;
- з метою поліпшення доступу до науково-методичних публікацій в ЧНУ оновлено репозитарій, а також для ознайомлення із специфікою роботи з даним ресурсом для викладачів і студентів проведено низку вебінарів;
- покращується освітнє середовище для осіб з особливими освітніми потребами.

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

Акредитація ОПП «Кібербезпека» за технологією НАЗЯВО відбувається вперше. Проте, враховуючи тривалу історію підготовки фахівців у сфері захисту інформації на кафедрі радіотехніки та інформаційної безпеки, під час попередніх акредитацій висловлювалися зауваження та пропозиції щодо покращення цієї підготовки. Серед них:

- активізувати процес підвищення кваліфікації співробітниками кафедри як у провідних ЗВО України, так і за кордоном;
- керівництву університету, завідувачу випускової кафедри забезпечити подальший розвиток учбових лабораторій та їх оснащення новими зразками сучасного інфокомунікаційного обладнання;
- завідувачу випускової кафедри продовжити роботу з ротації професорсько-викладацького складу та налагодження зв'язків зі спорідненими закордонними навчальними закладами;
- продовжити випуск навчальних посібників та організувати випуск підручників власної розробки з фахових дисциплін напрямку інформаційної та кібербезпеки;
- з метою підсилення практичних навичок студентів та їх адаптування до сучасних вимог ринку праці передбачити в освітньо-професійній програмі підготовки здобувачів "Кібербезпека" зі спеціальності 125 - Кібербезпека курсовий проект з дисципліни "Технології комплексного захисту інформації";
- керівництву університету, завідувачу випускової кафедри продовжити роботу над участю студентів та викладачів у процедурах сертифікації за фаховим спрямуванням та з іноземних мов, що дозволить підвищити рівень конкурентоздатності випускників;
- запровадити діяльність щодо оцінки захищеності приміщень та сертифікації програмно-апаратних засобів для службового користування підприємств та організацій Західного регіону.
Впродовж періоду, що минув з останньої акредитації, ці зауваження були виправлені в повній мірі.
Враховуючи зміни у технології проведення процесу акредитації, в ЧНУ розроблено процедури реагування на зауваження і пропозиції, які виникають в результаті роботи експертних груп з ОП різних спеціальностей. Висновки експертних груп та ГЕР розглядаються і аналізуються на Вчених і методичних радах ЧНУ і його підрозділів (http://surl.li/kybkr, http://surl.li/kybmh). Приймаються відповідні рішення і вживаються заходи щодо їх усунення. Під час роботи над оновленою редакцією ОПП «Кібербезпека» враховано результати акредитації інших ОП, а також відгуки здобувачів та стейкхолдерів (http://radiotech.chnu.edu.ua/opp_125_master/).

Опишіть, яким чином учасники академічної спільноти змістовно 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 ННІ ІФТКН, 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 ННІ ІФТКН забезпечення якості ОП контролюється випусковими кафедрами, методичною радою, адміністрацією.

Опишіть розподіл відповідальності між різними структурними підрозділами ЗВО у контексті здійснення процесів і процедур внутрішнього забезпечення якості освіти

У положенні ЧНУ «Про систему внутрішнього забезпечення якості освітньої діяльності та якості вищої освіти» (СВЗЯО) (https://drive.google.com/file/d/1YtQjLaZi8T7NeLfiRh3L7bKrjSoG-Srw/view) зазначено, що в університеті сформована інституційна основа системи забезпечення якості освіти на рівні:
а) університету – Навчально-методична комісія Вченої ради, яка розробляє концептуальні засади СВЗЯО і політику щодо забезпечення якості освітньої діяльності та вищої освіти університету, Центр моніторингу якості освітньої діяльності та якості вищої освіти з секторами моніторингу якості освітніх програм, моніторингу якості навчальної діяльності студентів, моніторингу якості освітньої діяльності освітньої та наукової діяльності викладачів. До реалізації цих процедур залучені комісія Вченої ради з питань кадрової роботи (забезпечення якості освітньої та наукової діяльності викладачів, їх професійного розвитку), відділ інформаційного забезпечення та публічності інформації;
б) Навчально-наукового інституту фізико-технічних та комп'ютерних наук – методична і Вчена рада інституту;
в) кафедри – забезпечується викладачами кафедри, навчально-методичною комісією кафедри при безпосередньому керівництві гаранта освітньої програми (завідувача кафедри);
г) здобувачів вищої освіти – соціологічною лабораторією університету щосеместрово здійснюються соціологічні опитування здобувачів вищої освіти щодо оцінки та покращення організації освітнього процесу в університеті.

9. Прозорість і публічність

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

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://drive.google.com/file/d/1Yc7snvzBdvcoPDi1oJDBz2LYbwWLS65z/view). 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.

Наведіть посилання на веб-сторінку, яка містить інформацію про оприлюднення на офіційному веб-сайті ЗВО відповідного проекту з метою отримання зауважень та пропозиції заінтересованих сторін (стейкхолдерів). Адреса веб-сторінки

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

Наведіть посилання на оприлюднену у відкритому доступі в мережі Інтернет інформацію про освітню програму (включаючи її цілі, очікувані результати навчання та компоненти)

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

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП?

Сильні сторони ОПП «Кібербезпека»:
значний та тривалий досвід кафедри радіотехніки та інформаційної безпеки ЧНУ у підготовці фахівців у сфері інформаційної безпеки;
врахування специфіки регіону та потреб ринку праці у фахівцях для підприємств і установ галузі;
впровадження студентоцентрованого навчання;
залучення професіоналів-практиків до підготовки здобувачів вищої освіти ОП;
забезпечення вільного доступу до електронного навчального середовища для здобувачів вищої освіти та науково-педагогічних працівників ОП;
компетентність, досвідченість та висока фаховість науково-педагогічних працівників ОП, які відповідають ліцензійним вимогам;
успішна участь здобувачів за ОПП «Кібербезпека» у конкурсах студентських наукових робіт за напрямком інформаційної безпеки та суміжних галузей;
налагоджені надійні партнерські відносини з профільними підприємствами та установами;
ОП забезпечує повноцінну підготовку магістрів до професійної, практичної та науково-дослідної діяльності, про що свідчать активний вступ випускників до аспірантури та регулярні звернення роботодавців щодо рекомендації їх до працевлаштування;
навчально-методичне, інформаційне та матеріально-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 у закріплюються ще і вибірковими компонентами;
відкритість науково-педагогічного колективу випускової кафедри та НН ІФТКН, готовність до співпраці та взаємодоповнюваність у навчальній та науковій діяльності, відкрите та приязне спілкування зі студентами і готовність надати консультацію за необхідності як в аудиторії, так і онлайн чи через електронні ресурси;
навчання за ОП проводиться в активному дослідницько-практичному середовищі, заснованому на науково-методичних розробках випускової кафедри і ЧНУ в цілому;
методи навчання та оцінювання результатів були переглянуті, розширені з урахуванням сучасних реалій (індивідуальне, дистанційне навчання).
Слабкі сторони:
Відсутність програми подвійних дипломів (процес укладання відповідних угод розпочато).
Відсутність програми дуальної освіти.
Недостатнє заохочення здобувачів вищої освіти, які навчаються за ОП, до академічної мобільності.
Слабка активність у підготовці та захисті докторських дисертацій.
Модернізація матеріально-технічного забезпечення навчання осіб з особливими потребами у разі появи таких здобувачів.

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:
1. Періодичне оновлення наявної ОПП «Кібербезпека» та врахування вимог професійних стандартів у сфері кібербезпеки.
2. 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.
3. Постійне осучаснення матеріально-технічної бази для забезпечення фахових дисциплін та інших ОК, зокрема обладнання навчально-наукових лабораторій.
4. Поєднання теоретичного та прикладного аспектів навчання, підвищення якості та ефективності виробничих практик здобувачів вищої освіти
5. Впровадження підвищення кваліфікації викладачів шляхом тренінгів щодо сучасних технологій навчання, в тому числі іноземною мовою.
6. Сприяння обміну студентами на основі двосторонніх угод між ЧНУ та закладами вищої освіти зарубіжних країн-партнерів, розширення можливостей міжнародного стажування для викладачів випускової кафедри.
7. Розширення партнерських відносин із закордонними підприємствами та компаніями в галузі інформаційної безпеки.
8. Впровадження адаптивного трансформаційного механізму дуальної освіти в умовах розриву освіти й виробництва, необхідності підвищення якості освітнього процесу з урахуванням інноваційних змін в технологіях та вимог роботодавців на ринку праці.
9. 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.

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: Петришин Роман Іванович

Дата: 28.09.2023 р.

Таблиця 1. Інформація про обов'язкові освітні компоненти ОП

Назва освітнього компонента	**Вид 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**	
ЗПО1. Наукова та професійна комунікація іноземною мовою	навчальна дисципліна	*ЗПО1_Наук. та проф. комунікація іноз. мовою.pdf*	wQsBbQfE9sfklzZIh5flDNIRd/vHOD1wHUaWzEBigaE=	*Для проведення очного/дистанційного навчання: аудиторний фонд; бібліотеки ЧНУ та кафедр; внутрішня корпоративна пошта та система електронного навчання Moodle (https://moodle.chnu.edu.ua); наявність каналів доступу до Інтернету.* *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.).*
ЗПО2. Науково-педагогічна діяльність та навчання персоналу в галузі ІБ	навчальна дисципліна	*ЗПО2_Наук_педагог_діяльність_в_галузі_ ІБ.pdf*	sxFF+HITnlI3UXiv7PRAGOzb/48LB/KaOudlNyvSfVU=	*Аудиторний фонд; бібліотеки ЧНУ та кафедри радіотехніки та інформаційної безпеки; 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 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*
ППО1. Технології комплексного захисту інформації	навчальна дисципліна	*ППО1_Технології_комплекс_зах_інф.pdf*	6Lw6Xcpv6+jn8IDHvAeAFKXGXYOLwcyQGiLSTJPs8Xk=	*Аудиторний фонд і необхідне обладнання; бібліотеки ЧНУ та кафедри радіотехніки та інформаційної безпеки, в тому числі електронні; внутрішня корпоративна пошта та система електронного навчання Moodle (https://moodle.chnu.edu.ua); наявність каналів доступу до Інтернету, в тому числі точка 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 Intel Core i3-10325/3.9GHz/DDR4 8GB 2400 MHz/SSD 256 GB з монітором 22" Acer (2021 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* *Проведення наочно-демонстраційних занять: Лабораторія "Технічних засобів захисту інформації".* *Обладнання:* *1. Комплекс АКОР-3 (1 шт.).* *2. Спеціалізований комплекс акустичного захисту мовної інформації КАЗМІ (1 шт.).* *3. Детектор поля PROTECT 1206i (2018 р., 2 шт.).* *4. Акустичний зашумлювач PIAC2BA (2019 р., 1 шт.).* *5. Генератор радіошуму PIAC-1M (2019 р., 1 шт.).* *6. Генератор акустичного шуму DNG-2000 (2022 р., 1 шт.).* *7. Віброметр BENETECH GM 63B (2018 р., 1 шт).* *8. Шумомір BENETECH GM1356 (2022 р., 1 шт.).* *9. Генератор зашумлення телефонних ліній STEALTH SEC model 2003 (2022 р., 2 шт.).* *10. Виявник GPS-трекерів, прихованих відеокамер та жучків GPS SIGNAL DETEKTOR K18 (2022 р., 1 шт.).* *11. Зразки акустичних та вібровипромінювачів.* *12. Інше обладнання лабораторії ТЗЗІ.* *https://drive.google.com/file/d/1kBOjxU27rEtyyBFKwvFa6kKclABS9zrH/view*
ППО2. Моделювання та оптимізація процесів у ІБ	навчальна дисципліна	*ППО2_Моделювання_та_оптимізація_процесів_у_ІБ.pdf*	+ZUoEpPATWNNlg8nbleJ64v/HZDPFaolwpmkGHsYQDg=	*Аудиторний фонд і необхідне обладнання; бібліотеки ЧНУ та кафедр, в тому числі електронні; внутрішня корпоративна пошта та система електронного навчання Moodle (https://moodle.chnu.edu.ua); наявність каналів доступу до Інтернету, в тому числі точка 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 р., 10 шт.).* *2. Проектор мультимедійний Epson EB-X31 (1 шт.).* *3. Екран (1 шт.).* *4. Веб-камера Logitech c170 (2019 р., 1 шт.).* *5. Акустична система Sven312 (1 шт.).*

				https://drive.google.com/file/d/1W8eDMDKMsb4cCNRIWM6OzKL5eA-yfq5f/view
ППО3. Перспективні напрямки розвитку систем кіберзахисту	навчальна дисципліна	*ППО3_Перспективні_напрямки_розвитку_систем_кібер зах.pdf*	lnOzUnXxW9keXCUb/BIxNydUBVyS7OPePsW+xnqyI3U=	*Аудиторний фонд і необхідне обладнання; бібліотеки ЧНУ та кафедр, в тому числі електронні; 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.* *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/1GYMHA6Ue3xvddQJLPgr3KbCk3Jxthb Iu/view*
ППО4. Особливості проектної діяльності в кібербезпеці	навчальна дисципліна	*ППО4_Особлив_проектної_діяльн_в_КБ.pdf*	6Ans5N4FoMuam8lCKo24iJXT+cjxjLw2rZdVBMfPxyo=	*Аудиторний фонд і необхідне обладнання; бібліотеки ЧНУ та кафедр, в тому числі електронні; 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 очного/дистанційного навчання:* *1. Комп'ютер Intel Core i3-10325/3.9GHz/DDR4 8GB 2400 з монітором 20" Acer (2018 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.).* *https://drive.google.com/file/d/115jr1gxMFBwopa5HgDrXRh5Oee1MJTRT/view*
ППО5. Вибрані розділи криптології	навчальна дисципліна	*ППО5_Вибрані_розділи_криптології.pdf*	nNjZf85WeuZ1Jd1hwf26NRtoAZs2kkY3qGQizdcE7Zs=	*Аудиторний фонд і необхідне обладнання; бібліотеки ЧНУ та кафедр, в тому числі електронні; внутрішня корпоративна пошта та система електронного навчання Moodle (https://moodle.chnu.edu.ua); наявність каналів доступу до Інтернету, в тому числі точка доступу Eduroam Ubiquiti UniFi AC LR AP (2021 р., 3 шт.) на КРТтаІБ.* *Проведення лекційних та лабораторних занять: аудиторія В10 - Лабораторія криптографії та стеганографії.* *Обладнання:* *1. Комп'ютер AMD A4-6300-/3.7GHz/DDR4 8GB 2400 MHz/SSD 256 GB з монітором 22" LG (2018 р., 10 шт.).* *2. Проектор мультимедійний Epson EB-X31 (1 шт.).* *3. Екран (1 шт.).* *4. Веб-камера Logitech c170 (2019 р., 1 шт.).* *5. Акустична система Sven312 (1*

				шт.). *https://drive.google.com/file/d/1W8eDMDKMsb4cCNRIWM6OzKL5eA-yfq5f/view*
ППО6. Ліцензування, атестація та сертифікація у сфері безпеки об'єктів інформаційної діяльності	навчальна дисципліна	*ППО6_Ліцензування_атестація_та_серт_в_СБОІД.pdf*	/WGwxTIK5G2sb3clpdPpbLLF1ipEPSg3HRE3CdFAkNA=	*Аудиторний фонд і необхідне обладнання; бібліотеки ЧНУ та кафедр, в тому числі електронні; внутрішня корпоративна пошта та система електронного навчання Moodle (https://moodle.chnu.edu.ua); наявність каналів доступу до Інтернету, в тому числі точка доступу Eduroam Ubiquiti UniFi AC LR AP (2021 р., 3 шт.) на КРТтаІБ.* *Проведення лекційних та практичних занять (в т.ч. в дистанційному форматі):* *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 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*
ППО7. Безпека інфокомунікацій та безперервність бізнес-процесів	навчальна дисципліна	*ППО7_Безпека_інфок_та_безп_бізн_проц.pdf*	1siNHhfuzNeEsBtdB30h8wCpXq20062/Rftt7/yd47E=	*Аудиторний фонд і необхідне обладнання; бібліотеки ЧНУ та кафедр, в тому числі електронні; внутрішня корпоративна пошта та система електронного навчання Moodle (https://moodle.chnu.edu.ua); наявність каналів доступу до Інтернету, в тому числі точка доступу Eduroam Ubiquiti UniFi AC LR AP (2021 р., 3 шт.) на КРТтаІБ.* *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.).* *2. Програмне забезпечення для проведення лабораторних та практичних робіт.* *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*
ППО8. Виробнича практика	практика	*ППО8_Виробнича практика.pdf*	tbOuPGJ1u+hP+4GP7q77Oi3kLGstgx5HRSNnXqY3EKk=	*Матеріально-технічне забезпечення баз практик відповідно до укладених договорів.* *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*
ППО9. Переддипломна практика	практика	*ППО9_Переддипломна_практика.pdf*	KyOLXINSzPSbHWFCR6dSEXOqrbAn2Yk1MsU4JgWoTiU=	*Аудиторний фонд і необхідне обладнання; бібліотеки ЧНУ та кафедр, в тому числі електронні; внутрішня корпоративна пошта та система електронного навчання Moodle (https://moodle.chnu.edu.ua); наявність каналів доступу до Інтернету, в тому числі точка 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*
ППО10. Дипломне проектування (кваліфікаційна	підсумкова атестація	*ППО10_Кваліф_робота.pdf*	WaJE2QfKxvD273wcX11iwwGUti+9bXT7mEHoruqsBIY=	*Лабораторії кафедри радіотехніки та інформаційної безпеки, інших структурних*

робота)				*підрозділів Чернівецького національного університету імені Юрія Федьковича (http://radiotech.chnu.edu.ua/labs/) та бази практик.* *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*

* 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 викладачів ОП

ID викладача	ПІБ	Посада	Структурний підрозділ	Кваліфікація викладача	Стаж	Навчальні дисципліни, що їх викладає викладач на ОП	Обґрунтування
375591	Горбулик Володимир Іванович	доцент, Основне місце роботи	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	Диплом спеціаліста, Чернівецький ордена Трудового Червоного Прапора державний університет, рік закінчення: 1982, спеціальність: фізика, Диплом магістра, Національний технічний університет "Харківський політехнічний інститут", рік закінчення: 2019, спеціальність: 141 Електроенергетика, електротехніка та електромеханіка, Диплом кандидата наук ДК 012321, виданий 14.11.2001, Атестат доцента 12ДЦ 043407, виданий 30.06.2015	14	ППО1. Технології комплексного захисту інформації	Стажування в Тернопільському національному технічному ун-ті імені Івана Пулюя, з 24.05.2021 по 18.06.2021. Свідоцтво ПК № 05408102/001716-21 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». Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 1, 5, 7, 19,20 п. 38 Чинних Ліцензійних умов «Досягнення у професійній діяльності». Методичний посібник : Кушнір М.Я., Горбулик В.І. Ліцензування, атестація та

							сертифікація в сфері безпеки об'єктів інформаційної діяльності. Електронний посібник. http://radiotech.chnu.edu.ua/educationbooks/ Mygushchenko, R., Kropachek, O., Suchkov, H., Rebrov, O., Horbulik, V., & Mygushchenko, K. (2022). Monitoring the state of industrial facilities units using vibration signals. Paper presented at the 2022 IEEE 3rd KhPI Week on Advanced Technology, KhPI Week 2022 – Conference Proceedings, doi:10.1109/KhPIWeek57572.2022.9916336 Retrieved Q4 (Scopus) . https://ieeexplore.ieee.org/document/9916336 . Організатор низки тренінгів та зустрічей студентів і викладачів університету з представниками СБУ, кіберполіції, IT-компаній в рамках Місяця кібербезпеки , 2021, (13.10.2021, 25.10.2021, 2.11.2021) Інженерна академія України, член-кореспондент пр. №26 від 03.07.2015
107190	Шпатар Петро Михайлович	завідувач кафедри, Основне місце роботи	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	Диплом магістра, Чернівецький державний університет імені Юрія Федьковича, рік закінчення: 1999, спеціальність: радіотехніка, Диплом кандидата наук ДК 042595, виданий 11.10.2007, Атестат доцента 12ДЦ 032416, виданий 26.09.2012	18	ППО7. Безпека інфокомунікацій та безперервність бізнес-процесів	Стажування: 1. Вінницький національний технічний університет Свідоцтво про підвищення кваліфікації СПК №301809 від 12.03.2018, 2. Стажування в Тернопільському національному технічному університеті імені Івана Пулюя. Свідоцтво ПК № 05408102/001751-21 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. (180 год, 6 кредитів) 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 06.03.2023-06.05.2023, 180 hours / 6 credits ECTS, Sertificate № 4-2023-ChNU, 06-05-2023. 4. Проходження навчання за програмою підвищення кваліфікації науково-педагогічних працівників щодо розроблення та експертизи завдань ЄДКІ (єдиний державний кваліфікаційний іспит), а саме: дистанційний експрес-курс «Основи тестології та розробки тестових завдань» і практичну частину: розробку та експертизу завдань ЄДКІ за спеціальністю 125 Кібербезпека. Тривалість навчання – 30 годин (1 кредит ECTS). Грудень 2022 - Квітень 2023 року. Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 1, 3, 4, 7, 12, 14, 15 п. 38 Чинних Ліцензійних умов «Досягнення у професійній діяльності». Наявність публікацій та посібників за профілем навчальної дисципліни: 1. Безпека інфокомунікацій та безперервність бізнес-процесів. Електронний навч. посібник. Косован Г.В., Ластівка Г. І., Шпатар П. М. Чернівці : Чернівецький нац. ун-

							т, 2023 р. 2. Методичні вказівки щодо виконання та оформлення випускових кваліфікаційних робіт (проектів): методичні вказівки / укл. : Кушнір М.Я., Ластівка Г. І., Рождественська М. Г., Саміла А.П., Шпатар П.М. [Навчальне електронне видання] – Чернівці : Чернівецький національний університет, 2020.– 81 с. 3. 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. 4. P.M. Shpatar, O.V. Hres, H.M. Rozorinov. Single photons receiver based on avalanche photodiodes. 15th International Conference on Correlation Optics. Ukraine, September 13-16, 2021 http://icco.chnu.edu.ua/2021/09/13/single-photons-receiver-based-on-avalanche-photodiodes/ 5. Криптографія. Методичні вказівки до вивчення дисципліни. Укл.: Шпатар П.М. Електронний навчальний посібник. http://radiotech.chnu.edu.ua/educationbooks/ 6. P.M. Shpatar, O.V. Hres, H.M. Rozorinov Single photons receiver based on avalanche photodiodes. 15th International Conference on Correlation Optics. Ukraine, September 13-16, 2021 Cite Score 2019 (Scopus) = 1.0 http://icco.chnu.edu.ua/2021/09/13/single-photons-receiver-based-on-avalanche-photodiodes 7. Політанський Л.Ф. Особливості програмної реалізації системи стиснення інформації з додатковим шифруванням/Л.Ф.

							Політанський, О.В. Гресь, П.М. Шпатар, Р.Л. Політанський, Г.М. Розорінов // Обробка сигналів і негаусівських процесів, VII Міжнародна науково-практична конференція. – Черкаси, Україна, 23–24 листопада, 2019. – С. 174-175.
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	ППО6. Ліцензування, атестація та сертифікація у сфері безпеки об'єктів інформаційної діяльності	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». Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 1, 6, 8, 10,19 п. 38 Чинних Ліцензійних умов «Досягнення у професійній діяльності». Методичний посібник : Кушнір М.Я., Горбулик В.І. Ліцензування, атестація та сертифікація в сфері безпеки об'єктів інформаційної діяльності. Електронний посібник. http://radiotech.chnu.edu.ua/educationbooks/ Член редколегії вісника університету «Україна», Серія ІНФОКОМУНІКАЦІЙНІ ТА КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ (Категорія Б) https://visn-icct.uu.edu.ua/index.php/icct/about/editorialTeam Науковий керівник двох 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, till 09.26, 2022 https://docs.google.com/document/d/16eXTjjLWItrbh-AoDAmOUCql2xkDTVn/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, 27.01. -27.08. 2023 https://docs.google.com/document/d/1R9nrF94mLZtCozob-nFhWU696PCeSHd_/edit
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	ЗПО1. Наукова та професійна комунікація іноземною мовою	Стажування: березень. 2013 ЧТЕІ КНТУ, каф. сучасних європейських мов № 79-ОП від 11.02.2013; 04.07.2015 – 11.07.2015 Літня школа Британської ради , м. Київ Університет Коньянг (Konyang), Нонсан, Республіка Корея. Науково-методичне стажування 22.09.2020-29.09.2020 (згідно плану стажування та наказу по університету). Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 1, 3, 4, 10, 12, 19, 20 п. 38 Чинних Ліцензійних умов «Досягнення у професійній діяльності». Наявність публікацій та посібників за профілем навчальної дисципліни: 1. 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.) 2. 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.) 3. Венкель Т.В. Англійська мова професійного спрямування. Кібербезпека: Загрози, проблеми, захист: Укл: Венкель Т.В. – Вид. 2-ге, перероблене, доповнене. – Чернівці, 2020. – 102 с. (посібник в електронній формі) 4. 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, Copyright © 2015 (Raef Meeuwisse. Raef Meeuwisse, Icutrain Ltd, First Printing: 2015 First published by: Icutrain Ltd) для студентів 2 курсу спеціальність – 125 "Кібербезпека". – Укл.: Венкель Т.В. – Чернівці, 2020. – 96 с. (посібник в електронній формі). 5. Tetiana Venkel, Olena Maniutina, Andriy Zeluk. Dissimilarity and Ambiguity in Ukrainian and English Cybersecurity Terminology. – Physical and technological problems of transmission, processing and storage

							of information in infocommunication systems: Proceedings of IXth International Scientific-Practical Conference. 21-23 October 2021, Chernivtsi-Suceava (Ukraine-Romania). - "Рута", Чернівці, 2021. - с. 86-87. 6. Участь у підготовці доповідей на міжнародних наукових конференціях: International Display Workshops (Саппоро, Японія, 27-29.11.2019); “CorrOpt” 2019, 2021 рр. – з публікацією доповідей у збірниках матеріалів конференції (у співавторстві з науковцями зазначеного університету). 7. Членство у редакційно-видавничій групі журналу «Безпека інфокомунікаційних систем та Інтернету речей» (https://journals.chnu.edu.ua/index.php/sisiot/about/editorialTeam).
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	ППО4. Особливості проектної діяльності в кібербезпеці	Стажування: кафедра економічної теорії ДВНЗ «Київський національний економічний університет імені Вадима Гетьмана» (2020р.) Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 1, 3, 4, 6, 7, 8, 9, 10, 12, 19 п. 38 Чинних Ліцензійних умов «Досягнення у професійній діяльності». Наявність публікацій та посібників за профілем навчальної дисципліни: 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., Волощук О.А.

Проектний менеджмент :Навчальний посібник. Чернівці, ЧНУ. 2018. 120 с.
3. Галушка З. І., Лусте О.О. Стратегії розвитку бізнесу: теорія і практика. Навчальний посібник. Чернівці. ЧНУ, 2021. 290 с.
4. 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.
5. 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.
6. Галушка З.І. Agile-менеджмент як інноваційний підхід до управління проектами. Інфраструктура ринку. Випуск 47.2020. С. 76-79. http://www.market-infr.od.ua/journals/2020/47_2020_ukr/16.pdf .
7. 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
8. 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
9. 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
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	ППО3. Перспективні напрямки розвитку систем кіберзахисту	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». Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 1, 3, 5, 6, 8, 10, 19 п. 38 Чинних Ліцензійних умов «Досягнення у професійній діяльності». Наявність публікацій та посібників за профілем навчальної дисципліни: 1. 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 2. 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 3. 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 4. 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 5. 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 Науковий керівник двох 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
118310	Ластівка Галина Іванівна	доцент, Основне місце роботи	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	Диплом магістра, Чернівецький державний університет ім. Ю. Федьковича,	17	ЗПО2. Науково-педагогічна діяльність та навчання персоналу в галузі ІБ	Стажування: 1. Lublin University of Technology, "Lubelska Politechnica", Poland. Traineeship: "New knowledge in the development of

				рік закінчення: 1999, спеціальність: Радіотехніка, Диплом кандидата наук ДК 064434, виданий 22.12.2010, Атестат доцента 12ДЦ 035476, виданий 31.05.2013			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. 2. Тернопільський національний технічний ун-т 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». 3. 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. 4. 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 STEM-практика з Інтернету речей та кібербезпеки). З 1.09.2020 по 25.10.2020. Сертифікат від 25.10.2020 р. Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується

							виконанням підпунктів 1, 3, 4, 7, 8, 10, 12, 14 п. 38 Чинних Ліцензійних умов «Досягнення у професійній діяльності». Наявність публікацій та посібників за профілем навчальної дисципліни: 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. Методичні вказівки щодо виконання та оформлення випускових кваліфікаційних робіт (проектів): методичні вказівки / укл. : Кушнір М.Я., Ластівка Г. І., Рождественська М. Г., СамілаА.П., Шпатар П.М. [Навчальне електронне видання] – Чернівці : Чернівецький національний університет, 2020.– 81 с. 3. 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). 4. 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 5. 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 6. 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 7. 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 8. 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=18208

							501513419092697&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.). Сертифікат LangSkill B2 Reference number 19Y138G019DQ1 15/07/2023.
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	12	ППО2. Моделювання та оптимізація процесів у ІБ	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). Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 1, 3, 4, 6, 7, 8 п. 38 Чинних Ліцензійних умов «Досягнення у професійній

							діяльності». Наявність публікацій та посібників за профілем навчальної дисципліни: 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. Springer, Cham. https://doi.org/10.1007/978-3-031-24963-1_35. 7. Управління інформаційною безпекою. Навчальний посібник / [уклад.: Толюпа С.В., Політанський Л.Ф., Політанський Р.Л., Лесінський В.В.] Чернівці.: Чернівецький нац. ун-т ім. Ю.Федьковича, 2021. – 540 с. 8. Членство у редколегії журналу «Безпека інфокомунікаційних систем та Інтернету речей» (https://journals.chnu.edu.ua/index.php/sisiot/about/editorialTeam).
107190	Шпатар Петро Михайлович	завідувач кафедри, Основне місце роботи	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	Диплом магістра, Чернівецький державний університет імені Юрія Федьковича, рік закінчення: 1999, спеціальність: радіотехніка, Диплом кандидата наук ДК 042595, виданий 11.10.2007, Атестат доцента 12ДЦ 032416, виданий 26.09.2012	18	ППО5. Вибрані розділи криптології	Стажування: 1. Вінницький національний технічний університет Свідоцтво про підвищення кваліфікації СПК №301809 від 12.03.2018, 2. Стажування в Тернопільському національному технічному університеті імені Івана Пулюя. Свідоцтво ПК № 05408102/001751-21 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. (180 год, 6 кредитів) 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 06.03.2023-06.05.2023, 180 hours / 6 credits ECTS, Sertificate № 4-2023-ChNU, 06-05-2023. 4. Проходження навчання за програмою підвищення кваліфікації науково-педагогічних працівників щодо розроблення та експертизи завдань ЄДКІ (єдиний державний кваліфікаційний іспит), а саме: дистанційний експрес-курс «Основи тестології та розробки тестових завдань» і практичну частину: розробку та експертизу завдань ЄДКІ за спеціальністю 125 Кібербезпека. Тривалість навчання – 30 годин (1 кредит ECTS). Грудень 2022 - Квітень 2023 року. Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 1, 3, 4, 7, 12, 14, 15 п. 38 Чинних Ліцензійних умов «Досягнення у професійній діяльності». Наявність публікацій та посібників за профілем навчальної дисципліни: 1. P.M. Shpatar, O.V. Hres, H.M. Rozorinov Single photons receiver based on avalanche photodiodes. 15th International Conference on Correlation Optics. Ukraine, September 13-16, 2021 Cite Score 2019 (Scopus) = 1.0 http://icco.chnu.edu.ua/2021/09/13/single-photons-receiver-based-on-avalanche-photodiodes

2. Shpatar P. M. Modified nonautonomous chaotic signal generator based on Chua's scheme / P. M. Shpatar, L. F. Politansky, S. M. Khrapko. // Наукові записки Українського науково-дослідного інституту зв'язку.. – 2017. – №2. – С. 90–97.
3. 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.
4. P.M. Shpatar, O.V. Hres, H.M. Rozorinov. Single photons receiver based on avalanche photodiodes. 15th International Conference on Correlation Optics. Ukraine, September 13-16, 2021 http://icco.chnu.edu.ua/2021/09/13/single-photons-receiver-based-on-avalanche-photodiodes/
5. Криптографія. Методичні вказівки до вивчення дисципліни. Укл.: Шпатар П.М. Електронний навчальний посібник. http://radiotech.chnu.edu.ua/educationbooks/
6. Методичні вказівки щодо виконання та оформлення випускових кваліфікаційних робіт (проектів): методичні вказівки / укл. : Кушнір М.Я., Ластівка Г. І., Рождественська М. Г., Саміла А.П., Шпатар П.М. [Навчальне електронне видання] – Чернівці : Чернівецький національний університет, 2020.– 81 с.
7. Гресь О.В. Лінійний режим фотореєстрації поодиноких фотонів в системі квантового розподілу ключів/О.В. Гресь, А.Я. Томулець, П.М. Шпатар// Міжнародна науково-практична конференція "Наукоємкі технології

							в інфокомунікаціях". НІСТ-2019. – 23-25 травня 2019. – Харків – Кам'янець-Подільський, Україна. С. 51-52. 8. Політанський Л.Ф. Особливості програмної реалізації системи стиснення інформації з додатковим шифруванням/Л.Ф. Політанський, О.В. Гресь, П.М. Шпатар, Р.Л. Політанський, Г.М. Розорінов // Обробка сигналів і негаусівських процесів, VII Міжнародна науково-практична конференція. – Черкаси, Україна, 23–24 листопада, 2019. – С. 174-175.

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**
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.	☒	ППО8. Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		ППО9. Переддипломна практика	Практика, дипломне проектування. 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) - захист звітів про проходження переддипломної практики на кафедрі.
		ППО4. 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,	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).

			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.	
		ППО3. 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 книгою: 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).
		ППО2. Моделювання та оптимізація процесів у ІБ	Лекції: пояснювально-ілюстративний метод, презентації; робота з книгою: з навчально-методичною, науковою літературою; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах, виступи, усні відповіді та доповіді on-line; самостійна робота: підготовка презентацій, рефератів, а також формуванням напрацювань для виконання і захисту практичних робіт.	Поточний контроль – усні та письмові (тестування, захист завдань практичного характеру, розширені відповіді, що висвітлюють теоретичні питання) відповіді здобувача освіти. Підсумковий контроль (залік) – усне або письмове опитування, тестовий контроль.
		ППО1. 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.	Поточний контроль: усні та письмові (контрольна робота,тестування) відповіді студента, захист курсових робіт. Підсумковий контроль: екзамен (усне, письмове опитування, тестовий контроль).

			.	
		ППО10. 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.
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.	☒	ЗПО1. 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.
		ППО3. 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 книгою: з науковою літературою, 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).
		ППО8. Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		ППО9. Переддипломна практика	Практика, дипломне проектування. Дослідницький метод;	Поточний контроль - презентація результатів виконання завдань.

			пояснення; бесіда; дискусія, робота з навчально-методичною та фаховою літературою, самостійна робота, проведення досліджень за обраною темою.	Підсумковий контроль (залік) - захист звітів про переддипломну практику на кафедрі.
		ППО10. 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.
		ППО7. 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, ділова гра, рольова гра 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.
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.	☒	ППО10. 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.
		ППО9. Переддипломна практика	Практика, дипломне проектування. 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) - захист звітів про проходження переддипломної практики на кафедрі.

		ППО8. Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		ППО3. 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 книгою: 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).
		ППО1. 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. .	Поточний контроль: усні та письмові (контрольна робота,тестування) відповіді студента, захист курсових робіт. Підсумковий контроль: екзамен (усне, письмове опитування, тестовий контроль).
		ЗПО2. Науково-педагогічна діяльність та навчання персоналу в галузі ІБ	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); робота з книгою: 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	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.

			індивідуальним завданням або за програмою навчальної дисципліни (реферат, доповідь тощо).	
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.	☒	ППО1. 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.	Поточний контроль: усні та письмові (контрольна робота,тестування) відповіді студента, захист курсових робіт. Підсумковий контроль: екзамен (усне, письмове опитування, тестовий контроль).
		ППО7. 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, ділова гра, рольова гра 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.
		ППО8. Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		ППО9. Переддипломна практика	Практика, дипломне проектування. 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) - захист звітів про проходження переддипломної практики на кафедрі.
		ППО10. Дипломне проектування (кваліфікаційна робота)	Дослідницький метод; словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з	Захист кваліфікаційної (дипломної) роботи.

			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.	
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.	☒	ППО10. 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.
		ППО9. Переддипломна практика	Практика, дипломне проектування. 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) - захист звітів про проходження переддипломної практики на кафедрі.
		ППО3. 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 книгою: 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).
		ППО5. Вибрані розділи криптології	Лекції: пояснювально-ілюстративний метод; лабораторні заняття: евристичний метод, метод проблемного викладу; самостійна робота: репродуктивний метод, дослідницький метод; опрацювання літературних джерел та інформаційних ресурсів.	Поточний контроль – виконання та захист завдань лабораторного практикуму, усне та фронтальне опитування. Підсумковий контроль – залік (письмове опитування, тестовий контроль).
		ППО8. Виробнича	Словесні методи (розповідь,	Підсумковий контроль

		практика	бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	(залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	☒	ППО9. Переддипломна практика	Практика, дипломне проектування. 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) - захист звітів про проходження переддипломної практики на кафедрі.
		ППО10. 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.
		ППО7. 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, ділова гра, рольова гра 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.
		ППО8. Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		ППО1. Технології комплексного захисту інформації	Лекції: пояснювально-ілюстративний метод, презентації;	Поточний контроль: усні та письмові (контрольна робота,тестування) відповіді

			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.	студента, захист курсових робіт. Підсумковий контроль: екзамен (усне, письмове опитування, тестовий контроль).
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.	☒	ППО1. 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.	Поточний контроль: усні та письмові (контрольна робота,тестування) відповіді студента, захист курсових робіт. Підсумковий контроль: екзамен (усне, письмове опитування, тестовий контроль).
		ППО3. 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 книгою: 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).
		ППО5. Вибрані розділи криптології	Лекції: пояснювально-ілюстративний метод; лабораторні заняття: евристичний метод, метод проблемного викладу; самостійна робота: репродуктивний метод, дослідницький метод; опрацювання літературних джерел та інформаційних ресурсів.	Поточний контроль – виконання та захист завдань лабораторного практикуму, усне та фронтальне опитування. Підсумковий контроль – залік (письмове опитування, тестовий контроль).
		ППО6. Ліцензування, атестація та сертифікація у сфері безпеки об'єктів	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); практичні заняття: наочні	Поточний контроль – усні та письмові (тестування, захист завдань практичного характеру) відповіді

		інформаційної діяльності	методи (презентації, ілюстрації, тощо); інтерактивні методи навчання: робота в малих групах та тренінги; 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 (реферат, доповідь тощо).	здобувача освіти. Підсумковий контроль (екзамен) – усне, письмове опитування, тестовий контроль.
		ППО7. 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, ділова гра, рольова гра 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.
		ППО8. Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		ППО9. Переддипломна практика	Практика, дипломне проектування. 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) - захист звітів про проходження переддипломної практики на кафедрі.
		ППО10. 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	Захист кваліфікаційної (дипломної) роботи.

			тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	☒	ППО10. 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.
		ППО1. 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.	Поточний контроль: усні та письмові (контрольна робота,тестування) відповіді студента, захист курсових робіт. Підсумковий контроль: екзамен (усне, письмове опитування, тестовий контроль).
		ППО7. 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, ділова гра, рольова гра 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.
		ППО8. Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод,	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.

			дослідницький метод.	
		ППО9. Переддипломна практика	Практика, дипломне проектування. 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) - захист звітів про проходження переддипломної практики на кафедрі.
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.	☒	ППО10. 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.
		ППО1. 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.	Поточний контроль: усні та письмові (контрольна робота,тестування) відповіді студента, захист курсових робіт. Підсумковий контроль: екзамен (усне, письмове опитування, тестовий контроль).
		ППО3. 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 книгою: 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).
		ППО4. Особливості проектної діяльності в	Лекції: пояснювально-ілюстративний метод,	Поточний контроль: усні та письмові (опитування під

		кібербезпеці	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.	час занять, тестування, обговорення завдань практичного характеру, доповідь за індивідуальною темою) відповіді студента. Підсумковий контроль – екзамен (усне або письмове опитування; тестовий контроль).
		ППО7. 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, ділова гра, рольова гра 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.
		ППО8. Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		ППО9. Переддипломна практика	Практика, дипломне проектування. 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) - захист звітів про проходження переддипломної практики на кафедрі.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі	☒	ППО1. Технології комплексного захисту інформації	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо);	Поточний контроль: усні та письмові (контрольна робота,тестування) відповіді студента, захист курсових робіт. Підсумковий контроль: екзамен (усне, письмове опитування, тестовий контроль).

стратегії і політики інформаційної безпеки.			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.	
		ППО8. Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		ППО9. Переддипломна практика	Практика, дипломне проектування. 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) - захист звітів про проходження переддипломної практики на кафедрі.
		ППО10. 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.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.	☒	ППО3. 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 книгою: 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).
		ППО1. Технології комплексного захисту	Лекції: пояснювально-ілюстративний метод,	Поточний контроль: усні та письмові (контрольна

		інформації	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.	робота,тестування) відповіді студента, захист курсових робіт. Підсумковий контроль: екзамен (усне, письмове опитування, тестовий контроль).
		ППО8. Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		ППО9. Переддипломна практика	Практика, дипломне проектування. 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) - захист звітів про проходження переддипломної практики на кафедрі.
		ППО10. 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.
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.	☐	ППО10. 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	Захист кваліфікаційної (дипломної) роботи.

			навчальної дисципліни.	
		ППО9. Переддипломна практика	Практика, дипломне проектування. 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) - захист звітів про проходження переддипломної практики на кафедрі.
		ЗПО2. Науково-педагогічна діяльність та навчання персоналу в галузі ІБ	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); робота з книгою: 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.
		ППО7. 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, ділова гра, рольова гра 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.
		ППО8. Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності	☒	ППО7. Безпека інфокомунікацій та безперервність бізнес-процесів	Лекції: пояснювально-ілюстративний метод, презентації; робота з книгою: з навчально-методичною, науковою та нормативною	Поточний контроль – усні та письмові (тестування, захист лабораторних робіт, захист завдань практичного характеру) відповіді здобувача освіти.

функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.			літературою; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах, ділова гра, рольова гра та тренінги; лабораторні заняття: метод проблемного підходу, дослідницький метод; самостійна робота: підготовка презентацій, рефератів, а також формуванням напрацювань для виконання і захисту лабораторних робіт.	Підсумковий контроль (екзамен) – усне або письмове опитування, тестовий контроль.
		ППО8. Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		ППО9. Переддипломна практика	Практика, дипломне проектування. 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) - захист звітів про проходження переддипломної практики на кафедрі.
		ППО10. 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.
РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.	☒	ППО9. Переддипломна практика	Практика, дипломне проектування. 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) - захист звітів про проходження переддипломної практики на кафедрі.
		ЗПО1. 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.	
		ЗПО2. Науково-педагогічна діяльність та навчання персоналу в галузі ІБ	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); робота з книгою: 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.
		ППО8. Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		ППО3. 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 книгою: 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).
		ППО10. 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	Захист кваліфікаційної (дипломної) роботи.

			навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	
		ППО6. Ліцензування, атестація та сертифікація у сфері безпеки об'єктів інформаційної діяльності	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); практичні заняття: наочні методи (презентації, ілюстрації, тощо); інтерактивні методи навчання: робота в малих групах та тренінги; 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 (реферат, доповідь тощо).	Поточний контроль – усні та письмові (тестування, захист завдань практичного характеру) відповіді здобувача освіти. Підсумковий контроль (екзамен) – усне, письмове опитування, тестовий контроль.
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.	☒	ППО4. 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).
		ППО8. Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		ППО9. Переддипломна практика	Практика, дипломне проектування. 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) - захист звітів про проходження переддипломної практики на кафедрі.

		ППО10. 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.
		ППО2. Моделювання та оптимізація процесів у ІБ	Лекції: пояснювально-ілюстративний метод, презентації; робота з книгою: з навчально-методичною, науковою літературою; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах, виступи, усні відповіді та доповіді on-line; самостійна робота: підготовка презентацій, рефератів, а також формуванням напрацювань для виконання і захисту практичних робіт.	Поточний контроль – усні та письмові (тестування, захист завдань практичного характеру, розширені відповіді, що висвітлюють теоретичні питання) відповіді здобувача освіти. Підсумковий контроль (залік) – усне або письмове опитування, тестовий контроль.
		ППО7. 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, ділова гра, рольова гра 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.
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.	☒	ЗПО2. Науково-педагогічна діяльність та навчання персоналу в галузі ІБ	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); робота з книгою: 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	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.

			«мозкового штурму», ділова гра, рольова гра та інші освітні технології; самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни (реферат, доповідь тощо).	
		ППО8. Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		ППО9. Переддипломна практика	Практика, дипломне проектування. 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) - захист звітів про проходження переддипломної практики на кафедрі.
		ППО10. 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.
		ППО3. 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 книгою: 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).
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з	☒	ЗПО2. Науково-педагогічна діяльність та навчання персоналу в галузі ІБ	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною,	Поточний контроль – тести, опитування (усне та письмове), представлення презентації, доповідь та аргументований захист у

персоналом у напряму інформаційної безпеки та/або кібербезпеки.			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).	процесі командної роботи. Підсумковий контроль (екзамен) – усне, письмове опитування, тестовий контроль.
		ППО8. Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		ППО9. Переддипломна практика	Практика, дипломне проектування. 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) - захист звітів про проходження переддипломної практики на кафедрі.
		ППО10. 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.
РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та	☒	ППО9. Переддипломна практика	Практика, дипломне проектування. 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) - захист звітів про проходження переддипломної практики на кафедрі.
		ППО10. Дипломне проектування (кваліфікаційна робота)	Дослідницький метод; словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо);	Захист кваліфікаційної (дипломної) роботи.

захисту інтелектуальної власності.			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.	
		ППО4. 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).
		ППО6. Ліцензування, атестація та сертифікація у сфері безпеки об'єктів інформаційної діяльності	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); практичні заняття: наочні методи (презентації, ілюстрації, тощо); інтерактивні методи навчання: робота в малих групах та тренінги; 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 (реферат, доповідь тощо).	Поточний контроль – усні та письмові (тестування, захист завдань практичного характеру) відповіді здобувача освіти. Підсумковий контроль (екзамен) – усне, письмове опитування, тестовий контроль.
		ППО8. Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі	☒	ППО3. Перспективні напрямки розвитку систем кіберзахисту	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; семінарські заняття:	Поточний контроль: усні та письмові (тестування, захист лабораторних робіт, представлення доповідей та захист рефератів) відповіді

інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.			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 книгою: з науковою та літературою професійного спрямування.	здобувача освіти. Підсумковий контроль – екзамен (усне або письмове опитування; тестовий контроль, в тому числі засобами платформ електронного навчання).
		ППО4. 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).
		ППО5. Вибрані розділи криптології	Лекції: пояснювально-ілюстративний метод; лабораторні заняття: евристичний метод, метод проблемного викладу; самостійна робота: репродуктивний метод, дослідницький метод; опрацювання літературних джерел та інформаційних ресурсів.	Поточний контроль – виконання та захист завдань лабораторного практикуму, усне та фронтальне опитування. Підсумковий контроль – залік (письмове опитування, тестовий контроль).
		ППО7. 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, ділова гра, рольова гра 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.

		ППО8. Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		ППО9. Переддипломна практика	Практика, дипломне проектування. 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) - захист звітів про проходження переддипломної практики на кафедрі.
		ППО10. 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.	☒	ППО10. 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.
		ППО2. Моделювання та оптимізація процесів у ІБ	Лекції: пояснювально-ілюстративний метод, презентації; робота з книгою: з навчально-методичною, науковою літературою; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах, виступи, усні відповіді та доповіді on-line; самостійна робота: підготовка презентацій, рефератів, а також формуванням напрацювань для виконання і захисту	Поточний контроль – усні та письмові (тестування, захист завдань практичного характеру, розширені відповіді, що висвітлюють теоретичні питання) відповіді здобувача освіти. Підсумковий контроль (залік) – усне або письмове опитування, тестовий контроль.

			практичних робіт.	
		ППО3. 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 книгою: 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).
		ППО9. Переддипломна практика	Практика, дипломне проектування. 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) - захист звітів про проходження переддипломної практики на кафедрі.
		ППО8. Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
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.	☒	ЗПО2. Науково-педагогічна діяльність та навчання персоналу в галузі ІБ	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); робота з книгою: 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.
		ППО2. Моделювання та оптимізація процесів у ІБ	Лекції: пояснювально-ілюстративний метод, презентації; робота з книгою: з навчально-методичною, науковою літературою; практичні заняття:	Поточний контроль – усні та письмові (тестування, захист завдань практичного характеру, розширені відповіді, що висвітлюють теоретичні питання) відповіді здобувача освіти.

			репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах, виступи, усні відповіді та доповіді on-line; самостійна робота: підготовка презентацій, рефератів, а також формуванням напрацювань для виконання і захисту практичних робіт.	Підсумковий контроль (залік) – усне або письмове опитування, тестовий контроль.
		ППО4. 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).
		ППО7. 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, ділова гра, рольова гра 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.
		ППО8. Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		ППО9. Переддипломна практика	Практика, дипломне проектування. Дослідницький метод; пояснення; бесіда; дискусія, робота з навчально-методичною та фаховою	Поточний контроль - презентація результатів виконання завдань. Підсумковий контроль (залік) - захист звітів про проходження

			літературою, самостійна робота, проведення досліджень за обраною темою.	переддипломної практики на кафедрі.
		ППО10. 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.
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.	☒	ППО5. Вибрані розділи криптології	Лекції: пояснювально-ілюстративний метод; лабораторні заняття: евристичний метод, метод проблемного викладу; самостійна робота: репродуктивний метод, дослідницький метод; опрацювання літературних джерел та інформаційних ресурсів.	Поточний контроль – виконання та захист завдань лабораторного практикуму, усне та фронтальне опитування. Підсумковий контроль – залік (письмове опитування, тестовий контроль).
		ППО6. Ліцензування, атестація та сертифікація у сфері безпеки об'єктів інформаційної діяльності	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); практичні заняття: наочні методи (презентації, ілюстрації, тощо); інтерактивні методи навчання: робота в малих групах та тренінги; 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 (реферат, доповідь тощо).	Поточний контроль – усні та письмові (тестування, захист завдань практичного характеру) відповіді здобувача освіти. Підсумковий контроль (екзамен) – усне, письмове опитування, тестовий контроль.
		ППО7. 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, ділова гра, рольова гра та тренінги; лабораторні заняття: метод проблемного підходу, дослідницький метод; самостійна робота: підготовка презентацій, рефератів, а також	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.

			формуванням напрацювань для виконання і захисту лабораторних робіт.	
		ППО8. Виробнича практика	Словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		ППО9. Переддипломна практика	Практика, дипломне проектування. 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) - захист звітів про проходження переддипломної практики на кафедрі.
		ППО10. 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.
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.	☒	ППО1. 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.	Поточний контроль: усні та письмові (контрольна робота,тестування) відповіді студента, захист курсових робіт. Підсумковий контроль: екзамен (усне, письмове опитування, тестовий контроль).
		ППО9. Переддипломна практика	Практика, дипломне проектування. 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) - захист звітів про проходження переддипломної практики на кафедрі.
		ППО8. Виробнича	Словесні методи (розповідь,	Підсумковий контроль

		практика	бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	(залік) – за результатами захисту звіту про виконання програми виробничої практики на кафедрі.
		ППО7. 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, ділова гра, рольова гра 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.
		ППО10. 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.
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.	☒	ППО7. 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, ділова гра, рольова гра 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.
		ППО8. Виробнича практика	Словесні методи (розповідь, бесіда, консультація,	Підсумковий контроль (залік) – за результатами

			дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з літературою професійного спрямування; самостійна робота: репродуктивний метод, дослідницький метод.	захисту звіту про виконання програми виробничої практики на кафедрі.
		ППО9. Переддипломна практика	Практика, дипломне проектування. 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) - захист звітів про проходження переддипломної практики на кафедрі.
		ППО10. 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.