

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	Чернівецький національний університет імені Юрія Федьковича
Освітня програма	22991 Кібербезпека
Рівень вищої освіти	Бакалавр
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	22991
Назва ОП	Кібербезпека
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Спеціалізація (за наявності)	<i>відсутня</i>
Рівень вищої освіти	Бакалавр
Тип освітньої програми	Освітньо-професійна
Вступ на освітню програму здійснюється на основі ступеня (рівня)	Повна загальна середня освіта, Фаховий молодший бакалавр, ОКР «молодший 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 іноземних мов, кафедра іноземних мов для природничих факультетів; факультет математики та інформатики, кафедра диференційних рівнянь; Навчально-науковий інститут фізико-технічних та комп'ютерних наук; факультет історії, політології та міжнародних відносин, кафедра історії України; факультет фізичної культури та здоров'я людини, кафедра фізичного виховання; філологічний факультет, кафедра історії та культури української мови, кафедра філософії та культурології.
Місце (адреса) провадження освітньої діяльності за ОП	Навчально-науковий ІФТКН, 58002, м. Чернівці, вул. Сторожинецька, 101
Освітня програма передбачає присвоєння професійної кваліфікації	<i>не передбачає</i>
Професійна кваліфікація, яка присвоюється за ОП (за наявності)	<i>відсутня</i>
Мова (мови) викладання	Українська
ID гаранта ОП у ЄДЕБО	118310
ПІБ гаранта ОП	Ластівка Галина Іванівна
Посада гаранта ОП	доцент
Корпоративна електронна адреса гаранта ОП	g.lastivka@chnu.edu.ua
Контактний телефон гаранта ОП	+38(037)-250-94-89
Додатковий телефон гаранта ОП	+38(098)-998-58-21

Форми здобуття освіти на ОП	Термін навчання
очна денна	3 р. 10 міс.

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

Освітньо-професійна програма «Кібербезпека» підготовки здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю 125 – Кібербезпека запроваджена у 2017 році; остання редакція затверджена Вченою радою ЧНУ 03.04.2023 р. (протокол №3) та введена в дію наказом №118 від 03.04.2023 р. За підготовку бакалаврів за ОП «Кібербезпека» відповідає кафедра радіотехніки та інформаційної безпеки (КРТтаІБ) Навчально-наукового інституту фізико-технічних та комп'ютерних наук ЧНУ.

Враховуючи значний досвід підготовки фахівців за напрямом «Інформаційна безпека», розпочато в ЧНУ у 2002 р., та зміни акцентів в інтересах абітурієнтів, аналіз ситуації на ринку праці та тенденцій його розвитку, пропозиції стейкхолдерів та досвід інших ЗВО, була розроблена нова освітньо-професійна програма «Кібербезпека», за якою в 2021 році відбувся перший випуск бакалаврів. На формування цієї ОП вплинула плідна співпраця кафедри КРТтаІБ ЧНУ з держструктурами та промисловими підприємствами Західного регіону, що створює можливості підготовки висококваліфікованих фахівців у сфері інформаційної безпеки та систем технічного захисту інформації.

В основу ОП «Кібербезпека» покладено ідею ґрунтовної базової підготовки майбутніх фахівців, а також формування індивідуальної освітньої траєкторії здобувача завдяки гнучкій системі, що поєднує вибіркові дисципліни, практику, тематику індивідуальних завдань та дипломного проектування і орієнтується на подальше працевлаштування випускника. Досвід діяльності ЧНУ та інших регіональних ЗВО підтверджують справедливості такого підходу.

Пізніше, враховуючи зміни нормативного характеру в ЧНУ було започатковано ОП «Кібербезпека та захист інформації» (протокол засідання Вченої ради №3 від 03.04.2023 р., наказ № 118 від 03.04.2023 р.). Набір у 2023-2024 н.р. здійснювався за оновленою ОП.

У 2019 році ОП «Кібербезпека» підготовки здобувачів першого (бакалаврського) рівня вищої освіти у Чернівецькому національному університеті імені Юрія Федьковича успішно пройшла акредитацію.

Зміст ОП регулярно оновлюється. Робоча група проводить зустрічі та опитування усіх зацікавлених в ОП, регулярно збирає зауваження та пропозиції для її вдосконалення. Блок вибірових 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	ОД
1 курс	2023 - 2024	26	26	2
2 курс	2022 - 2023	33	33	1
3 курс	2021 - 2022	21	21	0
4 курс	2020 - 2021	31	31	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	3250 Системи технічного захисту інформації 2402 Кібербезпека
третій (освітньо-науковий/освітньо-творчий) рівень	програми відсутні

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

	Загальна площа	Навчальна площа
Усі приміщення ЗВО	123622	32909
Власні приміщення ЗВО (на праві власності, господарського відання або оперативного управління)	116304	30535
Приміщення, які використовуються на іншому праві, аніж право власності, господарського відання або оперативного управління (оренда, безоплатне користування тощо)	7318	2374
Приміщення, здані в оренду	1284	0

Примітка. Для ЗВО із ВСП інформація зазначається:

- щодо ОП, яка реалізується у базовому ЗВО – без урахування приміщень ВСП;
- щодо ОП, яка реалізується у ВСП – лише щодо приміщень даного ВСП.

8. Документи щодо ОП

Документ	Назва файла	Хеш файла
Освітня програма	<i>ОПП (ЧНУ)_125_K66_бак_2023.pdf</i>	8XPUQKhlY5GaRj4bx+VdfT1M8VAIG3J27Todx37Ldk=
Навчальний план за ОП	<i>План_бак_кбб_2023_.pdf</i>	8l5uQmlC3wAhLEsBzsZfct+Y1BiWst8I6dhSatmB3Vo=
Рецензії та відгуки роботодавців	<i>Рец_ВНТУ.pdf</i>	kaFJOu9lxbYftrrfXwOhBprXoE3O3S9KGLlRrSBBENk=
Рецензії та відгуки роботодавців	<i>Рец_Cluster_Bit.pdf</i>	b6ser2QCjb8tKLlC6krGIPajaNwpp+woO9hootAOFAI=

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, конкурентоспроможних фахівців у сфері кібербезпеки та захисту інформації на основі співпраці з підприємствами, організаціями та державними установами Західного регіону (зокрема, Держспецзв'язку, Національна поліція України, СБУ, IT-компанії Datamі, SoftServe тощо), науково-дослідними та освітніми закладами України та інших країн, з урахуванням індивідуальних потреб здобувачів.

Особливостями програми є ґрунтовна підготовка з англійської мови, можливість отримати базові знання та практичні навички щодо методів і засобів забезпечення захисту інформації, а також інформаційно-телекомунікаційних систем і мереж, що відповідає запитам стейкхолдерів.

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

Згідно Стратегічного плану розвитку ЧНУ (<http://surl.li/afflo>), Статуту ЧНУ (<https://bit.ly/3vQ58vY>) та Концепції розвитку ЧНУ (https://www.chnu.edu.ua/media/fwmjte4r/kontseptsiia-rozvytku-universytetu_2023-2026.pdf) ОП «Кібербезпека» відповідає місії ЧНУ, яка передбачає інновативність, 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/>, <https://cutt.ly/MwXi8KtI>), 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 загалом задоволені ОП, проте 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 відчувати себе активним суб'єктом навчальної та майбутньої професійної діяльності, спроможним визначати особистісні цілі й засоби їх досягнення (<http://surl.li/qcfd>; <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 вибіркового ОК, а також коригуються форми й методи організації освітнього процесу тощо. Зокрема, враховано пропозицію здобувача Дубиняка О. відносно розширення переліку вибіркового ОК дисципліною «Основи штучного інтелекту», а здобувачкою Зайцевою В. запропоновано приділити більше уваги проблемам розроблення та тестування веб-додатків щодо їх захищеності від відомих загроз, що відображено у введенні відповідної теми до вибіркової дисципліни «Додаткові розділи програмування». Ці та інші пропозиції підтримані проектною групою для підсилення ПРН 4, 5, 20, 52 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 ІТ компаній 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>) було запропоновано розширити перелік вибіркового дисциплін курсом «Мережеве обладнання», що підсилює ПРН 13, ПРН 31 та ПРН 52. За пропозиціями представників ІТ компаній (зокрема регіональних представництв Datami та SoftServe) було скореговано визначений освітньою програмою ПРН55 (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» (https://radiotech.chnu.edu.ua/opp_125_bachelor/). 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 КНУ ім. Тараса Шевченка, НУ «Львівська політехніка». 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 (рецензента Яремчука Ю.Є., голів ЕК Толюпи С.В. та Стахіри П.Й.), що враховують сучасні тенденції розвитку ринку праці та підвищення ефективності набуття здобувачами ПРН 16, ПРН 28, ПРН29 та ПРН30, запроваджена ОК27.

Ефективність такої співпраці підсилюється залученням здобувачів освіти та викладачів випускової кафедри 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 та інші заінтересовані сторони вибудовують концепцію підготовки майбутніх випускників, тому під час формулювання цілей та ПРН 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 бакалаврів (<https://bit.ly/3r2uBn8>, <https://bit.ly/3QnyOIw>).

Водночас випусковою кафедрою проводиться активна робота та 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 ОК4, ОК12, ОК14 та ОК23 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 галузях, у повній мірі узгоджуються з програмними результатами ОП, сформульованими у відповідності до чинного стандарту освіти. Також конкурентна перевага на ринку праці підсилюється програмним результатом ПРН 55, набуття якого готує здобувачів до роботи в умовах реального бізнесу.

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 ПРН, 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 (<http://surl.li/qchsr>).

На регіональному рівні тенденції розвитку ОПП «Кібербезпека» враховують відповідні програми і плани розвитку Чернівецької області на період до 2027 р. (<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 вибірових 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 ПРН ОП враховано досвід провідних ЗВО України, зокрема: ХНУ, КНУ ім. Тараса Шевченка, КПІ імені Ігоря Сікорського, ВНТУ, а також ОПП «Кібербезпека» ТНТУ. 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 гостьових лекцій.

У рамках міжнародної співпраці представники робочої групи ознайомлюються з подібними ОП іноземних ЗВО. Зокрема, у формулюванні цілей та ПРН ОП враховано досвід Сучавського університету Штефана чел Маре (<https://fiesc.usv.ro/licenta-educatie/>, <http://surl.li/qcykt>), а саме впорядковано блоки обов'язкових та вибірових дисциплін.

У рамках міжнародного стажування представники робочої групи ознайомлюються з подібними ОП підготовки бакалаврів 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 ОК4, ОК22, ОК23, ОК27 та підкріплюють ПРН 4, 5, 52, 55.

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

ОПП «Кібербезпека» підготовки здобувачів першого (бакалаврського) рівня вищої освіти розроблена з урахуванням Стандарту вищої освіти за спеціальністю 125 – Кібербезпека галузі знань 12 – Інформаційні технології, затвердженого наказом № 1074 МОН України від 04.10.2018 р. (<https://mon.gov.ua/storage/app/media/vishcha-osvita/2022/Standarty.Vyshchoyi.Osvity/Zatverdzeni.Standarty/01/31/125-Kiberbezpeka-bak.31.01.22.pdf>).

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 першого (бакалаврського) рівня вищої освіти;

– згідно Стандарту вищої освіти, об'єктами професійної діяльності випускників в ОП виступають об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; технології забезпечення безпеки інформації; процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту;

– згідно Стандарту вищої освіти, теоретичний зміст ОП включає знання законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; теорії, моделей та принципів управління доступом до інформаційних ресурсів; теорії систем управління інформаційною та/або кібербезпекою; методів та засобів виявлення, управління та ідентифікації ризиків; методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; методів та засобів технічного та криптографічного захисту інформації;

сучасних інформаційно-комунікаційних технологій; сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; автоматизованих систем проектування;

- 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, методик, інформаційно-комунікаційних технологій та інших технологій забезпечення інформаційної та/ або кібербезпеки;
- в ОП передбачене застосування як інструментів та обладнання систем розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій;
- згідно Стандарту вищої освіти в ОП передбачено можливість вільного вибору дисциплін (25 %) 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?

Стандарт вищої освіти за спеціальністю 125 – Кібербезпека галузі знань 12 – Інформаційні технології затверджений наказом № 1074 МОН України від 04.10.2018 р. (<https://mon.gov.ua/storage/app/media/vishcha-osvita/2022/Standarty.Vyshchoyi.Osvity/Zatverdzeni.Standarty/01/31/125-Kiberbezpeka-bak.31.01.22.pdf>). Програмні результати навчання за ОПП «Кібербезпека» відповідають Стандарту вищої освіти за спеціальністю 125 – Кібербезпека за першим (бакалаврським) рівнем.

2. Структура та зміст освітньої програми

Яким є обсяг ОП (у кредитах ЄКТС)?

240

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)?

180

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

60

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 ПРН, що відповідають предметній області 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 висококваліфікованих, конкурентоспроможних фахівців у сфері кібербезпеки та захисту інформації на основі співпраці з підприємствами, організаціями та державними установами Західного регіону, науково-дослідними та освітніми закладами України та інших країн, з урахуванням індивідуальних потреб здобувачів. Особливостями програми є ґрунтовна підготовка з англійської мови, можливість отримати базові знання та практичні навички щодо методів і засобів забезпечення захисту інформації, а також інформаційно-телекомунікаційних систем і мереж, що відповідає запитам стейкхолдерів. 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 дослідницького характеру. ОП містить також практичну складову, до якої входять в тому числі ознайомча (ОК31) та виробничо-технологічна (ОК32) практики, 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 випускної кваліфікаційної роботи/проекту (ОК33) дозволяє здобувачу продемонструвати рівень засвоєння освітніх компонент, що враховують усі програмні результати навчання ОП.

Згідно Стандарту атестація випускників за ОП також передбачає складання єдиного кваліфікаційного іспиту. До освітніх компонент вибіркового блоку ОП можливе залучення інших кафедр НН ІФТКН та університету,

стейхолдерів 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 бакалавра, 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 вибіркового компоненту 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, бакалаврам 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 кваліфікаційної роботи/проекту з індивідуальними потребами професійної діяльності (https://radiotech.chnu.edu.ua/diploma_design/). Результативність такого підходу підтверджується наявністю патентів (наприклад, <https://iprop-ua.com/inv/7ccvpfhi>), актів впровадження у виробництво та освітній процес розробок бакалаврських робіт/проектів (https://radiotech.chnu.edu.ua/diploma_design/).

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

Можливість реалізувати своє право на вибір навчальних дисциплін регламентується «Положенням про порядок реалізації студентами ЧНУ права на вибір навчальних дисциплін» (надалі Положення) (<http://surl.li/affog>). Навчальні дисципліни за вибором здобувача вищої освіти вводяться в ОП з метою задоволення індивідуальних освітніх потреб студентів, посилення їх конкурентоспроможності на ринку праці, сприяють академічній мобільності бакалавра, а їх частка в ОПІ «Кібербезпека» складає 25% кредитів ЄКТС від загального обсягу.

Перелік вибіркового компоненту підготовки бакалавра за ОПІ «Кібербезпека» визначається випусковою кафедрою (http://radiotech.chnu.edu.ua/elective_subjects/).

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 реалізують 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 вибіркового компоненту. 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 вибіркового компоненту (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 вибіркового компоненту (<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, ознайомчої та виробничо-технологічної практик, які регламентуються «Положенням про проведення практики», (<https://drive.google.com/file/d/1EMTdogrzwMD6gmLzuThArr1uKS6U2Bj6/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 визначено коло підприємств, які здатні організувати 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 «Міжособистісне спілкування і побудова команд» (ОК7), «Філософія» (ОК9), «Вступ до кібербезпеки» (ОК10), «Основи комп'ютерних технологій» (ОК11), «Основи інфокомунікацій» (ОК13), «Безпека інформаційно-телекомунікаційних систем» (ОК28), а також практики (ОК31-32). Дисципліни, що передбачають групову форму виконання лабораторних робіт (наприклад, «Криптографія» (ОК23), «Канали витоку інформації» (ОК21), «Взаємодія між компонентами систем IoT» (ОК22)) тощо також забезпечують формування soft skills. Важливе місце у набутті студентами вміння вільно спілкуватись, доносити свою думку колегам та зацікавленим особам зрозуміло і ввічливо, використовуючи професійну термінологію, займають консультації перед захистом дипломних проєктів/робіт, що регулярно проводяться викладачами випускової кафедри протягом місяця, що передуює захисту в ЕК. На цих зустрічах бакалаври роблять доповіді за темою проєкту чи дослідження, отримують конструктивні зауваження щодо доповіді та її презентації, 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?

Робоча група ОП працює над тим, щоб врахувати вимоги професійного стандарту в оновленій редакції ОПП «Кібербезпека».

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/14UAVRHptFJkoS4NW5h35lDhfpsqOsytrp/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 бакалаврів становить 240 кредитів, з них

- загальна підготовка – 59 кредитів (24,6 %);

- професійна підготовка – 121 кредитів (50,4 %);

- вибіркові освітні компоненти – 60 кредитів (25 %).

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. Навчальним планом передбачено 2932 год. (40,7%) аудиторних занять та 3728 год. (51,8%) самостійної роботи, а також 540 год. (7,5%) відведені на ОК15, ОК24, ОК31-34.

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 Порядку прийому на навчання до закладів вищої освіти України в 2023 році. Правила прийому чіткі, не містять дискримінаційних положень. На навчання для здобуття першого (бакалаврського) рівня вищої освіти за ОПП «Кібербезпека» спеціальності 125 – Кібербезпека приймаються особи з повною загальною середньою освітою, а також на перший курс (зі скороченим терміном навчання), які здобули ОС МБ, ОКР МС, ОПС ФМБ. Особа може вступити до університету для здобуття ступеня бакалавра на основі ОС МБ / ОКР МС / ОПС ФМБ, здобутого за іншою спеціальністю. Особам, які здобули ОС МБ / ОКР МС / ОПС ФМБ, університет може перезарахувати кредити ЄКТС, максимальний обсяг яких визначено стандартом вищої освіти бакалавра. Предметами НМТ у 2023 р. були: українська мова і література (0,3), математика (0,5), історія України (0,2), іноземна мова (0,3), біологія (0,2), фізика (0,4), хімія (0,2). Мінімальна кількість балів до участі в конкурсі для зарахування на навчання за кошти державного бюджету повинна становити 125 балів.

Всі необхідні нормативні документи, розміщені на сайті Приймальної комісії ЧНУ (<http://surl.li/qczor>). Особливості ОП враховуються при виборі предметів ЗНО/НМТ, а вступ на навчання за ОПП «Кібербезпека» 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 проєктів, договорів про співробітництво між ЧНУ та іноземними або вітчизняними ЗВО (<https://bit.ly/3D95Qta>), 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-партнерів. До основних проблем під час визнання результатів навчання, отриманих в інших ЗВО, можна віднести розбіжність у змісті освітніх програм, практичної підготовки та технічному забезпеченні, а також графіку організації освітнього процесу. На ОПП «Кібербезпека» першого (бакалаврського) рівня є практика міжнародної академічної мобільності здобувачів освіти. Так, здобувачка Ленковська Марія впродовж двох семестрів навчалася у Словацькому технологічному університеті (м. Братислава) в рамках програми

Еразмус+. Результати навчання були представлені у формі звіту та обговорені на засіданні КРТАІБ (прот. № 20 від 15.06.23).

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 освіти у системі формальної освіти) у Чернівецькому національному університеті імені Юрія Федьковича» (зі змінами) (протокол №4 від 28.03.2022 р.) (<https://www.chnu.edu.ua/media/3aykf41y/polozhennia-pro-vzaiemodiiu-formalnoi-ta-neformalnoi-osvity.pdf>), в якому визначені критерії визнання результатів навчання, отриманих у неформальній освіті. Інформація про можливості неформальної освіти доступна на сайті ЧНУ. Про можливості неформальної освіти в контексті конкретних дисциплін здобувачів повідомляють викладачі, які забезпечують проведення занять, а також необхідні інформація регулярно доводиться до відома студентів кураторами академічних груп.

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

Зарахування результатів навчання, отриманих у неформальній освіті, здійснюється на підставі «Положенням про взаємодію формальної та неформальної освіти, визнання результатів навчання (здобутих шляхом неформальної та/або інформальної освіти у системі формальної освіти) у Чернівецькому національному університеті імені Юрія Федьковича» (зі змінами) (протокол №4 від 28.03.2022 р.) (<https://www.chnu.edu.ua/media/3aykf41y/polozhennia-pro-vzaiemodiiu-formalnoi-ta-neformalnoi-osvity.pdf>).

Випадків зарахування результатів навчання, отриманих у неформальній освіті, за ОП «Кібербезпека» як окремих предметів чи модулів освітніх компонент не було.

Проте, у вибірковій дисципліні «Захист і моніторинг комп'ютерних мереж»

(https://radiotech.chnu.edu.ua/elective_subjects/) передбачена можливість вивчення здобувачем курсу «CyberOps Associate» Мережної Академії CISCO, успішне проходження якого може бути зараховане бакалавру як Змістовий модуль 2 даної дисципліни із додаванням відповідних 24 балів до загальної підсумкової оцінки. Подібна практика може бути реалізована для ОК10, ОК11, ОК13, ОК14, ОК27.

В осінньому семестрі 2023-2024 н.р. здобувачі першого курсу успішно пройшли курс Мережної Академії CISCO «Вступ до кібербезпеки» на платформі Skills For All. За підсумками їм були додані бали до оцінки за змістовий модуль 2 ОК10 «Вступ до кібербезпеки» (протокол засідання КРТАІБ №9 від 21.11.2023 р.).

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 робочих 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 внутрішнього 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 соціопитування і анкетування (<http://surl.li/qcfd>, <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 захисту курсових та бакалаврських 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/university/normativni-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, з яким здобувачі вищої освіти також можуть ознайомитися на сайті кафедри (http://radiotech.chnu.edu.ua/syllabuses_krtib/) та у системі Moodle. В рамках цієї освітньої платформи здобувачі освіти мають доступ до електронних сторінок усіх 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 бакалаврів у дослідницькій діяльності: виконання завдань з науково-дослідною складовою у процесі вивчення фахових дисциплін (курсів роботи з ОК15 «Програмне забезпечення об'єктів кіберпростору» та ОК24 «Криптографія», а також міждисциплінарна курсова робота (ОК30); семінари з ОК4 «Інформаційний пошук у кібербезпеці» та ін.), а також доповіді результатів науково-дослідної роботи студентів за індивідуальною тематикою 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/studentaska-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/JCoc4Sp>, <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 (<https://radiotech.chnu.edu.ua/novyny/kafedra/page-12/>). Зокрема, студентом Дубиняком О. на Всеукраїнській науково-практичній конференції MEICS-2021 (м. Дніпро) представлялись результати досліджень методів виявлення штучно згенерованої мовної інформації (<http://meics.dnure.dp.ua/files/MEICS-2021.pdf>), а 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/7ccvprfhi/>).

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://www.chnu.edu.ua/media/vagbte04/pravya-pryznachennia-stypendii_final-01_2024.pdf).

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 практичних та лабораторних занять за ОК22, ОК23 та ОК28 враховано тематичний напрям наукових досліджень і науково-технічних розробок (<http://surl.li/rdclj>), а також відображені тенденції розвитку технологій забезпечення захисту інформації в інфокомунікаційних системах, які розглядалися на міжнародній науково-практичній конференції (<http://surl.li/rdcms>), що регулярно проводиться кафедрою радіотехніки та інформаційної безпеки ЧНУ.

За результатами стажування доц. кафедри Шпатаря П.М. в університеті «Люблінська політехніка» у в ОК23 («Криптографія») запроваджено тему «Застосування штучного інтелекту в розробленні алгоритмів шифрування», матеріали якої можуть використовуватися здобувачами освіти для виконання дипломних робіт. 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 організуються для освітян та студентів провідними компаніями та професійними спільнотами у сфері кібербезпеки (наприклад, <https://radiotech.chnu.edu.ua/novyny/kafedra/page-8/>, <http://surl.li/rdcms>). 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 англійських курсів Програми мережних академій Cisco для українських студентів (доц. Ластівка Г.І. та Рождественська М.Г. перекладали курси IT Essentials, DevNet Associate, CyberOps Associate).

Здобувачі 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 перевирити 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, а результати регулярно обговорюються на засіданнях випускової кафедри.

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, а також згідно Стандарту – у формі ЄДКІ.

Всі зазначені заходи повною мірою дозволяють перевірити досягнення студентами програмних результатів навчання.

З формами контрольних заходів певної навчальної дисципліни ОП здобувач може ознайомитися, переглянувши освітню програму, навчальний план, силабус та робочу програму цього ОК, які розміщуються на сайті кафедри та в рамках платформи Moodle.

При проведенні навчання у дистанційному форматі контроль здійснюється відповідно до Додатку до «Положення про організацію освітнього процесу в ЧНУ» за 100-бальною шкалою шляхом сумування балів, отриманих під час оцінювання рівня оволодіння теоретичним матеріалом та виконання практичної частини курсу.

Інструментом стимулювання до покращення якості навчання є рейтингове оцінювання успішності здобувачів вищої освіти, що регламентується «Положенням про рейтинг студентів ЧНУ» (<http://surl.li/ahdvp>, <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/1aDDzrMzuZ7OA1CervuLzeYLOEosLySV/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 контрольних заходів 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 критеріїв 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-AIQPDuSOLFgD6mN8/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 першим (бакалаврським) рівнем спеціальності 125 – Кібербезпека атестація

випускників ОПП «Кібербезпека» проводиться у формі Єдиного кваліфікаційного іспиту. У ЧНУ даною ОП передбачено також захист кваліфікаційної роботи/проекту. Атестація завершується видачею документу встановленого зразка про присудження здобувачу ступеня бакалавра із присвоєнням кваліфікації: бакалавр з кібербезпеки.

На атестацію виносяться сукупність знань, умінь, навичок, інших компетентностей, набутих здобувачем освіти під час навчання за даною спеціальністю. До атестації допускаються студенти, які виконали всі вимоги програми підготовки.

Кваліфікаційна робота/проект має передбачати розв'язання спеціалізованої задачі у сфері кібербезпеки та захисту інформації. Кваліфікаційну роботу/проект має бути перевірено на плагіат та оприлюднено на сайті університету/випускової кафедри.

Строк і тривалість проведення атестації здобувачів визначається графіком освітнього процесу та регулюються пунктами «Положення про атестацію здобувачів вищої освіти та організацію роботи Екзаменаційної комісії в ЧНУ» (https://drive.google.com/file/d/1-JYnU5bt8e_KIz4-ALQPDuSOLFGd6mN8/view).

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/1EMTdogrzwMD6gmLzuThArr1uKS6U2Bj6/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/universitytet/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»

(<http://surl.li/affxu>) 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» (<http://surl.li/aeufa>).

Процедури запобігання конфлікту інтересів регулюють «Правила академічної доброчесності ЧНУ»

(<http://surl.li/affyt>) та «Етичний кодекс ЧНУ» (<https://bit.ly/3Lflw03>).

Нормативні документи щодо врегулювання питань об'єктивності оцінювання, запобігання та вирішення конфліктів інтересів регулярно переглядаються та вдосконалюються (<http://surl.li/qdbbf>).

Для об'єктивності проведення захисту курсових проектів складається комісія з 3 викладачів кафедри. Захист бакалаврських робіт проводиться на відкритому засіданні ЕК за обов'язкової присутності голови комісії. Здобувачі та інші зацікавлені особи можуть вільно здійснювати аудіо-, відеозапис процесу захисту кваліфікаційної роботи. Всі курсові і дипломні роботи 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 урегулюють 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 академічної відпустки 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 ОК17 (Гажук Б. та Марчук В.); повторного захисту дипломних робіт впродовж 2019-2023 н.р. не було.

Яким чином процедури ЗВО урегулюють 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 вплинуло 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» (<http://surl.li/affyt>); «Положення про постійну комісію з питань академічної доброчесності, правових засад діяльності та регламенту Вченої ради ЧНУ» (<https://drive.google.com/file/d/1auN6M5FzyvagiVi3HW16No1Tt1IjuD7q/view>); «Етичний кодекс ЧНУ» (<https://bit.ly/3Lflwo3>); «Положення про виявлення та запобігання академічному плагіату в ЧНУ» та відповідні розпорядження по ЧНУ (<https://cutt.ly/mVH8mqi>, <http://surl.li/qdbgx>, <http://surl.li/qdbhi>). Дотримання канонів академічної доброчесності членами університетської спільноти задеклароване 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; посилення 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/polozenia-pro-vyivlennia-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 Unischeck. 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 кваліфікаційних робіт/проектів (прот. №6, 24.11.2020; №17, 10.05.2023).

За потреби можуть перевірятись й інші письмові роботи (курсіві, 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 проекту AcademIQ «Ініціатива академічної доброчесності та якості освіти» (<https://www.chnu.edu.ua/universytet/vazhlyvo/akademichna-dobrocheshnist/>). 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 були проведені вебінари за тематикою академічної доброчесності (<http://surl.li/rdcwe>, <http://surl.li/rdcwe>).

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_u7rPqGbGu3cccWuYTRXbI5-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-on4WmOXuAn4Q_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.п. 37, 38 Ліцензійних умов провадження освітньої діяльності. Викладачі випускової кафедри мають наукові публікації, методичні розробки, сертифікати тощо, що підтверджують їхню фаховість у тому освітньому компоненті, який вони забезпечують.

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://radiotech.chnu.edu.ua/agreements/>) 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 (https://radiotech.chnu.edu.ua/elective_subjects/), формуванні лаб. бази (Компанія Tektelic, ТОВ «ІнТех», КП «Сігма» <http://surl.li/fdxwm>, <https://bit.ly/3SdUCbg>, <http://surl.li/rdczc>), практик та дипломного проектування, вносять пропозиції до оновлення змісту ОП (https://radiotech.chnu.edu.ua/opp_125_bachelor/), що дозволить їм в перспективі поповнювати свій кадровий потенціал.

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 ОП залучаються професіонали-практики та провідні фахівці галузі. Зокрема, восени 2022 р. в рамках ОК23 професором кафедри безпеки інформ. систем і технологій ХНУ ім. В. Н. Каразіна, д.т.н. І. Д. Горбенком була прочитана серія лекцій, присвячених питанням прикладної криптології (<http://surl.li/rddcr>).

У 2023-2024 н.р. до проведення занять з питань ТЗІ був залучений професіонал-практик Прокоф'єв М.І.

В умовах вимушеного дистанційного навчання значно розширилися можливості залучення до освітнього процесу професіоналів та представників стейкхолдерів. Зокрема, за допомогою платформи Google Meet було організовано низку зустрічей зі студентами, присвячених питанням ІБ, що відповідає ОК10 та ОК28 (<http://surl.li/rdcms>).

Представники відділів кібербезпеки та техпідтримки 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.

В рамках угоди про співпрацю між ЧНУ та ХНУ проводилися гостьові лекції з елементами майстер-класу. Так, здобувачі ОПП «Кібербезпека» прослухали лекцію доцента кафедри кібербезпеки ХНУ, к.т.н., Тітової В. Ю. на тему

«Методологія атак на комп'ютерні мережі», що відповідає тематиці ОК13 (<http://surl.li/rddch>).

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

ЧНУ сприяє профрозвитку викладачів як складової системи забезпечення якості освітньої діяльності, згідно «Положення про підвищення кваліфікації науково-пед. працівників ЧНУ» (<http://surl.li/aeuhf>) Під час вимушеного переходу на дистанц. навч. в ЧНУ для НПП проведені курси підвищення каліф. «Основи користування Moodle» (зкр.), серія наук-метод. семінарів-практикумів «Алгоритм підготовки до викладання фах. дисциплін англ. мовою» (Ластівка Г.І.,Рожественська М.Г.) та організований безоплатний доступ до Coursera. У ЧНУ створено умови для здійснення програм академ. мобільності за Еразмус+ (<http://surl.li/ledmp>). Так, стажувалися у Сучавському універ. Штефана чел Маре (Румунія) – проф. Політанський Р.; «Люблінська політехніка» (Польща) – доц. Шпатар П. та ін

Інші приклади:

-підвищ. каліф. у ХНУРЕ (за курсами з оцінювання захищеності інформації) з відривом від виробництва за рахунок спецкоштів по платі за навчання зі збереженням середньомісячної зарплати 6-х викладачів КРтаІБ (нак. №54-від від 10.02.2020);
-підтримавши ініціативу НПП КРтаІБ, ЧНУ було профінансовано відрядження викладачів до ВНТУ з метою обміну досвідом, проф. розвитку та ознайомлення з ситуаційним центром кібербезпеки та кіберполігону Центру ІТ і ЗІ ВНТУ (5.11.2021,<http://surl.li/rdcms>);
-в ЧНУ є практика стимулювання НПП до нових проф. здобутків преміюванням, так керівники студ. робіт, які стали переможцями Всеукр. конкурсу студ. наук. робіт у 2020-2021 н.р., були премійовані вироб. премією (нак. № 853-к від 30.08.2021)

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 19 місце серед 72 кафедр ЧНУ (<https://www.chnu.edu.ua/nauka/naukovi-informatsiini-resursy/reitynhy-ta-zvitnist/vnutrishnouniversytetski-reitynhy/reitynh-kafedr-chnu-za-riznymy-vydamy-diialnosti/>). 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://old.chnu.edu.ua/index.php?page=ua/news/archive&data\[5013\]\[news_id\]=15264](http://old.chnu.edu.ua/index.php?page=ua/news/archive&data[5013][news_id]=15264)).

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 ПРН. Для виконання лабораторних і практичних робіт створено комп'ютерний клас та низку спеціалізованих лабораторій: ТЗЗІ в радіотех. 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 (ОК13, ОК22 та вибіркові курси). 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 eduoam.

Наукова бібліотека ЧНУ (з фондом біля 3 млн. книг) надає доступ до баз даних Scopus, Web of Science тощо (<http://surl.li/qcydd>, <http://www.library.chnu.edu.ua>). На випусковій кафедрі створено бібліотеку з фаховою літературою та навчальними посібниками. Для доступу бакалаврів до методичних матеріалів ОК, проведення контрольних заходів та навчання в дистанційній формі використовується система Moodle.

На території ЧНУ працюють їдальні, 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; 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, НДРС, організації дозвілля, побуту, оздоровлення тощо. Створена в ЧНУ соц. лабораторія періодично проводить опитування студентів щодо потреб та інтересів студентства та рівня їх задоволеності (<https://cutt.ly/6CU2V71>, <http://surl.li/kxyuu>, <http://surl.li/qcfdtd>).

Між викладачами та студентами стосунки будуються на основі взаємоповаги. Куратори спілкуються зі студентами, допомагають консультаціями та порадами, передають життєвий досвід, підтримують участь студентів у волонтерській діяльності. Крім цього, потребами та інтересами здобувачів ВО займається профспілка студентів та студ. 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 та порядку дій під час повітряної тривоги (<https://www.chnu.edu.ua/universitytet/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 даною ОП, 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/anoqj>). 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, діти чорнобильців та учасників бойових дій. Неповнолітні діти студентів отримують подарунки від профспілки ЗВО на день Св. Миколая. Для студентів-сиріт та осіб, позбавлених батьківського піклування, організовуються виплати, компенсації на продукти харчування, вони звільнюються від оплати за проживання в гуртожитку, отримують щорічну матеріальну допомогу. Спілкування кураторів зі студентами дозволяє виявляти соціально незахищених та тих, хто потребує доп. 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/3VВa2Ra>) 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. Засобами розв'язання конфлікту є: 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 даної ОП 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 студ. гуртожитках ЧНУ» та ін. докумен. (<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 («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»-97,6%, «так»-0,6%, «не хочу відповідати» - решта (<http://surl.li/pvqiu>), що засвідчує позитивну динаміку упродовж останніх років. У процесі реалізації даної ОП не виникало потреб застосування антикорупційних процедур; скарг, пов'язаних із сексуальними домаганнями та дискримінацією 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/rddjv>). Семінари до Дня дівчат у ІКТ, що проводились у ІФТКН, не виявили проявів гендерної дискримінації у ЧНУ та ОПП «Кібербезпека» (<https://cutt.ly/cVJiMa>)

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_JZovNab4J2x8tHTz2vfVmH4JOP/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/1BGtjpMStV35WLKnGjoozOwZMjofsBwnK/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/14UAVRHptFJkoS4NW5h35lDhfpsqOsyrg/view>).

Деякі аспекти роботи з реалізації та удосконалення освітніх програм регламентується «Положенням про організацію освітнього процесу в ЧНУ»

(https://drive.google.com/file/d/1x419wQ3yhhBioazmcm_xUod7zrSsdCVN/view) (прот. №9 від 30.09.2019) та

«Положенням про гарантії освітньої програми ЧНУ» (<https://www.chnu.edu.ua/media/qmapwn1b/polozhennia-pro-haranta-osvitnoi-prohramu.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», <http://surl.li/wlbc>) організовує керівник проектної групи з метою забезпечення належного рівня освітніх послуг і створення сприятливого й ефективного освітнього середовища для студентів. ОП удосконалюється робочою групою із залученням студентів та інших стейкхолдерів. У процесі реалізації ОП під час обговорень з НПП, здобувачами 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 визначені за результатами анкетування, показниками їх працевлаштування, участю у міжнародних програмах академ. мобільності, оцінками з боку роботодавців тощо. Оновлені ОП узгоджуються з представниками студентського самоврядування, зав. 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 КРТАБ ЧНУ (https://radiotech.chnu.edu.ua/opp_125_bachelor/). Серед ключових змін слід відзначити наступні:

-на основі пропозицій та їх обговорення з зацікавленими сторонами освітнього процесу ОПП «Кібербезпека», а також враховуючи зауваження моніторингової групи Центру ЗЯО ЧНУ, уточнено формулювання характеристик ОП, зазначений зв'язок ОП з місією та стратегічним планом розвитку ЧНУ на 2019-2026 р.;

-за пропозиціями здобувачів та представників академічності (рецензента Яремчука Ю.Є., голів ЕК Толюпи С.В. та Стахіри П.Й.), що враховують сучасні тенденції розвитку ринку праці та підвищення ефективності набуття здобувачами ПРН 16, ПРН 28, ПРН29 та ПРН30, запроваджена ОК27;

-за пропозиціями студентів, стейкхолдерів та моніторингової групи ЦЗЯВО ЧНУ для розширення можливостей щодо формування індивідуальної освітньої траєкторії здобувачів ВО змінений формат Переліку вибіркового освітнього компоненту ОП;

-враховуючи прикладне спрямування ОП і орієнтацію на здобуття студентами фахових знань, умінь та навичок для здійснення подальшої проф. діяльності, за рекомендаціями роботодавців та за підсумками реалізації освітнього проекту CRDF Global в G-202206-68835 «Integration of new Cybersecurity courses into the Curriculum of the Yuriy Fedkovych Chernivtsi National University» (<http://surl.li/qdred>) прийняте рішення розширити блок вибіркового дисциплін циклу проф. підготовки курсом «Захист та моніторинг комп'ютерних мереж».

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 посилання 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 здобувача Дубиняка О. відносно розширення переліку вибіркового ОК дисципліною «Основи штучного інтелекту»; здобувачкою Зайцевою В. запропоновано приділити більше уваги проблемам розроблення та тестування веб-додатків щодо їх захищеності від відомих загроз, що відображено у введенні відповідної теми до вибіркової дисципліни «Додаткові розділи програмування». Ці та інші пропозиції підтримані проектною групою для підсилення ПРН 4, 5, 20, 52 чинної на момент пропозиції редакції ОП, затверджені на засіданнях кафедри (прот. №16, 16.02.2022; №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 студентоцентрикований 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/universitytet/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 бакалаврату 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 КРТаІБ організуються 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 НП України, представників ІТ компаній тощо) здійснюється коригування цілей та ПРН ОП. Так, за пропозицією представників відділу ІБ Управління СБУ в Чернівецькій обл. та відділу протидії кіберзлочинам Департаменту кіберполіції в Чернівецькій обл. НП України (<http://surl.li/rdcms>, <http://surl.li/rddoz>) було запропоновано розширити перелік вибіркового курсом «Мережеве обладнання», що підсилює ПРН13, ПРН31 та ПРН52. За пропозиціями представників ІТ компаній (регіонал. представництв Datami та SoftServe) було скореговано визначений ОП ПРН55 (прот. №4 від 28.03.2022) в оновленій редакції ОПП «Кібербезпека» (https://radiotech.chnu.edu.ua/opp_125_bachelor). Також представники роботодавців залучаються до проведення занять, планування тематики кваліф. проєктів/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 КРТаІБ – 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 кваліфікаційних робіт в соціальних мережах, електронною поштою тощо поширюється інформація про наявні вакансії потенційних роботодавців. У ЧНУ створена асоціація випускників (<https://www.chnu.edu.ua/universitytet/pry-universitytet/asotsiatsiia-vyupusknykiv/>), що також сприяє підтримці зворотного зв'язку з випускниками та відслідковуванню траєкторій їх працевлаштування (<https://radiotech.chnu.edu.ua/gallery/>).

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://www.chnu.edu.ua/media/032exesg/polozhennia-szyavo.pdf>). 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/1BGtjpMStV35WLNKnGjoozOwZMjofsBwnK/view>) та «Положенням про розроблення та реалізацію освітніх програм ЧНУ» (https://drive.google.com/file/d/13O1K-SnZkg7h4vlnS8Nhr4uqaDjg_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 вибіркового курсу, 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 ЄВІ 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 ураховані 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:

1. Активізувати процес підвищення кваліфікації співробітниками кафедри як у провідних ЗВО України, так і за кордоном.

2. Керівництву університету, завідувачу випускової кафедри забезпечити подальший розвиток учбових лабораторій та їх оснащення новими зразками сучасного інфокомунікаційного обладнання.

3. Завідувачу випускової кафедри продовжити роботу з ротації професорсько-викладацького складу та налагодження зв'язків зі спорідненими закордонними навчальними закладами.

4. Продовжити випуск навчальних посібників та організувати випуск підручників власної розробки з фахових дисциплін напрямку інформаційної та кібербезпеки.

5. 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 збільшити кількість кредитів та годин з дисципліни "Криптографія".

6. Керівництву університету, завідувачу випускової кафедри продовжити роботу щодо участі студентів та викладачів у процедурах сертифікації за фаховим спрямуванням та з іноземних мов, що дозволить підвищити рівень конкурентоздатності випускників.

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>, <http://surl.li/qdsbv>). 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 (https://radiotech.chnu.edu.ua/opp_125_bachelor/).

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 НН 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 НН 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/1YtQjLaZi8T7NeLfiRh3L7bKrkjSoG-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» (<http://surl.li/bitga>). 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/university/normativni-dokumenty/>).
Також усі матеріали опубліковано у збірнику нормативних документів ЧНУ, наявному на кожній кафедрі та в деканаті (<https://drive.google.com/file/d/1oiZdkjt-oXmhqMaLm-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 пропозицій 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 ОП «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 ОП «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 бакалаврів до професійної, практичної та науково-дослідної діяльності, про що свідчать активний вступ випускників до магістратури 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 та ПЗ 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. Запровадити діяльність щодо оцінки захищеності приміщень та сертифікації програмно-апаратних засобів для службового користування підприємств та організацій Західного регіону.
8. Розширення партнерських відносин із закордонними підприємствами та компаніями в галузі інформаційної безпеки.
9. 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.
10. 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: 07.03.2024 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	
Англійська мова професійного спілкування	навчальна дисципліна	<i>Англійська мова професійного спілкування.pdf</i>	dTLET+dYuVQ7qIvA dsTscgckTW6qEyoDr t4p4x6Uqik=	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.). Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.
Основи побудови систем комплексного захисту інформації	навчальна дисципліна	<i>Основи побудови систем комплексного захисту.pdf</i>	kTrkK8B382594zVq 5yFlOiOJK9+ckp3Rp OxxZRrPsos=	Для проведення очного/дистанційного навчання: 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/12agr4j405uhdmL1XAfcAgDtCxEG3kA6h/view Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.
Криптографія (в тому числі курсова робота)	навчальна дисципліна	<i>Криптографія.pdf</i>	TD/CEm8tmqcn9oLl /5GqHpT9HoOoRJ5 fl4u2RVfcLsI=	Для проведення очного/дистанційного навчання: 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 КРТмаІБ.

Проведення лекційних, практичних 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.).

Програмне забезпечення:

1. ОС Windows 10 PRO FOR OEM SOFTWARE
2. Пакет математичних обчислень Maple 9.0
3. Віртуальна машина робочої станції CyberOps
4. Програмне забезпечення Visual Studio 2019
5. Інтегроване середовище розробки для мов програмування: Python 3.8, PyCharm, NetBeans, Eclipse, Idea Studio, C++, C#, Java, Notepad++, GoogleDocsRedactors
6. Збірка комп'ютерних програм «Система криптографічного захисту інформації «Шифр-Х.509» Версія 2» (без обмеження на кількість сертифікатів (ліцензія для використання в навчальному процесі НЛ №: СП-0922-01).

<https://drive.google.com/file/d/1W8eDMDKMs4cCNRIWM6OzKL5eA-yfq5f/view>

Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.

Іноземна мова (за професійним спрямуванням)	навчальна дисципліна	Іноземна мова (за професійним спрямуванням).pdf	utPP1BvstAxoQFwFZLEqKowoh+gKHvcQooBCUn6RYp4=	<p>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":</p> <ol style="list-style-type: none"> 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.). <p>Наявне матеріально-технічне</p>
---	----------------------	---	--	--

				забезпечення достатнє для реалізації ОП.
Програмне забезпечення об'єктів кіберпростору (в тому числі курсова робота)	навчальна дисципліна	Програмне забезпечення об'єктів кіберпростору.pdf	FQQO2WT3eiBH8OI+6kP/pS7qbzYhclXLvXayDRvYrFE=	<p>Для проведення очного/дистанційного навчання: аудиторний фонд і необхідне обладнання; бібліотека 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 ACLR AP (2021 р., 3 шт.) на КРТтаІБ.</p> <p>Проведення лекційних та лабораторних занять: аудиторія В10 – ЛАБОРАТОРІЯ КРИПТОГРАФІЇ ТА СТЕГАНОГРАФІЇ.</p> <p>Обладнання:</p> <ol style="list-style-type: none"> 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.). <p>Програмне забезпечення:</p> <ol style="list-style-type: none"> 1. Code::Blocks – вільне багатоплатформне середовище розробки програмного забезпечення (IDE) 2. Операційна система Ubuntu 22 3. Веб-переглядач Google Chrome (для презентації) https://drive.google.com/file/d/1W8eDMDKMSb4cCNRIWM6OzKL5eA-ufq5f/view <p>Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.</p>
Випускна кваліфікаційна робота/проект	підсумкова атестація	Дипломне проектування.pdf	usxrTXZF5Q6cR2kixcbflpWx3qp/FYgIvoBROMhBdzo=	<p>Матеріально-технічне забезпечення баз практик відповідно до укладених договорів</p> <p>Для проведення захистів:</p> <ol style="list-style-type: none"> 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.). <p>https://drive.google.com/file/d/115jr19xMFBwopa5HgDrXRh5Oee1MJTRT/view</p> <p>Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.</p>
Виробничо-технологічна практика	практика	Виробничо-технологічна практика.pdf	O9kdockPqCcuLVYa ssyDct5+2eo+ihwzbzcoTvxfhAg=	<p>Матеріально-технічне забезпечення баз практик відповідно до укладених договорів</p> <p>Для проведення захистів:</p> <ol style="list-style-type: none"> 1. Комп'ютер Intel Core i3-10325/3.9GHz/DDR4 8GB 2400 MHz/SSD 256 GB з монітором 22" Acer (2021 р., 1 шт.).

				<p>2. Проектор мультимедійний Epson EB-X04 (2019 р., 1 шт.).</p> <p>3. Веб-камера Logitech c270HD (2019 р., 1 шт.).</p> <p>4. Акустична система Sven312 (1 шт.).</p> <p>https://drive.google.com/file/d/115jr19xMFBwopa5HgDrXRh5Oee1MJTRT/view</p> <p>Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.</p>
Ознайомча практика	практика	Ознайомча практика.pdf	nPOVZp6U/iLeOMEzOTTbi69QOZlujS6UCLvGm6dzoXQ=	<p>Матеріально-технічне забезпечення баз практик відповідно до укладених договорів</p> <p>Для проведення захистів:</p> <p>1. Комп'ютер Intel Core i3-10325/3.9GHz/DDR4 8GB 2400 MHz/SSD 256 GB з монітором 22" Acer (2021 р., 1 шт.).</p> <p>2. Проектор мультимедійний Epson EB-X04 (2019 р., 1 шт.).</p> <p>3. Веб-камера Logitech c270HD (2019 р., 1 шт.).</p> <p>4. Акустична система Sven312 (1 шт.).</p> <p>https://drive.google.com/file/d/115jr19xMFBwopa5HgDrXRh5Oee1MJTRT/view</p> <p>Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.</p>
Міждисциплінарна курсова робота	курсдова робота (проект)	Міждисциплінарна курсова робота.pdf	liqOhHEFKXLXoWymWKJ7lsLNL3855n612hmv3ju5Pew=	<p>Для проведення очного/дистанційного навчання: 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 КРТтаБ.</p> <p>Обладнання аудиторії: проектор мультимедійний Epson EB-X04 (2019 р., 1 шт.), екран (1 шт.).</p> <p>Для проведення дистанційного навчання:</p> <p>1. Комп'ютер Intel Core i3-10325/3.9GHz/DDR4 8GB 2400 MHz/SSD 256 GB з монітором 22" Acer (2021 р., 1 шт.).</p> <p>2. Веб-камера Logitech c170 (2019, 1 шт.).</p> <p>3. Акустична система Sven312 (1 шт.).</p> <p>Для виконання курсової роботи:</p> <p>1. Офісний пакет LibreOffice.</p> <p>2. Cisco Packet Tracer v7.3 та вище.</p> <p>3. ПЗ CORAS Tool.</p> <p>https://drive.google.com/file/d/115jr19xMFBwopa5HgDrXRh5Oee1MJTRT/view</p> <p>Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.</p>
Технічні системи охорони об'єктів	навчальна дисципліна	Технічні системи охорони об'єктів.pdf	P9UtElvxtJiL2hiZgZaCCJ7InQBtIpLo4TEYaSsCeo=	<p>Для проведення очного/дистанційного навчання: аудиторний фонд і необхідне обладнання; бібліотеки ЧНУ та</p>

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 КРТмаІБ.

Проведення лабораторних та наочно-демонстраційних занять
**ЛАБОРАТОРІЯ
ТЕЛЕКОМУНІКАЦІЙНИХ
СИСТЕМ ТА МЕРЕЖ:**
Обладнання:
1. Осцилограф OWON DS5032E (2018 р., 2 шт.).
2. Автомобільна охоронна сигналізація «Сonvoy xs-5 v.2».
3. Пульст пожежної охорони FS-4008.
4. Панель системи охорони «ВАРТА ¼».
5. Датчик відкриття магнітоконтактний СОМК-1-8 (1 шт.), пасивний ІЧ-давач Crow SWAN Quad (1 шт.).
6. Відеореєстратор укомплектований камерами формату: TurboHD, HD-CVI, IP, CVI.
7. Система контролю доступу ATIS AC-05.

Інше 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:
2.1. Веб-переглядач Google Chrome v121.0.6.6167.185
2.2. Цифрові інструменти Google Workspace (зокрема, хмарний сервіс Google Drive).

Для проведення дистанційного навчання:
1. Ноутбук Lenovo 100-15ibd, i5-5200U CPU, 2.70GHz, 8GB RAM, SDD 240 GB з дисплеєм 15.6" (2020 р., 1 шт.).
2. Гарнітура Xiaomi Mi True Wireless Earphones 2 (2022 р., 1 шт.).

<https://drive.google.com/file/d/1L6eBqRfMujf79VF56W7DaoLN6nChwnkV/view>
Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.

Безпека інформаційно-телекомунікаційних систем	навчальна дисципліна	Безпека інформаційно-телекомунікаційних систем.pdf	FoJbhYcuolGgRNixYdXupUQc8yrGddNhCsfVSu4o8Uc=	Для проведення очного/дистанційного навчання: 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 КРТмаІБ.
--	----------------------	--	--	--

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 1206і (2018 р., 2 шт.).
7. Акустичний зашумлювач РІАС2ВА (2019 р., 1 шт.).
8. Генератор радіошуму РІАС-1М (2019 р., 1 шт.).
9. Генератор акустичного шуму DNG-2000 (2022 р., 1 шт.).
10. Віброметр VENETECH GM 63B (2018 р., 1 шт.).
11. Шумомір VENETECH 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 ДЕТЕКТОР K18 (2022 р., 1 шт.).
14. Зразки акустичних та віброшумлювачів.
15. Мережевий фільтр РІАС - 4ФМ/1 (2018 р., 1 шт.).
16. Розділовий трансформатор РІАС-4ТР/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:
 - 2.1. Norton Ghost версія 15.0.0.35659 - ПЗ для створення резервних копій або аналогічне. Доступний безкоштовний пробний період 30 днів.
 - 2.2. Comodo Firewall 2020 - мережевий захист, або аналогічне. Безкоштовне ПЗ для дому, школи, організації.
 - 2.3. GFI LANguard Network Security Scanner версія 12.3.2017.1219 - пошук вразливостей мережі на робочих станціях, або аналогічне. Доступний безкоштовний пробний період 30 днів.
 - 2.4. Jetico BestCrypt 9.08.2 - ПЗ для шифрування даних, або аналогічне. Доступний безкоштовний пробний період 21 день.
 - 2.5. Microsoft Access 2016 Professional Plus 2016 - захист даних в Microsoft Word і Excel їх версії. Безкоштовна пробна версія.
 - 2.6. Ontrack EasyRecovery Pro

14.0.0.4 - ПЗ для відновлення видалених даних, або аналогічне. Доступний безкоштовний пробний період 30 днів.

2.7. Disk Wipe 1.7 - ПЗ для остаточного видалення даних, або аналогічне. Безкоштовна ліцензія.

2.8. Symantec AntiVirus - ПЗ для антивірусного захисту, або аналогічне. Доступна безкоштовна пробна версія.

2.9. Revo Uninstaller Free 2.4.5 - ПЗ для повного очищення реєстру та залишків програм після їх видалення, або аналогічне. Безкоштовна версія.

2.10. Програма Ultimate ZIP Cracker версія 8.0.1.0 - ПЗ для пошуку паролів архівів, або аналогічне. Доступна пробна версія.

2.11. Програма Advanced Archive Password Recovery 4.66.266 - ПЗ для пошуку паролів архівів, або аналогічне. Доступний безкоштовний пробний період 30 днів.

2.12. ESET NOD32 Антивірус 16.0.24.0. Доступний безкоштовний пробний період 30 днів.

Для проведення дистанційного навчання:

- Ноутбук Lenovo V580c/ i5-3230M CPU, 2.60GHz, 6GB RAM, HDD 500 GB з дисплеєм 15.6".
- Гарнітура Sven AP-860MV (2019 р., 1 шт.).

<https://drive.google.com/file/d/1kBQjxU27rEtyuBFKwvFa6kKclABS9zrH/view>

<https://drive.google.com/file/d/1L6eBgRfMujf79VF56W7Da0LN6nChwnkV/view>

Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.

<p>Законодавчі питання інформаційної безпеки</p>	<p>навчальна дисципліна</p>	<p>Законодавчі питання інформаційної безпеки.pdf</p>	<p>oXY7u8y8hRGV3yHR+YEWaLq+oWoHTG2as7M3jof4cjc=</p>	<p>Для проведення очного/дистанційного навчання: аудиторний фонд і необхідне обладнання; бібліотека 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 КРТмаІБ.</p> <p>Проведення лекційних та практичних занять (в т.ч. в дистанційному форматі):</p> <ol style="list-style-type: none"> Комп'ютер Intel Core i3-10325/3.9GHz/DDR4 8GB 2400 MHz/SSD 256 GB з монітором 22" Acer (2021 р., 1 шт.). Проектор мультимедійний Acer X128HP (1 шт.) з екраном. Веб-камера Logitech c170 (2019, 1 шт.). Акустична система Sven312 (1 шт.). <p>https://drive.google.com/file/d/12agr4j405uhdmL1XAfcAgDtCxEG3kAbh/view</p> <p>Наявне матеріально-технічне</p>
--	-----------------------------	--	---	--

<p>Управління інформаційною безпекою</p>	<p>навчальна дисципліна</p>	<p>Управління інформаційною безпекою.pdf</p>	<p>kG4x5TI/UXeh5VTG XGW9MdaeZ4xD6Yk U1jdxKz9rH2A=</p> <p>забезпечення достатнє для реалізації ОП.</p> <p>Для проведення очного/дистанційного навчання: 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 КРТмаІБ.</p> <p>Проведення лекційних та практичних занять (в т.ч. в дистанційному форматі):</p> <ol style="list-style-type: none"> 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.). <p>https://drive.google.com/file/d/12agr4j405uhdmL1XAfcAgDtCxEg3kA6h/view</p> <p>Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.</p>
<p>Взаємодія між компонентами систем IoT</p>	<p>навчальна дисципліна</p>	<p>Взаємодія між компонентами систем IoT.pdf</p>	<p>bDaRqZwxc7OKPKP d1NIEHbYzZxUdQW KyECH3KFZrg9c=</p> <p>Для проведення очного/дистанційного навчання: 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, 3 шт.) на КРТмаІБ.</p> <p>Для проведення лекційних та наочно-демонстраційних занять застосовується обладнання Лабораторії "МОДЕЛЮВАННЯ І СИНТЕЗУ РАДІОЕЛЕКТРОННИХ ЗАСОБІВ РАДІОСПЕКТРОСКОПІЧНИХ ТА МЕДІАІНФОРМАЦІЙНИХ СИСТЕМ":</p> <ol style="list-style-type: none"> 1. Комп'ютер: IntelCore i3 3.9GHz, 8GB, 256GB з монітором PHILIPS 23.8 (2021, 4 шт.). 2. Комп'ютер Intel Core i5 3.0GHz, 32GB, 500GB M.2, HDD 4TB RAID, GTX 1060 (2021, 1 шт.). 3. проектор мультимедійний Acer X1123H (2021, 1 шт.). 4. інтерактивна дошка Intech RD82A (2021, 1 шт.), екран (1 шт.). <p>Для лабораторних та наочно-демонстраційних занять:</p> <ol style="list-style-type: none"> 1. Комп'ютер: IntelCore i3 3.9GHz, 8GB, 256GB з монітором PHILIPS 23.8 (2021, 4 шт.). 2. Плата розробника Intel DE1-SoC (FPGA Cyclone V) виробництва Terasic Technologies (2021).

				<p>3. Плата розробника Intel DE10 Lite (CPLD MAX10) виробництва Terasic Technologies (2021).</p> <p>4. Керований комутатор Mikrotik Cloud Smart Switch CSS326-24G2S+RM (2021, 1 шт.).</p> <p>5. Одноплатний міні-комп'ютер Raspberry Pi 4 Model B 2GB з LCD HDMI Waveshare, (2021, 4 шт.)</p> <p>6. Плата розробника Cypress CY8CKIT-044 PSoC® 4 M-Series Pioneer Kit, (2021).</p> <p>7. Шлюз LoRaWAN IoT Tektelic Kona Micro Lite Gateway з набором Smart Room Sensor (3 шт.).</p> <p>8. Аналізатор спектру Siglent SSA3032X (2021, 1 шт.).</p> <p>9. Осцилограф цифровий HANTEK DSO5072P (2021, 2 шт.).</p> <p>10. Осцилограф цифровий SIGLENT SDS1202CNL+ (2021, 1 шт.).</p> <p>11. Генератор сигналів FeelTech FY6600 (2 шт.).</p> <p>12. Цифровий двоканальний генератор довільних форм сигналів з функціями частотоміра OWON AG2052F (1 шт.).</p> <p>13. Мультиметр UNI-T UT801 (2 шт.).</p> <p>14. Блок живлення регульований Ваку ВК-305D 30V 5A (2 шт.).</p> <p>Для проведення дистанційного навчання:</p> <p>1. Intel Core i5 3.0GHz, 32GB, 500GB M.2, HDD 4TB RAID, GTX 1060 (2021, 1 шт.).</p> <p>2. Веб-камера logitech c270 (2019, 1 шт.).</p> <p>3. Гарнітура Sven AP-860MV (2019, 1 шт.).</p> <p>https://drive.google.com/file/d/1GYMHA6UezxvddQJLPgr3KbCk3JxthbIu/view</p> <p>Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.</p>
Канали витоку інформації	навчальна дисципліна	Канали витоку інформації.pdf	nR7IGU3KSHWTxTS+TLvf3l4s7uj4KZl4/vGqCPrс15g=	<p>Для проведення очного/дистанційного навчання: 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 КРТмаІБ.</p> <p>Проведення лекційних та практичних занять (в т.ч. в дистанційному форматі):</p> <p>1. Комп'ютер Intel Core i3-10325/3.9GHz/DDR4 8GB 2400 MHz/SSD 256 GB з монітором 22" Acer (2021 р., 1 шт.).</p> <p>2. Проектор мультимедійний Acer X128HP (1 шт.) з екраном.</p> <p>3. Веб-камера Logitech c170 (2019, 1 шт.).</p> <p>4. Акустична система Sven312 (1 шт.).</p> <p>https://drive.google.com/file/d/12agr4j405uhdmL1XAfcAgDtCxEg3kA6h/view</p>

				<p>Проведення лабораторних занять: ЛАБОРАТОРІЯ ТЕХНІЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ.</p> <p>Обладнання:</p> <ol style="list-style-type: none"> 1. Комплекс АКОР-3 (1 шт.). 2. Вимірювач P5-10 (1 шт.). 3. Спеціалізований комплекс акустичного захисту мовної інформації КАЗМІ (1 шт.). 4. Генератор сигналів ALT-G(2018, 1 шт.). 5. Осцилограф OWON DS5032E (2018, 2 шт.). 6. Детектор поля PROTECT 1206i (2018, 2 шт.). 7. Акустичний шумлювач PIAC-2BA (2019, 1 шт.). 8. Генератор радіошуму PIAC-1M (2019, 1 шт.). 9. Інше обладнання лабораторії. <p>Для проведення дистанційного навчання:</p> <ol style="list-style-type: none"> 1. Комп'ютер AMD Athlon II X245 2.9GHz/DDR3 2GB/HDD 512 GB з монітором 20" Acer (2018, 1 шт.). 2. Веб-камера logitech c170 (2019, 1 шт.). 3. Гарнітура Sven AP-860MV (2019, 1 шт.). <p>https://drive.google.com/file/d/1kB0jxU27rEtyuBFKwvFa6kKclABS9zrH/view</p> <p>Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.</p>
Архітектура і моделі безпеки	навчальна дисципліна	Архітектури і моделі безпеки.pdf	O8gCgJjdKn+6wgze miBwRlawhq7UUGs xPLWAms2plRE=	<p>Для проведення очного/дистанційного навчання: 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 КРТ та ІБ.</p> <p>Обладнання аудиторії: проектор мультимедійний Epson EB-X04 (2019 р., 1 шт.), екран (1 шт.).</p> <p>Для проведення дистанційного навчання:</p> <ol style="list-style-type: none"> 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.). <p>https://drive.google.com/file/d/115jr1gxMFBwopa5HgDrXRh5Oee1MJTRT/view</p> <p>Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.</p>
Міжособистісне спілкування і побудова команд	навчальна дисципліна	Міжособистісне спілкування та побудова команд.pdf	yfpoAhWtvPZ9+Hzn 70pql/03xWLOm951 JCYlgMDGF+Y=	<p>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.</p>

				<p>Проведення практичних занять: проектор мультимедійний ViewSonic PJD6211 (1 шт.), екран (1 шт.). Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.</p>
Інформаційний пошук у кібербезпеці	навчальна дисципліна	Інформаційний пошук у КБ.pdf	qMUhEjTjPei6ADZJEomtcWcW3Xmsyu2HxuZP4mk9iw=	<p>Для проведення очного/дистанційного навчання: 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 КРТмаІБ.</p> <p>Проведення лекційних та практичних занять (в т.ч. в дистанційному форматі):</p> <ol style="list-style-type: none"> 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.). <p>https://drive.google.com/file/d/12agr4j405uhdmL1XAfcAgDtCxEg3kA6h/view</p> <p>Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.</p>
Безпека розробки та підтримки додатків	навчальна дисципліна	Безпека розробки та підтримки додатків.pdf	nWnHtGpMiuB5980L4hiFF8ioUFcM5ou3RuEv7Y6c8BU=	<p>Для проведення очного/дистанційного навчання: 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 КРТмаІБ.</p> <p>Проведення лекційних та лабораторних занять: аудиторія В10 – ЛАБОРАТОРІЯ КРИПТОГРАФІЇ ТА СТЕГАНОГРАФІЇ.</p> <p>Обладнання:</p> <ol style="list-style-type: none"> 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.). <p>Програмне забезпечення:</p> <ol style="list-style-type: none"> 1. Дистрибутив Kali Linux 2023.4. 2. VirtualBox 7.0.14. 3. Ubuntu 22.04.3 LTS (Jammy Jellyfish). 4. Віртуальна машина OWASP_Broken_Web_Apps_VM_1 .2

				<p>5. Віртуальна машина Protostar 6. Середовище програмування для мов та оболонки: Python, C/C++, JavaScript, SQL, Bash, Assembler.</p> <p>https://drive.google.com/file/d/1W8eDMDKMsB4cCNRIWM6OzKL5eA-yfq5f/view Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.</p>
Теорія інформації та кодування	навчальна дисципліна	Теорія інформації та кодування.pdf	PVjlkz/9YIBoVXeBq1b387MRyHwegp4n5rYuSlc6Dks=	<p>Для проведення очного/дистанційного навчання: аудиторний фонд; бібліотека 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 КРТмаБ. 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/115jr19xMFBwopa5HgDrXRRh5Oee1MJTRT/view Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.</p>
Комп'ютерна електроніка	навчальна дисципліна	Комп'ютерна електроніка.pdf	e4okoTXiHZr77ZpVW3ssZXPDP6vY1wzhbZUEnc6oBE=	<p>Для проведення очного/дистанційного навчання: аудиторний фонд і необхідне обладнання; бібліотека 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 КРТмаБ. 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.). Програмне забезпечення: National Instruments Multisim 14.3 (Education Version).</p>

			<p>https://drive.google.com/file/d/1W8eDMDKMs4cCNRIWM6OzKL5eA-yfq5f/view Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.</p>
Основи інфокомунікацій	навчальна дисципліна	Основи інфокомунікацій.pdf	<p>tV6Qg7UswWU81Pckv3a+1zk7Wv7zTpUIk5HZzG6ZYcY=</p> <p>Для проведення очного/дистанційного навчання: 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 КРТтаБ. Проведення лекційних занять: проектор мультимедійний ViewSonic PJD6211 (1 шт.), екран (1 шт.). Проведення лабораторних занять: Частина перша: В4 – ЛАБОРАТОРІЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ. Обладнання: 1. Комп'ютери AMD Athlon II X245 2.9GHz/DDR3 2GB/HDD 512 GB з монітором 20" Acer (2018 р. 6 шт.). 2. Програмне забезпечення National Instruments Multisim 14.3 (Education Version). 3. Мережеве обладнання (switch TP-Link TL-SF1016D, 1шт.). Додаткове обладнання: 1. Осцилограф OWON SmartDS 5032E (2018, 1 шт). 2. Мультиметр UNI-T UT-803 (2019, 1 шт.). 3. Генератор FY6600-60M (2018, 1 шт). Лабораторний макет (еквівалент лінії) – 1 шт.</p> <p>Частина друга: Проведення 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.). Програмне забезпечення: 1. Базові мережеві утиліти ОС Windows 2. Wireshark 4.2.3. 3. Winbox 3.40. 4. Веб-переглядач Google Chrome v121.0.6.6167.185 5. Цифрові інструменти Google Workspace (зокрема, хмарний сервіс Google Drive). 6. Офісний пакет LibreOffice (модулі LibreOffice Writer, LibreOffice Calc, LibreOffice Impress). 7. Програмне забезпечення для</p>

				<p>віртуалізації Oracle VM VirtualBox 7.0.14. 8. Менеджер архівів 7-Zip 23-01. 9. Файлові менеджери (зокрема, Midnight Commander) та інше прикладне ПЗ для ОС Linux (VLC media player, KolourPaint, Inkscape тощо). 10. Утиліта PUTI Version 0.80 for Windows.</p> <p>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/1kBQjxU27rEtyyBFKwvFa6kKclABS9zrH/view https://drive.google.com/file/d/1L6eBgRfMujf79VF56W7Da0LN6nChwnkV/view Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.</p>
Комп'ютерна дискретна математика	навчальна дисципліна	Комп'ютерна дискретна математика.pdf	BSFtoXijkZb8x2+Xj3tRz2XRMhobQnSwudcdoTiIjaY=	<p>Для проведення очного/дистанційного навчання: 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 КРТ та ІБ.</p> <p>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/12agr4j405uhdmL1XAfcAgDtCxEg3kAbh/view Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.</p>
Українська мова (за професійним спрямуванням)	навчальна дисципліна	Українська мова (за професійним спрямуванням).pdf	xRvWV6wqGuZGWF A2kLbdrzdCpruyIe5ecNYm5na+Ig=	<p>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.</p> <p>Проведення практичних занять: проектор мультимедійний ViewSonic PJD6211 (1 шт.), екран (1 шт.). Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.</p>

Основи комп'ютерних технологій	навчальна дисципліна	Основи комп'ютерних технологій.pdf	Xsn3aN+nprn9S/cKj KnsEqOLJ7L6Vgelq XLMSsNAoEPA=	<p>Для проведення очного/дистанційного навчання: 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 ACLR AP (2021 р., 3 шт.) на КРТмаБ.</p> <p>Проведення лекційних, практичних та лабораторних занять: аудиторія В10 – ЛАБОРАТОРІЯ КРИПТОГРАФІЇ ТА СТЕГАНОГРАФІЇ.</p> <p>Обладнання:</p> <ol style="list-style-type: none"> 1. Комп'ютер AMD A4-6300-/3.7GHz/DDR4 8GB 2400 MHz/SSD 256 GB з монітором 22" LG (2018 р., 10 шт.). 2. Комп'ютер Intel Core i3 6, 8 GB RAM, 500 GB HDD; монітор Samsung 22" (2024 р., 1 шт.) 3. Проектор мультимедійний Epson EB-X31 (1 шт.). 4. Екран (1 шт.). 5. Веб-камера Logitech c170 (2019 р., 1 шт.). 6. Акустична система Sven312 (1 шт.). <p>Програмне забезпечення:</p> <ol style="list-style-type: none"> 1. Операційна система Windows 10 (10 ліц.), в тому числі вбудовані утиліти та сервіси, як-от gredit, taskschd тощо. 2. Операційна система Linux (Ubuntu 22.04.3 LTS). 3. Веб-переглядачі Google Chrome, Chromium. 4. Цифрові інструменти Google Workspace (зокрема, хмарний сервіс Google Drive). 5. Офісний пакет LibreOffice (модулі LibreOffice Writer, LibreOffice Calc, LibreOffice Impress). 6. Програмне забезпечення для віртуалізації Oracle VM VirtualBox 7.0.14. 7. Менеджер архівів 7-Zip 23-01. 8. Файлові менеджери (зокрема, Midnight Commander) та інше прикладне ПЗ для ОС Linux (VLC media player, KolourPaint, Inkscape тощо). 9. Веб-застосунок phpMyAdmin 5.2.1. 10. Утиліта CPU-Z Version 2.09 for Windows® x86/x64. 11. Cisco Packet Tracer v7.3 та вище. <p>Програмне забезпечення пп. 2-10 – безкоштовне, яке регулярно оновлюється з виходом нових версій. https://drive.google.com/file/d/1W8eDMDKMsB4cCNRIWM6OzKL5eA-yfq5f/view</p> <p>Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.</p>
Вступ до кібербезпеки	навчальна дисципліна	Вступ до кібербезпеки.pdf	DPLDRB6ZUqSdUO MSS1n9wBDCuW8Z qYwo8ObizMuWBG E=	<p>Для проведення очного/дистанційного навчання: аудиторний фонд; бібліотеки ЧНУ та кафедри радіотехніки та інформаційної безпеки;</p>

				<p>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 КРТмаІБ.</p> <p>Обладнання аудиторії: проектор мультимедійний Epson EB-X04 (2019 р., 1 шт.), екран (1 шт.).</p> <p>Для проведення дистанційного навчання:</p> <ol style="list-style-type: none"> 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.). <p>https://drive.google.com/file/d/115j719xMFBwopa5HgDrXRh5Oee1MJTRT/view</p> <p>Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.</p>
Філософія	навчальна дисципліна	<i>Філософія.pdf</i>	OG2qZB9hMSyXYbAftGfP+wG2yMdvTtsR1OpnRhbbDrY=	<p>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.</p> <p>Проведення практичних занять: проектор мультимедійний ViewSonic PJD6211 (1 шт.), екран (1 шт.).</p> <p>Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.</p>
Актуальні питання історії і культури України	навчальна дисципліна	<i>Актуальні питання історії та культури України.pdf</i>	QGbYIGfBm+FKMPvE7zT+ARIFqIPpZjwhiWR7Q+XtG8Q=	<p>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.</p> <p>Проведення практичних занять: проектор мультимедійний ViewSonic PJD6211 (1 шт.), екран (1 шт.).</p> <p>Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.</p>
Вища математика	навчальна дисципліна	<i>Вища математика.pdf</i>	FfPVFEwEsT7m5PMv9jvcaSsCaCDU5UZCRz8QLZq2IYM=	<p>Для проведення очного/дистанційного навчання: 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 КРТмаІБ.</p> <p>Обладнання аудиторії: проектор мультимедійний Epson EB-X04 (2019 р., 1 шт.), екран (1 шт.).</p>

				<p>Для проведення дистанційного навчання:</p> <ol style="list-style-type: none"> 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.). <p>https://drive.google.com/file/d/115jr19xMFBwopa5HgDrXRh5Oee1MJTRT/view Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.</p>
Вибрані розділи фізики	навчальна дисципліна	Вибрані розділи фізики.pdf	YCeEJJiDdod/bdAAE8lP6Dd+JUbGxRzoda/bzV9/cIA=	<p>Для проведення очного/дистанційного навчання: 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.</p> <p>Проведення лекційних та практичних занять: проектор мультимедійний Epson EB-X31 (2018 р. 1 шт.); екран (1 шт.).</p> <p>Проведення лабораторних занять: А107.</p> <p>Лабораторні роботи виконуються фронтальним методом на лабораторній установці (6 шт.).</p> <p>Обладнання лабораторної установки:</p> <ol style="list-style-type: none"> 1. Стенд лабораторний універсальний УДЛІС (з набором компонентів, оновлений, (2019 р. 1 шт.). 2. Генератор FY6600-60M – (2018, 1 шт.) 3. Осцилограф OWON SmartDS 5032E, (2018, 1 шт.) 4. Вольтметр В7-38, 1 шт. 5. Мультиметр Uni-T UT50D, (2018, 1 шт.). <p>Крім того, в лабораторії наявні наступні прилади:</p> <ol style="list-style-type: none"> 1. Вимірювач індуктивності та ємності MASTECH MY6243, (2018, 1 шт.). 2. Генератор сигналів ALT-G, (2018, 2 шт.) <p>Працездатність лабораторного обладнання засвідчена комісією КРТІБ (прот. №1 від 28.08.2023 р.).</p> <p>https://drive.google.com/file/d/1biMnOoEo6V-8U7OWcTlJgPreOrjwiHKJ/view Наявне матеріально-технічне забезпечення достатнє для реалізації ОП.</p>
Методи і засоби проведення спеціальних вимірювань в ІТС	навчальна дисципліна	Методи і засоби проведення спеціальних вимірювань в ІТС.pdf	8LTeRHlyinvwF5/VqFjc9MDePUtjr48nnRqQjf5qHM=	<p>Для проведення очного/дистанційного навчання: аудиторний фонд і необхідне обладнання; бібліотеки ЧНУ та кафедр, в тому числі електронні; внутрішня корпоративна пошта та система електронного навчання Moodle</p>

(<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 КРТмаІБ.

Проведення практичних, лабораторних та наочно-демонстраційних занять:
ЛАБОРАТОРІЯ ТЕХНІЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ.
Обладнання:

1. Комплекс АКОР-3 (1 шт.).
2. Вимірювач P5-10 (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 ПРОТЕСТ 1206і (2018 р., 2 шт.).
7. Акустичний шумлювач РІАС2ВА (2019 р., 1 шт.).
8. Генератор радіошуму РІАС-1М (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.).

Спеціалізоване програмне забезпечення:
"Система АКОР-М" базова версія 7.9.3459, входить в комплект поставки, та оновлення для неї версія 8.3.3499. Свідоцтво про приймання автоматизованого комплексу АКОР-3 АСЧА 411168.003, дата випуску 30.05.2018 р.
Ноутбук до АКОР HP 250 G6 S/N CND73584P7.
Операційна система Windows 10 Pro (ліц.)

Інше обладнання лабораторії ТЗЗІ (наочно-демонстраційне використання):

1. Генератор шумлення телефонних ліній STEALTH SEC model 2003 (2022 р., 2 шт.).
2. Виявник GPS-трекерів, прихованих відеокамер та жучків GPS SIGNAL ДЕТЕКТОР K18 (2022 р., 1 шт.).
3. Зразки акустичних та вібровипромінювачів.
4. Мережевий фільтр РІАС - 4ФМ/1 (2018 р., 1 шт.).
5. Розділовий трансформатор РІАС-4ТР/1 (2018 р., 1 шт.).

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/1kBOjxU27rEtyuBFKwvFa6kKclABS9zrH/view>
<https://drive.google.com/file/d/1L6eBgRfMvjf79VF56W7Da0LN6nChwnkV/view>
Наявне матеріально-технічне забезпечення достатнє для реалізації ОІП.

* 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
77220	Венкель Тетяна Василівна	доцент, Основне місце роботи	Факультет іноземних мов	Диплом спеціаліста, Чернівецький орден 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	Англійська мова професійного спілкування	<p>Кандидат філологічних наук 10.02.04 – германські мови, 2005 р., (диплом ДК № 030073) «Синтагматичні, парадигматичні та епідигматичні характеристики прикметників на позначення кольору в англійській мові»; доцент кафедри іноземних мов (12 ДЦ № 019997).</p> <p>Стажування та підвищення кваліфікації:</p> <p>Університет Коньянг (KonuYang), Нонсан, Республіка Корея Курс лекцій з основ Академічної англійської мови для аспірантів та наукових співробітників кафедри біомедичної інженерії університету Коньянг, Корея 3 22.09.2020 по 29.09.2020, 180 годин, 6 кредитів</p> <p>Наявність публікацій, монографій та посібників за профілем навчальної дисципліни:</p> <p>1. Jung-Young Son, Tetiana Venkel, Aleksei Chernyshov, Hyoung Lee and Hyun-Woo Kim, Characterization of Distortions in Electro-Holographic Image by A Shack-Hartmann Wavefront Sensor – Proc. Of SPIE, Vol. 11369, 113690U, 2020, SPIE CCC code: 0277-786X/20/\$21 doi 10.1117/12.2556446, – 10 pp. https://www.spiedigitallibrary.org/conference-proceedings-of-spie/11369/2556446/Characterization-of-distortions-in-electro-holographic-image-by-</p>

A-
Shack/10.1117/12.25564
46.short
IF 0.42, SNIP 0.39)
ISSN:0277-786X E-
ISSN:1996-756X
CiteScore 02.2019 –
0.42
2. Vashpanov, Y.; Heo,
G.; Kim, Y.; Venkel, T.;
Son, J.-Y. Detecting
Green Mold Pathogens
on Lemons Using
Hyperspectral Images.
– Appl. Sci. 2020, 10,
1209;
doi:10.3390/app100412
09. –
www.mdpi.com/journal
/applsoci. – 15 pp.
ISSN 2076-3417;
CODEN: ASPCC7
IMPACT FACTOR:
2.474 (2019) ; 5-Year
Impact Factor: 2.458
(2019)
Citations Scopus 3 Web
of Science 3 Crossref 3
CiteScore Q2
3. Jung-Young Son,
Hyoung Lee, Jung Kim,
Beom-Ryeol Lee,
Wook-Ho Son, Tetiana
Venkel [3D8/3DSA8-2]
A HMD for users with
any interocular
distance. – Proceedings
of the International
Display Workshops
Volume 26 (IDW '19) –
<https://doi.org/10.36463/idw.2019.0995>
[https://confit.atlas.jp/guide/organizer/idw/idw2019/subject/3D8_3DSA8-2](https://confit.atlas.jp/guide/organizer/idw/idw2019/subject/3D8_3DSA8-2/search;jsessionid=1B948D3818ECA2E553DD88EE025A3602?eventCode=idw2019&subjectCode=3D8_3DSA8-2) – P. 995-998
(Міжнародна
конференція, 27-29
листопада 2019 р.,
Саппоро, Японія)
ISSN-L 1883-
249/26/0995©2019
ITE and SID ISBN
9781713806301
<http://www.proceedings.com/53345.html>
4. Венкель О.В.,
Венкель Т.В.,
Манютіна О.І.
Англійська мова за
професійним
спрямуванням для
студентів відділу
комп'ютерних
технологій : навч.
посіб. для студентів
комп'ютерних
спеціальностей вищих
навчальних закладів у
2 ч. Чернівці : ПБКФ
Технодрук, 2020. Ч. 1.
160 с.
(рекомендований
Вченою радою ЧНУ
протокол № 10 від 02

						<p>листопада 2020 р.) 5. Венкель О.В., Венкель Т.В., Манютина О.І. Англійська мова за професійним спрямуванням для студентів відділу комп'ютерних технологій : навч. посіб. для студентів комп'ютерних спеціальностей вищих навчальних закладів у 2 ч. Чернівці : ПВКФ Технодрук, 2020. Ч. 2. 140 с. (рекомендований Вченою радою ЧНУ протокол № 10 від 02 листопада 2020 р.) 6. Венкель Т.В. Англійська мова професійного спрямування. Кібербезпека: Загрози, проблеми, захист / уклад.: Венкель Т.В. – Вид. 2- ге, перероблене, доповнене. – Чернівці, 2020. – 102 С. (посібник в електронній формі) 7. Венкель Т.В. Методична розробка з аналітичного фахового читання англійською мовою до монографії: "CYBERSECURITY FOR BEGINNERS" Raef Meeuwisse "Кібербезпека для початківців" Raef Meeuwisse, Cybersecurity for Beginners, Copyright © 2015 для студентів 2 курсу спеціальність – 125 "Кібербезпека". – Укл.: Венкель Т.В. – Чернівці, 2020. – 95 С. (посібник в електронній формі)</p> <p>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</p>	
454724	Прокоф'єв Михайло Іванович	професор, Сумісництво	Навчально- науковий інститут фізико- технічних та комп'ютерних наук	Диплом спеціаліста, Київський ордена Леніна політехнічний інститут, рік закінчення: 1972, спеціальність: Конструюванн я виробництва	0	Технічні системи охорони об'єктів	<p>Фахівець-практик. 1997 р. – 2021 р. – директор НДЦ «ТЕЗІС» КПІ ім. Ігоря Сікорського.</p> <p>Наявність публікацій, монографій та посібників за профілем навчальної дисципліни:</p>

				радіоапаратури , Диплом доктора наук ДД 009872, виданий 14.05.2020, Диплом кандидата наук ДК 026418, виданий 26.02.2015			1. M. Prokofiev, A. Yanenko, S. Peregudov. K. Shevchenko. Perspectives of the using mm-range radiometry in telecommunication systems of information transmission" // Adv. InfCommun. Technol., vol. 59, 2019. 2. Konstantyn Shevchenko, Oleksiy Yanenko, Mikhail Prokofiev, Sergey Peregudov, Vasyl Kuz, Stanislav Ustenko. MEASUREMENT OF THE REFLECTION COEFFICIENT OF MOIST MATERIALS AT ULTRAHIGH FREQUENCIES // Journal of the Technical University of Gabrovo. 2019. 3. Konstantyn Shevchenko, Oleksiy Yanenko, Mikhail Prokofiev, Sergey Peregudov, Vasyl Kuz. MICROWAVE FOOD FAT METER // Proceedings of the international scientific conference "UNITECH 2020" 4. Konstantyn Shevchenko, Oleksiy Yanenko, Mikhail Prokofiev, Sergey Peregudov, Vasyl Kuz. Commutation-modulation method and means of determining acupuncture points // Proceedings of the international scientific conference "UNITECH 2021"
66231	Косован Григорій Васильович	асистент, Основне місце роботи	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	Диплом магістра, Чернівецький національний університет імені Юрія Федьковича, рік закінчення: 2009, спеціальність: Захист інформації з обмеженим доступом та автоматизація її обробки, Диплом кандидата наук ДК 052173, виданий 23.04.2019	9	Безпека інформаційно-телекомунікаційних систем	Стажування та підвищення кваліфікації: Центр перепідготовки та післядип. освіти, Тернопільський нац. технічний ун-т ім. І.Пулюя, з 24.05.2021 по 18.06.2021. Свідоцтво ПК № 05408102 / 001738-21 від 18.06.2021 Тема: «Наукові основи та прогр.- апаратні засоби запровадження технологій електрон. навчання в освітній процес з метрології, телеком. електр. інженерії та поліграфії» Кафедра безпеки інф. технологій Харківського нац. університету радіоелектроніки. 3

11.02.2020 по
21.02.2020 р.
Свідоцтво АА №
02071197 / 000004-20
від 19.02.2020
Тема: «Оцінювання
захищеності
інформації. Експертні
оцінювання у сфері
захисту інформації».

Кафедра безпеки інф.
технологій
Харківського нац.
університету
радіоелектроніки. З
11.02.2020 по
21.02.2020. Свідоцтво
АА № 02071197 /
000010-20 від
21.02.2020.
Тема: «Виявлення
закладних пристроїв».

Захист кандидатської
дисертації, 2019 р.

Наявність публікацій,
монографій та
посібників за
профілем навчальної
дисципліни:

1. Косован Г.В.
Безпека
інфокомунікацій та
безперервність бізнес-
процесів / укл.: Г.В.
Косован, Г.І. Ластівка,
П.М. Шпатар.
Чернівці:
Чернівецький
національний
університет, 2023. –
152 с.
<https://radiotech.chnu.edu.ua/educationbooks/>
2. Mykola Kushnir
Synthesis of
pseudorandom
sequences generators
based on chaotic
systems and study of
their statistical
characteristics / Mykola
Kushnir, Hryhorii
Kosovan, Andrii Veryga
and Serhii Haliuk //
Information Security in
Critical Infrastructures.
Collective monograph.
Edited Ivan D.
Gorbenko and Alexandr
A. Kuznetsov. ASC
Academic Publishing,
USA, 2019. 445p.
3. Mykola Kushnir
Encryption of the
images on the basis of
two chaotic systems
with the use of fuzzy
logic / Mykola Kushnir,
Hryhorii Kosovan,
Petro Krojalo and
Andrii Komarnytsky //
15th International
Conference on
Advanced Trends in
Radioelectronics,
Telecommunications

and Computer Engineering (TCSET - 2020), February 25-29, 2020. Lviv-Slavske, Ukraine. – 4 Pp.

4. Кушнір М. Я. Дослідження властивостей хаотичних генераторів псевдовипадкових послідовностей, побудованих із використанням нечіткої логіки / Кушнір М. Я. Семенко А. І., Косован Г. В., Крояло П.М. // Науковий журнал Вісник Університету «Україна» Серія ІНФОКОМУНІКАЦІЙНІ ТА КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ. № 1 (01) 2021. Київ. Україна. С 63-72.

5. Kushnir M. Ya. Properties of generators of pseudo-random sequences constructed using fuzzy logic and two-dimensional chaotic systems / Kushnir M. Ya., Kosovan Hr. V., Kroyalo P. M. // The scientific journal “Radio Electronics, Computer Science, Control”. 2022. № 1. Vol.60. P. 39-47. p-ISSN 2313-688X.

6. Kushnir M. Method of encrypting images based on two multidimensional chaotic systems using fuzzy logic / Kushnir M., Kosovan Hr., Kroyalo P. // The scientific journal “Radioelectronic and Computer Systems”. 2022. № 4. Vol. 104. P. 117-128. p-ISSN 1814-4225.

7. Засоби радіопротидії в інформаційно-телекомунікаційних системах/ Браїловський В.В., Рождественська М.Г., Гресь О.В., Косован Г.В./ Електронний навч. посібник, Чернівці: Чернівецький нац. університет, 2021. URL: <http://surl.li/jwsdf>

Підготовлено студентів до участі у всеукраїнському конкурсі студентських наукових робіт з галузі знань “Інформатика та Кібернетика”. (22-23 квітня 2021р.). Здобуто 3 місце. Студенти Мочернюк

						<p>Т. М., Антоняк С. М. Тема роботи: “Метод шифрування зображень на основі хаотичних систем із застосуванням нечіткої логіки”</p> <p>Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 1, 3, 4, 5, 12, 14 п. 38 чинних Ліцензійних умов «Досягнення у професійній діяльності»</p>	
118310	Ластівка Галина Іванівна	доцент, Основне місце роботи	Навчально- науковий інститут фізико- технічних та комп'ютерних наук	<p>Диплом магістра, Чернівецький державний університет ім. Ю. Федьковича, рік закінчення: 1999, спеціальність: Радіотехніка, Диплом кандидата наук ДК 064434, виданий 22.12.2010, Атестат доцента 12ДЦ 035476, виданий 31.05.2013</p>	21	<p>Основи побудови систем комплексного захисту інформації</p>	<p>Стажування та підвищення кваліфікації:</p> <p>Lublin University of Technology, “Lubelska Politechnica”, Poland. Traineeship: “New knowledge in the development of information technologies through the use of new technologies in the field of research of image processing, machine learning, deep learning, artificial intelligence, intelligent data analysis, neural networks, security technologies, development of information-measuring systems diagnostic monitoring”, during 15.05.2023-15.07.2023, 180 hours / 6 credits ECTS, Certificate № 5-2023-ChNU, 15-07-2023.</p> <p>Стажування в Тернопільському національному технічному ун-ті імені Івана Пулюя, з 24.05.2021 по 18.06.2021. Свідоцтво ПК № 05408102/001740-21 від 18.06.2021. Тема: «Наукові основи та програмно-апаратні засоби запровадження технології електронного навчання в освітній процес з метрології, телекомунікацій, електричної інженерії та поліграфії».</p> <p>Програма підвищення каліф. з серії наук.-метод. семінарів-</p>

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.

Підвищення
кваліфікації у Центрі
підтримки академії
Cisco Нац. технічного
університету
«Харківський
політехнічний
інститут» в рамках
Програми Академії
Cisco (курс «Основи
апаратного та
програмного
забезпечення ПК» та
СТЕМ-практика з
Інтернету речей та
кібербезпеки).
З 1.09.2020 по
25.10.2020.
Сертифікат від
25.10.2020 р.

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
міжнародних освітніх
грантів 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.):
- G-202206-68835
«Integration of new
Cybersecurity courses
into the Curriculum of
the Yuriy Fedkovych
Chernivtsi National
University»
<https://docs.google.com/document/d/16eXTjjLWlTrbh-MAoDAmOUCql2xkDTVn/edit>
- G-202301-69802
«Promotion of the
Cyber Hygiene E-
Learning course at the
Yuriy Fedkovych
Chernivtsi National
University» (1.02.2023-
30.06.2023)

https://docs.google.com/document/d/1R9nrF94mLZtCozob-nFhWU696PCeSHd_/edit.

Сертифікат LangSkill
B2 Reference number
19Y138G019DQ1
15/07/2023.

Наявність публікацій,
монографій та
посібників за
профілем навчальної
дисципліни:

1. Методи і засоби ТЗІ:
методичні вказівки
до курсу.

проектування/ укл.:
Ластівка Г. І., Гресь О.
В. [Навч. ел. видання]
– Чернівці:
Чернівецький нац.
університет, 2022. –
90 с.

<https://drive.google.com/file/d/19gvHSMhwKACWvo6UnW1NH4QWgtAvDvn4/view>

2. Косован Г.В.
Безпека
інфокомунікацій та
безперервність бізнес-
процесів / укл.: Г.В.
Косован, Г.І. Ластівка,
П.М. Шпатар.
Чернівці:

Чернівецький
національний
університет, 2023. –
152 с.

<https://radiotech.chnu.edu.ua/educationbooks/>

3. Міждисциплінарна
курсова робота:
методичні вказівки до
курсowego
проектування/ укл. :

Ластівка Г. І.,
Рождественська М. Г.
[Навчальне
електронне видання]
– Чернівці :

Чернівецький
національний
університет, 2023.– 57
с.

<https://radiotech.chnu.edu.ua/educationbooks/>

4. Oleksandr Dubyniak,
Halyna Lastivka,
Oleksandr Lastivka
Study of methods of
artificially generated
voice information
detection // IX
International Scientific-
Practical Conference
Physical and
Technological Problems
of Transmission,
Processing and Storage
of Information in
Infocommunication
Systems 21-23 October
2021, Chernivtsi-
Suceava (Ukraine-

Romania).
5. Samila, A.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=18208501513419092697&btnI=1&hl=uk>
Академічна та професійна

							кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 1, 3, 4, 7, 8, 10, 12, 13, 14, 20 п. 38 чинних Ліцензійних умов «Досягнення у професійній діяльності»
60708	Кушнір Микола Ярославович	доцент, Основне місце роботи	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	Диплом спеціаліста, Чернівецький орден 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	Законодавчі питання інформаційної безпеки	<p>Стажування та підвищення кваліфікації:</p> <p>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».</p> <p>Наявність публікацій, монографій та посібників за профілем навчальної дисципліни:</p> <p>1. Кушнір М.Я., Горбулк В.І. Ліцензування, атестація та сертифікація в сфері безпеки об'єктів інформаційної діяльності. Електронний посібник. http://radiotech.chnu.edu.ua/educationbooks/</p> <p>2. Kushnir, M., Semenko, A., Kosovan, G., Bokla, N., & Shestopal, Y. (2019). Increasing the Cryptosecurity of Telecom. Systems with Spread Spectrum by Using Pseudorandom Sequences Based on Two Ergodic Chaotic Signals. In 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019 - Proceedings (pp. 455–458). Institute of Electrical and Electronics Engineers Inc.</p>

<https://doi.org/10.1109/AIACT.2019.8847913>
(Scopus)

2. З. Кушнір М. Я. Дослідження властивостей хаотичних генераторів псевдовипадкових послідовностей, побудованих із використанням нечіткої логіки / Кушнір М. Я. Семенко А. І., Косован Г. В., Крояло П.М. // Науковий журнал Вісник Університету «Україна» Серія Інфокомунікаційні та комп'ютерні технології. № 1 (01) 2021. Київ, Україна. С 63-72.

4. Kushnir, M., and K. Tokarieva. "A Generalization of the Arima Model to the Nonlinear and Continuous Cases." //Cybernetics and Systems Analysis, 2023. Vol. 59, pp. 900-909. <https://link.springer.com/article/10.1007/s10559-023-00625-8>

Член редколегії вісника університету «Україна», Серія ІНФОКОМУНІКАЦІЙНІ ТА КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ (Категорія Б)

Керівництво дисертації на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації (Косован Г.В.)

Керівник двох міжнародних освітніх грантів 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.):
- G-202206-68835 «Integration of new Cybersecurity courses into the Curriculum of the Yuriy Fedkovych Chernivtsi National University»
<https://docs.google.com/document/d/16eXTjjLWlTrbh-MAoDAmOUCql2xkDTVn/edit>
- G-202301-69802 «Promotion of the

						<p>Cyber Hygiene E-Learning course at the Yuriy Fedkovych Chernivtsi National University» (1.02.2023-30.06.2023) https://docs.google.com/document/d/1R9nrF94mLZtCozobnFhWU696PCeSHd_/edit</p> <p>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»</p>	
66231	Косован Григорій Васильович	асистент, Основне місце роботи	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	<p>Диплом магістра, Чернівецький національний університет імені Юрія Федьковича, рік закінчення: 2009, спеціальність: Захист інформації з обмеженим доступом та автоматизація її обробки, Диплом кандидата наук ДК 052173, виданий 23.04.2019</p>	9	Управління інформаційною безпекою	<p>Стажування та підвищення кваліфікації: Центр перепідготовки та післядип. освіти, Тернопільський нац. технічний ун-т ім. І.Пулюя, з 24.05.2021 по 18.06.2021. Свідоцтво ПК № 05408102 / 001738-21 від 18.06.2021 Тема: «Наукові основи та прогр.- апаратні засоби запровадження технологій електрон. навчання в освітній процес з метрології, телеком. електр. інженерії та поліграфії»</p> <p>Кафедра безпеки інф. технологій Харківського нац. університету радіоелектроніки. З 11.02.2020 по 21.02.2020 р. Свідоцтво АА № 02071197 / 000004-20 від 19.02.2020 Тема: «Оцінювання захищеності інформації. Експертні оцінювання у сфері захисту інформації».</p> <p>Кафедра безпеки інф. технологій Харківського нац. університету радіоелектроніки. З 11.02.2020 по 21.02.2020. Свідоцтво АА № 02071197 / 000010-20 від 21.02.2020. Тема: «Виявлення складних пристроїв».</p>

Захист кандидатської дисертації, 2019 р.

Наявність публікацій, монографій та посібників за профілем навчальної дисципліни:

1. Mykola Kushnir
Synthesis of pseudorandom sequences generators based on chaotic systems and study of their statistical characteristics / Mykola Kushnir, Hryhorii Kosovan, Andrii Veryga and Serhii Haliuk // Information Security in Critical Infrastructures. Collective monograph. Edited Ivan D. Gorbenko and Alexandr A. Kuznetsov. ASC Academic Publishing, USA, 2019. 445p.
2. Mykola Kushnir
Encryption of the images on the basis of two chaotic systems with the use of fuzzy logic / Mykola Kushnir, Hryhorii Kosovan, Petro Krojalo and Andrii Komarnytsky // 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET - 2020), February 25-29, 2020. Lviv-Slavske, Ukraine. – 4 Pp.
3. Кушнір М. Я.
Дослідження властивостей хаотичних генераторів псевдовипадкових послідовностей, побудованих із використанням нечіткої логіки / Кушнір М. Я. Семенко А. І., Косован Г. В., Крояло П.М. // Науковий журнал Вісник Університету «Україна» Серія ІНФОКОМУНІКАЦІЙНІ ТА КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ. № 1 (01) 2021. Київ. Україна. С 63-72.
4. Kushnir M. Ya.
Properties of generators of pseudo-random sequences constructed using fuzzy logic and two-dimensional chaotic systems / Kushnir M. Ya., Kosovan Hr. V., Kroyalo P. M. // The scientific journal "Radio Electronics, Computer Science, Control". 2022. № 1. Vol.60. P. 39-47.

						<p>p-ISSN 2313-688X. 5. Kushnir M. Method of encrypting images based on two multidimensional chaotic systems using fuzzy logic / Kushnir M., Kosovan Hr., Kroyalo P. // The scientific journal "Radioelectronic and Computer Systems". 2022. № 4. Vol. 104. P. 117-128. p-ISSN 1814-4225. 6. Косован Г.В. Безпека інфокомунікацій та безперервність бізнес-процесів / укл.: Г.В. Косован, Г.І. Ластівка, П.М. Шпатар. Чернівці: Чернівецький національний університет, 2023. – 152 с. https://radiotech.chnu.edu.ua/educationbooks</p> <p>Підготовлено студентів до участі у всеукраїнському конкурсі студентських наукових робіт з галузі знань "Інформатика та Кібернетика". (22-23 квітня 2021р.). Здобуто 3 місце. Студенти Мочернюк Т. М., Антоняк С. М. Тема роботи: "Метод шифрування зображень на основі хаотичних систем із застосуванням нечіткої логіки"</p> <p>Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 1, 3, 4, 5, 12, 14 п. 38 чинних Ліцензійних умов «Досягнення у професійній діяльності»</p>	
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	21	Криптографія (в тому числі курсова робота)	<p>Стажування та підвищення кваліфікації:</p> <p>1. Стажування в Тернопільському національному технічному університеті імені Івана Пулюя. Свідоцтво ПК № 05408102/001751-21 від 18.06.2021 Тема: Наукові основи та програмно-</p>

11.10.2007,
Атестат
доцента 12/ДЦ
032416,
виданий
26.09.2012

апаратні засоби
запровадження
технології
електронного
навчання в освітній
процес з метрології,
телекомунікацій,
електричної інженерії
та поліграфії. (180
год, 6 кредитів)
2. 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,
Certificate № 4-2023-
ChNU, 06-05-2023.
3. 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.

Наявність публікацій,
монографій 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/singlephotons-receiverbased-on-avalanchephotodiodes>
2. 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/wpcontent/uploads/2021/03/VKNU-TS-2020-N6-291-1.pdf>.

3. Косован Г.В.
Безпека інфокомунікацій та безперервність бізнес-процесів / укл.: Г.В. Косован, Г.І. Ластівка, П.М. Шпатар.
Чернівці: Чернівецький національний університет, 2023. – 152 с.
<https://drive.google.com/file/d/1VKk9f3CLavO5ctgWucTXOkZKhR1FQOW/view>

4. 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.

5. 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.

6. В. В. Браїловський, Г. І. Ластівка, І. С. Паюк, М. Г. Рождественська, П. М. Шпатар.
Використання засобів платформи MOODLE

						<p>для підготовки здобувачів вищої освіти з кібербезпеки до ЄДКІ. XI Міжнар. науково-практична конференція "Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій", 12–14 грудня 2022 р., м. Запоріжжя.- С. 89-91. URL: https://scholar.google.com/scholar?oi=bibs&cluster=18208501513419092697&btnI=1&hl=uk</p> <p>Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 1, 3, 4, 7, 12, 14, 15, 20 п. 38 чинних Ліцензійних умов «Досягнення у професійній діяльності»</p>	
96194	Гресь Олександр Володимирович	асистент, Основне місце роботи	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	<p>Диплом бакалавра, Чернівецький національний університет імені Юрія Федьковича, рік закінчення: 2007, спеціальність: 1601 Інформаційна безпека, Диплом спеціаліста, Чернівецький національний університет імені Юрія Федьковича, рік закінчення: 2008, спеціальність: Захист інформації з обмеженим доступом та автоматизація її обробки, Диплом кандидата наук ДК 056646, виданий 14.05.2020</p>	12	Взаємодія між компонентами систем IoT	<p>Стажування та підвищення кваліфікації:</p> <p>Lublin University of Technology, "Lubelska Politechnica", Poland. Traineeship: "New knowledge in the development of information technologies through the use of new technologies in the field of research of image processing, machine learning, deep learning, artificial intelligence, intelligent data analysis, neural networks, security technologies, development of information-measuring systems diagnostic monitoring", during 06.03.2023-06.05.2023, 180 hours / 6 credits ECTS, Sertificate № 3-2023-ChNU, 06-05-2023.</p> <p>Підвищення кваліфікації на тему: "Оцінювання захищеності інформації. Експертні оцінювання у сфері технічного захисту інформації", ("Information protection assessment. Expert evaluation in the technical protection of</p>

information”,
Харківський нац.
університет
радіоелектроніки,
2020 р.
Свідоцтво про підв.
квал. №АА
02071197/000002-20
від 19 лютого 2020
року

Підвищення
кваліфікації на тему:
“Виявлення закладних
пристроїв”,
(“Development of
rocket devices”,
Харківський нац.
університет
радіоелектроніки,
2020 р.
Свідоцтво про підв.
квал. №АА
02071197/000008-20
від 21 лютого 2020
року

Захист кандидатської
дисертації, 2020 р.

Наявність публікацій,
монографій та
посібників за
профілем навчальної
дисципліни:

1. Larin V., Rozorinov H., Hres O., Rusyn V., Subbotin S., Chichikalo N., Larina K. (2022) Decision-making Algorithm in Case of Failure of the Electric Motor of a Multi-rotor Unmanned Aerial Vehicle. CEUR Workshop Proceedings, 3137, 154-163, ISSN 1613-0073. <https://ceur-ws.org/Vol-3137/paper13.pdf>
2. Rozorinov, H., Hres, O., Rusyn, V. (2022) GENERALIZED MODEL OF INFORMATION PROTECTION PROCESS IN AUDIOVISUAL CONTENT DISTRIBUTION NETWORKS. Informatyka, Automatyka, Pomiar w Gospodarce i Ochronie Srodowiska, 12(4), pp. 21–25, ISSN 2083-0157 <https://ph.pollub.pl/index.php/iapgos/article/view/3317>
1. 3. Rozorinov H., Hres O., Rusyn V., Shpatar P. Environment of electromagnetic compatibility of radio-electronic communication means. IAPGOŚ. 2020. №1. Pp. 16-19. <https://ph.pollub.pl/in>

dex.php/iapgos/article/view/917/1281
4. Гресь О. В., Розорінов Г. М., Пількевич Ю. Г., Костяк М. Ю., Пархуць Л. Т. Програмна реалізація системи потокового шифрування інформації на основі дискретних відображень. Вимірювальна та обчислювальна техніка в технологічних процесах. 2020. №1. С.60-66.
<https://journals.khnu.km.ua/index.php/MeasComp/article/view/2021/2480>
5. Шпатар П.М., Гресь О.В., Качур В.В., Томулець А.Я. Детектування поодиноких фотонів в квантових криптографічних системах. Вісник ХНУ, Серія: технічні науки. 2020. №6. С. 28-32. ISSN 2307-5732
<http://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/03/VKNU-TS-2020-N6-291-1.pdf>
6. Rozorinov H. Generalized model of the process of information protection in audiovisual content networks / Rozorinov H., Sirchenko I., Shpatar P., Hres O., Nychy B. // Proceedings of IX International Scientific and Practical Conference “Physical and technical problems of information transmission, processing and storage of information communication systems”. – 21-23 October, 2021, Chernivtsi Suceava (Ukraine-Romania). – Pp. 78-80.
7. Гресь О.В., Косован В.М. Програмні засоби для дослідження властивостей генератора псевдовипадкових послідовностей на основі дискретного відображення / О.В. Гресь, В.М. Косован // Міжнародна наукова інтернет конференція “Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення”,

						<p>6-7 липня 2023. – Тернопіль, Україна – Переворськ, Польща. Випуск 79, С. 12-15. http://www.konferenciainline.org.ua/ua/article/id-1243/</p> <p>8. Методи і засоби ТЗІ: методичні вказівки до курс. проектування/ укл.: Ластівка Г. І., Гресь О. В. [Навч. ел. видання] – Чернівці: Чернівецький нац. університет, 2022. – 90 с. https://drive.google.com/file/d/19gvHSMhwKACWvo6UnW1NH4QWgtAvDvn4/view</p> <p>Виконання функцій члена редакційної колегії наукового видання, включеного до переліку фахових видань України. (з жовтня 2022 року): наукове фахове видання України (Категорія Б), науково-технічний журнал: “Вимірювальна та обчислювальна техніка в технологічних процесах” https://vottp.khmnu.edu.ua/index.php/vottp/about/editorialTeam</p> <p>Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПН, що засвідчується виконанням підпунктів 1, 4, 5, 8, 12, 14 п. 38 чинних Ліцензійних умов «Досягнення у професійній діяльності»</p>	
118310	Ластівка Галина Іванівна	доцент, Основне місце роботи	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	<p>Диплом магістра, Чернівецький державний університет ім. Ю. Федьковича, рік закінчення: 1999, спеціальність: Радіотехніка, Диплом кандидата наук ДК 064434, виданий 22.12.2010, Атестат доцента 12ДЦ 035476, виданий 31.05.2013</p>	21	Канали витоку інформації	<p>Стажування та підвищення кваліфікації:</p> <p>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</p>

technologies, development of information-measuring systems diagnostic monitoring”, during 15.05.2023-15.07.2023, 180 hours / 6 credits ECTS, Certificate № 5-2023-ChNU, 15-07-2023.

Стажування в Тернопільському національному технічному ун-ті імені Івана Пулюя, з 24.05.2021 по 18.06.2021. Свідоцтво ПК № 05408102/001740-21 від 18.06.2021. Тема: «Наукові основи та програмно-апаратні засоби запровадження технології електронного навчання в освітній процес з метрології, телекомунікацій, електричної інженерії та поліграфії».

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.

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.

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 міжнародних освітніх грантів 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.):
- G-202206-68835
«Integration of new Cybersecurity courses into the Curriculum of the Yuriy Fedkovych Chernivtsi National University»
<https://docs.google.com/document/d/16eXTjjLWlTrbh-MAoDAmOUCql2xkDTVn/edit>
- G-202301-69802
«Promotion of the Cyber Hygiene E-Learning course at the Yuriy Fedkovych Chernivtsi National University» (1.02.2023-30.06.2023)
https://docs.google.com/document/d/1R9nrF94mLZtCozob-nFhWU696PCeSHd_/edit

Сертифікат LangSkill B2 Reference number 19Y138G019DQ1 15/07/2023.

Наявність публікацій, монографій 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., Саміла А.П. [Навчальне електронне видання] – Чернівці : Чернівецький

національний
університет, 2023.– 88
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 ^{115}In
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

						<p>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=18208501513419092697&btnI=1&hl=uk</p> <p>Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 1, 3, 4, 7, 8, 10, 12, 13, 14, 20 п. 38 чинних Ліцензійних умов «Досягнення у професійній діяльності»</p>	
66231	Косован Григорій Васильович	асистент, Основне місце роботи	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	Диплом магістра, Чернівецький національний університет імені Юрія Федьковича, рік закінчення: 2009, спеціальність: Захист інформації з обмеженим доступом та автоматизація її обробки, Диплом кандидата наук ДК 052173, виданий	9	Архітектура і моделі безпеки	<p>Стажування та підвищення кваліфікації:</p> <p>Центр перепідготовки та післядип. освіти, Тернопільський нац. технічний ун-т ім. І. Пулюя, з 24.05.2021 по 18.06.2021. Свідоцтво ПК № 05408102 / 001738-21 від 18.06.2021 Тема: «Наукові основи та прогр.- апаратні засоби запровадження технологій електрон. навчання в освітній процес з метрології, телеком. електр.</p>

23.04.2019

інженерії та поліграфії»

Кафедра безпеки інф. технологій
Харківського нац. університету радіоелектроніки. З 11.02.2020 по 21.02.2020 р.
Свідоцтво АА № 02071197 / 000004-20 від 19.02.2020
Тема: «Оцінювання захищеності інформації. Експертні оцінювання у сфері захисту інформації».

Кафедра безпеки інф. технологій
Харківського нац. університету радіоелектроніки. З 11.02.2020 по 21.02.2020. Свідоцтво АА № 02071197 / 0000010-20 від 21.02.2020.
Тема: «Виявлення закладних пристроїв».

Захист кандидатської дисертації, 2019 р.

Наявність публікацій, монографій та посібників за профілем навчальної дисципліни:

1. Mykola Kushnir
Synthesis of pseudorandom sequences generators based on chaotic systems and study of their statistical characteristics / Mykola Kushnir, Hryhorii Kosovan, Andrii Veryga and Serhii Haliuk // Information Security in Critical Infrastructures. Collective monograph. Edited Ivan D. Gorbenko and Alexandr A. Kuznetsov. ASC Academic Publishing, USA, 2019. 445p.
2. Mykola Kushnir
Encryption of the images on the basis of two chaotic systems with the use of fuzzy logic / Mykola Kushnir, Hryhorii Kosovan, Petro Krojalo and Andrii Komarnytsky // 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET - 2020), February 25-29, 2020. Lviv-Slavske, Ukraine. – 4 Pp.
3. Кушнір М. Я.
Дослідження

властивостей хаотичних генераторів псевдовипадкових послідовностей, побудованих із використанням нечіткої логіки / Кушнір М. Я. Семенко А. І., Косован Г. В., Крояло П. М. // Науковий журнал Вісник Університету «Україна» Серія ІНФОКОМУНІКАЦІЙНІ ТА КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ. № 1 (01) 2021. Київ. Україна. С 63-72.

4. Kushnir M. Ya. Properties of generators of pseudo-random sequences constructed using fuzzy logic and two-dimensional chaotic systems / Kushnir M. Ya., Kosovan Hr. V., Kroyalo P. M. // The scientific journal "Radio Electronics, Computer Science, Control". 2022. № 1. Vol.60. P. 39-47. p-ISSN 2313-688X.

5. Kushnir M. Method of encrypting images based on two multidimensional chaotic systems using fuzzy logic / Kushnir M., Kosovan Hr., Kroyalo P. // The scientific journal "Radioelectronic and Computer Systems". 2022. № 4. Vol. 104. P. 117-128. p-ISSN 1814-4225.

6. Косован Г.В. Безпека інфокомунікацій та безперервність бізнес-процесів / укл.: Г.В. Косован, Г.І. Ластівка, П.М. Шпатар. Чернівці: Чернівецький національний університет, 2023. – 152 с. URL: <https://radiotech.chnu.edu.ua/educationbooks/>

Підготовлено студентів до участі у всеукраїнському конкурсі студентських наукових робіт з галузі знань "Інформатика та Кібернетика". (22-23 квітня 2021р.). Здобуто 3 місце. Студенти Мочернюк Т. М., Антоняк С. М. Тема роботи: "Метод шифрування зображень на основі хаотичних систем із застосуванням нечіткої логіки"

						Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОШП, що засвідчується виконанням підпунктів 1, 3, 4, 5, 12, 14 п. 38 чинних Ліцензійних умов «Досягнення у професійній діяльності»
77220	Венкель Тетяна Василівна	доцент, Основне місце роботи	Факультет іноземних мов	Диплом спеціаліста, Чернівецький орден 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	Іноземна мова (за професійним спрямуванням) Кандидат філологічних наук 10.02.04 – германські мови, 2005 р., (диплом ДК № 030073) «Синтагматичні, парадигматичні та епідигматичні характеристики прикметників на позначення кольору в англійській мові»; доцент кафедри іноземних мов (12 ДЦ № 019997). Стажування та підвищення кваліфікації: Університет Коньянг (KonYang), Нонсан, Республіка Корея Курс лекцій з основ Академічної англійської мови для аспірантів та наукових співробітників кафедри біомедичної інженерії університету Коньянг, Корея 3 22.09.2020 по 29.09.2020, 180 годин, 6 кредитів Наявність публікацій, монографій та посібників за профілем навчальної дисципліни: 1. Jung-Young Son, Tetiana Venkel, Aleksei Chernyshov, Nyoung Lee and Hyun-Woo Kim, Characterization of Distortions in Electro-Holographic Image by A Shack-Hartmann Wavefront Sensor – Proc. Of SPIE, Vol. 11369, 113690U, 2020, SPIE CCC code: 0277-786X/20/\$21 doi 10.1117/12.2556446, – 10 pp. https://www.spiedigitallibrary.org/conference-proceedings-of-spie/11369/2556446/Characterization-of-distortions-in-electro-

holographic-image-by-A-
Shack/10.1117/12.25564
46.short
IF 0.42, SNIP 0.39)
ISSN:0277-786X E-
ISSN:1996-756X
CiteScore 02.2019 –
0.42
2. Vashpanov, Y.; Heo,
G.; Kim, Y.; Venkel, T.;
Son, J.-Y. Detecting
Green Mold Pathogens
on Lemons Using
Hyperspectral Images.
– Appl. Sci. 2020, 10,
1209;
doi:10.3390/app100412
09. –
www.mdpi.com/journal
/appls. – 15 pp.
ISSN 2076-3417;
CODEN: ASPCC7
IMPACT FACTOR:
2.474 (2019) ; 5-Year
Impact Factor: 2.458
(2019)
Citations Scopus 3 Web
of Science 3 Crossref 3
CiteScore Q2
3. Jung-Young Son,
Hyoung Lee, Jung Kim,
Beom-Ryeol Lee,
Wook-Ho Son, Tetiana
Venkel [3D8/3DSA8-2]
A HMD for users with
any interocular
distance. – Proceedings
of the International
Display Workshops
Volume 26 (IDW '19) –
<https://doi.org/10.36463/idw.2019.0995>
[https://confit.atlas.jp/guide/organizer/idw/idw2019/subject/3D8_3DSA8-2](https://confit.atlas.jp/guide/organizer/idw/idw2019/subject/3D8_3DSA8-2/search;jsessionid=1B948D3818ECA2E553DD8EE025A3602?eventCode=idw2019&subjectCode=3D8_3DSA8-2) – P. 995-998
(Міжнародна
конференція, 27-29
листопада 2019 р.,
Саппоро, Японія)
ISSN-L 1883-
249/26/0995©2019
ITE and SID ISBN
9781713806301
<http://www.proceedings.com/53345.html>
4. Венкель Т.В.,
Манютина 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 : ПБКФ
Технодрук, 2020. Ч. 1.
160 с.
(рекомендований
Вченою радою ЧНУ

						<p>протокол № 10 від 02 листопада 2020 р.)</p> <p>5. Венкель О.В., Венкель Т.В., Манютіна О.І. Англійська мова за професійним спрямуванням для студентів відділу комп'ютерних технологій : навч. посіб. для студентів комп'ютерних спеціальностей вищих навчальних закладів у 2 ч. Чернівці : ПБКФ Технодрук, 2020. Ч. 2. 140 с. (рекомендований Вченою радою ЧНУ протокол № 10 від 02 листопада 2020 р.)</p> <p>6. Венкель Т.В. Англійська мова професійного спрямування. Кібербезпека: Загрози, проблеми, захист / уклад.: Венкель Т.В. – Вид. 2-ге, перероблене, доповнене. – Чернівці, 2020. – 102 С. (посібник в електронній формі)</p> <p>7. Венкель Т.В. Методична розробка з аналітичного фахового читання англійською мовою до монографії: "CYBERSECURITY FOR BEGINNERS" Raef Meeuwisse "Кібербезпека для початківців" Raef Meeuwisse, Cybersecurity for Beginners, Copyright © 2015 для студентів 2 курсу спеціальність – 125 "Кібербезпека". – Укл.: Венкель Т.В. – Чернівці, 2020. – 95 С. (посібник в електронній формі)</p> <p>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</p>	
66231	Косован Григорій Васильович	асистент, Основне місце роботи	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	Диплом магістра, Чернівецький національний університет імені Юрія Федьковича, рік закінчення: 2009, спеціальність:	9	Методи і засоби проведення спеціальних вимірювань в ІТС	<p>Стажування та підвищення кваліфікації:</p> <p>Центр перепідготовки та післядип. освіти, Тернопільський нац. технічний ун-т ім. І.Пулюя, з 24.05.2021 по 18.06.2021.</p>

Захист
інформації з
обмеженим
доступом та
автоматизація
її обробки,
Диплом
кандидата наук
ДК 052173,
виданий
23.04.2019

Свідоцтво ПК №
05408102 / 001738-21
від 18.06.2021
Тема: «Наукові основи
та прогр.- апаратні
засоби запровадження
технологій електрон.
навчання в освітній
процес з метрології,
телеком. електр.
інженерії та
поліграфії»

Кафедра безпеки інф.
технологій
Харківського нац.
університету
радіоелектроніки. З
11.02.2020 по
21.02.2020 р.
Свідоцтво АА №
02071197 / 000004-20
від 19.02.2020
Тема: «Оцінювання
захищеності
інформації. Експертні
оцінювання у сфері
захисту інформації».

Кафедра безпеки інф.
технологій
Харківського нац.
університету
радіоелектроніки. З
11.02.2020 по
21.02.2020. Свідоцтво
АА № 02071197 /
0000010-20 від
21.02.2020.
Тема: «Виявлення
закладних пристроїв».

Захист кандидатської
дисертації, 2019 р.

Наявність публікацій,
монографій та
посібників за
профілем навчальної
дисципліни:

1. Mykola Kushnir
Synthesis of
pseudorandom
sequences generators
based on chaotic
systems and study of
their statistical
characteristics / Mykola
Kushnir, Hryhorii
Kosovan, Andrii Veryga
and Serhii Haliuk //
Information Security in
Critical Infrastructures.
Collective monograph.
Edited Ivan D.
Gorbenko and Alexandr
A. Kuznetsov. ASC
Academic Publishing,
USA, 2019. 445p.
2. Mykola Kushnir
Encryption of the
images on the basis of
two chaotic systems
with the use of fuzzy
logic / Mykola Kushnir,
Hryhorii Kosovan,
Petro Krojalo and
Andrii Komarnytskyi //
15th International
Conference on

Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET - 2020), February 25-29, 2020. Lviv-Slavske, Ukraine. – 4 Pp.
3. Кушнір М. Я. Дослідження властивостей хаотичних генераторів псевдовипадкових послідовностей, побудованих із використанням нечіткої логіки / Кушнір М. Я. Семенко А. І., Косован Г. В., Крояло П.М. // Науковий журнал Вісник Університету «Україна» Серія ІНФОКОМУНІКАЦІЙНІ ТА КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ. № 1 (01) 2021. Київ. Україна. С 63-72.
4. Kushnir M. Ya. Properties of generators of pseudo-random sequences constructed using fuzzy logic and two-dimensional chaotic systems / Kushnir M. Ya., Kosovan Hr. V., Kroyalo P. M. // The scientific journal “Radio Electronics, Computer Science, Control”. 2022. № 1. Vol.60. P. 39-47. p-ISSN 2313-688X.
5. Kushnir M. Method of encrypting images based on two multidimensional chaotic systems using fuzzy logic / Kushnir M., Kosovan Hr., Kroyalo P. // The scientific journal “Radioelectronic and Computer Systems”. 2022. № 4. Vol. 104. P. 117-128. p-ISSN 1814-4225.
6. Засоби радіопротидії в інформаційно-телекомунікаційних системах/ Браїловський В.В., Рождественська М.Г., Гресь О.В., Косован Г.В./ Електронний навч. посібник, Чернівці: Чернівецький нац. університет, 2021.
URL:
<http://surl.li/jwsdf>

Підготовлено студентів до участі у всеукраїнському конкурсі студентських наукових робіт з галузі знань “Інформатика та Кібернетика”. (22-23

						<p>квітня 2021р.). Здобуто 3 місце. Студенти Мочернюк Т. М., Антоняк С. М. Тема роботи: “Метод шифрування зображень на основі хаотичних систем із застосуванням нечіткої логіки”</p> <p>Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПН, що засвідчується виконанням підпунктів 1, 3, 4, 5, 12, 14 п.. 38 чинних Ліцензійних умов «Досягнення у професійній діяльності»</p>	
375264	Круліковський Олег Валерійович	асистент, Основне місце роботи	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	<p>Диплом бакалавра, Чернівецький національний університет імені Юрія Федьковича, рік закінчення: 2013, спеціальність: 090701 Радіотехніка, Диплом магістра, Чернівецький національний університет імені Юрія Федьковича, рік закінчення: 2014, спеціальність: Радіотехніка, Диплом кандидата наук ДК 047445, виданий 16.05.2018</p>	6	Безпека розробки та підтримки додатків	<p>Стажування та підвищення кваліфікації:</p> <p>1. Участь у міжнародному проєкті „DetectorulLHCb, producțiaderarticule în ciocniri proton-protonlaLHC pentrurapiditățimari, dezintegrărialehadronil orgrei, programuldeupgrade”, contract PN III, Program 5/Subprogram 5.2/Modulul CERN-RO, nr. 09/10.03.2020” https://usv.ro/wp-content/uploads/2020/08/Rezultat-concurs-ACS-in-electronica-aplicata.pdf</p> <p>2. Керівництво командою студентів у Міжнародному конкурсі з інформаційної безпеки CTF-USV Suceava 2023. https://drive.google.com/drive/folders/1Jx6HTevjLW39c-w17V9lISmciuZrAGQ</p> <p>Наявність публікацій, монографій та посібників за профілем навчальної дисципліни:</p> <p>1. Програмне забезпечення об'єктів кіберпростору. Мова програмування С: методичні рекомендації до виконання лабораторних робіт/ укл.: Галюк С.Д., Круліковський О.В. - Чернівці : Чернівецький нац. ун-т, 2022. 101 с.</p>

						<p>https://archer.chnu.edu.ua/jspui/handle/123456789/5654</p> <p>2. Програмне забезпечення об'єктів кіберпростору: методичні рекомендації до виконання лабораторних робіт/ укл.: Галюк С.Д., Круліковський О.В., Політанський Л.Ф. - Чернівці : Чернівецький нац. ун-т, 2019. 120 с. https://drive.google.com/file/d/179BVwg9G5axwHoKKfpSq9LvGAgMgEOm/view</p> <p>1. Oleh Krulikovskiy, Serhii Haliuk, Ihor Safronov and Ivan Gorbenko. Ukrainian National Encryption Standards for FPGA Based Embedded Systems // Security of Infocommunication Systems and Internet of Things. - Vol. 1 No. 1 (2023) . DOI: https://doi.org/10.31861/sisiot2023.1.01005</p> <p>2. Haliuk Serhii, Krulikovskiy Oleh, Vovchuk Dmytro, Corinto Fernando, Memristive Structure-Based Chaotic System for PRNG // Symmetry. 2022. – V. 14. – № 1. – A. № 68.</p> <p>3. Serhii Haliuk Studying the properties of pixels permutations based on discretized standard map / Serhii Haliuk, Oleh Krulikovskiy, Vitalii Vlasenko // Informatyka, Automatyka, Pomiarzy w Gospodarce i Ochronie Środowiska, 10(1), 2020, 48-51 - pp.</p> <p>Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПІ, що засвідчується виконанням підпунктів 1, 3, 4, 10, 14, 19 п. 38 чинних Ліцензійних умов «Досягнення у професійній діяльності»</p>	
91742	Галюк Сергій Дмитрович	асистент, Основне місце роботи	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	Диплом магістра, Чернівецький національний університет імені Юрія Федьковича,	10	Програмне забезпечення об'єктів кіберпростору (в тому числі курсова робота)	<p>Стажування та підвищення кваліфікації:</p> <p>Підвищення кваліфікації: Тернопільський</p>

рік закінчення:
2008,
спеціальність:
090701
Радіотехніка,
Диплом
кандидата наук
ДК 011656,
виданий
25.01.2013

національний
технічний університет
імені Івана Пулюя.
Тема: «Наукові основи
та програмно –
апаратні засоби
запровадження
технологій
електронного
навчання в освітній
процес з метрології,
телекомунікацій,
електричної інженерії
та поліграфії».
Свідоцтво ПК
05408102/001732-2

Наявність публікацій,
монографій та
посібників за
профілем навчальної
дисципліни:

1. Програмне забезпечення об'єктів кіберпростору. Мова програмування C: методичні рекомендації до виконання лабораторних робіт/ укл.: Галюк С.Д., Круліковський О.В. - Чернівці : Чернівецький нац. ун-т, 2022. 101 с. <https://archer.chnu.edu.ua/jspui/handle/123456789/5654>
2. Програмне забезпечення об'єктів кіберпростору: методичні рекомендації до виконання лабораторних робіт/ укл.: Галюк С.Д., Круліковський О.В., Політанський Л.Ф. - Чернівці : Чернівецький нац. ун-т, 2019. 120 с. <https://drive.google.com/file/d/179BVwg9G5axwHoKKfpSqngLvGAgMgEOm/view>

1. Oleh Krulikovskiy, Serhii Haliuk, Ihor Safronov and Ivan Gorbenko. Ukrainian National Encryption Standards for FPGA Based Embedded Systems // Security of Infocommunication Systems and Internet of Things. - Vol. 1 No. 1 (2023) . DOI: <https://doi.org/10.31861/sisiot2023.1.01005>
2. Haliuk Serhii, Krulikovskiy Oleh, Vovchuk Dmytro, Corinto Fernando, Memristive Structure-Based Chaotic System for PRNG // Symmetry. 2022. – V. 14. – № 1. – A. № 68.

						<p>3. Kushnir M., Vovchuk D., Haliuk S., Ivaniuk P., Politanskyi R. 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, 2021, PP. 207-227.</p> <p>4. Serhii Haliuk Studying the properties of pixels permutations based on discretized standard map / Serhii Haliuk, Oleh Krulikovskiy, Vitalii Vlasenko // Informatyka, Automatyka, Pomiar w Gospodarce i Ochronie Środowiska, 10(1), 2020, 48-51 - pp.</p> <p>Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПН, що засвідчується виконанням підпунктів 1, 3, 4, 8, 12, 14 п. 38 чинних Ліцензійних умов «Досягнення у професійній діяльності»</p>	
48065	Гуцуляк Ірина Георгіївна	доцент, Основне місце роботи	Філологічний факультет	<p>Диплом спеціаліста, Чернівецький державний університет імені Юрія Федьковича, рік закінчення: 1996, спеціальність: українська мова і література, Диплом кандидата наук ДК 034916, виданий 11.05.2006, Аттестат доцента 12ДЦ 034844, виданий 28.03.2013</p>	26	Українська мова (за професійним спрямуванням)	<p>Кандидат філологічних наук зі спеціальності 10.02.01 - українська мова. Тема дисертації: "Мовостиль українського поетичного бароко".</p> <p>Стажування та підвищення кваліфікації:</p> <p>Прикарпатський національний університет імені Василя Стефаника, наказ № 71 від 03.03.2021 р. Тема стажування: «Методика викладання історико-лінгвістичних дисциплін» (з 11.03 до 11.06.2021 р.). Довідка № 01-23/282 від 23.06.2021 р.</p> <p>Наявність публікацій, монографій та посібників за профілем навчальної</p>

						<p>дисципліни:</p> <p>1. Гуцуляк І. Рецепція Біблії у символіці українського поетичного бароко. Лінгвостилістичні студії. 2020. Вип. 12. С. 37–53. https://lingvostud.vnu.edu.ua/index.php/lingvostud/article/view/303 ISSN 2413-0923.</p> <p>2. Мар'яна Білич Науковий керівник – доц. Гуцуляк І. Г. Вплив звука на зміст поетичного тексту (на матеріалі табірної поезії Василя Стуса)//Матеріали студ. наукової конференції Чернівецького національного університету імені Юрія Федьковича. 5-8 квітня 2022 р. Чернівці. – С.179-180 . https://www.chnu.edu.ua/media/neqaujmy/fil-fak-studentska-konferentsiia_2022.pdf</p> <p>3. Інна Романюк Науковий керівник – доц. Гуцуляк І. Г. Мовні засоби вираження часу в романі Марії Матіос «Солодка Даруся»//Матеріали студ. наукової конференції Чернівецького національного університету імені Юрія Федьковича. 20-21квітня 2021 р. Чернівці. – С.195-196 . https://www.chnu.edu.ua/media/i2mnyzxo/zbirnykpratsifilfak2021.pdf</p> <p>Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 10, 11, 15, 19 п. 38 чинних Ліцензійних умов «Досягнення у професійній діяльності»</p>	
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, рік закінчення: 1999, спеціальність: Радіотехніка,	21	Інформаційний пошук у кібербезпеці	<p>Стажування та підвищення кваліфікації:</p> <p>Lublin University of Technology, "Lubelska Politechnica", Poland. Traineeship: "New knowledge in the development of information</p>

Диплом
кандидата наук
ДК 064434,
виданий
22.12.2010,
Атестат
доцента 12ДЦ
035476,
виданий
31.05.2013

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, Certificate № 5-2023-ChNU, 15-07-2023.

Стажування в Тернопільському національному технічному ун-ті імені Івана Пулюя, з 24.05.2021 по 18.06.2021.
Свідоцтво ПК № 05408102/001740-21 від 18.06.2021.
Тема: «Наукові основи та програмно-апаратні засоби запровадження технології електронного навчання в освітній процес з метрології, телекомунікацій, електричної інженерії та поліграфії».

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.

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.

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 міжнародних освітніх грантів 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.):
- G-202206-68835
«Integration of new Cybersecurity courses into the Curriculum of the Yuriy Fedkovych Chernivtsi National University»
<https://docs.google.com/document/d/16eXTjjLWlTrbh-MAoDAmOUCql2xkDTVn/edit>
- G-202301-69802
«Promotion of the Cyber Hygiene E-Learning course at the Yuriy Fedkovych Chernivtsi National University» (1.02.2023-30.06.2023)
https://docs.google.com/document/d/1R9nrF94mLZtCozob-nFhWU696PCeSHd_/edit

Сертифікат LangSkill B2 Reference number 19Y138G019DQ1 15/07/2023.

Наявність публікацій, монографій 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., Саміла А.П. [Навчальне електронне видання] – Чернівці : Чернівецький національний університет, 2023.– 88 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 ^{115}In 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

						<p>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</p> <p>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</p> <p>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=18208501513419092697&btnI=1&hl=uk</p> <p>Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 1, 3, 4, 7, 8, 10, 12, 13, 14, 20 п. 38 чинних Ліцензійних умов «Досягнення у професійній діяльності»</p>	
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	15	Комп'ютерна електроніка	<p>Стажування та підвищення кваліфікації:</p> <p>1. Стажування в Сучавському університеті «Штефан чел Маре» (Румунія) (міжнародний сертифікат «Certificat</p>

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

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 14.01.2020)
2. Навчальний курс
INTRODUCTION TO
QUANTUM
INFORMATION на
платформі Coursera
(розробник Korea
Advanced Institute of
Science and
Technology(KAIST)).
Сертифікат від
27.01.2023
(<https://www.coursera.org/account/accomplishments/verify/DUBMHBUZKMYT>)

Наявність публікацій,
монографій та
посібників за
профілем навчальної
дисципліни:
1. Основи
електротехніки й
радіоелектроніки :
навч. посіб. / Махній,
В. П.; Павлюк, М. Ф.;
Політанський, Р. Л.;
Політанський, Л. Ф. ;
Чернівець. нац. ун-т ім.
Юрія Федьковича. -
Чернівці : Рута, 2019. -
271 с.
https://drive.google.com/file/d/1JGMe8LOtWJW2r2kJUCnoXso_Bw1z6CnR/view
2. Politanskyi, R.,
Vistak, M., Veryga, A.
and Ruda, T. Modelling
of spintronic devices for
application in random
access memory /
Informatyka,
Automatyka, Pomiarы w
Gospodarce i Ochronie
Środowiska. 2020,
10(1), pp. 62-65
DOI:
<https://doi.org/10.35784/iapgos.915> .
3. A. Veryga, R.
Politanskyi. Time
interval switching
device / IAPGOS /
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> .
4. 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 .

5. 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.

6. Політанський Р. Л. Детектори електромагнітного поля на основі пристроїв спінтроніки / Р. Л. Політанський, П. М. Шпатар, М. В. Вісьтак, І. Т. Когут, І. С. Дісковський, Ю. А. Рудяк // Фізика і хімія твердого тіла. - 2023. - Т. 24. - № 3. - С. 433-440.

7. R Politanskyi, A Samila, L Politanskyi, V Vlasenko. Investigation of High-Speed Methods for Determining the Equilibrium State of a Network Based on the Principle of Maximum Entropy / IEEE International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, 2022. https://link.springer.com/chapter/10.1007/978-3-031-24963-1_35

Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПІ, що засвідчується виконанням підпунктів 1, 3, 4, 6, 7, 8 п. 38 чинних Ліцензійних умов «Досягнення у професійній

53134	Мельничук Лілія Михайлівна	доцент, Основне місце роботи	Факультет математики та інформатики	Диплом спеціаліста, Чернівецький державний університет імені Юрія Федьковича, рік закінчення: 1993, спеціальність: математика, Диплом кандидата наук ДК 001517, виданий 11.11.1998, Атестат доцента 02ДЦ 002248, виданий 21.10.2004	27	Вища математика	<p>діяльності» Стажування та підвищення кваліфікації:</p> <p>1. Івано-Франківський національний технічний університет нафти і газу, кафедра вищої математики. Термін стажування 11.10.2021 – 10.12.2021 рр. Наказ №199/4 від 05.10.2021 р.</p> <p>2. Сучавський університет "Штефан чел Маре" з 27.06.22 по 5.08.22 Наказ №165</p> <p>Наявність публікацій, монографій та посібників за профілем навчальної дисципліни:</p> <p>1. Мельничук Л.М. Інтерпретована динамічна візуальна мова програмування (Scratch): навч. посібник/ Л.М. Мельничук, В.М. Лучко, Г.М. Перун. - Чернівці: Чернівец. нац. ун-т ім. Ю. Федьковича, 2021. - 128 с.</p> <p>2. Нормативно-документальна основа вчителя інформатики початкової школи НУШ : навч. посіб. / уклад.: В.М. Лучко, Л.М. Мельничук, Г.М. Перун. Чернівці: Чернівец. нац. ун-т ім. Ю. Федьковича, 2022. 228 с.</p> <p>3. Практикум з вищої математики. Частина 2: навчальний посібник / В.М. Мойсишин, Я.І. Савчук, А.І. Бандура, І.М. Гураль, Л.М. Мельничук, Л.А. Мойсеєнко, Л.Р. Смолівик, В.В. Тирлич; За ред. В.М. Мойсишина, Я.І. Савчука. – Івано-Франківськ: ІФНТУНГ, 2022. – 658 с.</p> <p>4. Мельничук Л.М. Фундаментальний розв'язок задачі Коші для параболічного рівняння другого порядку зі зростаючими коефіцієнтами та з операторами Бесселя різних порядків // Буков. мат. журн. - 2022. – 10, № 2. – С. 176 – 184.</p> <p>5. Мельничук Л., Яшан Б., Кондур О. Поглиблене вивчення</p>
-------	----------------------------	------------------------------	-------------------------------------	---	----	-----------------	--

						<p>робототехніки у школі впровадженням вибіркового навчальних курсів // Освітні обрії. 2022. – 55, № 2 – С. 59-64.</p> <p>6. Л. Мельничук. Структура та властивості фундаментального розв'язку задачі Коші для ультрапараболічного рівняння із зростаючими коефіцієнтами групи молодших членів та з операторами Бесселя різних порядків // Сучасні проблеми диференціальних рівнянь та їх застосування: Матеріали міжнародної наукової конференції, присвяченої 100-річчю від дня народження професора С.Д. Ейдельмана, 16–19 вересня 2020 р. – Чернівці: Чернівецький нац. ун-т, 2020. – С. 167-168.</p> <p>7. Мельничук Л.М. Методичні особливості дистанційного навчання при вивченні середовища програмування Скретч // Міжнародна наукова конференція, присвячена 75-річчю кафедри диференціальних рівнянь та 85-річчю від дня народження Михайла Павловича Ленюка, 28 – 30 жовтня 2021 р., Чернівці: матеріали конференції. – Чернівці, 2021. – С. 116–117.</p> <p>Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 3, 4, 12, 19 п. 38 чинних Ліцензійних умов «Досягнення у професійній діяльності»</p>	
48055	Чаплак Ян Васильович	доцент, Основне місце роботи	Факультет педагогіки, психології та соціальної роботи	Диплом спеціаліста, Чернівецький державний університет імені Юрія Федьковича,	26	Міжособистісне спілкування і побудова команд	<p>Стажування та підвищення кваліфікації:</p> <p>1.Український науково-методичний центр практичної</p>

рік закінчення:
1997,
спеціальність:
Початкове
навчання,
практична
психологія,
Диплом
кандидата наук
ДК 040017,
виданий
15.03.2007,
Атестат
доцента 12ДЦ
028142,
виданий
01.07.2011

психології і соціальної
роботи, 25.10.2019-
05.12.2019.,
Тема: «Психологічна
допомога особистості
на теренах цифрового
світу»
Сертифікат № 7 від 12
грудня 2019 року.
Наказ №828-від від
26 листопада 2019 р.
https://drive.google.com/file/d/1BXGxHvsq7H1s_kwjLU2byEmTVGq06-vR/view?usp=sharing
2. ЧНУ ім.
Федьковича,
сертифікат «Основи
користування
Moodle», 02.04.20,
<https://drive.google.com/drive/folders/1P4FQiOTGKNiWNFbSdzk1Snxt44NJq>
3. Свідоцтво
підвищення
кваліфікації для
педагогічних
працівників та
психологів про
проходження курсу
«Перша психологічна
допомога під час та
після війни», в обсязі 1
кредит ЄКТС (МОНУ,
Інститут модернізації
змісту освіти)
4.08.2022.
№84415829
<https://drive.google.com/file/d/13mogsM7kYv-dc9G4iTn-BPZO9d5WDERG/view?usp=sharing>
4. Сертифікат про
проходження курсу
"Критичне мислення
для освітян", кількість
годин - 30 годин (1
кредит ЄКТС),
prometheus.
29.01.2022
https://drive.google.com/file/d/1suP1XdMLC6Qh_xdMtYuLIUAMkmG_ufun/view?usp=sharing
5. Сертифікат, що
засвідчує участь у
Всеукраїнському
міжвідомчому
психологічному
форумі "Забезпечення
психологічної
допомоги у секторі
сил оборони країни",
12 годин (0,4 кредиту)
Міністерство
внутрішніх справ,
Державний науково-
дослідний інститут
МВС України
https://drive.google.com/file/d/1io_SGGa_UyJxjLaC8Lcjo4dg_Ivuf9tR/view?usp=sharing
6. Сертифікат
засвідчує
проходження курсу
"Знати як допомогти",

6 год. (0,2 кредити ЄКТС) 29.11.2022
Національна програма психічного здоров'я та психосоціальної підтримки
https://drive.google.com/file/d/1KFo_DhsmnkZ_Ze-oClogQS6U4ZtE71x/vi
ew?usp=sharing

7. Сертифікат учасника у міжнародній науково-практичній конференції “Результати сучасних наукових досліджень та розвитку” - 24 год., 0,8 кредитів ECTS (2021р.)
<https://drive.google.com/file/d/14VEzKO9CmmQH1ZtJQDMVzJfVJgLfuiNii/view?usp=sharing>

8. Сертифікат учасника I Міжнародної наукової конференції “воєнні конфлікти та техногенні катастрофи” - 18 год., 0,6 кредитів ECTS. (2021р.)
https://drive.google.com/file/d/1iivhTfyU72bNpZaMyt9lbSIKokp_4CSrT/view?usp=sharing

9. Сертифікат підтверджує проходження курсу “Перша психологічна допомога в екстрених і кризових ситуаціях”
12 год. (0,4 кредиту ECTS) №083399, 2022
<https://drive.google.com/file/d/1LT3MwoXtjaDWCATUNJGstyyN2iKXuPoV/view?usp=sharing>

10. Сертифікат підтверджує проходження курсу “Діалог та медіація: Шлях до порозуміння”.
Кількість годин - 30 годин (1 кредит ЄКТС). 2022 рік.
https://drive.google.com/file/d/1GF9gwBfXBQ_E8CgfJGojnoKZy2jkVNAM/view?usp=sharing

11. Сертифікат засвідчує проходження курсу “Нові підходи до надання психологічних послуг учасникам освітнього процесу в дистанційних умовах” (0,1 кредиту ЄКТС). 2022 рік. МОНУ, НПА, Швейцарська Конфедерація
<https://drive.google.co>

m/file/d/1a3DyF4liQvB
ZLeCziCIyKkNfAOj6n4j
4/view?usp=sharing
12.Сертифікат
засвідчує
проходження курсу
“Психічне здоров’я та
психологічний
добробут на робочому
місці” (0,1 кредиту
ЄКТС). 2022 рік.
Центр психічного
здоров’я і моніторингу
наркотиків та
алкоголю МОЗ
<https://drive.google.com/file/d/1VUrNFIVF4UGqoCxVdFbqiw9APWIK4u4l/view?usp=sharing>

Наявність публікацій,
монографій та
посібників за
профілем навчальної
дисципліни:

1. Чуйко Г.В., Чаплак Я.В. Міжособистісна довіра як передумова партнерських стосунків між людьми. Психологічний часопис : збірник наукових праць / за ред. С.Д. Максименка. 2020. Т.6. Вип. 1. К. : Інститут психології імені Г.С. Костюка НАПН України. С.29-39. URL: DOI: 10.31108/1.2020.6.1.3; <https://www.apsijournal.com/index.php/psyjournal/article/view/811/496>
2. Чуйко Г.В., Чаплак Я.В. Толерантність у житті людини і суспільства. Психологічний часопис : збірник наукових праць / за ред. С.Д. Максименка. 2020. Т.6. Вип. 2. К. : Інститут психології імені Г.С. Костюка НАПН України. С.29-42. URL: DOI: 10.31108/1.2020.6.2.3. <https://www.apsijournal.com/index.php/psyjournal/article/view/845/511>
3. Yan Chaplak, Halyna Chuyko, Andrievia Yaroslava. Psychological aspects of the influence of information bubbles on person and society. Psychological journal. 2023. 9(5). 38-51. URL: <https://apsijournal.com/index.php/psyjournal/article/view/1573>
4. Колтунович Т.А., Чуйко Г.В., Чаплак Я.В.

						<p>Соціальнопсихологічні і експерименти : навч. посібник. Чернівці : Чернівець. нац. ун-т ім. Ю. Федьковича, 2022. 192 с. ISBN: 978-966-423-745-8 URL: https://archer.chnu.edu.ua/xmlui/handle/123456789/6213</p> <p>5. Чуйко Г.В., Чаплак Я.В., Комісарик М.І. Особливості проблеми слухання в психології. Наукові перспективи. 2022. 5(23). С.564-579. URL: http://perspectives.pp.ua/index.php/np/issue/view/59/85</p> <p>6. Chuyko H., Chaplak Y., Komisaryk M. Peculiarities of manifestations of communicative tolerance of students in the conditions of quarantine insulation. Psychological journal. 2022. 8(3). 27-45. URL: https://apsijournal.com/index.php/psyjournal/issue/view/57</p> <p>7. Чуйко Г.В., Чаплак Я.В., Комісарик М.І. Психологічна безпека особистості в нестабільному світі. Психологічний часопис. Т.7. № 1(45). 2021. С.65-81. URL: https://www.apsijournal.com/index.php/psyjournal/article/view/1155/718</p> <p>Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПН, що засвідчується виконанням підпунктів 1, 3, 4, 12, 19 п. 38 чинних Ліцензійних умов «Досягнення у професійній діяльності»</p>	
375591	Горбулик Володимир Іванович	доцент, Основне місце роботи	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	Диплом спеціаліста, Чернівецький ордену Трудового Червоного Прапора державний університет, рік закінчення: 1982, спеціальність: фізика, Диплом магістра, Національний технічний	14	Вибрані розділи фізики	<p>Чернівецький ордену Трудового Червоного Прапора державний університет імені Юрія Федьковича, 1982 р., фізика, викладач фізики (диплом ЖВ-І 0915 4 7, виданий 12.06.1982 р.).</p> <p>Стажування та підвищення кваліфікації:</p> <p>Тернопільський національний</p>

університет
"Харківський
політехнічний
інститут", рік
закінчення:
2019,
спеціальність:
141
Електроенерге
тика,
електротехніка
та
електромехані
ка, Диплом
кандидата наук
ДК 012321,
виданий
14.11.2001,
Атестат
доцента 12ДЦ
043407,
виданий
30.06.2015

технічний університет
імені Івана Пулюя.
Свідоцтво ПК №
05408102/001716-21
від 18.06.2021 р.
Тема: "Наукові основи
та програмно-
апаратні засоби
запровадження
технології
електронного
навчання в освітній
процес з метрології,
телекомунікацій,
електричної інженерії
та поліграфії".

Наявність публікацій,
монографій та
посібників за
профілем навчальної
дисципліни:

1. Contribution of
Fluorescence and
Exciplex Emission into
Efficient White OLED/
Khrystyna Ivaniuk,
Pavlo Stakhira, Igor
Helzhynskyy, Stepan
Kutsiy, Zenon Hotra,
Titas Deksnys, Dmytro
Volyniuk, Juozas Vidas
Grazulevicius,
Volodymyr
Gorbulic//2020 IEEE
15th International
Conference on
Advanced Trends in
Radioelectronics,
Telecommunications
and Computer
Engineering (TCSET).-
2020.- P.821-824.
ISBN: 978-172815566-1
2. S. Kutsiy, Y. Danyliv,
I. Danyliv, M. Hladun,
N. Barylo, P. Stakhira,
A. Fechan, V.
Gorbulik/The
development of non-
doped oled base donor
– acceptor
atetrachloropyridine -
carbazolematerial with
the emission in "deep -
blue " region / In
formation and
communication
technologies, electronic
engineering. Vol. 1, N o.
2, pp. 123–130 (2021)
3. Р. Л. Політанський.
Моделювання
процесів росту на
поверхні кристалів /
Р. Л. Політанський, В.
І. Горбулик, І. Т.
Когут, М. В. Вістак. //
Фізика і хімія твердого
тіла. Т. 23, № 2 (2022)
С. 387-393. DOI:
10.15330/pcss.23.2.387-
393

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».	
56654	Бродецький Олександр Євгенович	доцент, Основне місце роботи	Філологічний факультет	<p>Диплом спеціаліста, Чернівецький національний університет імені Юрія Федьковича, рік закінчення: 2001, спеціальність: 030101 Філософія, Диплом доктора наук ДД 006748, виданий 26.06.2017, Диплом кандидата наук ДК 045813, виданий 09.04.2008, Аттестат доцента 12ДЦ 026189, виданий 20.01.2011</p>	17	Філософія	<p>Доктор філософських наук зі спеціальності 09.00.11 – релігієзнавство. Тема дисертації: "Антропологічно-ціннісні засади гуманістичного потенціалу релігійної етики".</p> <p>Стажування та підвищення кваліфікації:</p> <p>Хмельницький національний університет, кафедра філософії та соціально-гуманітарних наук. Термін підвищення кваліфікації – з 19.05.2022 по 30.06.2022 р. Обсяг стажування – 180 год. (6 ЄКТС). Тема стажування: «Збалансування соціальних та академічних аспектів функціонування гуманітарно-світоглядного знання». Довідка про стажування № 19/22 від 04.07.2022 р. ХНУ.</p> <p>Наявність публікацій, монографій та посібників за профілем навчальної дисципліни:</p> <ol style="list-style-type: none"> 1. Brodestkyi O, Horokholinska I., Lahodych M. Ukraine Orthodoxy Autocephaly: Social and Value Challenges // Occasional Papers on Religion in Eastern Europe: Vol. 40 : Iss. 9 , Article 3. Available at: https://digitalcommons.georgefox.edu/ree/vol40/iss9/3 2. Бродецький О.Є. Смыслові горизонти релігійно-етичних ідей М. Бердяєва та їхня актуальна значущість // Релігія та соціум. Міжнародний часопис. – Чернівці: Чернівецький нац. ун-т, 2019. – №1-2 (33-34). – С.101 -106. 3. Бродецький О.Є.

						<p>Гуманістичні ефекти ціннісної синергії релігійно-етичних ідей: методологічне підґрунтя та прикладні горизонти / О.Є. Бродецький // Українське релігієзнавство. – №89. – 2019. – С. 13-25.</p> <p>4. Бродецький О. Є., Горохолінська І. В. Безпековий ресурс світоглядного знання в освіті: кейс релігієзнавства. Educational Discourse: Collection of Scientific Papers, 2021, Vol 35, Issue 7, p. 7. DOI 10.33930/ed.2019.5007.35(7)-1</p> <p>5. Brodestkyi O., Horokholinska I. The Security Dimensions of Religious Life in Ukraine: A Focus On Orthodoxy in the Cross-Border Chernivtsi Region, Occasional Papers on Religion in Eastern Europe, 2023. – Vol. 43 (6), 5. https://digitalcommons.georgefox.edu/cgi/viewcontent.cgi?article=2440&context=ree</p> <p>Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 1, 3, 4, 7, 12, 14, 15, 19 п. 38 чинних Ліцензійних умов «Досягнення у професійній діяльності».</p>	
80085	Рождественська Маргарита Григорівна	доцент, Основне місце роботи	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	<p>Диплом магістра, Чернівецький державний університет ім. Ю. Федьковича, рік закінчення: 1992, спеціальність: Радіотехніка, Диплом кандидата наук ДК 005488, виданий 12.01.2000, Атестат доцента ДЦ 13126, виданий 15.06.2006</p>	24	Вступ до кібербезпеки	<p>Стажування та підвищення кваліфікації:</p> <p>1. Підвищення кваліфікації в Тернопільському національному технічному університеті (з 5.04.2019 по 14.05.2019) з курсу: «Аналітик кібербезпеки». Свідоцтво СПК 001670 від 14.05.2019 р.</p> <p>2. З 29.01.2020 по 25.06.2020. Програма підвищення кваліфікації з серії науково-метод.</p>

семінарів-практикумів «Алгоритм підготовки до викладання фахових дисциплін англійською мовою» (ЧНУ імені Юрія Федьковича). Сертифікат, наказ №190 від 17.07.2020. 3. З 1.09.2020 по 25.10.2020. Підвищення кваліфікації у Центрі підтримки академії Cisco Нац. технічного університету «Харківський політехнічний інститут» в рамках Програми Академії Cisco (курс «Основи апаратного та програмного забезпечення ПК» та СТЕМ-практика з Інтернету речей та кібербезпеки). Сертифікат від 25.10.2020. 4. З 04.10.2021 до 18.10.2021. ТОВ «Академія цифрового розвитку». Підвищення кваліфікації «Цифрові інструменти Google для закладів вищої, фахової передвищої освіти». Сертифікат №8GW-0106 від 19.10.2021. 5. З 26.07.2023 до 1.09.2023. SoftServe Academy. Навчальний курс TECH SUMMER BOOTCAMP FOR TEACHERS. Сертифікат ZO № 14134/2023 від 1.09.2023.

Наявність публікацій, монографій та посібників за профілем навчальної дисципліни:

1. Приймання прихованих оптичних сигналів видимого діапазону / Браїловський В.В., Іванчук М.М., Пислар І.В., Рождественська М.Г., Пшонник В.О. // Сучасний захист інформації. – 2019. - № 2(38) с. 47-53. <http://journals.dut.edu.ua/index.php/dataprotect/article/view/2316>
2. 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>
3. Патент України на винахід. №120773, МПК (2017.01) G01N 25/00, UA122808. «Спосіб маскування інформаційних світлових імпульсів видимого діапазону і передачі інформації по каналах зв'язку»: Чернівецький національний університет ім. Ю. Федьковича; автори: Браїловський В.В., Пислар І.В., Рождественська М.Г. заяв. 28.02.2017, опуб. 10.02.2020, Бюл. №3 <https://iprop-ua.com/inv/421ztt74/>
4. І.В. Пислар, В.В. Браїловський, М.Г.Рождественська. До питання забезпечення прихованості світлових імпульсів видимого діапазону. II Міжнародна науково-практична конференція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS). - 11-12 квітня 2019 р, Київ. - С.188-190.
5. 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 Міжнародна науково-практична конференція "Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій", 12–14 грудня 2022 р., м. Запоріжжя.- С. 89-91.
URL:

<https://scholar.google.com/scholar?oi=bibs&cluster=18208501513419092697&btnI=1&hl=uk>
6. В. В. Браїловський, Г. І. Ластівка, М. Г. Рождественська. До питання підвищення ефективності підготовки здобувачів вищої освіти інженерно-технічних спеціальностей з базових дисциплін. V Всеукраїнська

						<p>науково-методична конференція «Забезпечення якості вищої освіти», 12-14 квітня 2023 р. м. Одеса.</p> <p>Участь в роботі міжнародних освітніх грантів 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.): - G-202206-68835 «Integration of new Cybersecurity courses into the Curriculum of the Yuriy Fedkovych Chernivtsi National University» https://docs.google.com/document/d/16eXTjjLWlTrbh-MAoDAmOUCql2xkDTVn/edit - G-202301-69802 «Promotion of the Cyber Hygiene E-Learning course at the Yuriy Fedkovych Chernivtsi National University» (1.02.2023-30.06.2023) https://docs.google.com/document/d/1R9nrF94mLZtCozobnFhWU696PCeSHd_/edit.</p> <p>Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 2, 3, 4, 10, 11, 12 п. 38 чинних Ліцензійних умов «Досягнення у професійній діяльності»</p>	
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,	15	Основи комп'ютерних технологій	<p>Стажування та підвищення кваліфікації:</p> <p>1. Стажування в Сучавському університеті «Штефан чел Марє» (Румунія) (міжнародний сертифікат «Certificat De Participare» № 01/14.02.2020 від 14.02.2020 р., тема «Кібербезпека, інформаційні технології, засоби телекомунікацій та</p>

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

радіотехніки та
інструменти і методи
дослідження у
європейських
університетах» (наказ
по університету № 13-
від 14.01.2020)
2. Навчальний курс
INTRODUCTION TO
QUANTUM
INFORMATION на
платформі Coursera
(розробник Korea
Advanced Institute of
Science and
Technology(KAIST)).
Сертифікат від
27.01.2023
(<https://www.coursera.org/account/accomplishments/verify/DUBMHBUZKMYT>)

Наявність публікацій,
монографій 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, Pomiar w Gospodarce i Ochronie Środowiska. 2020, 10(1), pp. 62-65
DOI:
<https://doi.org/10.35784/iargos.915>.
2. A. Veryga, R. Politanskyi. Time interval switching device / IARGOS / 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/iargos.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 .
4. Kushnir M., Vovchuk D., Haliuk S., Ivaniuk P., Politanskyi R. (2021) Approaches to Building a Chaotic Communication

						<p>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.</p> <p>5. Поліганський Р. Л. Детектори електромагнітного поля на основі пристроїв спінтроники / Р. Л. Поліганський, П. М. Шпатар, М. В. Вісьтак, І. Т. Когут, І. С. Дісковський, Ю. А. Рудяк // Фізика і хімія твердого тіла. - 2023. - Т. 24. - № 3. - С. 433-440.</p> <p>6. R Politanskyi, A Samila, L Politanskyi, V Vlasenko. Investigation of High-Speed Methods for Determining the Equilibrium State of a Network Based on the Principle of Maximum Entropy / IEEE International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, 2022. https://link.springer.com/chapter/10.1007/978-3-031-24963-1_35</p> <p>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»</p>	
60708	Кушнір Микола Ярославович	доцент, Основне місце роботи	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	Диплом спеціаліста, Чернівецький орден Трудового Червоного Прапора державний університет, рік закінчення: 1978, спеціальність: Фізика, Диплом кандидата наук ФМ 026676, виданий 25.06.1986, Аттестат	36	Комп'ютерна дискретна математика	<p>Стажування та підвищення кваліфікації:</p> <p>Стажування в Тернопільському національному технічному університеті 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»</p>

доцента 02ДЦ
000432,
виданий
24.12.2003

електронного навчання в освітній процес з метрології, телекомунікацій, електричної інженерії та поліграфії».

Наявність публікацій, монографій та посібників за профілем навчальної дисципліни:

1. Kushnir, M., Semenko, A., Kosovan, G., Bokla, N., & Shestopal, Y. (2019). Increasing the Cryptosecurity of Telecom. Systems with Spread Spectrum by Using Pseudorandom Sequences Based on Two Ergodic Chaotic Signals. In 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019 - Proceedings (pp. 455–458). Institute of Electrical and Electronics Engineers Inc.

<https://doi.org/10.1109/AIACT.2019.8847913> (Scopus)

2. 2. Кушнір М.Я. Оцінка ефективності застосування генератора ПВП на основі двох хаотичних систем для шифрування інформації / Кушнір М.Я., Косован Г.В., Крояло П.М. // II Міжнародна наук.-практична конф. "Проблеми кібербезпеки інформ.-телеком. систем". PCSITS'2019. 11-12 квітня 2019. Київ, Україна. С. 202 – 206.

https://drive.google.com/open?id=1uW6Ft3kaojjhZfZrwpP9aEAm4Z_YLlF

3. Кушнір М. Я. Дослідження властивостей хаотичних генераторів псевдовипадкових послідовностей, побудованих із використанням нечіткої логіки / Кушнір М. Я. Семенко А. І., Косован Г. В., Крояло П.М. // Науковий журнал Вісник Університету «Україна» Серія Інфокомунікаційні та комп'ютерні технології. № 1 (01) 2021. Київ. Україна. С 63-72.

4. 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
<https://www.scopus.com/record/display.uri?eid=2-s2.0-85146827813&origin=resultslist&sort=plf-f>

5. Kushnir, M., and K. Tokarieva. "A Generalization of the Arima Model to the Nonlinear and Continuous Cases." //Cybernetics and Systems Analysis, 2023. Vol. 59, pp. 900-909. <https://link.springer.com/article/10.1007/s10559-023-00625-8>

Член редколегії
вісника університету
«Україна», Серія
ІНФОКОМУНІКАЦІЙ
І ТА КОМП'ЮТЕРНІ
ТЕХНОЛОГІЇ
(Категорія Б)

Керівництво
дисертації на здобуття
наукового ступеня
кандидата технічних
наук за спеціальністю
05.13.21 – системи
захисту інформації
(Косован Г.В.)

Керівник двох
міжнародних освітніх
грантів 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.):
- G-202206-68835
«Integration of new
Cybersecurity courses
into the Curriculum of
the Yuriy Fedkovych
Chernivtsi National
University»
<https://docs.google.com/document/d/16eXTjjLWlTrbhMAoDAmOUCql2xkDTVn/edit>
- G-202301-69802

						<p>«Promotion of the Cyber Hygiene E-Learning course at the Yuriy Fedkovych Chernivtsi National University» (1.02.2023-30.06.2023) https://docs.google.com/document/d/1R9nrF94mLZtCozob-nFhWU696PCeSHd_/edit</p> <p>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»</p>
149490	Лесінський Валентин Вікторович	доцент, Основне місце роботи	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	<p>Диплом бакалавра, Чернівецький національний університет імені Юрія Федьковича, рік закінчення: 2008, спеціальність: 0502 Менеджмент, Диплом магістра, Чернівецький національний університет імені Юрія Федьковича, рік закінчення: 2004, спеціальність: 090701 Радіотехніка, Диплом кандидата наук ДК 011681, виданий 25.01.2013, Атестат доцента АД 005427, виданий 24.09.2020</p>	18	<p>Основи інфокомунікацій</p> <p>Стажування та підвищення кваліфікації:</p> <p>04-28.11.2019 р. Сучавський університет імені Штефана чел Маре, м. Сучава, Румунія, тема: «Система викладання предметів у галузі комп'ютерних наук, засобів телекомунікації та електронної техніки; дослідницька робота у європейських університетах», (Наказ № 739 від 4.11.2019 р.), міжнародний сертифікат № 35/29.11.2019</p> <p>11-21.02.20. Харківський національний університет радіоелектроніки. Теми: Оцінювання захищеності інформації, Свідоцтво: 001132 (19.02.2020); Виявлення закладних пристроїв;», Свідоцтво: 001138 (21.02.2020)</p> <p>Наявність публікацій, монографій та посібників за профілем навчальної дисципліни:</p> <p>1. Системи захисту інформації / С. В. Толюпа, С. С. Бучик, О. А. Лаптев, В. В. Лесінський. К. : Міленіум. 2022. - 390 с. 2. Lesinskiy V. Devising</p>

a toolset for assessing the potential of loan financing of projects aimed at implementing energy-saving technologies /O.Yemelyanov, O.Zarytska, A.Symak, T.Petrushka// Eastern-European Journal of Enterprise Technologiethis, Vol. 4 No. 13(112) (2021) p. 15–33: Transfer of technologies: industry, energy, nanotechnology, Режим доступу: <http://journals.uran.ua/eejet/article/view/238795/237878>, DOI: 10.15587/1729-4061.2021.238795, Scopus, ISSN: 1729-3774

3. Lesynskyi V. Development of a toolkit for assessing and overcoming barriers to the implementation of energy saving projects / O.Yemelyanov, O.Zarytska, A.Symak, T.Petrushka // Eastern-European Journal of Enterprise Technologiethis, Vol. 4 No. 3(107) (2020) p. 24–38, Режим доступу: <http://journals.uran.ua/eejet/article/view/214997>, DOI: 10.15587/1729-4061.2020.214997, Scopus, ISSN: 1729-3774

4. Lesynskyi, V., Yemelyanov, O., Zarytska, O., Petrushka, T., Myroshchenko, N. DESIGNING A TOOLSET FOR ASSESSING THE ORGANIZATIONAL AND TECHNOLOGICAL INERTIA OF ENERGY CONSUMPTION PROCESSES AT ENTERPRISES. Eastern-European Journal of Enterprise Technologieshis link is disabled, 2022, 6(13-120), pp. 29–40

Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 1, 3, 4, 7, 10 п. 38 чинних Ліцензійних умов «Досягнення у

							професійній діяльності».
65803	Руснак Олександр Валерійович	асистент, Основне місце роботи	Факультет історії, політології та міжнародних відносин	Диплом магістра, Чернівецький національний університет імені Юрія Федьковича, рік закінчення: 2007, спеціальність: 030301 Історія, Диплом кандидата наук ДК 066984, виданий 23.02.2011	15	Актуальні питання історії і культури України	<p>Кандидат історичних наук, спеціальність 07.00.01 - Історія України, тема дисертації "Соціально-економічний розвиток Північної Буковини і Хотинщини у 1918-1940 рр.".</p> <p>Стажування та підвищення кваліфікації:</p> <p>Кам'янець-Подільський національний університет імені Івана Огієнка з 25.11.2020 р. по 11.01.2021 р.</p> <p>Наявність публікацій, монографій та посібників за профілем навчальної дисципліни:</p> <ol style="list-style-type: none"> 1. Ботушанський В.М., Добржанський О.В., Руснак О.В. Чернівецький національний університет імені Юрія Федьковича – 145: колективна монографія / гол. ред. Р. Петришин. – Чернівці: Чернівецький нац. ун-т ім. Ю. Федьковича, 2020. – 392 с. 2. Rusnak O. The 2014 Annexation of Crimea – An Example of Disintegration of the State's Territories // Disintegration and Integration in East-Central Europe: the current relevance of regional cooperation / ed.: Nicolae Păun. – Cluj-Napoca: Presa Universitară Clujeană, 2020. – P. 43-75. 3. Rusnak O. The Place of Crimea in the Neo-Emperor Policy of Russia (1991–2020) // History Journal of Yuriy Fedkovych Chernivtsi National University. – No 1. – 2020. – pp. 48-58. 4. Rusnak O. The State of the Banking System of Northern Bukovyna and Khotyn Region in the Interwar Period // History Journal of Yuriy Fedkovych Chernivtsi National University. – No 2. – 2020. – pp. 107-117. 5. Rusnak O. Main tendencies of healthcare system development of

Northern Bukovyna and Khotyn region during the interwar period // History Journal of Yuriy Fedkovych Chernivtsi National University. – No 1. – 2021. – pp. 77-89.
6. Rusnak o., ilkiv m., kalinichenko v. Seals of the khotyn county in the interwar period. Historical and sphragistic analysis //codrul cosminului. – 2023. – V. 29. – №. 1. – pp. 7-29.

Конференції:

1. Per aspera ad astra: до 100-літнього ювілею відомого археолога Бориса Тимощука. Міжнародна наукова конференція (м. Чернівці, 8 квітня 2019 р.)
2. XII Буковинська міжнародна історико-краєзнавча конференція, присвячена 185-й річниці від дня народження Юрія Федьковича та 160-й річниці від дня народження Степана Смаль-Стоцького (м. Чернівці, 1 – 2 листопада 2019 р.)
3. Археологічні дослідження – складова охорони культурної спадщини (до 100-річчя від дня народження Б.О. Тимощука). XVI науково-практична конференція (м. Хотин, 27 вересня 2019 р.)
4. Археологія Буковини: здобутки та перспективи. III міжнародний науковий семінар, присвячений 100-літтю від дня народження відомого науковця Бориса Тимощука (м. Чернівці, 13 грудня 2019 р.)
5. The International Scientific Conference «From Intermarium to Three Seas Initiative. Integration and Collective Security Conceptions in Central and Eastern Europe in the 20th and 21st Centuries» under the Patronage of the Chief of National Security Bureau of the Republic of Poland, Minister Paweł Soloch (Ostrowiec Świętokrzyski, Poland,

						<p>October 16-18, 2019) 6. Special Edition of the «Disintegration and Integration in East-Central Europe» International Conference (DIECE) «The current relevance of regional cooperation» (Cluj-Napoca, Romania, November 28-29, 2019) 7. Хотинська фортеця у літописах (до 350-річчя від дня народження Самійла Величка). XVII науково-практична конференція (м. Хотин, 15 жовтня 2020 р.) 8. Археологія Буковини: здобутки та перспективи. IV міжнародний науковий семінар (м. Чернівці, 11 грудня 2020 р.) 9. XIII Буковинська міжнародна історико-краєзнавча конференція, присвячена 400-річчю Хотинської війни (м. Чернівці, 22 – 23 жовтня 2021 р.)</p> <p>Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОПП, що засвідчується виконанням підпунктів 1, 3, 4, 12, 15, 19 п. 38 чинних Ліцензійних умов «Досягнення у професійній діяльності»</p>	
86449	Політанський Руслан Леонідович	професор, Основне місце роботи	Навчально-науковий інститут фізико-технічних та комп'ютерних наук	<p>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</p>	15	Теорія інформації та кодування	<p>Стажування та підвищення кваліфікації:</p> <p>1. Стажування в Сучавському університеті «Штефан чел Марє» (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 14.01.2020) 2. Навчальний курс INTRODUCTION TO</p>

29.03.2012,
Атестат
професора АП
002287,
виданий
02.11.2020

QUANTUM
INFORMATION на
платформі Coursera
(розробник Korea
Advanced Institute of
Science and
Technology(KAIST)).
Сертифікат від
27.01.2023
(<https://www.coursera.org/account/accomplishments/verify/DUBMHBUZKMYT>)

Наявність публікацій,
монографій та
посібників за
профілем навчальної
дисципліни:

1. Політанський, Р. Л., Качур, В. В. Дослідження ентропії двійкових послідовностей фрагментованих на підпослідовності сталої довжини. 2022. Vol. 2. No 1. P. 96-101. <https://science.lpnu.ua/uk/ict/vsi-vypusky/volume-2-issue-1-2022/doslidzhennya-entropiyi-dviykovyh-poslidovnostey>
2. Politanskyi R. L., Bobalo Y. Y., Zarytska O. L., Kiselychnyk M. D., Vistak M. V. Entropy calculation for networks with determined values of flows in nodes. Mathematical Modeling and Computing. 2022. Vol 9. No 4. P. 936-944. <https://www.scopus.com/record/display.uri?eid=2-s2.0-85142361440&origin=reultslist&sort=plf-f>
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 .
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.

						<p>Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer. DOI: 10.1007/978-3-030-43070-2_11. 5. Politanskyi, R.L., Zarytska, O.L., Vistak, M.V., Vlasenko, V.V. Research of distribution of information flows in a network. Mathematical Modeling and Computing. 2021. Vol. 8. No 4. P. 821–829. https://www.scopus.com/record/display.uri?eid=2-s2.0-85121706153&origin=resultslist&sort=plf-f.</p> <p>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»</p>
--	--	--	--	--	--	--

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

Програмні результати навчання ОП	ПРН відповідає результату навчання, визначено му стандартом вищої освіти (або охоплює його)	Обов'язкові освітні компоненти, що забезпечують ПРН	Методи навчання	Форми та методи оцінювання
<i>ПРН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.</i>	☒	Безпека інформаційно-телекомунікаційних систем	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	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.

			лабораторних робіт.	
		Основи побудови систем комплексного захисту інформації	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; комп'ютерні засоби навчання (ресурси: дистанційні, web-конференції; інструменти: програмні виконання завдань розрахункового характеру та моделювання); самостійна робота: підготовка презентацій, рефератів; робота з навчально-методичною, науковою, нормативною літературою.	Поточний контроль: усні та письмові (контрольна робота, тестування) відповіді студента. Підсумковий контроль: залік (усне, письмове опитування, тестовий контроль).
		Управління інформаційною безпекою	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
<i>ПРН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.</i>	☒	Міждисциплінарна курсова 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 вебіари тощо); самостійна робота над індивідуальним завданням.	Курсова робота: захист.
		Безпека інформаційно-телекомунікаційних систем	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 завдань практичного характеру) відповіді здобувача освіти. Підсумковий контроль (екзамен) – усне або письмове опитування, тестовий контроль.

		Канали витоку інформації	Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.
		Безпека розробки та підтримки додатків	Лекції: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод, метод проблемного викладу.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – екзамен: письмове опитування, тестування.
		Програмне забезпечення об'єктів кіберпростору (в тому числі курсова робота)	Лекції: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод; виконання курсової роботи: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – залік/екзамен: письмове опитування, тестування. Курсова робота: захист.
		Основи побудови систем комплексного захисту інформації	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; комп'ютерні засоби навчання (ресурси: дистанційні, web-конференції; інструменти: програмні виконання завдань розрахункового характеру та моделювання); самостійна робота: підготовка презентацій, рефератів; робота з навчально-методичною, науковою, нормативною літературою.	Поточний контроль: усні та письмові (контрольна робота, тестування) відповіді студента. Підсумковий контроль: залік (усне, письмове опитування, тестовий контроль).
ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-	<input checked="" type="checkbox"/>	Основи інфокомунікацій	Лекції, практичні заняття: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод,	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – залік/екзамен: письмове опитування, тестування.

<p>телекомунікаційних систем.</p>		<p>інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод.</p>	
	<p>Канали витоку інформації</p>	<p>Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.</p>	<p>Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.</p>
	<p>Випускна кваліфікаційна робота/проект</p>	<p>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 індивідуальною темою.</p>	<p>Кваліфікаційна (дипломна) робота – захист.</p>
	<p>Міждисциплінарна курсова робота</p>	<p>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.</p>	<p>Курсова робота: захист.</p>
	<p>Безпека інформаційно-телекомунікаційних систем</p>	<p>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.</p>	<p>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.</p>
	<p>Криптографія (в тому</p>	<p>Лекції та практичні заняття:</p>	<p>Поточний контроль – усне,</p>

		числі курсова робота)	інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод; виконання курсової роботи: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу.	фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – залік/екзамен: письмове опитування, тестування. Курсова робота: захист.
		Взаємодія між компонентами систем IoT	Лекції – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод, дослідницький метод.	Формами поточного контролю є усна чи письмова (тестування, реферат, лабораторна робота) відповідь студента та ін. Формами підсумкового контролю є залік, усне опитування або комплексне тестування.
		Теорія інформації та кодування	Лекції, практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, метод проблемного викладу, робота з навчально-методичною, нормативною літературою; самостійна робота студентів: використання учбових матеріалів на основі курсів пропонує компанією Coursera за підтримки компанії Ukraine Response.	Поточний контроль – усне опитування; письмові контрольні роботи із практичними задачами; тестування. Підсумковий контроль – іспит: проведення письмового іспиту із використанням екзаменаційних білетів із практичними задачами та теоретичними питаннями; тестування.
<p><i>ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.</i></p>	<input checked="" type="checkbox"/>	Міждисциплінарна курсова 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.	Курсова робота: захист.
		Безпека інформаційно-телекомунікаційних систем	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	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.

			метод; самостійна робота: підготовка презентацій, рефератів, а також формуванням напрацювань для виконання і захисту лабораторних робіт.	
		Управління інформаційною безпекою	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
		Основи комп'ютерних технологій	Лекції, практичні та лабораторні заняття – пояснювально-ілюстративний та репродуктивний методи. Словесні методи (співбесіда, консультація, дискусія); наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Поточний контроль: тести, опитування, контрольні, самостійні роботи за індивідуальними завданнями; звіти, презентації результатів виконання завдань практичного характеру; оцінювання завдань, що виконувались в лабораторіях, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – екзамен: усне або письмове опитування, тестування.
		Канали витоку інформації	Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.
ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.	<input checked="" type="checkbox"/>	Методи і засоби проведення спеціальних вимірювань в ІТС	Методи навчання: словесні методи (лекція, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.

			завданням або за програмою навчальної дисципліни.	
<p><i>ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.</i></p>	<input checked="" type="checkbox"/>	<p>Архітектура і моделі безпеки</p>	<p>Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.</p>	<p>Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.</p>
		<p>Управління інформаційною безпекою</p>	<p>Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.</p>	<p>Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.</p>
<p><i>ПРН 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і/або кібербезпеки.</i></p>	<input checked="" type="checkbox"/>	<p>Архітектура і моделі безпеки</p>	<p>Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.</p>	<p>Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.</p>
		<p>Управління інформаційною безпекою</p>	<p>Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за</p>	<p>Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.</p>

			програмою навчальної дисципліни.	
		Технічні системи охорони об'єктів	Лекції: пояснювально-ілюстративний метод, презентації; робота з книгою: з навчально-методичною, науковою та нормативною літературою; 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) відповіді здобувача освіти. Підсумковий контроль (екзамен) – усне або письмове опитування, тестовий контроль.
		Безпека інформаційно-телекомунікаційних систем	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.
		Основи побудови систем комплексного захисту інформації	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; комп'ютерні засоби навчання (ресурси: дистанційні, web-конференції; інструменти: програмні виконання завдань розрахункового характеру та моделювання); самостійна робота: підготовка презентацій, рефератів; робота з навчально-методичною, науковою, нормативною літературою.	Поточний контроль: усні та письмові (контрольна робота, тестування) відповіді студента. Підсумковий контроль: залік (усне, письмове опитування, тестовий контроль).
ПРН 36. Виявляти небезпечні сигнали технічних засобів.	☒	Міждисциплінарна курсова 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 вебіари тощо); самостійна робота над індивідуальним завданням.	Курсова робота: захист.

		Канали витоку інформації	Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.
		Методи і засоби проведення спеціальних вимірювань в ІТС	Методи навчання: словесні методи (лекція, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування. контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
<i>ПРН 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментальною контролю процесів захисту інформації та визначити ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.</i>	☒	Міждисциплінарна курсова 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.	Курсова робота: захист.
		Канали витоку інформації	Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.
		Методи і засоби проведення спеціальних вимірювань в ІТС	Методи навчання: словесні методи (лекція, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо);	Формами поточного контролю є усні і письмові, опитування. контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що

			робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
<p><i>ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.</i></p>	<input checked="" type="checkbox"/>	Міждисциплінарна курсова 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 вебіари тощо); самостійна робота над індивідуальним завданням.	Курсова робота: захист.
		Канали витоку інформації	Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.
		Методи і засоби проведення спеціальних вимірювань в ІТС	Методи навчання: словесні методи (лекція, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
<p><i>ПРН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму</i></p>	<input checked="" type="checkbox"/>	Методи і засоби проведення спеціальних вимірювань в ІТС	Методи навчання: словесні методи (лекція, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання;

секретності із фіксуванням результатів у відповідних документах.			літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки.	☒	Методи і засоби проведення спеціальних вимірювань в ІТС	Методи навчання: словесні методи (лекція, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
		Вступ до кібербезпеки	Лекції, практичні заняття – пояснювально-ілюстративний метод, презентації; метод проблемного викладу, доповідь та захист підготовлених презентацій; самостійна робота – репродуктивний метод.	Поточний контроль – усне та письмове опитування (тестування, захист виконаних завдань для самостійної роботи). Підсумковий контроль – залік: усне або письмове опитування.
		Виробничо-технологічна 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 виробничо-технологічної практики на кафедрі.
		Ознайомча 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 практики на випусковій кафедрі.
		Безпека інформаційно-телекомунікаційних систем	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,	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.

			рефератів, а також формуванням напрацювань для виконання і захисту лабораторних робіт.	
		Основи побудови систем комплексного захисту інформації	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; комп'ютерні засоби навчання (ресурси: дистанційні, web-конференції; інструменти: програмні виконання завдань розрахункового характеру та моделювання); самостійна робота: підготовка презентацій, рефератів; робота з навчально-методичною, науковою, нормативною літературою.	Поточний контроль: усні та письмові (контрольна робота, тестування) відповіді студента. Підсумковий контроль: залік (усне, письмове опитування, тестовий контроль).
		Управління інформаційною безпекою	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
		Безпека розробки та підтримки додатків	Лекції: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод, метод проблемного викладу.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – екзамен: письмове опитування, тестування.
ПРН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.	☒	Виробничо-технологічна 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 виробничо-технологічної практики на кафедрі.
		Ознайомча 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 практики на випусковій кафедрі.

		<p>Управління інформаційною безпекою</p>	<p>Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.</p>	<p>Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.</p>
		<p>Вступ до кібербезпеки</p>	<p>Лекції, практичні заняття – пояснювально-ілюстративний метод, презентації; метод проблемного викладу, доповідь та захист підготовлених презентацій; самостійна робота – репродуктивний метод.</p>	<p>Поточний контроль – усне та письмове опитування (тестування, захист виконаних завдань для самостійної роботи). Підсумковий контроль – залік: усне або письмове опитування.</p>
<p><i>ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.</i></p>	<p>☒</p>	<p>Безпека інформаційно-телекомунікаційних систем</p>	<p>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.</p>	<p>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.</p>
		<p>Управління інформаційною безпекою</p>	<p>Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.</p>	<p>Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.</p>
		<p>Програмне забезпечення об'єктів кіберпростору (в тому числі курсова робота)</p>	<p>Лекції: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод;</p>	<p>Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – залік/екзамен: письмове опитування, тестування. Курсова робота: захист.</p>

			виконання курсової роботи: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу.	
<p><i>ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.</i></p>	<input checked="" type="checkbox"/>	<p>Безпека інформаційно-телекомунікаційних систем</p>	<p>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.</p>	<p>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.</p>
		<p>Законодавчі питання інформаційної безпеки</p>	<p>Словесні методи (лекції, 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 вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни (реферат, доповідь тощо).</p>	<p>Поточний контроль – усні та письмові (тестування, захист завдань практичного характеру) відповіді здобувача освіти. Підсумковий контроль (залік) – усне, письмове опитування, тестовий контроль.</p>
		<p>Управління інформаційною безпекою</p>	<p>Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.</p>	<p>Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.</p>
<p><i>ПРН 44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною</i></p>	<input checked="" type="checkbox"/>	<p>Управління інформаційною безпекою</p>	<p>Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари</p>	<p>Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове</p>

безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.			тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	опитування, тести.
ПРН 45. Застосовувати рині класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.	☒	Управління інформаційною безпекою	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
ПРН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.	☒	Міждисциплінарна курсова 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 вебіари тощо); самостійна робота над індивідуальним завданням.	Курсова робота: захист.
		Безпека інформаційно-телекомунікаційних систем	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.
		Управління інформаційною безпекою	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
		Основи комп'ютерних	Лекції, практичні та	Поточний контроль: тести,

		технологій	лабораторні заняття – пояснювально-ілюстративний та репродуктивний методи. Словесні методи (співбесіда, консультація, дискусія); наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	опитування, контрольні, самостійні роботи за індивідуальними завданнями; звіти, презентації результатів виконання завдань практичного характеру; оцінювання завдань, що виконувались в лабораторіях, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – екзамен: усне або письмове опитування, тестування.
		Канали витоку інформації	Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.
<p><i>ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.</i></p>	<input checked="" type="checkbox"/>	Безпека інформаційно-телекомунікаційних систем	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.
		Криптографія (в тому числі курсова робота)	Лекції та практичні заняття: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод; виконання курсової роботи: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – залік/екзамен: письмове опитування, тестування. Курсова робота: захист.
<p><i>ПРН 48. Виконувати</i></p>	<input checked="" type="checkbox"/>	Безпека інформаційно-	Лекції: пояснювально-ілюстративний метод,	Поточний контроль – усні та письмові (тестування, захист

<p><i>впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.</i></p>		<p>телекомунікаційних систем</p>	<p>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.</p>	<p>лабораторних робіт, захист завдань практичного характеру) відповіді здобувача освіти. Підсумковий контроль (екзамен) – усне або письмове опитування, тестовий контроль.</p>
		<p>Криптографія (в тому числі курсова робота)</p>	<p>Лекції та практичні заняття: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод; виконання курсової роботи: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу.</p>	<p>Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – залік/екзамен: письмове опитування, тестування. Курсова робота: захист.</p>
<p><i>ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.</i></p>	<p>☒</p>	<p>Канали витоку інформації</p>	<p>Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.</p>	<p>Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.</p>
		<p>Управління інформаційною безпекою</p>	<p>Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.</p>	<p>Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.</p>
		<p>Міждисциплінарна курсова робота</p>	<p>Дослідницький метод; словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з навчально-методичною, науковою,</p>	<p>Курсова робота: захист.</p>

			нормативною літературою; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням.	
		Безпека інформаційно-телекомунікаційних систем	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.
<i>ПРН 50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).</i>	<input checked="" type="checkbox"/>	Безпека інформаційно-телекомунікаційних систем	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.
<i>ПРН 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгень в інформаційно-телекомунікаційних системах.</i>	<input checked="" type="checkbox"/>	Безпека інформаційно-телекомунікаційних систем	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.
<i>ПРН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-</i>	<input checked="" type="checkbox"/>	Безпека інформаційно-телекомунікаційних систем	Лекції: пояснювально-ілюстративний метод, презентації; робота з книгою: з навчально-методичною, науковою та нормативною літературою;	Поточний контроль – усні та письмові (тестування, захист лабораторних робіт, захист завдань практичного характеру) відповіді здобувача освіти.

телекомунікаційних системах.			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.
		Основи інфокомунікацій	Лекції, практичні заняття: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – залік/екзамен: письмове опитування, тестування.
ПРН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.	☒	Безпека розробки та підтримки додатків	Лекції: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод, метод проблемного викладу.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – екзамен: письмове опитування, тестування.
		Програмне забезпечення об'єктів кіберпростору (в тому числі курсова робота)	Лекції: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод; виконання курсової роботи: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – залік/екзамен: письмове опитування, тестування. Курсова робота: захист.
		Безпека інформаційно-телекомунікаційних систем	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	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.

<p><i>ПРН 54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.</i></p>	<input checked="" type="checkbox"/>	<p>Філософія</p>	<p>лабораторних робіт.</p> <p>Словесні методи (лекція, семінари, співбесіда, консультація, дискусія); наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з навчально-методичною, науковою, літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні); самостійна робота над індивідуальним завданням та за програмою навчальної дисципліни; інноваційні технології (роботи в малих групах, семінари – дискусії), тощо.</p>	<p>Засоби оцінювання: екзамен, тести, опитування, контрольні, самостійні роботи за індивідуальними завданнями, звіти, реферати, статті; презентації результатів виконання завдань, інші види індивідуальних та групових завдань.</p> <p>Види та форми контролю: усні та письмові відповіді й доповіді студентів; письмові творчі роботи (есе; аналітичні повідомлення, реферати, порівняльні таблиці); проекти дискусійних заходів та їхня організація (в аудиторному або дистанційному форматах); презентації; тестові завдання, термінологічні диктанти тощо.</p>
		<p>Актуальні питання історії і культури України</p>	<p>Лекції: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; семінарські заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод.</p>	<p>Поточний контроль – усне, фронтальне опитування, тестовий контроль. Екзамен – усне, письмове опитування, тести.</p>
		<p>Міжособистісне спілкування і побудова команд</p>	<p>Методи навчання: лекції та практичні заняття (інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод). Самостійна робота: опрацювання матеріалів лекцій та літературних джерел, підготовка презентацій та рефератів за індивідуальним завданням. Інтерактивні методи: робота в малих групах та тренінги.</p>	<p>Поточного контролю: усні та письмові (тестування, захист завдань практичного характеру, ІНДЗ) відповіді здобувача освіти. Підсумковий контроль – залік: письмове опитування, тестування.</p>
<p><i>ПРН 55. Забезпечувати супровід систем захисту інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах, брати участь у розробці нормативної документації та стандартів щодо систем інформаційної та/або кібербезпеки англійською мовою.</i></p>	<input type="checkbox"/>	<p>Ознайомча практика</p>	<p>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.</p>	<p>Підсумковий контроль (залік) – за результатами захисту звіту про виконання програми практики на випусковій кафедрі.</p>
		<p>Основи побудови систем комплексного захисту інформації</p>	<p>Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; комп'ютерні засоби навчання (ресурси: дистанційні, web-конференції; інструменти: програмні виконання завдань розрахункового</p>	<p>Поточний контроль: усні та письмові (контрольна робота, тестування) відповіді студента. Підсумковий контроль: залік (усне, письмове опитування, тестовий контроль).</p>

			характеру та моделювання); самостійна робота: підготовка презентацій, рефератів; робота з навчально-методичною, науковою, нормативною літературою.	
		Законодавчі питання інформаційної безпеки	Словесні методи (лекції, 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 вебіари 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 (залік) – усне, письмове опитування, тестовий контроль.
		Вступ до кібербезпеки	Лекції, практичні заняття – пояснювально-ілюстративний метод, презентації; метод проблемного викладу, доповідь та захист підготовлених презентацій; самостійна робота – репродуктивний метод.	Поточний контроль – усне та письмове опитування (тестування, захист виконаних завдань для самостійної роботи). Підсумковий контроль – залік: усне або письмове опитування.
		Виробничо-технологічна 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 виробничо-технологічної практики на кафедрі.
		Випускна кваліфікаційна робота/проект	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 вебіари тощо); самостійна робота над індивідуальною темою.	Кваліфікаційна (дипломна) робота – захист.
ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.	<input checked="" type="checkbox"/>	Безпека інформаційно-телекомунікаційних систем	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	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.

			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.	
		Управління інформаційною безпекою	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
<p><i>ПРН 27.</i> <i>Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.</i></p>	<input checked="" type="checkbox"/>	Основи побудови систем комплексного захисту інформації	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; комп'ютерні засоби навчання (ресурси: дистанційні, web-конференції; інструменти: програмні виконання завдань розрахункового характеру та моделювання); самостійна робота: підготовка презентацій, рефератів; робота з навчально-методичною, науковою, нормативною літературою.	Поточний контроль: усні та письмові (контрольна робота, тестування) відповіді студента. Підсумковий контроль: залік (усне, письмове опитування, тестовий контроль).
		Криптографія (в тому числі курсова робота)	Лекції та практичні заняття: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод; виконання курсової роботи: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – залік/екзамен: письмове опитування, тестування. Курсова робота: захист.
		Взаємодія між компонентами систем IoT	Лекції – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод,	Формами поточного контролю є усна чи письмова (тестування, реферат, лабораторна робота) відповідь студента та ін. Формами підсумкового контролю є залік, усне опитування або комплексне тестування.

	метод проблемного викладу; самостійна робота – репродуктивний метод, дослідницький метод.	
Канали витоку інформації	Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.
Архітектура і моделі безпеки	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
Теорія інформації та кодування	Лекції, практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, метод проблемного викладу, робота з навчально-методичною, нормативною літературою; самостійна робота студентів: використання учбових матеріалів на основі курсів пропонує компанією Coursera за підтримки компанії Ukraine Response.	Поточний контроль – усне опитування; письмові контрольні роботи із практичними задачами; тестування. Підсумковий контроль – іспит: проведення письмового іспиту із використанням екзаменаційних білетів із практичними задачами та теоретичними питаннями; тестування.
Основи комп'ютерних технологій	Лекції, практичні та лабораторні заняття – пояснювально-ілюстративний та репродуктивний методи. Словесні методи (співбесіда, консультація, дискусія); наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Поточний контроль: тести, опитування, контрольні, самостійні роботи за індивідуальними завданнями; звіти, презентації результатів виконання завдань практичного характеру; оцінювання завдань, що виконувались в лабораторіях, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – екзамен: усне або письмове опитування, тестування.

		<p>Безпека інформаційно-телекомунікаційних систем</p>	<p>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.</p>	<p>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.</p>
		<p>Міждисциплінарна курсова робота</p>	<p>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.</p>	<p>Курсова робота: захист.</p>
<p><i>ПРН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).</i></p>	<input checked="" type="checkbox"/>	<p>Технічні системи охорони об'єктів</p>	<p>Лекції: пояснювально-ілюстративний метод, презентації; робота з книгою: з навчально-методичною, науковою та нормативною літературою; лабораторні заняття: метод проблемного підходу, дослідницький метод; самостійна робота: підготовка презентацій, рефератів, а також формуванням напрацювань для виконання і захисту лабораторних робіт.</p>	<p>Поточний контроль – усні та письмові (тестування, захист лабораторних робіт) відповіді здобувача освіти. Підсумковий контроль (екзамен) – усне або письмове опитування, тестовий контроль.</p>
		<p>Безпека інформаційно-телекомунікаційних систем</p>	<p>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.</p>	<p>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.</p>
		<p>Архітектура і моделі безпеки</p>	<p>Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія,</p>	<p>Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за</p>

			тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
<p><i>ПРН 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.</i></p>	<input checked="" type="checkbox"/>	Технічні системи охорони об'єктів	Лекції: пояснювально-ілюстративний метод, презентації; робота з книгою: з навчально-методичною, науковою та нормативною літературою; 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) відповіді здобувача освіти. Підсумковий контроль (екзамен) – усне або письмове опитування, тестовий контроль.
		Безпека інформаційно-телекомунікаційних систем	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.
		Взаємодія між компонентами систем IoT	Лекції – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод, дослідницький метод.	Формами поточного контролю є усна чи письмова (тестування, реферат, лабораторна робота) відповідь студента та ін. Формами підсумкового контролю є залік, усне опитування або комплексне тестування.
		Управління інформаційною безпекою	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види

			засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
<p><i>ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.</i></p>	☒	Ознайомча 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 практики на випусковій кафедрі.
		Міждисциплінарна курсова 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 вебіари тощо); самостійна робота над індивідуальним завданням.	Курсова робота: захист.
		Безпека інформаційно-телекомунікаційних систем	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.
		Управління інформаційною безпекою	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
		Канали витоку інформації	Лекції та практичні заняття – інформаційно-рецептивний метод,	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий

			репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.
		Вступ до кібербезпеки	Лекції, практичні заняття – пояснювально-ілюстративний метод, презентації; метод проблемного викладу, доповідь та захист підготовлених презентацій; самостійна робота – репродуктивний метод.	Поточний контроль – усне та письмове опитування (тестування, захист виконаних завдань для самостійної роботи). Підсумковий контроль – залік: усне або письмове опитування.
		Виробничо-технологічна 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 виробничо-технологічної практики на кафедрі.
ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.	☒	Міждисциплінарна курсова 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.	Курсова робота: захист.
		Безпека інформаційно-телекомунікаційних систем	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.
		Основи побудови систем комплексного захисту інформації	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; практичні заняття: репродуктивний метод, дослідницький метод;	Поточний контроль: усні та письмові (контрольна робота, тестування) відповіді студента. Підсумковий контроль: залік (усне, письмове

	інтерактивні методи навчання: робота в малих групах та тренінги; комп'ютерні засоби навчання (ресурси: дистанційні, web-конференції; інструменти: програмні виконання завдань розрахункового характеру та моделювання); самостійна робота: підготовка презентацій, рефератів; робота з навчально-методичною, науковою, нормативною літературою.	опитування, тестовий контроль).
Канали витоку інформації	Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.
Архітектура і моделі безпеки	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
Інформаційний пошук у кібербезпеці	Лекції, семінарські заняття – пояснювально-ілюстративний метод, презентації; метод проблемного викладу, доповідь та захист підготовлених презентацій; самостійна робота – репродуктивний метод, пов'язаний з опрацюванням матеріалів лекцій та літературних джерел за відповідною тематикою, формуванням напрацювань для підготовки презентацій та доповідей.	Поточний контроль: усні та письмові (тестування) відповіді студента; представлення презентації, доповідь та аргументований захист під час командної роботи. Підсумковий контроль – залік: усне та письмове опитування, тестовий контроль.
Українська мова (за професійним спрямуванням)	Методи навчання: словесний метод (дискусія); практичний метод (практичні заняття, практичні завдання); наочний метод (ілюстрація, демонстрація, презентація);	Поточний контроль – усні та письмові відповіді на практичних заняттях, письмові роботи різних видів (диктанти, редагування текстів, створення фахових текстів),

			робота з навчально-методичною літературою (конспектування, тезування, анотування, рецензування, складання реферату); методи дистанційного навчання; самостійна робота (розв'язання завдань); індивідуальна науково-дослідна робота здобувачів першого рівня освіти.	тестування, творчі роботи, ІНДЗ. Підсумковий контроль – залік: усне та письмове опитування, тестовий контроль.
		Англійська мова професійного спілкування	Комунікативно-діяльнісний підхід, метод комунікативних завдань, система навчання CLLL 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 – виконання практичних завдань, усне, фронтальне опитування, оцінка активності. Підсумковий контроль (залік/іспит) – усне та письмове опитування, тестовий контроль.
		Іноземна мова (за професійним спрямуванням)	Комунікативно-діяльнісний підхід, метод комунікативних завдань, система навчання CLLL 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 – виконання практичних завдань, усне, фронтальне опитування, оцінка активності. Підсумковий контроль (залік/іспит) – усне та письмове опитування, тестовий контроль.
		Управління інформаційною безпекою	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
<i>ПРН 2. Організувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній</i>	☒	Вступ до кібербезпеки	Лекції, практичні заняття – пояснювально-ілюстративний метод, презентації; метод проблемного викладу, доповідь та захист підготовлених презентацій; самостійна робота – репродуктивний метод.	Поточний контроль – усне та письмове опитування (тестування, захист виконаних завдань для самостійної роботи). Підсумковий контроль – залік: усне або письмове опитування.
		Філософія	Словесні методи (лекція, семінари, співбесіда, консультація, дискусія); наочні методи (презентації,	Засоби оцінювання: екзамен, тести, опитування, контрольні, самостійні роботи за індивідуальними

<p>діяльності, оцінювати їхню ефективність.</p>		<p>ілюстрації, відеоматеріали, тощо); робота з навчально-методичною, науковою, літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні); самостійна робота над індивідуальним завданням та за програмою навчальної дисципліни; інноваційні технології (роботи в малих групах, семінари – дискусії), тощо.</p>	<p>завданнями, звіти, реферати, статті; презентації результатів виконання завдань, інші види індивідуальних та групових завдань. Види та форми контролю: усні та письмові відповіді й доповіді студентів; письмові творчі роботи (есе; аналітичні повідомлення, реферати, порівняльні таблиці); проекти дискусійних заходів та їхня організація (в аудиторному або дистанційному форматі); презентації; тестові завдання, термінологічні диктанти тощо.</p>
	<p>Міжособистісне спілкування і побудова команд</p>	<p>Методи навчання: лекції та практичні заняття (інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод). Самостійна робота: опрацювання матеріалів лекцій та літературних джерел, підготовка презентацій та рефератів за індивідуальним завданням. Інтерактивні методи: робота в малих групах та тренінги.</p>	<p>Поточного контролю: усні та письмові (тестування, захист завдань практичного характеру, ІНДЗ) відповіді здобувача освіти. Підсумковий контроль – залік: письмове опитування, тестування.</p>
	<p>Вища математика</p>	<p>Методи навчання: словесний метод (лекція, дискусія); практичний метод (практичні заняття, практичні завдання); робота з навчально-методичною літературою (конспектування, тезування, анотування); методи дистанційного навчання; самостійна робота (розв'язання завдань).</p>	<p>Оцінювання рівня знань студентів з предмету «Вища математика» здійснюється на основі результатів поточного контролю та іспиту. Екзамен – усне, письмове опитування, тести.</p>
	<p>Комп'ютерна дискретна математика</p>	<p>словесний метод (лекція, дискусія); практичний метод (практичні заняття, практичні завдання); робота з навчально-методичною літературою (конспектування, тезування, анотування); методи дистанційного навчання; самостійна робота (опрацювання матеріалів лекцій та літературних джерел за відповідною тематикою, підготовка презентацій, рефератів); інтерактивні методи навчання (робота в малих групах та тренінги).</p>	<p>Поточний контроль – опитування під час занять; контрольні роботи; стандартизовані тести; реферати; презентації результатів виконаних практичних завдань. Підсумковий контроль (залік/іспит) – усне та письмове опитування, тестовий контроль.</p>
	<p>Комп'ютерна електроніка</p>	<p>Лекції, практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу;</p>	<p>Поточний контроль – усне та фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – екзамен: усне або письмове опитування.</p>

	самостійна робота – репродуктивний метод, дослідницький метод.	
Теорія інформації та кодування	Лекції, практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, метод проблемного викладу, робота з навчально-методичною, нормативною літературою; самостійна робота студентів: використання учбових матеріалів на основі курсів пропонувані компанією Coursera за підтримки компанії Ukraine Response.	Поточний контроль – усне опитування; письмові контрольні роботи із практичними задачами; тестування. Підсумковий контроль – іспит: проведення письмового іспиту із використанням екзаменаційних білетів із практичними задачами та теоретичними питаннями; тестування.
Методи і засоби проведення спеціальних вимірювань в ІТС	Методи навчання: словесні методи (лекція, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
Випускна кваліфікаційна робота/проект	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 вебіари тощо); самостійна робота над індивідуальною темою.	Кваліфікаційна (дипломна) робота – захист.
Виробничо-технологічна 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 виробничо-технологічної практики на кафедрі.
Ознайомча 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 практики на випусковій кафедрі.
Міждисциплінарна курсова робота	Дослідницький метод; словесні методи (розповідь, бесіда, консультація,	Курсова робота: захист.

	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.	
Безпека інформаційно-телекомунікаційних систем	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.	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.
Основи побудови систем комплексного захисту інформації	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; комп'ютерні засоби навчання (ресурси: дистанційні, web-конференції; інструменти: програмні виконання завдань розрахункового характеру та моделювання); самостійна робота: підготовка презентацій, рефератів; робота з навчально-методичною, науковою, нормативною літературою.	Поточний контроль: усні та письмові (контрольна робота, тестування) відповіді студента. Підсумковий контроль: залік (усне, письмове опитування, тестовий контроль).
Управління інформаційною безпекою	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебінари	Формами поточного контролю є усні і письмові, опитування. контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове

			тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	опитування, тести.
		Канали витоку інформації	Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.
		Архітектура і моделі безпеки	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.	☒	Випускна кваліфікаційна робота/проект	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 індивідуальною темою.	Кваліфікаційна (дипломна) робота – захист.
		Виробничо-технологічна 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 виробничо-технологічної практики на кафедрі.
		Міждисциплінарна курсова робота	Дослідницький метод; словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з навчально-	Курсова робота: захист.

	методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням.	
Безпека інформаційно-телекомунікаційних систем	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.
Законодавчі питання інформаційної безпеки	Словесні методи (лекції, 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 вебіари 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 (залік) – усне, письмове опитування, тестовий контроль.
Управління інформаційною безпекою	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
Канали витоку інформації	Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною,	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.

	нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	
Архітектура і моделі безпеки	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
Ознайомча 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 практики на випусковій кафедрі.
Безпека розробки та підтримки додатків	Лекції: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод, метод проблемного викладу.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – екзамен: письмове опитування, тестування.
Методи і засоби проведення спеціальних вимірювань в ІТС	Методи навчання: словесні методи (лекція, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
Програмне забезпечення об'єктів кіберпростору (в тому	Лекції: інформаційно-рецептивний метод, репродуктивний метод,	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий

числі курсова робота)	евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод; виконання курсової роботи: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу.	контроль. Підсумковий контроль – залік/екзамен: письмове опитування, тестування. Курсова робота: захист.
Комп'ютерна дискретна математика	Методи навчання: словесний метод (лекція, дискусія); практичний метод (практичні заняття, практичні завдання); робота з навчально-методичною літературою (конспектування, тезування, анотування); методи дистанційного навчання; самостійна робота (опрацювання матеріалів лекцій та літературних джерел за відповідною тематикою, підготовка презентацій, рефератів); інтерактивні методи навчання (робота в малих групах та тренінги).	Поточний контроль – опитування під час занять; контрольні роботи; стандартизовані тести; реферати; презентації результатів виконаних практичних завдань. Підсумковий контроль (залік/іспит) – усне та письмове опитування, тестовий контроль.
Основи комп'ютерних технологій	Лекції, практичні та лабораторні заняття – пояснювально-ілюстративний та репродуктивний методи. Словесні методи (співбесіда, консультація, дискусія); наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Поточний контроль: тести, опитування, контрольні, самостійні роботи за індивідуальними завданнями; звіти, презентації результатів виконання завдань практичного характеру; оцінювання завдань, що виконувались в лабораторіях, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – екзамен: усне або письмове опитування, тестування.
Вступ до кібербезпеки	Лекції, практичні заняття – пояснювально-ілюстративний метод, презентації; метод проблемного викладу, доповідь та захист підготовлених презентацій; самостійна робота – репродуктивний метод.	Поточний контроль – усне та письмове опитування (тестування, захист виконаних завдань для самостійної роботи). Підсумковий контроль – залік: усне або письмове опитування.
Міжособистісне спілкування і побудова команд	Методи навчання: лекції та практичні заняття (інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод). Самостійна робота: опрацювання матеріалів лекцій та літературних джерел, підготовка презентацій та рефератів за індивідуальним завданням. Інтерактивні методи: робота в малих групах та тренінги.	Поточного контролю: усні та письмові (тестування, захист завдань практичного характеру, ІНДЗ) відповіді здобувача освіти. Підсумковий контроль – залік: письмове опитування, тестування.

		Вища математика	Методи навчання: словесний метод (лекція, дискусія); практичний метод (практичні заняття, практичні завдання); робота з навчально-методичною літературою (конспектування, тезування, анотування); методи дистанційного навчання; самостійна робота (розв'язання завдань).	Оцінювання рівня знань студентів з предмету «Вища математика» здійснюється на основі результатів поточного контролю та іспиту. Екзамен – усне, письмове опитування, тести.
		Вибрані розділи фізики	Лекції, практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод, дослідницький метод.	Поточний контроль – усне та фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – екзамен: письмове опитування.
		Інформаційний пошук у кібербезпеці	Лекції, семінарські заняття – пояснювально-ілюстративний метод, презентації; метод проблемного викладу, доповідь та захист підготовлених презентацій; самостійна робота – репродуктивний метод, пов'язаний з опрацюванням матеріалів лекцій та літературних джерел за відповідною тематикою, формуванням напрацювань для підготовки презентацій та доповідей.	Поточний контроль: усні та письмові (тестування) відповіді студента; представлення презентації, доповідь та аргументований захист під час командної роботи. Підсумковий контроль – залік: усне та письмове опитування, тестовий контроль
<p><i>ПРН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.</i></p>	☒	Теорія інформації та кодування	Лекції, практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, метод проблемного викладу, робота з навчально-методичною, нормативною літературою; самостійна робота студентів: використання учбових матеріалів на основі курсів пропонованих компанією Coursera за підтримки компанії Ukraine Response.	Поточний контроль – усне опитування; письмові контрольні роботи із практичними задачами; тестування. Підсумковий контроль – іспит: проведення письмового іспиту із використанням екзаменаційних білетів із практичними задачами та теоретичними питаннями; тестування.
		Комп'ютерна електроніка	Лекції, практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод, дослідницький метод.	Поточний контроль – усне та фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – екзамен: усне або письмове опитування.
		Комп'ютерна	Методи навчання:	Поточний контроль –

дискретна математика	словесний метод (лекція, дискусія); практичний метод (практичні заняття, практичні завдання); робота з навчально-методичною літературою (конспектування, тезування, анотування); методи дистанційного навчання; самостійна робота (опрацювання матеріалів лекцій та літературних джерел за відповідною тематикою, підготовка презентацій, рефератів); інтерактивні методи навчання (робота в малих групах та тренінги).	опитування під час занять; контрольні роботи; стандартизовані тести; реферати; презентації результатів виконаних практичних завдань. Підсумковий контроль (залік/іспит) – усне та письмове опитування, тестовий контроль.
Міжособистісне спілкування і побудова команд	Методи навчання: лекції та практичні заняття (інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод). Самостійна робота: опрацювання матеріалів лекцій та літературних джерел, підготовка презентацій та рефератів за індивідуальним завданням. Інтерактивні методи: робота в малих групах та тренінги.	Поточного контролю: усні та письмові (тестування, захист завдань практичного характеру, ІНДЗ) відповіді здобувача освіти. Підсумковий контроль – залік: письмове опитування, тестування.
Вибрані розділи фізики	Лекції, практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод, дослідницький метод.	Поточний контроль – усне та фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – екзамен: письмове опитування.
Архітектура і моделі безпеки	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
Канали витоку інформації	Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною,	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.

	нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	
Законодавчі питання інформаційної безпеки	Словесні методи (лекції, 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 (залік) – усне, письмове опитування, тестовий контроль.
Управління інформаційною безпекою	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування. контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
Випускна кваліфікаційна робота/проект	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 індивідуальною темою.	Кваліфікаційна (дипломна) робота – захист.
Міждисциплінарна курсова 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	Курсова робота: захист.

			над індивідуальним завданням.	
		Безпека інформаційно-телекомунікаційних систем	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.
<i>ПРН 5. Адаптуватися в умовах частоті зміни технологій професійної діяльності, прогнозувати кінцевий результат.</i>	☒	Випускна кваліфікаційна робота/проект	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 індивідуальною темою.	Кваліфікаційна (дипломна) робота – захист.
		Виробничо-технологічна 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 виробничо-технологічної практики на кафедрі.
		Ознайомча 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 практики на випусковій кафедрі.
		Безпека інформаційно-телекомунікаційних систем	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,	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.

	рефератів, а також формуванням напрацювань для виконання і захисту лабораторних робіт.	
Управління інформаційною безпекою	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування. контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
Безпека розробки та підтримки додатків	Лекції: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод, метод проблемного викладу.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – екзамен: письмове опитування, тестування.
Комп'ютерна електроніка	Лекції, практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод, дослідницький метод.	Поточний контроль – усне та фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – екзамен: усне або письмове опитування.
Вступ до кібербезпеки	Лекції, практичні заняття – пояснювально-ілюстративний метод, презентації; метод проблемного викладу, доповідь та захист підготовлених презентацій; самостійна робота – репродуктивний метод.	Поточний контроль – усне та письмове опитування (тестування, захист виконаних завдань для самостійної роботи). Підсумковий контроль – залік: усне або письмове опитування.
Вибрані розділи фізики	Лекції, практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод, дослідницький метод.	Поточний контроль – усне та фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – екзамен: письмове опитування.
Теорія інформації та	Лекції, практичні заняття –	Поточний контроль – усне

		кодування	інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, метод проблемного викладу, робота з навчально-методичною, нормативною літературою; самостійна робота студентів: використання учбових матеріалів на основі курсів пропонує компанією Coursera за підтримки компанії Ukraine Response.	опитування; письмові контрольні роботи із практичними задачами; тестування. Підсумковий контроль – іспит: проведення письмового іспиту із використанням екзаменаційних білетів із практичними задачами та теоретичними питаннями; тестування.
ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.	☒	Вибрані розділи фізики	Лекції, практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод, дослідницький метод.	Поточний контроль – усне та фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – екзамен: письмове опитування.
		Філософія	Словесні методи (лекція, семінари, співбесіда, консультація, дискусія); наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з навчально-методичною, науковою, літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні); самостійна робота над індивідуальним завданням та за програмою навчальної дисципліни; інноваційні технології (роботи в малих групах, семінари – дискусії), тощо.	Засоби оцінювання: екзамен, тести, опитування, контрольні, самостійні роботи за індивідуальними завданнями, звіти, реферати, статті; презентації результатів виконання завдань, інші види індивідуальних та групових завдань. Види та форми контролю: усні та письмові відповіді й доповіді студентів; письмові творчі роботи (есе; аналітичні повідомлення, реферати, порівняльні таблиці); проекти дискусійних заходів та їхня організація (в аудиторному або дистанційному форматах); презентації; тестові завдання, термінологічні диктанти тощо.
		Вступ до кібербезпеки	Лекції, практичні заняття – пояснювально-ілюстративний метод, презентації; метод проблемного викладу, доповідь та захист підготовлених презентацій; самостійна робота – репродуктивний метод.	Поточний контроль – усне та письмове опитування (тестування, захист виконаних завдань для самостійної роботи). Підсумковий контроль – залік: усне або письмове опитування.
		Теорія інформації та кодування	Лекції, практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, метод проблемного викладу, робота з навчально-методичною, нормативною літературою; самостійна робота студентів: використання учбових матеріалів на основі курсів пропонує компанією Coursera за підтримки компанії Ukraine Response.	Поточний контроль – усне опитування; письмові контрольні роботи із практичними задачами; тестування. Підсумковий контроль – іспит: проведення письмового іспиту із використанням екзаменаційних білетів із практичними задачами та теоретичними питаннями; тестування.

Випускна кваліфікаційна робота/проект	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 індивідуальною темою.	Кваліфікаційна (дипломна) робота – захист.
Виробничо-технологічна 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 виробничо-технологічної практики на кафедрі.
Міждисциплінарна курсова 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.	Курсова робота: захист.
Безпека інформаційно-телекомунікаційних систем	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.
Основи побудови систем комплексного захисту інформації	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; комп'ютерні засоби навчання (ресурси: дистанційні, web-конференції; інструменти: програмні виконання завдань розрахункового	Поточний контроль: усні та письмові (контрольна робота, тестування) відповіді студента. Підсумковий контроль: залік (усне, письмове опитування, тестовий контроль).

	характеру та моделювання); самостійна робота: підготовка презентацій, рефератів; робота з навчально-методичною, науковою, нормативною літературою.	
Управління інформаційною безпекою	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
Канали витоку інформації	Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.
Архітектура і моделі безпеки	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
Ознайомча 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 практики на випусковій кафедрі.
Комп'ютерна електроніка	Лекції, практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий	Поточний контроль – усне та фронтальне опитування, оцінка активності, тестовий контроль.

			метод, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод, дослідницький метод.	Підсумковий контроль – екзамен: усне або письмове опитування.
<i>ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.</i>	☒	Основи побудови систем комплексного захисту інформації	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; комп'ютерні засоби навчання (ресурси: дистанційні, web-конференції; інструменти: програмні виконання завдань розрахункового характеру та моделювання); самостійна робота: підготовка презентацій, рефератів; робота з навчально-методичною, науковою, нормативною літературою.	Поточний контроль: усні та письмові (контрольна робота, тестування) відповіді студента. Підсумковий контроль: залік (усне, письмове опитування, тестовий контроль).
		Законодавчі питання інформаційної безпеки	Словесні методи (лекції, 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 вебіари 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 (залік) – усне, письмове опитування, тестовий контроль.
<i>ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.</i>	☒	Міждисциплінарна курсова 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 вебіари тощо); самостійна робота над індивідуальним завданням.	Курсова робота: захист.
		Безпека інформаційно-телекомунікаційних систем	Лекції: пояснювально-ілюстративний метод, презентації; робота з книгою: з навчально-	Поточний контроль – усні та письмові (тестування, захист лабораторних робіт, захист завдань практичного

	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.	характеру) відповіді здобувача освіти. Підсумковий контроль (екзамен) – усне або письмове опитування, тестовий контроль.
Законодавчі питання інформаційної безпеки	Словесні методи (лекції, 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 (залік) – усне, письмове опитування, тестовий контроль.
Управління інформаційною безпекою	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
Канали витоку інформації	Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.
Теорія інформації та кодування	Лекції, практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий	Поточний контроль – усне опитування; письмові контрольні роботи із практичними задачами;

			метод, метод проблемного викладу, робота з навчально-методичною, нормативною літературою; самостійна робота студентів: використання учбових матеріалів на основі курсів пропонує компанією Coursera за підтримки компанії Ukraine Response.	тестування. Підсумковий контроль – іспит: проведення письмового іспиту із використанням екзаменаційних білетів із практичними задачами та теоретичними питаннями; тестування.
<i>ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.</i>	☒	Міждисциплінарна курсова 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.	Курсова робота: захист.
		Взаємодія між компонентами систем IoT	Лекції – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод, дослідницький метод.	Формами поточного контролю є усна чи письмова (тестування, реферат, лабораторна робота) відповідь студента та ін. Формами підсумкового контролю є залік, усне опитування або комплексне тестування.
		Канали витоку інформації	Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.
		Архітектура і моделі безпеки	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота	Формами поточного контролю є усні і письмові, опитування. контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.

			над індивідуальним завданням або за програмою навчальної дисципліни.	
		Теорія інформації та кодування	Лекції, практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, метод проблемного викладу, робота з навчально-методичною, нормативною літературою; самостійна робота студентів: використання учбових матеріалів на основі курсів пропонувані компанією Coursera за підтримки компанії Ukraine Response.	Поточний контроль – усне опитування; письмові контрольні роботи із практичними задачами; тестування. Підсумковий контроль – іспит: проведення письмового іспиту із використанням екзаменаційних білетів із практичними задачами та теоретичними питаннями; тестування.
		Комп'ютерна електроніка	Лекції, практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод, дослідницький метод.	Поточний контроль – усне та фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – екзамен: усне або письмове опитування.
		Основи інфокомунікацій	Лекції, практичні заняття: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – залік/екзамен: письмове опитування, тестування.
		Основи комп'ютерних технологій	Лекції, практичні та лабораторні заняття – пояснювально-ілюстративний та репродуктивний методи. Словесні методи (співбесіда, консультація, дискусія); наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Поточний контроль: тести, опитування, контрольні, самостійні роботи за індивідуальними завданнями; звіти, презентації результатів виконання завдань практичного характеру; оцінювання завдань, що виконувались в лабораторіях, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – екзамен: усне або письмове опитування, тестування.
ПРН 11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.	<input checked="" type="checkbox"/>	Архітектура і моделі безпеки	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною,	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання;

			науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
		Теорія інформації та кодування	Лекції, практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, метод проблемного викладу, робота з навчально-методичною, нормативною літературою; самостійна робота студентів: використання учбових матеріалів на основі курсів пропонує компанією Coursera за підтримки компанії Ukraine Response.	Поточний контроль – усне опитування; письмові контрольні роботи із практичними задачами; тестування. Підсумковий контроль – іспит: проведення письмового іспиту із використанням екзаменаційних білетів із практичними задачами та теоретичними питаннями; тестування.
<i>ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.</i>	☒	Управління інформаційною безпекою	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування. контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
		Канали витоку інформації	Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.
		Архітектура і моделі безпеки	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним	Формами поточного контролю є усні і письмові, опитування. контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.

	завданням або за програмою навчальної дисципліни.	
Методи і засоби проведення спеціальних вимірювань в ІТС	Методи навчання: словесні методи (лекція, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
Вступ до кібербезпеки	Лекції, практичні заняття – пояснювально-ілюстративний метод, презентації; метод проблемного викладу, доповідь та захист підготовлених презентацій; самостійна робота – репродуктивний метод.	Поточний контроль – усне та письмове опитування (тестування, захист виконаних завдань для самостійної роботи). Підсумковий контроль – залік: усне або письмове опитування.
Законодавчі питання інформаційної безпеки	Словесні методи (лекції, 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 (залік) – усне, письмове опитування, тестовий контроль.
Безпека інформаційно-телекомунікаційних систем	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.
Міждисциплінарна	Дослідницький метод;	Курсова робота: захист.

		курсова робота	словесні методи (розповідь, бесіда, консультація, дискусія, тощо); наочні методи (презентації, ілюстрації, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (ресурси: мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням.	
		Ознайомча 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 практики на випусковій кафедрі.
		Випускна кваліфікаційна робота/проект	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 індивідуальною темою.	Кваліфікаційна (дипломна) робота – захист.
		Виробничо-технологічна 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 виробничо-технологічної практики на кафедрі.
<p><i>ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.</i></p>	<input checked="" type="checkbox"/>	Міждисциплінарна курсова 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.	Курсова робота: захист.
		Канали витоку інформації	Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою;	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.

			лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	
		Теорія інформації та кодування	Лекції, практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, метод проблемного викладу, робота з навчально-методичною, нормативною літературою; самостійна робота студентів: використання учбових матеріалів на основі курсів пропонувані компанією Coursera за підтримки компанії Ukraine Response.	Поточний контроль – усне опитування; письмові контрольні роботи із практичними задачами; тестування. Підсумковий контроль – іспит: проведення письмового іспиту із використанням екзаменаційних білетів із практичними задачами та теоретичними питаннями; тестування.
		Основи інфокомунікацій	Лекції, практичні заняття: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – залік/екзамен: письмове опитування, тестування.
<p><i>ПРН 22.</i> <i>Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки.</i></p>	☒	Виробничо-технологічна 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 виробничо-технологічної практики на кафедрі.
		Ознайомча 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 практики на випусковій кафедрі.
		Міждисциплінарна курсова 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.	Курсова робота: захист.
		Основи побудови систем комплексного захисту інформації	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; практичні заняття: репродуктивний метод,	Поточний контроль: усні та письмові (контрольна робота, тестування) відповіді студента. Підсумковий контроль:

			дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; комп'ютерні засоби навчання (ресурси: дистанційні, web-конференції; інструменти: програмні виконання завдань розрахункового характеру та моделювання); самостійна робота: підготовка презентацій, рефератів; робота з навчально-методичною, науковою, нормативною літературою.	залік (усне, письмове опитування, тестовий контроль).
		Канали витоку інформації	Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.
		Архітектура і моделі безпеки	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування. контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
		Вступ до кібербезпеки	Лекції, практичні заняття – пояснювально-ілюстративний метод, презентації; метод проблемного викладу, доповідь та захист підготовлених презентацій; самостійна робота – репродуктивний метод.	Поточний контроль – усне та письмове опитування (тестування, захист виконаних завдань для самостійної роботи). Підсумковий контроль – залік: усне або письмове опитування.
ПРН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки та інформаційних та	<input checked="" type="checkbox"/>	Архітектура і моделі безпеки	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси –	Формами поточного контролю є усні і письмові, опитування. контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль –

інформаційно-телекомунікаційних (автоматизованих) системах.		ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	іспит: усне або письмове опитування, тести.
	Канали витоку інформації	Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.
	Управління інформаційною безпекою	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
	Основи побудови систем комплексного захисту інформації	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих групах та тренінги; комп'ютерні засоби навчання (ресурси: дистанційні, web-конференції; інструменти: програмні виконання завдань розрахункового характеру та моделювання); самостійна робота: підготовка презентацій, рефератів; робота з навчально-методичною, науковою, нормативною літературою.	Поточний контроль: усні та письмові (контрольна робота, тестування) відповіді студента. Підсумковий контроль: залік (усне, письмове опитування, тестовий контроль).
	Безпека інформаційно-телекомунікаційних систем	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	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.

			підходу, дослідницький метод; самостійна робота: підготовка презентацій, рефератів, а також формуванням напрацювань для виконання і захисту лабораторних робіт.	
		Міждисциплінарна курсова 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.	Курсова робота: захист.
<p><i>ПРН 23. Реалізувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.</i></p>	<input checked="" type="checkbox"/>	Міждисциплінарна курсова 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.	Курсова робота: захист.
		Технічні системи охорони об'єктів	Лекції: пояснювально-ілюстративний метод, презентації; робота з книгою: з навчально-методичною, науковою та нормативною літературою; 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) відповіді здобувача освіти. Підсумковий контроль (екзамен) – усне або письмове опитування, тестовий контроль.
		Безпека інформаційно-телекомунікаційних систем	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.

		Канали витоку інформації	Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.
<p><i>ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.</i></p>	<input checked="" type="checkbox"/>	Випускна кваліфікаційна робота/проект	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 індивідуальною темою.	Кваліфікаційна (дипломна) робота – захист.
		Виробничо-технологічна 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 виробничо-технологічної практики на кафедрі.
		Міждисциплінарна курсова 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.	Курсова робота: захист.
		Безпека інформаційно-телекомунікаційних систем	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	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.

			лабораторних робіт.	
		Криптографія (в тому числі курсова робота)	Лекції та практичні заняття: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод; виконання курсової роботи: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – залік/екзамен: письмове опитування, тестування. Курсова робота: захист.
		Канали витоку інформації	Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.
		Вступ до кібербезпеки	Лекції, практичні заняття – пояснювально-ілюстративний метод, презентації; метод проблемного викладу, доповідь та захист підготовлених презентацій; самостійна робота – репродуктивний метод.	Поточний контроль – усне та письмове опитування (тестування, захист виконаних завдань для самостійної роботи). Підсумковий контроль – залік: усне або письмове опитування.
		Ознайомча 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 практики на випусковій кафедрі.
ПРН 18. Використовувати програмні та апаратні комплекси захисту інформаційних ресурсів.	<input checked="" type="checkbox"/>	Безпека інформаційно-телекомунікаційних систем	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.

		Взаємодія між компонентами систем IoT	Лекції – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод, дослідницький метод.	Формами поточного контролю є усна чи письмова (тестування, реферат, лабораторна робота) відповідь студента та ін. Формами підсумкового контролю є залік, усне опитування або комплексне тестування.
		Методи і засоби проведення спеціальних вимірювань в ІТС	Методи навчання: словесні методи (лекція, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.	☒	Безпека інформаційно-телекомунікаційних систем	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.
		Безпека розробки та підтримки додатків	Лекції: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод, метод проблемного викладу.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – екзамен: письмове опитування, тестування.
		Комп'ютерна електроніка	Лекції, практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, робота з книгою: з навчально-методичною,	Поточний контроль – усне та фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – екзамен: усне або письмове

			нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод, дослідницький метод.	опитування.
		Програмне забезпечення об'єктів кіберпростору (в тому числі курсова робота)	Лекції: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод; виконання курсової роботи: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – залік/екзамен: письмове опитування, тестування. Курсова робота: захист.
ПРН 12. Розробляти моделі загроз та порушника.	☒	Управління інформаційною безпекою	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
		Канали витоку інформації	Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.
		Архітектура і моделі безпеки	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.

			тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	
		Комп'ютерна дискретна математика	Методи навчання: словесний метод (лекція, дискусія); практичний метод (практичні заняття, практичні завдання); робота з навчально-методичною літературою (конспектування, тезування, анотування); методи дистанційного навчання; самостійна робота (опрацювання матеріалів лекцій та літературних джерел за відповідною тематикою, підготовка презентацій, рефератів); інтерактивні методи навчання (робота в малих групах та тренінги).	Поточний контроль – опитування під час занять; контрольні роботи; стандартизовані тести; реферати; презентації результатів виконаних практичних завдань. Підсумковий контроль (залік/іспит) – усне та письмове опитування, тестовий контроль.
		Вища математика	Методи навчання: словесний метод (лекція, дискусія); практичний метод (практичні заняття, практичні завдання); робота з навчально-методичною літературою (конспектування, тезування, анотування); методи дистанційного навчання; самостійна робота (розв'язання завдань).	Оцінювання рівня знань студентів з предмету «Вища математика» здійснюється на основі результатів поточного контролю та іспиту. Екзамен – усне, письмове опитування, тести.
		Міждисциплінарна курсова 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.	Курсова робота: захист.
<p><i>ПРН 16. Реалізувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.</i></p>	<input checked="" type="checkbox"/>	Технічні системи охорони об'єктів	Лекції: пояснювально-ілюстративний метод, презентації; робота з книгою: з навчально-методичною, науковою та нормативною літературою; 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) відповіді здобувача освіти. Підсумковий контроль (екзамен) – усне або письмове опитування, тестовий контроль.
		Основи побудови систем комплексного захисту інформації	Лекції: пояснювально-ілюстративний метод, презентації; дослідницький метод; практичні заняття: репродуктивний метод, дослідницький метод; інтерактивні методи навчання: робота в малих	Поточний контроль: усні та письмові (контрольна робота, тестування) відповіді студента. Підсумковий контроль: залік (усне, письмове опитування, тестовий контроль).

			<p>групах та тренінги; комп'ютерні засоби навчання (ресурси: дистанційні, web-конференції; інструменти: програмні виконання завдань розрахункового характеру та моделювання); самостійна робота: підготовка презентацій, рефератів; робота з навчально-методичною, науковою, нормативною літературою.</p>	
		Управління інформаційною безпекою	<p>Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.</p>	<p>Формами поточного контролю є усні і письмові, опитування. контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання практичних завдань; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.</p>
<p>ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.</p>	<input checked="" type="checkbox"/>	<p>Безпека інформаційно-телекомунікаційних систем</p>	<p>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.</p>	<p>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.</p>
		<p>Взаємодія між компонентами систем IoT</p>	<p>Лекції – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод, дослідницький метод.</p>	<p>Формами поточного контролю є усна чи письмова (тестування, реферат, лабораторна робота) відповідь студента та ін. Формами підсумкового контролю є залік, усне опитування або комплексне тестування.</p>
		<p>Канали витоку інформації</p>	<p>Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою;</p>	<p>Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.</p>

			лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	
		Теорія інформації та кодування	Лекції, практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, метод проблемного викладу, робота з навчально-методичною, нормативною літературою; самостійна робота студентів: використання учбових матеріалів на основі курсів пропонованих компанією Coursera за підтримки компанії Ukraine Response.	Поточний контроль – усне опитування; письмові контрольні роботи із практичними задачами; тестування. Підсумковий контроль – іспит: проведення письмового іспиту із використанням екзаменаційних білетів із практичними задачами та теоретичними питаннями; тестування.
		Основи інфокомунікацій	Лекції, практичні заняття: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – залік/екзамен: письмове опитування, тестування.
		Основи комп'ютерних технологій	Лекції, практичні та лабораторні заняття – пояснювально-ілюстративний та репродуктивний методи. Словесні методи (співбесіда, консультація, дискусія); наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Поточний контроль: тести, опитування, контрольні, самостійні роботи за індивідуальними завданнями; звіти, презентації результатів виконання завдань практичного характеру; оцінювання завдань, що виконувались в лабораторіях, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – екзамен: усне або письмове опитування, тестування.
		Міждисциплінарна курсова 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 вебіари тощо); самостійна робота над індивідуальним завданням.	Курсова робота: захист.
ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-	<input checked="" type="checkbox"/>	Методи і засоби проведення спеціальних вимірювань в ІТС	Методи навчання: словесні методи (лекція, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо);	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що

<p>телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.</p>		<p>робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебіари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.</p>	<p>виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.</p>
	<p>Теорія інформації та кодування</p>	<p>Лекції, практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, частково-пошуковий метод, метод проблемного викладу, робота з навчально-методичною, нормативною літературою; самостійна робота студентів: використання учбових матеріалів на основі курсів пропонованих компанією Coursera за підтримки компанії Ukraine Response.</p>	<p>Поточний контроль – усне опитування; письмові контрольні роботи із практичними задачами; тестування. Підсумковий контроль – іспит: проведення письмового іспиту із використанням екзаменаційних білетів із практичними задачами та теоретичними питаннями; тестування.</p>
	<p>Програмне забезпечення об'єктів кіберпростору (в тому числі курсова робота)</p>	<p>Лекції: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод; виконання курсової роботи: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу.</p>	<p>Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – залік/екзамен: письмове опитування, тестування. Курсова робота: захист.</p>
	<p>Безпека розробки та підтримки додатків</p>	<p>Лекції: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод, метод проблемного викладу.</p>	<p>Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – екзамен: письмове опитування, тестування.</p>
	<p>Канали витоку інформації</p>	<p>Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.</p>	<p>Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.</p>
	<p>Міждисциплінарна курсова робота</p>	<p>Дослідницький метод; словесні методи (розповідь,</p>	<p>Курсова робота: захист.</p>

			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 вебіари тощо); самостійна робота над індивідуальним завданням.	
		Безпека інформаційно-телекомунікаційних систем	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.
<p><i>ПРН 17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.</i></p>	☒	Технічні системи охорони об'єктів	Лекції: пояснювально-ілюстративний метод, презентації; робота з книгою: з навчально-методичною, науковою та нормативною літературою; 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) відповіді здобувача освіти. Підсумковий контроль (екзамен) – усне або письмове опитування, тестовий контроль.
		Міждисциплінарна курсова 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 вебіари тощо); самостійна робота над індивідуальним завданням.	Курсова робота: захист.
		Безпека інформаційно-телекомунікаційних систем	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	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.

		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.	
	Канали витоку інформації	Лекції та практичні заняття – інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу, робота з книгою: з навчально-методичною, нормативною літературою; лабораторні заняття – дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; самостійна робота – репродуктивний метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий – екзамен: усне та/або письмове опитування, тестування.
	Архітектура і моделі безпеки	Методи навчання: словесні методи (лекція, практичні заняття, співбесіда, консультація, дискусія, тощо); лабораторний практикум; наочні методи (презентації, ілюстрації, відеоматеріали, тощо); робота з книгою: з навчально-методичною, науковою, нормативною літературою; комп'ютерні засоби навчання (курси – ресурси мультимедійні, дистанційні, web-конференції та вебінари тощо); самостійна робота над індивідуальним завданням або за програмою навчальної дисципліни.	Формами поточного контролю є усні і письмові, опитування, контрольні, самостійна робота за індивідуальними завданнями; звіти, оцінювання завдань, що виконувались в лабораторіях та на об'єктах, комп'ютерне моделювання; інші види індивідуальних та групових завдань. Підсумковий контроль – іспит: усне або письмове опитування, тести.
	Основи інфокомунікацій	Лекції, практичні заняття: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу; лабораторні заняття: дослідницький метод, інформаційно-рецептивний метод, репродуктивний метод; самостійна робота: репродуктивний метод, дослідницький метод.	Поточний контроль – усне, фронтальне опитування, оцінка активності, тестовий контроль. Підсумковий контроль – залік/екзамен: письмове опитування, тестування.