НАЦІОНАЛЬНЕ АГЕНТСТВО ІЗ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	**Державний вищий навчальний заклад "Ужгородський національний університет"**
Освітня програма	**8481 Безпека інформаційних і комунікаційних систем**
Рівень вищої освіти	**Магістр**
Спеціальність	**125 Кібербезпека**

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

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

Використані скорочення:

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

Загальні відомості

1. Інформація про ЗВО (ВСП ЗВО)

Реєстраційний номер ЗВО у ЄДЕБО	**207**
Повна назва ЗВО	**Державний вищий навчальний заклад "Ужгородський національний університет"**
Ідентифікаційний код ЗВО	**02070832**
ПІБ керівника ЗВО	**Смоланка Володимир Іванович**
Посилання на офіційний веб-сайт ЗВО	**http://www.uzhnu.edu.ua**

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

https://registry.edbo.gov.ua/university/207

3. Загальна інформація про ОП, яка подається на акредитацію

ID освітньої програми в ЄДЕБО	**8481**
Назва ОП	**Безпека інформаційних і комунікаційних систем**
Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека**
Спеціалізація (за наявності)	*відсутня*
Рівень вищої освіти	**Магістр**
Тип освітньої програми	**Освітньо-професійна**
Вступ на освітню програму здійснюється на основі ступеня (рівня)	**Бакалавр, Магістр (ОКР «спеціаліст»)**
Структурний підрозділ (кафедра або інший підрозділ), відповідальний за реалізацію ОП	**Кафедра твердотільної електроніки та інформаційної безпеки**
Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП	**Кафедра іноземних мов**
Місце (адреса) провадження освітньої діяльності за ОП	**м. Ужгород, вул. Волошина, 54**
Освітня програма передбачає присвоєння професійної кваліфікації	*не передбачає*
Професійна кваліфікація, яка присвоюється за ОП (за наявності)	***відсутня***
Мова (мови) викладання	**Українська**
ID гаранта ОП у ЄДЕБО	**127444**
ПІБ гаранта ОП	**Різак Василь Михайлович**
Посада гаранта ОП	**завідувач кафедри**
Корпоративна електронна адреса гаранта ОП	**vrizak@uzhnu.edu.ua**
Контактний телефон гаранта ОП	**+38(067)-312-25-87**
Додатковий телефон гаранта ОП	*відсутній*

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

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

Підготовку фахівців галузі 1701 “Інформаційна безпека” за освітнім рівнем "бакалавр" розпочато в Державному вищому навчальному закладі «Ужгородський національний університет» у 2007 році на кафедрі твердотільної електроніки фізичного факультету. Саме тоді була одержана ліцензія на підготовку бакалаврів зі спеціальності «Системи технічного захисту інформації». У 2010 році отримано ліцензію та розпочато підготовку бакалаврів за напрямом 6.170101 Безпека інформаційних та комунікаційних систем, а з 2014 року - підготовку магістрів відповідної спеціальності. На кафедрі утворено секцію “Інформаційна безпека” (після подальшого вдосконалення кафедра отримала назву “Кафедра твердотільної електроніки та інформаційної безпеки” (ТЕІБ)). У 2017 році магістерська спеціальність 8.17010101 Безпека інформаційних та комунікаційних систем була успішно акредитована. Розроблення освітніх програм в ДВНЗ “УжНУ” здійснюється відповідно до “Положення про порядок розроблення, моніторинг та періодичний перегляд освітніх програм у ДВНЗ «УжНУ»” (https://www.uzhnu.edu.ua/uk/infocentre/get/22968). Освітньо-професійна програма «Безпека інформаційних і комунікаційних систем» другого (магістерського) рівня вищої освіти за спеціальністю 125 Кібербезпека була розроблена робочою групою із числа науково-педагогічних працівників (НПП) кафедри ТЕІБ із врахуванням вимог Стандарту вищої освіти України, затвердженого 18 березня 2021 року. У 2022 році проведено акредитацію цієї ОП, за результатами якої Національне агентство ухвалило рішення про умовну (відкладену) акредитацію.
Відповідно оновлення та доопрацювання представленої ОП «Безпека інформаційних і комунікаційних систем» за спеціальністю 125 Кібербезпека та захист інформації відбувалося впродовж січня-березня 2023 року в ході тривалих консультацій із працівниками Державної служби спеціального зв'язку та захисту інформації України, Департаменту кіберполіції НПУ і учасниками ГО “Асоціація спеціалістів кібербезпеки”. Проект ОП також обговорювався на зустрічі робочої групи з провідними науковцями Національного авіаційного університету, Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова, Інституту проблем реєстрації інформації НАН України та випускниками спеціальності Кібербезпека (http://teib.info/?p=6190). Рекомендації, напрацьовані в ході цієї зустрічі, зауваження рецензентів і побажання здобувачів ВО були максимально враховані при модернізації даної ОП (протоколи засідання робочої групи №2, №3).
Головна увага була приділена усуненню недоліків виявлених в процесі попередньої акредитації (Критерій 2 та Критерій 8), а також врахуванні професійного стандарту, галузевих та регіональних тенденцій розвитку захисту інформації в організаціях, установах, об’єктах критичної інфраструктури і спрямована на задоволення потреб регіонального ринку праці та держави у висококваліфікованих фахівцях (особливо у період режиму воєнного стану). Інтегральна, загальні, фахові компетентності та програмні результати навчання 1-23 представленої ОП однозначно відповідають компетентностям та програмним результатам Стандарту ВО за відповідною спеціальністю.
Модернізована ОП «Безпека інформаційних і комунікаційних систем» затверджена рішенням Вченої ради ДВНЗ «УжНУ» (протокол №3 від 23.03.2023 р.) https://www.uzhnu.edu.ua/uk/infocentre/17752 і введена в дію наказом ректора ДВНЗ “УжНУ” №147/01-04 від 04.04.2023 р

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	15	15	0
2 курс	2022 - 2023	12	21	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	**8484 Безпека інформаційних і комунікаційних систем** **9275 Системи технічного захисту інформації**
другий (магістерський) рівень	**8481 Безпека інформаційних і комунікаційних систем** **9770 Системи технічного захисту інформації, автоматизація її обробки**

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	138627	95294
Власні приміщення ЗВО (на праві власності, господарського відання або оперативного управління)	128922	85589
Приміщення, які використовуються на іншому праві, аніж право власності, господарського відання або оперативного управління (оренда, безоплатне користування тощо)	9705	9705
Приміщення, здані в оренду	799	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	*OPP_BIKS_Mahistr 2023_UzhNU.pdf*	DaSShtQmYBdMM8WSOdC4IJ7P5d3sBwQit+wbtFAGA1Q=
Навчальний план за ОП	*NP OPP BIKS 2023.pdf*	BhNGpfaokqZLQYwk+bc3w+LNAAm9cXoQq2fx4froZUo=
Рецензії та відгуки роботодавців	*Retsenziya KIBERPOLITSIYA.pdf*	PzJmbStzYVrrTafJdinblFFPNKhvqNbzraFT1TA8wBw=
Рецензії та відгуки роботодавців	*Retsenziya NAU.pdf*	JXYWwKIESBCQrqXBTqHzKYZYahAFyDP93S7JaJUfXvo=

1. Проектування та цілі освітньої програми

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

Метою ОП “Безпека інформаційних і комунікаційних систем” є навчання та підготовка фахівців, які мають знання, вміння та навички щодо впровадження та застосування сучасних технологій кібербезпеки, а також розробки технологій і засобів захисту інформації та проектування систем й комплексів забезпечення кібербезпеки; фахівців, здатних розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. Особливістю даної ОП є врахування вимог професійного стандарту “Фахівець сфери захисту інформації” та її спрямованість на підготовку фахівців з кібербезпеки, здатних надавати консультативні послуги та технічну допомогу з питань технічного, криптографічного захисту інформації та кіберзахисту, а також здійснювати професійну діяльність у контексті регіонального транскордонного співробітництва, забезпечувати захищеність інформаційних і комунікаційних систем транскордонної та регіональної інфраструктури, функціонування об’єктів критичної інфраструктури, державних установ та органів місцевого самоврядування в умовах ризику стороннього кібернетичного впливу. Результатом унікальності ОП є широкий спектр працевлаштування випускників, наприклад, суб’єкти національної системи кібербезпеки, об’єкти критичної інфраструктури, ІТ-індустрія, банки, правоохоронні та органи спеціального призначення, а також ЗСУ.

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

ОП «Безпека інформаційних і комунікаційних систем» відповідає місії та стратегії університету, які викладені у «Концепції інноваційного розвитку ДВНЗ «УжНУ» на 2015 - 2025 рр.» (https://www.uzhnu.edu.ua/uk/infocentre/get/8662) та «Стратегії інтернаціоналізації ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/20139). Мета програми відповідає компонентам місії ДВНЗ «Ужгородський національний університет» у розрізі наукової складової - проведення фундаментальних і прикладних досліджень. ОПП орієнтована на глибоке засвоєння фундаментальних знань, оволодіння загальними і фаховими компетентностями, необхідними для здійсненні професійної діяльності, що тісно переплітається з основними концептуальними положеннями стратегії інноваційного розвитку ДВНЗ «УжНУ». Освітня складова забезпечує підготовку нової генерації фахівців, готових для здійснення інноваційної, навчальної, дослідницької, управлінської діяльності з урахуванням сучасних національних та світових тенденцій розвитку кібербезпеки. Згідно з концепцією, місією ДВНЗ «УжНУ» є не тільки підготовка висококваліфікованих фахівців для Закарпатського

регіону, але і приведення її у відповідність до викликів сучасності на шляху до інтеграції у європейську і світову спільноту. Концепція дає змогу реалізувати цю стратегію в контексті транскордонного співробітництва.

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

Робоча група постійно аналізує результати опитування здобувачів ВО (https://www.uzhnu.edu.ua/uk/infocentre/50180) та обговорює їх (http://teib.info/?p=6211). Крім того, до складу робочої групи входить представник здобувачів Білич Ю.О, яка аналізує, систематизує та представляє поточні побажання здобувачів ВО. Напр., у даній ОП враховані їх інтереси отримувати знання, вміння та навички щодо впровадження та застосування сучасних технологій кібербезпеки, а також розробки технологій і засобів захисту інформації та проектування систем і комплексів забезпечення кібербезпеки (цілі даної ОП). Пропозиції здобувачів також обговорювались під час круглого столу (https://cutt.ly/7wcMvN9d) і були враховані при формуванні ПРН14 та ПРН25 даної ОП, а також виборі професійної спрямованості ОП згідно стандарту "Фахівець сфери захисту інформації" (протокол №2 засідання робочої групи).
Після вивчення курсу в системі освітнього контенту Moodle УжНУ здобувачі мають можливість проходити опитування щодо змістового наповнення окремого навчального курсу та ефективності його використання при вивченні дисципліни. Результати опитування аналізуються викладачами відповідних навчальних дисциплін та обговорюються на засіданні кафедри.
Інтереси та пропозиції випускників спеціальності Кібербезпека попередніх років вивчаються через онлайн-опитування (http://surl.li/iubhk). Також найактивніші випускники були запрошені на одне із засідань робочої групи (протокол №3), а їх побажання враховані у формулюванні ПРН24 та удосконаленні навчального плану даної ОП.

- роботодавці

При оновленні ОП "Безпека інформаційних і комунікаційних систем" було враховано пропозиції потенційних роботодавців (Закарпатська ОВА, Управління Держспецзв'язку в Закарпатській області, Департамент кіберполіції НПУ, ТОВ «Спецтелеком»). Адміністрація цих організацій періодично зустрічається з робочою групою ОП, викладачами кафедри та здобувачами ОП (наприклад, http://teib.info/?p=5915 , http://teib.info/?p=5810 та https://carpathia.gov.ua/news/oleksandr-patskan-zavitav-na-lektsiiu-do-maibutnikh-fakhivtsiv-z-kiberbezpeky). Пропозиції роботодавців щодо набуття здобувачами ВО навичок командної роботи та здатності розв'язувати задачі дослідницького та інноваційного характеру у сфері інформаційної та/або кібербезпеки відображено в цілях даної ОП, а побажання щодо практичної та дослідницької складової підготовки здобувачів ВО враховано в робочих програмах науково-дослідної у сфері безпеки інформаційних і комунікаційних систем (ОК10) та переддипломної практик (ОК11) для забезпеченням необхідних результатів навчання, зокрема ПРН3, ПРН19, ПРН20, ПРН23. Також за рекомендаціями потенційних роботодавців (Управління Держспецзв'язку в Закарпатській обл., Закарпатська обласна та районні державні адміністрації) робочою групою ОП акцентовано важливість підготовки здобувачів у галузі розподілених інформаційних систем (ПРН24) з фокусом на безпеці інформаційно-комунікаційних систем, що забезпечується передусім ОК7 - ОК10 (протокол №3).

- академічна спільнота

Розробка освітньої програми супроводжувалася консультаціями та обговореннями в академічному середовищі, зокрема за участі провідних науковців Національного авіаційного університету, Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Інституту проблем реєстрації інформації НАН України (http://teib.info/?p=6190). Інтереси академічної спільноти відображені в компетенціях та результатах навчання, спрямованих на підготовку висококваліфікованого фахівця, здатного знаходити, аналізувати, оцінювати та використовувати інформацію з різних джерел, необхідну для розв'язання професійних завдань (ПРН6, ПРН9, ПРН11), застосовувати здобутки фундаментальних і прикладних наук для аналізу та комп'ютерного моделювання у сфері інформаційної безпеки та/або кібербезпеки (ПРН2, ПРН5, ПРН21), дотримуватися принципів академічної доброчесності під час навчання і дослідницької діяльності (ПРН3, ПРН17, ПРН18). Ці інтереси та пропозиції академічної спільноти забезпечуються ОК 3 (Наукові комунікації та основи наукових досліджень у сферах кіберзахисту і технічного захисту інформації) та комплексом професійно-орієнтованих дисциплін, а також залученням здобувачів ВО до науково-дослідної у сфері безпеки інформаційних і комунікаційних систем (ОК10) та переддипломної практик (ОК11), виконання кваліфікаційної роботи, участі у наукових конференціях, актуальних для забезпечення інформаційної безпеки в Україні загалом та в Закарпатській області зокрема.

- інші стейкхолдери

Базові документи ДВНЗ "УжНУ" вказують на пріоритетність залучення стейкхолдерів як до формування освітніх програм так і до їх корекції. Напр, в УжНУ відбулася нарада учасників освітнього проекту, що базувалася на ідеї необхідності внесення змін до базових програм підготовки фахівців з кібербезпеки (https://cutt.ly/3wc8KJkR). Метою зустрічі стало навчання студентів спеціальності Кібербезпека на основі базових вимог сертифікату CISSP, діючого законодавства, сучасних світових методологій, посадових інструкцій та практичної підготовки. Закладені базові принципи підготовки фахівців за міжнародними стандартами відображено в ПРН1, ПРН7, ПРН17 та ПРН20 даної ОП. При формуванні ПРН, фахових компетентностей і спрямованості ОП згідно з діючими професійними стандартами були враховані побажання працівників Закарпатської військової адміністрації (зокрема заступника голови ЗОВА О.М. Пацкана), Департаменту кіберполіції НПУ та членів ГО «Асоціація спеціалістів кібербезпеки», які активно долучилися до обговорення ОП. Напр., враховано побажання стейкхолдерів поглибити професійну підготовку здобувачів у галузі безпеки розподілених інформаційних систем та приділити увагу вивченню питання

виникнення та протидії кібербулінгу у молодіжному середовищі (додано відповідні ОК та ВК даної ОП). Крім того, проект даної ОП обговорювався також на засіданнях науково-технічної ради з питань інформатизації та електронного урядування Закарпатської ОДА, оскільки до її складу входять гарант, члени робочої групи та викладачі даної ОП (https://cutt.ly/Rwc8KEIW).

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

Під час формулювання мети та ПРН цієї ОП було враховано тенденції розвитку спеціальності 125 Кібербезпека та захист інформації, а також вакансій ринку праці. Головною ціллю навчання за ОП, яка акредитується, є формування компетентностей, необхідних для виконання професійних обов'язків майбутніми фахівцями, враховуючи вимоги професійного стандарту «Фахівець сфери захисту інформації». Розробка і впровадження ефективних систем захисту інформації і протидії кіберзагрозам, надання рекомендацій щодо запобігання та розслідування кіберінцидентів в інформаційній інфраструктурі потребує спеціалістів зі специфічними компетентностями (що формуються при підготовці за даною ОП), здатних застосовувати кращі практики, методи і засоби технічного та криптографічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури (ПРН даної ОП, що відповідають діючим освітньому і професійним стандартам).
Згідно із аналітичними оглядами ринку праці США у галузі кібербезпеки (https://cybersecurityventures.com/jobs/) відбувається значне зростання попиту (350% за 8 років спостережень) і ця тенденція зберігатиметься принаймні до 2025 р. Моніторинг вакансій ринку праці в Україні також виявив потребу у фахівцях такого профілю. Крім цього, найближчим часом варто очікувати сталого зростання потреби у фахівцях із кібербезпеки як у зв'язку із цифровою трансформацією державного управління, так і з потребою ефективно протистояти постійним кібератакам на українські інформаційні ресурси з боку держави – агресора.

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

Формулювання цілей, особливостей та ПРН даної ОП здійснено з урахуванням унікального географічного положення Закарпатської області, яка межує з чотирма країнами ЄС, в контексті міжнародного співробітництва. Така специфіка регіону потребує застосування суб'єктами транскордонного співробітництва держав-сусідів єдиного підходу та узгоджених спільних дій у сфері надання електронних інфокомунікаційних послуг, розбудови інформаційної та комунікаційної транскордонної інфраструктури в умовах ризику стороннього кібернетичного впливу.
ДВНЗ «УжНУ» є єдиним ЗВО в Закарпатській області, що готує фахівців за спеціальністю 125 Кібербезпека на першому (бакалаврському) та другому (магістерському) рівнях ВО. Тісна взаємодія між УжНУ та бізнес-структурами, ІТ-компаніями є необхідною умовою для формування якісно нової робочої сили, покращення ситуації на ринку праці. Тільки в Закарпатському ІТ-кластері, який активно співпрацює з ДВНЗ "УжНУ" (https://cutt.ly/Jwc837VH) і об'єднує понад 20 офіційно зареєстрованих ІТ-компаній (http://life.ko.net.ua/?p=147546) зайнято тисячі фахівців.
На ринку праці зростає кількість вакансій для пентестерів, аналітиків та архітекторів кібербезпеки, інженерів безпеки програмного забезпечення у різних сферах діяльності (наприклад, https://jobs.dou.ua/vacancies/?category=Security).
Цілі та ПРН даної ОП віддзеркалюють компетентності, визначені в стандарті ВО, і стан запитів ІТ-ринку праці регіону, оскільки включають і відображають галузевий контекст і стратегію розвитку регіону.

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 програмних результатів навчання представленої ОП було враховано досвід аналогічних вітчизняних освітніх програм другого (магістерського) рівня вищої освіти, а саме: ОПП «Безпека інформаційних і комунікаційних систем» Національного авіаційного університету (29.04.2021 р.), https://cutt.ly/0wc87HAh, ОПП «Безпека інформаційних і комунікаційних систем» Харківського національного університету радіоелектроніки (03.06.2021 р.), https://cutt.ly/lwc873qk та недавно акредитованої ОПП «Безпека інформаційних і комунікаційних систем» Національного університету «Львівська політехніка» (29.06.2021 р), https://cutt.ly/Ewc85pqg.
Серед іноземних освітніх програм, доступних для ознайомлення, використано досвід: Champlain College (USA) (https://cutt.ly/mwc85zii) та International University of Applied Sciences (Germany) (https://cutt.ly/Pwc85RQ4). Також враховано рекомендації найбільшого у світі освітнього та наукового обчислювального товариства ACM, що формує рекомендації (https://cutt.ly/4wc85LDP) щодо навчальних програм (в т.ч. освітніх програм з кібербезпеки) в умовах швидкого й мінливого розвитку ІТ.
Аналіз забезпечення фахових компетентностей та програмних результатів навчання у ОП вищезгаданих ЗВО та міжнародних організаціях дозволив визначити підходи до формування обов'язкових та вибіркових освітніх компонент даної ОП та уточнити їх змістовне наповнення.

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

Стандарт вищої освіти України для другого (магістерського) рівня за спеціальністю 125 Кібербезпека затверджений 18 березня 2021 року. Розроблена ОП передбачає забезпечення програмних результатів навчання, визначених Стандартом (ПРН1-ПРН23), у повній мірі. Так, вивчення ОК3, а також науково-дослідної у сфері безпеки інформаційних і комунікаційних систем (ОК10) та переддипломної практик (ОК11) навчають здобувачів другого

рівня вищої освіти провадити дослідницьку та/або інноваційну діяльність у сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації (ПРН3); критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук (ПРН5). Обов'язкові компоненти ОП «Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки», "Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем", "Безпека хмарних технологій та розподілених обчислень" (ОК5 - ОК7) забезпечує здобуття ПРН6, ПРН8, ПРН10 - ПРН12, ПРН15, ПРН17. Ці результати навчання забезпечують професійні можливості здобувачів забезпечувати інформаційну безпеку та/або кібербезпеку об'єктів інформаційної діяльності та критичної інфраструктури; забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів; досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам та попереджувати їх. ОК2 забезпечує ПРН1, ПРН5, ПРН17, які формують навички представлення і обговорення результатів досліджень та інновацій, автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, вміння аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання, а також супроводжувати та контролювати роботу з персоналом щодо інформаційної безпеки та/або кібербезпеки (ПРН18). ОК10 та ОК11 сприяють досягненню програмних результатів ПРН3, ПРН5, ПРН6, ПРН11, ПРН14 - ПРН16, ПРН19 - ПРН21 та ПРН23. Задля повного забезпечення ПРН 1 введено ОК 1 Іноземна мова для професійної діяльності під час оновлення цієї ОП з метою усунення недоліків виявлених в процесі попередньої акредитації.
Обов'язкові компоненти ОК4 - ОК5 забезпечують досягнення здобувачами ПРН3, ПРН4, ПРН13, ПРН21, ПРН25, що стосуються криптографічного аспекту забезпечення кібербезпеки; фізичних та математичних методів і моделей в сфері інформаційної безпеки та/або кібербезпеки; впровадження результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого ПЗ.
Закладені в ОП програмні результати навчання, загальні та фахові компетентності досягаються належним формуванням взаємодоповнюючих обов'язкових і вибіркових компонент ОП, а також видами і змістовним наповненням практик.

Якщо стандарт вищої освіти за відповідною спеціальністю та рівнем вищої освіти відсутній, поясніть, яким чином визначені ОП програмні результати навчання відповідають вимогам Національної рамки кваліфікацій для відповідного кваліфікаційного рівня?

Стандарт вищої освіти України для другого (магістерського) рівня за спеціальністю 125 Кібербезпека затверджений 18 березня 2021 року.

2. Структура та зміст освітньої програми

Яким є обсяг ОП (у кредитах ЄКТС)?

90

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

67

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

23

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

Зміст ОП повністю відповідає предметній області спеціальності, дана ОП розроблена з дотриманням вимог Стандарту ВО за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти галузі знань 12 «Інформаційні технології» з орієнтацією на українські та міжнародні стандарти в сфері кібербезпеки. Метою даної ОП є навчання та підготовка фахівців, які мають знання, вміння та навички щодо впровадження та застосування сучасних технологій кібербезпеки, а також розробки технологій і засобів захисту інформації та проектування систем й комплексів забезпечення кібербезпеки; фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки.
Програма передбачає вивчення законодавчої, нормативно-правової бази України та вимог міжнародних стандартів і практик щодо здійснення професійної діяльності (наприклад, ОК 6 «Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки»); принципів створення, застосування та супроводу систем і комплексів інформаційної та/або кібербезпеки, а також систем, комплексів та засобів кіберзахисту, технологій створення та використання спеціалізованого програмного забезпечення (ОК 7 "Безпека хмарних технологій та розподілених обчислень", ОК 8 "Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем"); методів та засобів оцінювання захищеності інформації, аудиту та моніторингу ефективності функціонування інформаційних систем і технологій (ОК 9 "Моніторинг та аудит інформаційно-комунікаційних систем"); теорії, технологій, фізичних та математичних методів і моделей в сфері інформаційної безпеки та/або кібербезпеки, а

також методів та засобів криптографічного і технічного захисту інформації (ОК 3 “Наукові комунікації та основи наукових досліджень у сферах кіберзахисту і технічного захисту інформації”, ОК 4 “Методи побудови та аналізу криптосистем”, ОК 5 “Математичне моделювання процесів та систем у сфері захисту інформації”).
Дана ОП складається із 12 обов'язкових ОК, які у сукупності покривають перелік усіх компетентностей (1 інтегральна, 6 загальних і 11 фахових компетентностей), що відповідають предметній області спеціальності 125 Кібербезпека та захист інформації. Теоретична спрямованість ОП висвітлюється в ОК4-ОК9 (обов'язкові ОК професійної підготовки). Практичні навички здобуваються при виконанні практичних і лабораторних робіт, проходженні науково-дослідної у сфері безпеки інформаційних і комунікаційних систем (ОК10) та переддипломної практик (ОК11), а також під час виконання та захисту кваліфікаційної роботи магістра (ОК12).

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

Процедура вибору здобувачами ВО індивідуальної освітньої траєкторії регламентується «Положенням про навчання студентів за індивідуальним графіком» (https://cutt.ly/QwcHSVX5), «Положенням про організацію освітнього процесу» (https://cutt.ly/iwcHHc8V) та «Положенням про індивідуальний план здобувача ВО» (https://cutt.ly/QwcHH2dp). Індивідуальна освітня траєкторія здобувача реалізується через: вільний вибір навчальних дисциплін; формування індивідуального навчального плану; складання індивідуальних графіків навчання; широких можливостей навчання в регіональній Академії Cisco, що діє при кафедрі ТЕІБ; дистанційну освіту; участь у програмах академічної мобільності в українських та іноземних ЗВО; право на академічну відпустку; визнання результатів навчання, отриманих в інших ЗВО та у неформальній освіті; вибір теми кваліфікаційної роботи. При розробці навчальних планів формування каталогу вибіркових компонент здійснюється відповідно до «Положення про реалізацію здобувачами вищої освіти права на вільний вибір навчальних дисциплін в ДВНЗ «УжНУ» (https://cutt.ly/7wcHKJO4). Індивідуальна освітня траєкторія відображається в індивідуальному навчальному плані здобувача та передбачає можливість індивідуального вибору навчальних дисциплін у межах, передбачених відповідною ОП та робочим навчальним планом (в обсязі, що становить не менш як 25 % загальної кількості кредитів ЄКТС, передбачених для відповідного рівня вищої освіти), з дотриманням послідовності їх вивчення відповідно до структурно-логічної схеми підготовки фахівця.

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

Своє право на вибір навчальних дисциплін здобувачі ВО за даною ОП можуть реалізувати відповідно до «Положення про порядок реалізації здобувачами вищої освіти права на вільний вибір навчальних дисциплін у ДВНЗ «УжНУ»» (https://www.uzhnu.edu.ua/uk/infocentre/get/22963).
Згідно з положенням, здобувач може реалізувати своє право шляхом вибору:
- дисципліни або спеціалізованого блоку дисциплін із каталогу вибіркових дисциплін освітньої програми, за якою навчається здобувач (https://www.uzhnu.edu.ua/uk/infocentre/50191);
-із обов’язкових або вибіркових дисциплін навчального плану іншої ОП того ж рівня вищої освіти;
- дисципліни навчального плану іншої ОП іншого рівня вищої освіти (за обов’язковим погодженням декана факультету, де реалізується ОП, з навчального плану якої обрана дисципліна);
- дисципліни із загальноуніверситетського каталогу вибіркових дисциплін (https://www.uzhnu.edu.ua/uk/infocentre/40666);
- навчальних дисциплін в іншому ЗВО в рамках реалізації права здобувача на академічну мобільність.
Для реалізації здобувачами права на вільний вибір навчальних дисциплін деканат факультету ознайомлює здобувачів з порядком, термінами та особливостями запису і формування груп для вивчення вибіркових компонент ОПП. Студенти можуть ознайомитися з робочими програмами дисциплін та їх розширеними анотаціями (https://www.uzhnu.edu.ua/uk/infocentre/50191). Здобувачі вищої освіти після ознайомлення із запропонованими матеріалами самостійно формують перелік вибіркових компонентів ОП для свого індивідуального навчального плану і реєструються на вибіркові дисципліни на листі реєстрації. На підставі листів реєстрації деканат здійснює попереднє формування груп для вивчення окремих вибіркових навчальних дисциплін. Остаточне формування груп здійснюється розпорядженням декана, після чого інформація про вибіркові дисципліни вноситься до індивідуального навчального плану здобувача. Вибрані здобувачами навчальні дисципліни вносяться до робочих навчальних планів і визначають науково-педагогічне навантаження кафедри та конкретного наукового-педагогічного працівника. Кафедри оновлюють перелік вибіркових дисциплін з урахуванням кон’юнктури ринку праці, інтересів і побажань роботодавців і здобувачів. Вибір навчальних дисциплін здійснюється здобувачем вищої освіти у межах, які передбачені ОПП та навчальним планом і складає 25 % від загальної кількості кредитів ЄКТС.

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

Проведення практики здобувачів вищої освіти регламентується Положенням про практику студентів ДВНЗ «УжНУ» (https://cutt.ly/IwcJqLU8). ОП передбачає виконання завдань практичних і лабораторних робіт, проходження науково-дослідної у сфері безпеки інформаційних і комунікаційних систем (4,5 кредита) та переддипломної практик (10,5 кредитів), а також виконання та захист кваліфікаційної роботи магістра (19,5 кредитів). Під час проходження практик формуються компетентності КЗ 1-3, КЗ 6, КФ1-3, КФ5-8, КФ10 (що відповідають Стандарту ВО) та ЗК.01-ЗК.07, Б4, Д1-Д2, Е1-Е4 (що відповідають професійному стандарту “Фахівець сфери захисту інформації”).
Роботодавці беруть активну участь в організації та проведенні практик для здобувачів ВО за даною ОП, керують проходженням їх практик, надають інформацію для написання звітів із практик.
Базами практик є кіберполігон і науково-навчальні лабораторії кафедри ТЕІБ, ТОВ “Флекстронікс”, ТОВ «Спецтелеком» та інші організації. Нещодавно також підписано Меморандуми про співпрацю ДВНЗ “УжНУ” з компанією DAI Global LLC та Департаментом кіберполіції Національної поліції України (https://cutt.ly/fwcJrqro).

Заплановано підписання меморандуму про співпрацю з Управлінням держспецзв'язку у Закарпатській області. Кафедра постійно працює над розширенням списку ІТ-компаній-партнерів. Як свідчать результати опитування, студенти задоволені набутими під час практик практичними знаннями і вміннями (https://cutt.ly/ywcJrNoU).

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

Навчання за ОП дає змогу забезпечити набуття здобувачами соціальних навичок (soft skills) упродовж усього періоду навчання. Такі навички відображено у загальних та фахових компетентностях, набуття яких забезпечується насамперед ОК1, ОК2, ОК3, ОК10, ОК11, ОК12 що сприяють розвитку широкого світобачення, здатності логічно мислити, провадити науково-педагогічну діяльність, ефективно працювати з персоналом та представниками інших професійних груп, знань англійської мови у здобувачів ВО. Формуванню вищезгаданих компетентностей сприяє досягнення ПРН1-ПРН2, ПРН15, ПРН17-ПРН18. Враховуючи рекомендації ГЕР під час попередньої акредитаційної експертизи, ОК2 і ОК3 було доповнено темами, які забезпечують формування професійних соціальних навичок за спеціальністю.
Набуттю соціальних навичок сприяють також ряд вибіркових навчальних дисциплін із загальноуніверситетського каталогу (https://www.uzhnu.edu.ua/uk/infocentre/get/55451), наприклад "Англійська мова для професійної комунікації (у галузі інформаційних технологій)", "Бізнес-етика та ділові комунікації", "Соціальна відповідальність та корпоративна культура".
Процес формування «soft skills» реалізується за допомогою таких методів і техніки навчання як робота в команді, розробка презентацій та підготовка доповідей. Уміння спілкуватися, обговорювати загальні та професійні проблеми також розвивається під час проходження практик і захисті кваліфікаційної роботи магістра. Крім того, УжНУ періодично проводить заходи, що сприяють формуванню «soft skills» (напр, https://cutt.ly/uwcJo5Bb).

Яким чином зміст ОП ураховує вимоги відповідного професійного стандарту?

ОП розроблена у повній відповідності до стандарту ВО за спеціальністю 125 Кібербезпека для другого (магістерського) рівня, затвердженого й уведеного в дію наказом МОН України від 18.03.2021 р. № 332, із врахуванням професійного стандарту «Фахівець сфери захисту інформації», затвердженого наказом Адміністрації Держспецзв'язку України 25 листопада 2022 року № 715. Згідно з цим професійним стандартом навчання на магістерському рівні за спеціальністю 125 Кібербезпека та захист інформації є первинною професійною підготовкою для отримання професійних кваліфікацій "Провідний фахівець сфери захисту інформації" та "Системний фахівець сфери захисту інформації" за умови забезпечення під час навчання відповідних професійних компетентностей (Б4, Д та Е), які визначають трудові функції "Оцінювання відповідності засобів КЗІ", "Унормування системи технічного і криптографічного захисту інформації" та "Координація діяльності з технічного та криптографічного захисту інформації".
Задля забезпечення цих компетентностей даною ОП уточнено зміст ОК і додано матрицю відповідності загальних та професійних компетентностей фахівця сфери захисту інформації (за професійним стандартом) компонентам ОП. Відповідні цим професійним компетентностям ПРН1, ПРН7, ПРН15, ПРН18 та ПРН25 повністю забезпечуються освітніми компонентами із урахуванням мети і особливостей даної ОП.

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

Організація освітнього процесу регламентується «Положенням про організацію освітнього процесу в ДВНЗ «УжНУ» (https://cutt.ly/iwcHHc8V), в якому зазначено, що організація освітнього процесу здійснюється відповідно до ЄКТС. Рекомендована структура кредиту ЄКТС для другого (магістерського) рівня становить, як правило, 33 % аудиторних занять.
Загальне навантаження за даною ОП становить 2700 год. (90 кредитів ЄКТС), з яких на аудиторну роботу припадає 634 год (21,1 кредити ЄКТС), або 23,5 % від загальної кількості годин. За навчальним планом розподіл аудиторних годин здійснюється на лекції – 290 год (45,7 % від загальної кількості аудиторних годин), лабораторні та практичні заняття - 344 год (54,3 %). На СР здобувача відведено 1376 год (45,9 кредитів ЄКТС), що становить 50,9 % від загального навантаження. Індивідуальна робота під керівництвом викладача (курсова робота, практики, кваліфікаційна робота) – 690 годин (23 кредити ЄКТС, або 25,6 % від загального навантаження). Щотижневе аудиторне навантаження – 18-19 годин. Такий розподіл забезпечує баланс між дисциплінами, відображає практичне спрямування ОПП та індивідуалізацію освітньої траєкторії. З метою покращення організації самостійної роботи та забезпечення постійної комунікації студента з викладачем, окрім живого спілкування, використовуються електронні ресурси й технології: електронна пошта, система електронного навчання Moodle УжНУ, месенджери та інші сучасні методи спілкування, що є особливо актуальним під час змішаної форми навчання

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

Дуальна освіта не впроваджена.

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

https://www.uzhnu.edu.ua/uk/cat/abiturient/master_degree

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

Правила прийому до ДВНЗ "УжНУ" у 2023 році розроблені Приймальною комісією відповідно до Порядку прийому на навчання для здобуття вищої освіти в 2023 році (https://www.uzhnu.edu.ua/uk/infocentre/57409). Розроблені Правила прийому схвалені Вченою радою ДВНЗ "УжНУ" та введені в дію наказом ректора. Детальну інформацію про умови вступу для здобуття освітнього ступеня магістра (на основі ОС бакалавр, магістр або ОКР спеціаліст) можна отримати за посиланням https://cutt.ly/BwcJEA7X.
У 2023 році конкурсний відбір проводиться за результатами Єдиного вступного іспиту (ЄВІ) та фахового іспиту у ДВНЗ "УжНУ", програму якого можна знайти у відповідному каталозі (https://www.uzhnu.edu.ua/uk/infocentre/2108). Підготовку тестових завдань для вступних випробувань організовує голова фахової атестаційної комісії. Тестові завдання розробляються на основі результатів навчання за ОП спеціальності 125 Кібербезпека та захист інформації першого (бакалаврського) рівня ВО - "Безпека інформаційних і комунікаційних систем" та "Системи технічного захисту інформації". Таким чином, програма фахового вступного випробування враховує особливості даної ОП. Також вступити на дану ОП можна на основі НРК6 або НРК7, здобутого за іншою спеціальністю (напрямом підготовки), за умови успішного проходження вступних випробувань. Необхідність здачі фахового іспиту забезпечує наявність необхідних теоретичних знань та підґрунтя для навчання за даною ОП.

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

Згідно Положення про академічну мобільність студентів у ДВНЗ «Ужгородський національний університет» (https://www.uzhnu.edu.ua/uk/infocentre/get/8324), надається можливість студентам брати участь у навчальному процесі іншого вищого навчального закладу (в Україні або за кордоном), проходити навчальну, виробничу або переддипломну практику чи проводити наукові дослідження з можливістю перезарахування в установленому порядку освоєних навчальних дисциплін чи практик. З порядком визнання (перезарахування) кредитів ЄКТС для учасників програм академічної мобільності можна ознайомитися за посиланням
https://www.uzhnu.edu.ua/uk/infocentre/get/21266
Крім того, згідно Положення про порядок перезарахування результатів навчання та визначення академічної різниці в ДВНЗ "УжНУ" (https://www.uzhnu.edu.ua/uk/infocentre/get/28875), надається можливість перезарахування результатів навчання при переведенні з інших закладів вищої освіти на навчання до ДВНЗ «УжНУ». Усі документи, що регламентують можливості академічної мобільності студентів, порядок визнання кредитів ЄКТС та перезарахування результатів навчання, розміщені у відкритому доступі на вебсторінці "Академічна мобільність студентів" (https://www.uzhnu.edu.ua/uk/infocentre/21265) сайту ДВНЗ "УжНУ".

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

На цій ОП вказані правила не застосовувались

Яким документом ЗВО регулюється питання визнання результатів навчання, отриманих у неформальній освіті? Яким чином забезпечується його доступність для учасників освітнього процесу?

Визнання результатів навчання, отриманих у неформальній освіті регламентується Положенням про порядок визнання в Державному вищому навчальному закладі «Ужгородський національний університет» результатів навчання, здобутих у неформальній освіті (https://www.uzhnu.edu.ua/uk/infocentre/get/22966). Згідно з положенням університет може визнати результати навчання, здобуті у неформальній освіті, обсяг яких, як правило, не перевищує 10% загального обсягу кредитів ЄКТС за ОП. Процедура визнання результатів навчання визначається пп. 2.7-2.19 Положення. Зазначений документ знаходиться у відкритому доступі на сайті ЗВО. Зарахування результатів неформальної освіти здійснюється на добровільній основі та передбачає підтвердження того, що здобувач вищої освіти досяг часткових результатів навчання, передбачених ОП, за якою він навчається.
Загальноприйнято, що сертифікат на рівні не нижче В2+ дає право на зарахування з максимальною оцінкою дисципліни «Іноземна мова для професійної діяльності» з навчального плану здобувача другого (магістерського) рівня вищої освіти.

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

За час дії ОП «Безпека інформаційних і комунікаційних систем» випадків визнання результатів навчання, отриманих у неформальній освіті за «повними» освітніми компонентами не було. Проте, при оцінюванні знань та вмінь, що відповідають деяким модулям і темам певних освітніх компонент, викладачі враховують результати (підтверджені відповідними сертифікатами), що отримані у неформальній освіті. Зокрема, в ОК 6 "Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки" та ОК 9 "Моніторинг та аудит інформаційно-

комунікаційних систем" враховуються результати вивчення відповідних курсів в Cisco Networking Academy та Official Training Center MikroTik.

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 та методи навчання регламентуються Положенням про організацію освітнього процесу в ДВНЗ «Ужгородський національний університет» (https://www.uzhnu.edu.ua/uk/infocentre/get/31357). В окремих випадках (оголошення карантину, в умовах воєнного стану, тощо) освітній процес може здійснюватися в дистанційному або змішаному режимі, а ЗВО самостійно визначає способи організації й технології для дистанційного або змішаного навчання.
Починаючи з 2020 року частина навчання за даною ОП відбувається в дистанційній формі з використанням сучасних технологій, що забезпечують надання інформації в інтерактивному режимі за допомогою використання інформаційно-комунікаційних технологій: сервіси Google, система електронного навчання (https://e-learn.uzhnu.edu.ua/) та ін.
Задля досягнення програмних результатів навчання поєднуються традиційні методи навчання (лекції, лабораторні та практичні заняття, курсові проекти та магістерські кваліфікаційні роботи, науково-дослідна та переддипломна практики, презентації, індивідуальні заняття та домашня самопідготовка, консультації, заліки, екзамени) та сучасні (інтерактивні методи навчання, робота в малих групах, індивідуальні консультації). При цьому використовуються проблемно-пошукові та дослідницькі методи, робота з науковою літературою. Викладання здійснюється з активним використанням мультимедійних засобів, спеціалізованого програмного забезпечення та необхідного технічного обладнання.

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?

Положенням про організацію освітнього процесу в Державному вищому навчальному закладі «Ужгородський національний університет» (https://www.uzhnu.edu.ua/uk/infocentre/get/31357) передбачено, що організація освітнього процесу в Університеті ґрунтується на засадах студентоцентрованого навчання та компетентнісного підходу. Учасникам освітнього процесу надається інформація щодо цілей, змісту, очікуваних результатів навчання, критеріїв оцінювання у межах окремих освітніх компонент. Студентоцентрований підхід забезпечується вибором тем та керівників кваліфікаційних робіт магістра, а також баз практик. Здобувачі формують індивідуальну освітню траєкторію завдяки вільному вибору дисциплін, що передбачено Положенням про порядок реалізації здобувачами вищої освіти права на вільний вибір навчальних дисциплін у ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/22963), Положенням про індивідуальний навчальний план здобувача вищої освіти у ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/22965), Положення про навчання студентів за індивідуальним графіком у ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/20152).
Рівень задоволеності здобувачів методами навчання визначається через анкетування (https://www.uzhnu.edu.ua/uk/infocentre/50180). Результати опитування студентів обговорюються на засіданнях кафедри. За результатами анонімного анкетування, що періодично проводиться, усі здобувачі магістерського рівня вищої освіти виявили задоволеність у виборі методів навчання на цій ОП.

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

В ДВНЗ «УжНУ» використовуються принципи академічної свободи з урахуванням обмежень, встановлених законами «Про вищу освіту» (https://zakon.rada.gov.ua/laws/show/1556-18), а ЗВО, у межах своєї компетенції, гарантує її дотримання і реалізацію. Методи та форми навчання базуються на принципах свободи слова та доброчесності, поширення знань та інформації, проведення наукових досліджень і використання їх результатів. Викладач обирає ті форми та методи навчання, які вважає доцільними відповідно до дисципліни для забезпечення формування компетентностей здобувачів освіти у відповідності до мети та особливостей ОП.
Для здобувачів ВО за ОП «Безпека інформаційних і комунікаційних систем» академічна свобода реалізується через: вільний вибір тематики написання курсових проектів та магістерських кваліфікаційних робіт; формування вибіркових компонент ОП та індивідуального навчального плану; можливості презентувати результати своїх досліджень на конференціях та участь у роботі студентських наукових організацій, рад; організації самостійної роботи; вибору місць проходження практик.
Принцип академічної свободи реалізується викладачами при складанні робочих програм навчальних дисциплін, безпосередньо у їх самостійному виборі методів навчання та оцінювання, що визначаються, як правило, метою і завданнями навчальної дисципліни; змістом тем; навчальними можливостями здобувачів тощо.

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 *

Інформація про організацію освітнього процесу регламентуються Положенням про організацію освітнього процесу в

ДВНЗ «Ужгородський національний університет» (https://www.uzhnu.edu.ua/uk/infocentre/get/31357). Інформація щодо цілей, змісту та очікуваних результатів навчання, порядку та критеріїв оцінювання подається викладачами на початку викладання ОК або настановних зборах перед початком практики. Дану інформацію також розміщено в робочих програмах освітніх компонентів, які є у відкритому доступі (https://www.uzhnu.edu.ua/uk/infocentre/50191). Розклад занять, контрольних заходів та захисту кваліфікаційних робіт студенти мають у вільному доступі - https://www.uzhnu.edu.ua/uk/infocentre/206. Крім того, кожен здобувач отримує доступ до електронних ресурсів Університету з інформацією щодо обсягу, структури та очікуваних результатів навчання в межах ОК (система електронного навчання Moodle https://e-learn.uzhnu.edu.ua/). Результати поточного контролю студенти мають змогу дізнатися від лектора, а також в онлайн-журналі на сайті електронного навчання ДВНЗ «УжНУ» (система Moodle). Критерії оцінювання відповідають Положенню про організацію освітнього процесу в ДВНЗ «УжНУ» та вибираються викладачем з урахуванням особливостей навчальної дисципліни.

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

Відповідно до «Положення про організацію освітнього процесу в УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/31357), «Положення про наукове товариство студентів, аспірантів, докторантів і молодих вчених ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/9199) та «Положення про раду молодих вчених ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/5620) освітня діяльність університету ґрунтується на принципах нерозривності процесів навчання і наукових досліджень та необхідності залучення здобувачів до НДР з метою набуття ними практичного досвіду. Поєднання навчання і досліджень здобувачів ВО в межах даної ОП відбувається через залучення їх до індивідуальних тем досліджень НПП, через підтримку власних наукових ідей і проектів здобувачів ВО та через наукову тематику відповідних ОК. На кафедрі ТЕІБ виконуються такі наукові теми: НТР “Методи ланцюгових дробів у задачах криптографії та криптоаналізу” (керівник роботи проф. Пагіря М.М., державний реєстраційний №0123U100842) та НДР “Нанокомпозитні плівкові структури на основі халькогенідів та біомолекул для застосування у кібербезпеці та захисті інформації” (керівник роботи проф. Різак В.М., державний реєстраційний №0121U114176). Як правило, на основі наукових досліджень за темами кваліфікаційних робіт магістра, індивідуальних завдань чи науково-дослідної практики, здобувачі ВО готують тези доповідей та/або наукові статті. Наприклад, кращі студенти - магістри нещодавно прийняли участь XII Міжнародній науково-технічній конференції ITSEC-2023, що проходила на базі ДВНЗ “УжНУ” (https://mediacenter.uzhnu.edu.ua/news/pro-kiberbezpeku-v-konteksti-vijny-ta-pidhotovku-fakhivtsiv-dyskutuvaly-na-mizhnarodnij-konferentsii-itsec-bezpeka-informatsijnykh-tekhnolohij/2023-05-09-55660). Презентовані тут студентські доповіді опубліковано у збірнику тез ITSEC-2023 (http://bit.nau.edu.ua/wp-content/uploads/2023/05/2023-ITSec_zbirnyk-1.pdf), наприклад: Л. Боценюк, Ю. Матьовка. Віддалений контроль і захист персонального комп'ютера від несанкціонованого доступу на основі телеграм бота; М. Пригара, І. Опірський, М. Різак. Оцінка виявлених ризиків інформаційної безпеки в освіті в умовах надзвичайних ситуацій; Б. Маліцький, О. Черепов, В. Буковецький, В. Різак. Полігон для проведення комплексних навчань з багаторівневого захисту від кібератак.
Усі здобувачі магістерського рівня ВО беруть участь у науково-практичній конференції “Інформаційні технології у житті студентів та молодих науковців Закарпаття” Ця конференція проводиться кожні 2 роки, а її організатором є відповідальна за підготовку здобувачів в межах даної ОП кафедра ТЕІБ. З програмою, матеріалами конференції та нагородами для авторів кращих робіт можна ознайомитись на сайті кафедри ТЕІБ (наприклад ІКТ-2021 http://teib.info/?page_id=4467, ІКТ-2019 http://teib.info/?page_id=4467).

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

Згідно “Положення про організацію освітнього процесу в ДВНЗ “УжНУ” (https://cutt.ly/iwcHHc8V) робоча програма навчальної дисципліни (РПНД) розробляється на термін до 5 років і повністю оновлюється у випадках зміни стандартів ВО, затвердження нової редакції ОП та внесення змін до навчального плану, технології навчання. Оскільки оновлення даної ОП відбулося недавно (з метою усунення зауважень попередньої акредитаційної експертизи та врахування поточних зауважень стейкхолдерів), то РПНД також було повністю оновлено чи замінено внаслідок впровадження нових дисциплін. Разом з цим зміст окремих ОК коригується на основі сучасних наукових досягнень в галузі (основним інструментом для цього є власні наукові дослідження та досвід участі НПП в міжнародних конференціях, круглих столах, семінарах), а також на основі імплементації зарубіжного досвіду та сучасних практик (за результатами міжнародних стажувань, взаємодії із стейкхолдерами та підвищення кваліфікації НПП, що забезпечують ОК).
Напр., на основі власних наукових досягнень (Пригара М.П. Захищена система технічної підтримки процесів дистанційного волевиявлення : автореф. дис. на здобуття наук. ступ. к.т.н.: спец. 05.13.21 „Системи захисту інформації”, статті у фахових виданнях) доц. Пригара М.П. доповнив зміст ОК 8 “Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем” темами, що присвячені питанням розробки, впровадження та експлуатації захищених ІКС під час дистанційного волевиявлення. Проф. Пагіря М.М. оновив зміст ОК 4 “Методи побудови та аналізу криптосистем”, доповнивши науковими досягненнями здобутими під час виконання НПП кафедри НТР “Методи ланцюгових дробів у задачах криптографії та криптоаналізу”. Проф. Давиденко А.М., що забезпечує ОК 7 “Безпека хмарних технологій та розподілених обчислень”, розробив програму цієї дисципліни, частково використовуючи результати власних наукових досліджень, отриманих ним у дисертації (Давиденко А.М. Методи та моделі адаптивного захисту та розмежування доступу до розподілених інформаційних ресурсів - Дис. на здобуття наук. ступ. д.т.н. за спец. 05.13.21 – «Системи захисту інформації»). Також на основі сучасних практик у відповідних галузях оновлено зміст навчальних дисциплін, а саме: ОК 2 “Методика викладання фахових дисциплін у вищій школі” (проф. Різак В.М., на основі власного наукового досвіду, а також підвищення кваліфікації в ЗІППО, "Інноваційні методи навчання у закладі вищої освіти", 2022 р та стажування в Університеті ім. Шафарика, Erasmus+ Mobility - Staff Training, 2023 р); ОК 9 розроблено та викладається із залученням курсів "CCNA Cybersecurity Operations" та “CyberOps Associate” Cisco Academy (доц. Чобаль О.І., сертифікований інструктор

Мережевої академії Cisco); ВК “Системи захисту мовної інформації на об’єктах інформаційної діяльності” та “Оптоволоконні комунікаційні системи” оновлено на основі власного практичного досвіду і професійних досягнень (Маркевич П.В., начальник Управління ДССЗЗІ в Закарпатській обл).

Опишіть, яким чином навчання, викладання та наукові дослідження у межах ОП пов’язані із інтернаціоналізацією діяльності ЗВО

Інтернаціоналізація діяльності ЗВО регламентується Стратегією інтернаціоналізації ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/20139). На жаль, через Covid-пандемію та обмеження перетину кордону в умовах воєнного стану міжнародна активність учасників освітнього процесу в межах ОП дещо знизилась і частково перейшла в онлайн режим. Однак кафедра ТЕІБ і надалі залишається одним із лідерів інтернаціоналізації діяльності в УжНУ. Викладачі кафедри періодично проводять наукові дослідження та підвищують кваліфікацію (https://www.uzhnu.edu.ua/uk/infocentre/50190) в європейських закладах. Приймаючи участь у міжнародному проекті ACCELERATE (https://cordis.europa.eu/project/id/731112) НПП проводили закордонні наукові дослідження, а студенти - відвідали зимову школу NESY в Австрії (http://teib.info/?p=4025). Кафедра ТЕІБ впродовж майже 20 років є постійним організатором практик університетами Словаччини (наприклад, http://teib.info/?page_id=2649). Інтернаціоналізація ОП реалізується також через можливість проходження магістрами ВК “Захист комунікаційних мереж засобами Cisco” англійською мовою на основі Cisco Networking Academy із зарахуванням результатів навчання, а викладачі ОП (доц. Петрушко І.А., доц. Чобаль О.І.) є сертифікованими інструкторами Cisco. Усі студенти безкоштовно мають можливість здобувати додаткову неформальну освіту та отримувати професійні сертифікати Cisco, які визнаються провідними роботодавцями, і успішно конкурувати на міжнародному ринку праці.

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

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

Оцінювання результатів навчання і контроль здійснюється відповідно до «Положення про організацію освітнього процесу в ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/31357). Контрольні заходи поділяються на модульний і підсумковий семестровий контроль. Модульний контроль складається з поточного контролю та модульного контрольного оцінювання. Форми поточного та модульного контрольного оцінювання обираються розробником робочої програми навчальної дисципліни. Підсумковий семестровий контроль проводиться згідно із «Положенням про порядок та методику проведення семестрових екзаменів та заліків» (https://www.uzhnu.edu.ua/uk/infocentre/get/5952). Форми підсумкового контролю кожного компонента висвітлені у ОП, робочих програмах навчальних дисциплін (https://www.uzhnu.edu.ua/uk/infocentre/50191) та у навчальних планах (https://www.uzhnu.edu.ua/uk/infocentre/50186)
З метою всебічного оцінювання ПРН здобувачів ВО застосовується усний (індивідуальне, фронтальне опитування, співбесіда, презентація, виступ ін.) та письмовий контроль або їх комбінація (тестування; виконання індивідуальних завдань, творчої роботи, аналітичного дослідження для перевірки сформованості інтегральної компетентності), комп’ютерний контроль, у т .ч. тестове опитування, що використовується для об’єктивізації оцінювання, самоконтроль – для розвитку у здобувачів уміння оцінювати свої досягнення.
Екзаменаційні білети з кожної дисципліни затверджуються на засіданнях кафедри. Захист практик (ОК 10, ОК 11) відбувається шляхом написання звіту про практичну роботу, заповнення щоденника практики та захисту проведеної роботи.
Атестація здобувачів проводиться у формі публічного захисту кваліфікаційної роботи магістра (ОК 12). На захист кваліфікаційних робіт запрошуються представники стейкхолдерів-роботодавців регіону, що забезпечує оцінку досягнення ПРН не лише академічною спільнотою, а і фахівцями-практиками.
Зазначені форми контрольних заходів у межах навчальних дисциплін ОП дозволяють перевірити досягнення програмних результатів навчання.

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

Чіткість та зрозумілість форм контрольних заходів та критеріїв оцінювання навчальних досягнень у межах навчальних дисциплін ОП забезпечена «Положенням про організацію освітнього процесу в ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/31357).
Результати екзаменів і диференційованих заліків оцінюються за 100-бальною шкалою, диференційованою шкалою («відмінно», «добре», «задовільно», «незадовільно») та шкалою ЄКТС, а заліків - за 100-бальною шкалою, недиференційованою («зараховано», «незараховано») та шкалою ЄКТС. Критерії оцінювання результатів навчання здобувачів освіти на екзаменах та заліках визначаються робочими програмами навчальних дисциплін, що розміщені у вільному доступі на сайті ЗВО (https://www.uzhnu.edu.ua/uk/infocentre/50191). Структурування ОК за видами робіт і ваговими коефіцієнтами та зміст контрольних завдань і критерії їх оцінювання висвітлюються в робочих програмах навчальних дисциплін. Впродовж семестру НПП контролюють хід виконання здобувачами планових завдань, надають консультації. НПП, академнаставники груп, працівники деканату постійно проводять роз’яснювальну роботу щодо форм та процедур контрольних заходів та критеріїв оцінювання навчальних досягнень. Результати оцінювання у вигляді модульного контролю доводяться до здобувачів ВО, обговорюються на засіданні кафедри та Вченої ради факультету за участю представників студентського самоврядування.

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

Контрольні заходи проводяться відповідно до «Положення про організацію освітнього процесу у УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/31357). Інформація про форми і терміни контрольних заходів доводиться до студентів завчасно на початку семестру під час аудиторних занять та оприлюднюється на стенді і сайті фізичного факультету (https://www.uzhnu.edu.ua/uk/infocentre/206), під час проведення планових консультацій. На початку семестру НПП, що викладає навчальну дисципліну, повідомляє здобувачам вищої освіти обсяг навчального матеріалу, який виноситься на підсумковий семестровий контроль, терміни та форми проведення модульного контролю, терміни виконання індивідуальних завдань, а також критерії оцінювання. Модульні контрольні роботи проводяться згідно розкладу навчального процесу, екзамени та заліки - за затвердженим графіком екзаменаційної сесії. Захист практик проводиться після її завершення і оформлення студентом всіх звітних документів впродовж 5 днів. Захист кваліфікаційної роботи магістра та складання комплексного державного екзамену проводяться згідно попередньо затвердженого розкладу.

Яким чином форми атестації здобувачів вищої освіти відповідають вимогам стандарту вищої освіти (за наявності)?

Атестація здобувачів вищої освіти за ОП проводиться у формі публічного захисту кваліфікаційної роботи магістра відповідно до вимог Стандарту ВО за спеціальністю 125 Кібербезпека для другого (магістерського) рівня вищої освіти. Захист кваліфікаційної (магістерської) роботи відбувається як публічна презентація. Кваліфікаційна робота розміщується на гугл-диску, посилання на який розміщено в інфо-центрі фізичного факультету (https://www.uzhnu.edu.ua/uk/infocentre/182). Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

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

Процедура проведення контрольних заходів визначена у: «Положенні про організацію освітнього процесу в УжНУ», затверджене наказом ректора ДВНЗ «УжНУ» N61/01-04 від 24.12.2020 р. (https://www.uzhnu.edu.ua/uk/infocentre/get/31357); «Положенні про порядок та методику проведення семестрових екзаменів та заліків», затверджене наказом ректора ДВНЗ «УжНУ» N698/01-17 від 08.05.2015 р. (https://www.uzhnu.edu.ua/uk/infocentre/get/5952); робочими програмами навчальних дисциплін (https://www.uzhnu.edu.ua/uk/infocentre/50191). Усі документи, що регулюють процедуру контрольних заходів, знаходяться у вільному доступі на сайті ЗВО.

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

Згідно з "Положенням про організацію освітнього процесу" оцінювання досягнень студентів є одним із принципів забезпечення доброчесності. Об'єктивність екзаменаторів забезпечується рівними умовами всіх здобувачів - інформація про тривалість контрольного заходу, кількість завдань, механізм підрахунку результатів, оприлюднення строків здачі контрольних завдань, критерієм оцінки. Також встановлені перездачі контрольних заходів. Для процедури забезпечення об'єктивності викладачі керуються такими документами: «Положення про порядок застосування заходів з врегулювання конфліктів та спорів (суперечок) у діяльності співробітників та здобувачів вищої освіти» (https://cutt.ly/AwcZuwY5), Етичний кодекс ДВНЗ "УжНУ" (https://cutt.ly/MwcZrlhY), Напрями запобігання та протидії корупції в ДВНЗ «УжНУ» (https://cutt.ly/OwcZef7c) та Порядок організації заходів із запобігання та врегулювання конфлікту інтересів (https://cutt.ly/xwcZiy98)
Для вирішення конфліктних ситуацій діє «Скринька довіри» (скринька розміщена у головному корпусі фізичного факультету, а також діє електронна анонімна скринька на сайті кафедри ТЕІБ http://teib.info/?page_id=6062). При наявності повідомлень щодо необ'єктивності контролю оцінювання, на факультеті створюється комісія (за рішенням декана). Для запобігання таких явищ завкафедри періодично відвідує контрольні заходи, а викладачі дотримуються визначених правил. Випадків оскарження результатів контрольних заходів та атестації здобувачами ВО на даній ОП не було, конфліктних ситуацій також не було.

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

Відповідно до «Положення про порядок та методику проведення семестрових (курсових) екзаменів і заліків в УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/5952) регламентовано порядок повторного проходження контрольних заходів, яке урегульовується графіком проведення заліково-екзаменаційної сесії, де визначено дні ліквідації академічної неуспішності. Дозволяється ліквідувати академзаборгованість не більше ніж з трьох дисциплін. Студент має право і зобов'язаний після завершення екзаменаційної сесії, якщо має академічну заборгованість її ліквідувати. Здобувач ВО не може бути допущений до перескладання екзамену з дисципліни, якщо не виконав усі види запланованих завдань передбачені робочою програмою. Повторне складання іспитів чи заліків допускається не більше двох разів з кожної дисципліни: один раз викладачу, другий раз – комісії, яку створює завідувач кафедри (у окремих випадках, на підставі заяви до ректора – третій раз). Студенти, які не ліквідували академзаборгованість або отримали незадовільні оцінки з чотирьох дисциплін, відраховуються з університету. Повторний захист кваліфікаційної роботи магістра можливий через рік після попереднього захисту. Студенти, які не з'явилися на екзамен, залік чи захист практики або кваліфікаційної роботи без поважних причин, вважаються

такими, що отримали оцінку “незадовільно”. Частина здобувачів освіти за даною ОП мають досвід повторного проходження підсумкового контролю окремих освітніх компонентів ОП.

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

Порядок оскарження процедури та результатів проведення контрольних заходів в УжНУ є доступним за посиланням https://www.uzhnu.edu.ua/uk/infocentre/get/22967.
У разі виникнення конфліктної ситуації здобувач ВО має право звернутися з письмовою заявою щодо результатів проведення контрольних заходів, до уповноваженої ректором особи – декана фізичного факультету проф. Лазура В.Ю. У відповідь на подання скарги особа, яка приймає скаргу, повинна повідомити про місце і час засідання апеляційної комісії. Декан своїм письмовим розпорядженням створює комісію, як правило, із трьох осіб. До складу комісії включається декан факультету чи його заступник та два фахівці кафедри, до якої належить освітній компонент, результати контрольного заходу з якого оскаржуються. Скарга повинна бути розглянута апеляційною комісією не пізніше двох днів. Така сама процедура може проводитися і за заявою викладача, однієї із сторін конфлікту.
Зі студентами періодично обговорюється порядок оскарження результатів оцінювання та політика і механізми вирішення можливих конфліктних ситуацій під час реалізації освітніх програм на кафедрі ТЕІБ (напр., https://www.uzhnu.edu.ua/uk/news/studenti-kafedri-teib-v-obgovorenni-zmin-osvy-program.htm). Варто відмітити, що за період дії ОП «Безпека інформаційних і комунікаційних систем» оскаржень здобувачами ВО процедури проведення та результатів контрольних заходів не було.

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

Дотримання академічної доброчесності регулюється «Положенням про академічну доброчесність в ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/12223). Свою обізнаність в академічній доброчесності підвищили на онлайн курсах «Академічна доброчесність в університеті» (платформа ВУМ online) як викладачі кафедри (https://www.uzhnu.edu.ua/uk/infocentre/50190) так і здобувачі вищої освіти (https://www.uzhnu.edu.ua/uk/infocentre/50193). Академічна доброчесність – це сукупність етичних принципів та правил, які визначені законом, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової діяльності з метою забезпечення довіри до результатів навчання або наукових досягнень. Дотримання академічної доброчесності здобувачами освіти передбачає: самостійне виконання навчальних завдань, модульного поточного контролю, підсумкового контролю результатів навчання; посилання на інформації у разі використання думок, розробок, ідей тощо; дотримання норм законодавства про авторське право і суміжні права; надання достовірної інформації про результати власної наукової і навчальної діяльності, використання методики досліджень і джерела інформації.

Які технологічні рішення використовуються на ОП як інструменти протидії порушенням академічної доброчесності?

ДВНЗ «УжНУ» сприяє дотриманню академічної доброчесності учасниками освітнього процесу, у відповідності до прийнятого «Положення про академічну доброчесність в ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/12223). На факультеті питання дотримання академічної доброчесності учасниками освітнього процесу періодично піднімаються на Вченій раді та на засіданнях кафедри. НПП та здобувачі ВО ознайомлюються з відповідним положенням ДВНЗ “УжНУ”. Для перевірки на плагіат в ЗВО використовують ІТ-інструменти Unicheck та Strike plagiatism (https://unicheck.com/uk-ua, https://strikeplagiarism.com/en/). Після отримання результатів перевірки кваліфікаційної роботи на наявність ознак плагіату рішення про допуск до захисту приймає завідувач кафедри проф. Різак В.М. на підставі подання наукового керівника роботи. Разом з цим, кафедра формує у співпраці із роботодавцями, стейкхолдерами, здобувачами ВО та затверджує перелік тем кваліфікаційних робіт магістрів, в якому відображено регіональні особливості ОП, що також значно скорочує ймовірність порушення академічної доброчесності. Викладач даної ОП, доц. Мисло Ю.М. є відповідальною особою за перевірку студентських робіт на наявність текстових запозичень (https://www.uzhnu.edu.ua/uk/infocentre/get/49920).

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

У 2018 році в рамках Проєкту сприяння академічної доброчесності в Україні (SAIUP), студенти прослухали лекцію про впроваджену у ДВНЗ «УжНУ» систему Unicheck та Strikeplagiatism. Популяризації сприяв проведений круглий стіл «Чесність починається з тебе», метою якого було формування нової академічної культури, яка базуватиметься на довірі, чесності, прозорості, реальному навчанні, справжній науковій роботі. В університеті час від часу проводяться лекції чи онлайн зустрічі, що присвячені питанням дотримання академічної доброчесності, наприклад вебінар «Академічна доброчесність – запорука якісної освіти” (https://www.uzhnu.edu.ua/uk/news/vebinar-akademichna-dobrochesnist-zaporuka-yakisnoji-osviti.htm). ДВНЗ «УжНУ» став учасником проєкту «Ініціатива академічної доброчесності» від Американських Рад з міжнародної освіти за підтримки Посольства США в Україні, МОН України та НАЗЯВО (https://www.uzhnu.edu.ua/uk/news/proyekt-Initsiativa-akademichnoji-dobrochesnosti---Academic-IQ.htm). Про порушення академічної доброчесності викладачі, які забезпечують реалізацію ОП, інформують та закликають студентів дотримуватися законодавства щодо авторського права шляхом посилання на джерела використаної інформації при роботі над науковими, рефективними, курсовими, кваліфікаційними роботами. Обговорюється важливість цих питань для інтеграції в європейський освітній простір.

Яким чином ЗВО реагує на порушення академічної доброчесності? Наведіть приклади відповідних

ситуацій щодо здобувачів вищої освіти відповідної ОП

Кваліфікаційні роботи перевіряються поетапно, студенти представляють матеріал для розгляду в електронному вигляді (науковим керівникам і завідувачу кафедри), де визначається стан і рівень виконаної роботи. Здобувачі ознайомлені з «Положенням про академічну доброчесність в ДВНЗ «УжНУ» заздалегідь. З метою дотримання академічної доброчесності, за необхідністю, скликається комісія зі складу науково-викладацького складу кафедри і факультету. При виявленні фактів порушення академічної доброчесності передбачена відповідальність, регламентована п.7.1. «Положення про академічну доброчесність» (https://www.uzhnu.edu.ua/uk/infocentre/get/12223), застосовуються заходи юридичної відповідальності відповідно до вимог законодавства України, Статуту «УжНУ» (https://www.uzhnu.edu.ua/en/infocentre/get/9268), Правил внутрішнього розпорядку та інших локальних нормативних актів «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/453). Порушення загальноприйнятих норм поведінки, ігнорування норм етики, моралі та громадської свідомості, етичних норм академічної та наукової діяльності може розглядатися комісією з питань академічної доброчесності та етики як вчинення аморального проступку, що за своїм характером несумісний із продовженням роботи, навчання в ДВНЗ «УжНУ» (п.7.2. Положення про академічну доброчесність) (https://www.uzhnu.edu.ua/uk/infocentre/get/12223). Випадків виявлення порушення академічної доброчесності на ОП не зафіксовано.

6. Людські ресурси

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

Добором кадрів займаються відповідні відділи ДВНЗ «УжНУ» за поданням завідувачів кафедр. Керуючись «Порядком проведення конкурсного відбору при заміщенні вакантних посад науково-педагогічних працівників та укладання з ними трудових договорів (контрактів) в ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/46615) на посади науково-педагогічних працівників обираються особи, які мають наукові ступені та/або вчені звання відповідно до профілю кафедри, магістри та особи, які мають багаторічний досвід практичної роботи в галузі інформаційної та/або кібербезпеки. Необхідною умовою є також наявність у претендента на посаду професора або доцента 5-х статей у фахових наукових виданнях (з яких не менше 2-х публікацій у журналах, що входять до Scopus, WoS) та виданих підручників або навчальних посібників. Конкурс на заміщення вакантної посади оголошується ректором УжНУ. Оголошення про проведення конкурсу, терміни та умови його проведення публікуються на офіційному сайті університету (https://www.uzhnu.edu.ua/uk/cat/s_subdivisions-dep_personal/vacancies). Кандидатури обговорюються на засіданні кафедри ТЕІБ. Перевага надається викладачам, показники професіоналізму та рейтингового оцінювання яких є вищими, а також фахівцям та науковцям в галузі інформаційної та/або кібербезпеки. Обрання на посади проводиться таємним голосуванням на засіданні Вченої ради факультету.

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

Базові документи ДВНЗ “УжНУ” вказують на пріоритетність залучення роботодавців як до формування освітніх програм так і до їх корекції. Наприклад, в УжНУ відбулася нарада учасників освітнього проекту ініційована американської компанією Rayter Inc., що базувалася на ідеї необхідності внесення змін до освітнього стандарту підготовки фахівців з кібербезпеки (https://www.uzhnu.edu.ua/uk/news/v-uzhnu-vidbulasya-narada-uchasnikiv-proektu-s.htm). Частина ідей розроблених під час цих нарад лежить в основі даної ОП. Частими є зустрічі здобувачів ВО із представниками державної влади та Держспецзв’язку (наприклад, https://carpathia.gov.ua/news/oleksandr-patskan-zavitav-na-lektsiiu-do-maibutnikh-fakhivtsiv-z-kiberbezpeky), а також з потенційними роботодавцями (https://www.uzhnu.edu.ua/uk/news/pravoohoronci-zakarpattia-zaproshuut-na-robotu-v-policiu.htm) Стейкхолдери та роботодавці також широко залучені до реалізації освітнього процесу. Практично одночасно з появою на кафедрі спеціальностей галузі знань 1701 "Інформаційна безпека" за сумісництвом почали викладати тут: Самохвалов М.П., директор ТОВ “Спецтелеком”, ліцензіат у галузі ТЗІ; представники СБУ (Корольчук С., Гребенніков В., Трефілов Ю.); Пагіря М.М., професор МДУ, а згодом – Маркевич П.В., начальник регіонального управління ДССЗЗІ, який працює тут до цього часу.

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

ЗВО забезпечує можливість залучення професіоналів-практиків (експертів галузі, представників роботодавців) до викладання, керівництва практикою і кваліфікаційними роботами шляхом зарахування на частину ставки і погодинної оплати їх праці, а також за сумісництвом. Науково-педагогічний склад кафедри ТЕІБ (http://teib.info/?page_id=12) постійно об'єднує професіоналів-практиків, експертів галузі та представників роботодавців.
Зокрема, ОК 6 та ОК 7 даної ОП забезпечує експерт галузі, член робочих груп з розробки професійних стандартів з кібербезпеки, д.т.н, проф. Давиденко А.М. Довгий час на посаді ст. викл. кафедри ТЕІБ за сумісництвом працював професіонал-практик з багаторічним досвідом і водночас роботодавець, директор ТОВ “Спецтелеком” (єдина організація в Закарпатті, що має ліцензію на проведення робіт в галузі технічного та криптографічного захисту інформації). Експерт галузі та роботодавець, начальник управління Держспецзв’язку в Закарпатській обл., Маркевич П.В. забезпечує науково-дослідну практику у сфері безпеки інформаційних і комунікаційних систем

(ОК10) та викладає ВК “Оптоволоконні комунікаційні системи”, працюючи на кафедрі за сумісництвом більше 5 років. Практичні заняття з ОК 9 забезпечує професіонал-практик ІТ-галузі Фролов А., колишній випускник кафедри ТЕІБ у галузі знань “Інформаційна безпека” (https://www.linkedin.com/in/artem-frolov-61809a6b/?originalSubdomain=ua).

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

ЗВО постійно дбає про професійний розвиток викладачів ОП. Напр., науково-дослідна частина та відділ міжнародних зв’язків здійснюють регулярні розсилки анонсів конференцій, конкурсів та грантів (https://www.uzhnu.edu.ua/uk/cat/science-cat_grants).
Завдяки сприянню ЗВО викладачі ОП з 2017 по 2021 рр приймали участь у міжнародному науковому та освітньому проекті ACCELERATE (в межах Рамкової програми ЄС «Horizon 2020» (керівник проекту від ДВНЗ “УжНУ” проф. Різак В.М., гарант ОП). Також багато викладачів (що забезпечують ОК та ВК даної ОП) пройшли підвищення кваліфікації або стажування у провідних освітніх закладах та/або ІТ-організаціях (https://www.uzhnu.edu.ua/uk/infocentre/50190):
проф. Різак В.М. - Pavol Jozef Šafárik University in Kosice (17.07-21.07.23); Департамент кіберполіції НПУ (24.07-31.08.23); Управління Держспецзв'язку в Закарпатській обл. (11.09-22.09.23);
проф. Пагіря М.М. - НАУ (01.03.23 - 30.06.23); ТОВ “Спецтелеком” (03.10.22 - 11.11.22);
доц. Чобаль О.І. - НАУ (01.03.23 - 30.06.23); Matej Bel University in Banská Bystrica (01.04.22 - 31.07.22); Cisco Networking Academy: CyberOps Associate (Instructor level, 23.01.21 - 23.04.21);
доц. Попович Н.І. - University of Security Management in Kosice (26.08.22 - 10.10.22)
ЗВО підтримує прагнення викладачів ОП для отримання кваліфікаційних професійних сертифікацій. Починаючи з 2017 року доц. Петрушко І.А. і доц. Чобаль О.І. періодично проходять навчальні курси в Мережевій академії Cisco, здобуваючи відповідні сертифікати інструкторського рівня.

Продемонструйте, що ЗВО стимулює розвиток викладацької майстерності

У ДВНЗ «УжНУ» стимулюється розвиток викладацької майстерності науково-педагогічних працівників згідно із «Положенням про визначення рейтингів науково-педагогічних працівників ДВНЗ УжНУ», затверджене ректором від 27.10.2020 р. N23/01-04 (https://www.uzhnu.edu.ua/uk/infocentre/get/29355). Дане положення є підставою для визначення індивідуального рейтингу науково-педагогічних працівників, що впливає на їх стимулювання (преміювання).
Також в УжНУ преміюють науковців університету за публікації у виданнях, що входять у міжнародні наукометричні бази даних Scopus та мають імпакт фактор IFCiteScore. Заохочувальні виплати за статті встановлюються в залежності від імпакт-фактору IFCiteScore журналу. Це регламентовано «Розпорядженням про преміювання авторських колективів» та Розпорядження No38-Р від 18.02.2021 р. (https://www.uzhnu.edu.ua/uk/infocentre/get/33679). Таку премію неодноразово отримували авторські колективи, що входять до наукової групи проф. Різака В.М., гаранта ОП. Разом з цим, в УжНУ щорічно проводиться конкурс на кращі підручники та посібники (https://www.uzhnu.edu.ua/uk/news/redaktsijno-vidavnicha-rada-viznachila-krashchi-pidruchniki-ta.htm), що також стимулює розвиток викладацької майстерності НПП.

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?

Навчання за ОП забезпечується матеріально-технічною базою УжНУ, яка відповідає ліцензійним вимогам провадження освітньої діяльності. Використовуються навчальні мультимедійні лабораторії, практикум з інформаційних технологій, лабораторія CISCO, спеціалізована лабораторія з методів та засобів захисту інформації, лабораторія твердотільної електроніки та біотехнологій і т.д.
На кафедрі є вільний доступ до навчальних матеріалів Мережевої академії Cisco і курсів платформи Coursera (в рамках Coursera for Ukraine Initiative); використовується хмарна платформа RangeForce, безкоштовне ПЗ, trial-версії або ліцензійне ПЗ, наприклад JetBrains Tools. Лабораторні заняття проводяться на емуляторі Cisco Packet Tracer та комплектах мережевих пристроїв, серед яких: комутатор, маршрутизатор, брандмауер (firewall), перехідники USB-COM (RS232), WiFi-маршрутизатори та інше. На кафедрі створено полігон кібербезпеки для симуляції проведення кібератак і захисту від них у стилі Red vs Blue team змагання (на основі Metasploitable 2).
Університет має найбільшу в регіоні бібліотеку. Здобувачі ВО та викладачі ОП мають вільний доступ до наукових БД ScienceDirect та Scopus. Відмітимо, що у 2017 р. була проведена акредитаційна експертиза підготовки магістрів зі спеціальності 8.17010101 БІКС, за результатами якої рекомендовано покращувати МТЗ даної спеціальності. Під час останньої акредитації ОП (2022 р) згідно висновку ГЕР встановлено, що “рекомендації щодо покращення МТЗ за результатами даної експертизи ЗВО виконано в достатньому обсязі”.

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 «Положення про організацію освітнього процесу в УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/31357) здобувачі мають право користуватися безоплатно інтернетом, бібліотеками, інформаційними фондами, навчальною, науковою, спортивною базою університету. Всі особи із особливими потребами мають можливість і доступність до всіх заходів життєдіяльності університету. На студентському самоврядуванні проводяться консультації, опитування, зустрічі щодо вирішення питань удосконалення навчального процесу. На кафедрі проводиться анкетування студентів щодо врахування потреб та інтересів студентів в освітньому процесі. У корпусі фізичного факультету розміщено анонімну скриньку довіри. Враховуючи побажання експертів під час попередньої акредитації, на сайті кафедри ТЕІБ реалізовано електронну форму для надсилання повідомлень до анонімної скриньки довіри для здобувачів ВО (http://teib.info/?page_id=6062).
Між викладачами і студентами вибудовуються стосунки взаємоповаги та порозуміння. Інституція академнаставництва на факультеті допомагає студентству консультаціями, порадами, передають життєві настанови. Для підтримання здоров'я, як фізичного так і психоемоційного у всіх учасників освітнього процесу на належному рівні у ДВНЗ «УжНУ» активно функціонують такі структурні підрозділи: Спортивно-оздоровчий комплекс; Студентський центр дозвілля «Ювентус»; Центр гуманітарно-виховної роботи, профорієнтації та працевлаштування; Медіацентр; Волонтаріат УжНУ; Соціально-психологічна служба; Студентське містечко.

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

Питання безпеки життя та здоров'я здобувачів ВО відображені в таких нормативних документах: Концепція інноваційного розвитку ДВНЗ «УжНУ» на 2015-2025 рр. (https://www.uzhnu.edu.ua/uk/infocentre/get/8662), Правила внутрішнього розпорядку у студентських гуртожитках (https://www.uzhnu.edu.ua/uk/infocentre/get/10134), Правила внутрішнього розпорядку ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/453), Порядок супроводу осіб з інвалідністю та інших маломобільних груп населення у ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/22035) та ін.
На факультеті студенти щороку проходять інструктаж з техніки безпеки, виробничої санітарії, протипожежної безпеки, що фіксується у спеціальних журналах. На кафедрі наявні медична аптечка, аудиторіях і лабораторіях факультету витримуються відповідні санітарні умови стосовно площі приміщень, температурного режиму, освітлення. В корпусах цілодобова охорона. Медичні послуги студенти отримують в медпунктах та студентській поліклініці. В УжНУ працює відділ соціально-психологічної служби (https://www.uzhnu.edu.ua/uk/cat/dep_hum_ed_work-centre_psy), де психологи проводять практичні семінари-тренінги та лекції, тренінги навичок поведінки в конфліктних ситуаціях.
На факультеті створюється доброзичлива атмосфера співробітництва і підтримки, проводяться вечори дозвілля студентів і викладачів (День першокурсника, День Архімеда). При проведенні таких заходів викладачі і студенти пізнають один одного в неформальній обстановці.

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?

В УжНУ забезпечується, освітня, соціальна, інформаційна та консультативна підтримка студентів, що здійснюється відповідно до закону України «Про вищу освіту» і Статуту ДВНЗ «УжНУ». В університеті працює центр гуманітарно-виховної роботи (https://www.uzhnu.edu.ua/uk/cat/s_subdivisions-dep_hum_ed_work), юридична клініка (https://www.uzhnu.edu.ua/uk/cat/s_subdivisions-law_clinic), Студентська рада (https://www.uzhnu.edu.ua/uk/cat/student-self_government). Підтримка здобувачів відбувається через взаємодію з працівниками деканату і кафедр, де вони можуть отримати необхідну інформацію, що стосується освітнього процесу, загальних питань, організації навчання, проживання в гуртожитку тощо. Деканат розглядає конфліктні ситуації між викладачем і студентом, розглядає організаційні та соціальні потреби студентів. Основним джерелом інформації є офіційний сайт ДВНЗ «УжНУ» та кафедри ТЕІБ (teib.info). Соціальну підтримку отримують студенти таких категорій, як сироти, інваліди, переселенці, чорнобильці, діти учасників бойових дій. Студенти, які мають дітей, отримують подарунки до дня Святого Миколая від профспілки УжНУ. Студентам-сиротам, дітям учасників бойових дій гуртожиток надається безкоштовно.
Проводиться анкетування (опитування) здобувачів, з метою визначити рівень задоволеності студентів в наданні різнобічної підтримки з боку УжНУ, результати якого показують достатньо високий рівень (https://www.uzhnu.edu.ua/uk/infocentre/50180).

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)

В ДВНЗ «УжНУ» створені умови для реалізації права на освіту особами з особливими освітніми потребами. Таким здобувачам надається постійна і тимчасова додаткова підтримка для повної реалізації їх прав на здобуття освіти, розвитку особистості, покращення стану здоров'я та якості життя, підвищення рівня участі у житті академічної спільноти університету. Це реалізується завдяки нормативній базі під час будівництва чи реконструкції навчальних закладів. Наказом N424/01-04 від 31.05.2018 року затверджено Порядок супроводу (надання допомоги) осіб з інвалідністю та інших маломобільних груп населення в ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/22035). В ЗВО, та на фізичному факультеті зокрема, створене безбар'єрне доступне середовище для осіб з обмеженими руховими можливостями (пандус на 1 поверсі, ліфти в головному корпусі). Нещодавно додатково були встановлені пандуси біля студентських гуртожитків №4 і №5 (https://www.uzhnu.edu.ua/uk/news/v-uzhnu-bilya-gurtozhitkiv-4-i-5-ustanovili-pandusi-.htm). Серед здобувачів

ступеня магістра за ОП «Безпека інформаційних і комунікаційних систем» не було і на сьогодні немає осіб з особливими освітніми потребами, але потенційно на ОП можуть навчатися особи з такими потребами.

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?

В ДВНЗ «УжНУ» чітка і зрозуміла політика та процедури вирішення конфліктних ситуацій. Освітня діяльність проходить із дотриманням демократичних цінностей свободи, справедливості рівності прав і можливостей. Врегулювання конфлікту інтересів в УжНУ здійснюється відповідно до «Положення про порядок застосування заходів з врегулювання конфліктів та спорів (суперечок) у діяльності співробітників та здобувачів вищої освіти» затвердженого наказом ректора ДВНЗ «УжНУ» N159/01-04 від 3 березня 2020 р (https://www.uzhnu.edu.ua/uk/infocentre/get/22964), етичного кодексу (https://www.uzhnu.edu.ua/en/infocentre/get/22896) та статуту ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/en/infocentre/get/9268).
В університеті створено Комісію з врегулювання конфліктних ситуацій. Якщо учасники освітнього процесу ДВНЗ «УжНУ» вважають, що у відношенні до них в університеті були порушені права, тоді вони мають право подати скаргу до Комісії з врегулювання конфліктних ситуацій. Скарга повинна бути подана протягом 30 днів з моменту вчинення порушення прав або з дня, коли стало відомо про його вчинення. Також урегулювання конфліктних ситуацій для учасників освітнього процесу на ОП здійснюється можливістю написання письмового звернення до завідувача кафедри ТЕІБ або до ректора УжНУ.
Розгляд звернень і скарг, які надходять, відбувається згідно Закону України «Про доступ до публічної інформації», Закону України «Про порядок звернення громадян», особистого прийому громадян керівництвом. Протягом періоду впровадження ОП таких ситуацій не було.

8. Внутрішнє забезпечення якості освітньої програми

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

У ДВНЗ «Ужгородський національний університет» процедури розроблення, затвердження, моніторингу та періодичного перегляду освітніх програм регулюються Положенням про порядок розроблення, моніторинг та періодичний перегляд освітніх програм в ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/22968) та Положенням про систему внутрішнього забезпечення якості освіти ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/19667).

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

Згідно "Положення про порядок розроблення, моніторинг та періодичний перегляд ОП у ДВНЗ «УжНУ»" основними підставами для зміни або перегляду (оновлення або модернізації) ОП є зміни в НД, які регулюють питання змісту освіти за відповідною спеціальністю, прийняття нових освітніх і професійних стандартів, а також результати внутрішнього моніторингу та зовнішнього оцінювання якості ОП. Підставами для оновлення ОП можуть бути також ініціатива та пропозиції гаранта ОП, основних стейкхолдерів, членів робочої групи, викладачів кафедри. Перегляд відбувається з використанням результатів оцінювання якості освітньої програми, які було отримано під час самооцінювання ОП, результатів опитувань здобувачів ВО, випускників, роботодавців.
При передостанньому оновленні даної ОП (травень - грудень 2021 р) були внесені зміни, що стосувалися переліку ОК та ВК, обсягів та змісту дисциплін, а також ПРН у відповідності до затвердженого СВО за спеціальністю 125 Кібербезпека.
Під час останньої модернізації даної ОП (січень - березень 2023 р) внесено перераховані нижче зміни з метою удосконалення ОП на основі таких підстав:
1) ЗАТВЕРДЖЕННЯ 6 ПРОФЕСІЙНИХ СТАНДАРТІВ У ГАЛУЗІ КІБЕРБЕЗПЕКИ (25.11.22 р):
оновлено зміст ОП в частині переліку професій (придатність до працевлаштування), спеціалізації та особливостей ОП;
додано загальні і професійні компетентності (за трудовою дією або групою трудових дій) згідно профстандарту «Фахівець сфери захисту інформації», а також матрицю їх відповідності компонентам ОП;
оновлено зміст ОК і ВК даної ОП з метою повного забезпечення професійних компетентностей обраного профстандарту;
2) ЗАУВАЖЕННЯ ЕГ ТА РЕКОМЕНДАЦІЇ ГЕР ПІД ЧАС ОСТАННЬОЇ АКРЕДИТАЦІЙНОЇ ЕКСПЕРТИЗИ (жовтень - грудень 2022 р):
перенесено навчальну дисципліну "Іноземна мова для професійної діяльності" із вибіркових компонент ОП у ОК;
уточнено назви і доповнено зміст ОК2, ОК3 темами, які забезпечують формування професійних соціальних навичок;
додано ОК 9, а також уточнено назви і доповнено зміст ОК6 - ОК8 циклу професійної підготовки з метою максимального забезпечення формування професійних навичок і ПРН відповідно до назви та предметної області ОП, а також вимог СВО та профстандарту "Фахівець сфери захисту інформації";
зміст ОК 5 приведено у відповідність до предметної області спеціальності 125 Кібербезпека та захист інформації, а також зменшено його обсяг до 4 кредитів;

вилучено ОК “Педагогічна практика”, а вивільнені кредити перерозподілено між іншими ОК, що забезпечують практичну підготовку професійного спрямування (це також було одним із побажань здобувачів ВО);
усунуто ОК “Атестація. Складання комплексного державного екзамену” як форму атестації здобувачів ВО, а вивільнений час додано до ОК12;
розширено каталог вибіркових навчальних дисциплін професійного спрямування
3) ПРОПОЗИЦІЇ ЗДОБУВАЧІВ ТА СТЕЙКХОЛДЕРІВ
враховано професійний стандарт “Фахівець сфери захисту інформації”;
додано ОК7 і ОК9, уточнено назву і зміст ОК8, ОК9
додано ВК “Кібергігієна та протидія кібербулінгу”

Продемонструйте, із посиланням на конкретні приклади, як здобувачі вищої освіти залучені до процесу періодичного перегляду ОП та інших процедур забезпечення її якості, а їх позиція береться до уваги під час перегляду ОП

Залучення здобувачів до процесу періодичного перегляду ОП та інших процедур забезпечення її якості здійснюється у результаті особистого спілкування та анкетування, в ході якого встановлюється актуальність навчальних дисциплін, повнота розкриття матеріалу, цілісність та послідовність його викладання. До складу робочої групи даної ОП входить здобувач магістерського рівня ВО Білич Ю.О., староста групи, яка також аналізує, систематизує та представляє побажання здобувачів ВО на засіданнях робочої групи.
Наприклад, під час обговорення проекту даної ОП (https://cutt.ly/7wcMvN9d) було проведено круглий стіл робочої групи і здобувачів ВО (студентів 4-го курсу бакалаврату і 1-го курсу магістратури), де обговорювались перспективи впровадження професійних стандартів в межах даної ОП, вдосконалення змісту ОП, започаткування нових ОК та розширення каталогів вибіркових дисциплін. Пізніше ці побажання були систематизовані і враховані під час засідання робочої групи (протокол №2).
Також студенти, що навчаються за спеціальністю 125 Кібербезпека та захист інформації періодично проходять анкетування щодо якості ОП (http://surl.li/isumr) і задоволеності наданням освітніх послуг (https://surl.li/ieuur) згідно розпоряджень ректора УжНУ (наприклад, https://drive.google.com/drive/folders/1L5fAFJRn3xx-vHMA5YunRn5-FCVBqpT5). Результати подібних анкетувань (https://www.uzhnu.edu.ua/uk/infocentre/50180) обговорюються із здобувачами (http://teib.info/?p=6211) і беруться до уваги при перегляді ОПП.

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

Органи студентського самоврядування ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/7357), згідно з «Положенням про систему внутрішнього забезпечення якості освіти ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/18747), беруть участь у процедурах внутрішнього забезпечення якості ОП, наприклад: обговорення та вирішення питань удосконалення освітнього процесу, внесення пропозиції щодо змісту навчальних планів і програм, аналіз успішності за проміжним і підсумковим контролями, участь у роботі стипендіальної комісії, запрошення до участі в засіданнях кафедри ТЕІБ, участі в опитуваннях (усних та анкетування). На фізичному факультеті діє структура студентського самоврядування, яка включає студентські раду і профбюро, студентське наукове товариство, які можуть вирішувати питання надання їм послуг в УжНУ і вносити відповідні рекомендації деканатам та кафедрам для прийняття управлінських рішень, в тому числі через анонімні запити в скриньках довіри. Органи студентського самоврядування за квотами входять до складу Вченої ради фізичного факультету і тому можуть додатково висловлювати свої побажання щодо вдосконалення ОП. Здобувачі вищої освіти беруть участь у формуванні робочого навчального плану, вибираючи навчальні дисципліни з переліку дисциплін вільного вибору.

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

Зустрічі з роботодавцями відбуваються на розширених засіданнях кафедри ТЕІБ, зустрічах із студентами (напр., http://teib.info/?p=6156), у період проведення конференцій (наприклад, ITSEC-2023 https://mediacenter.uzhnu.edu.ua/news/pro-kiberbezpeku-v-konteksti-vijny-ta-pidhotovku-fakhivtsiv-dyskutuvaly-na-mizhnarodnij-konferentsii-itsec-bezpeka-informatsijnykh-tekhnolohij/2023-05-09-55660), ділових зустрічей, серед яких традиційні “Ярмарка вакансій” чи “День кар’єри” (наприклад, “День кар’єри ЄС: Ужгород” https://www.uzhnu.edu.ua/uk/news/studenti-uzhnu-vchilis-pid-chas-dnya-karyeri-Yes-uzhgorod.htm та https://www.uzhnu.edu.ua/uk/news/uzhnu-vzyav-uchast-v-yarmarku-vakansij.htm). Крім того, потенційний роботодавець, начальник управління Держспецзв’язку в Закарпатській області Петро Маркевич є членом робочої групи з розробки даної ОП. Наприклад, після обговорення оприлюдненого проекту даної ОП (https://www.uzhnu.edu.ua/uk/infocentre/52499) з представниками місцевих РВА, Маркевич П.В. вніс пропозицію щодо удосконалення ОП у частині змістового наповнення дисциплін циклу професійної підготовки (протокол №3 засідання робочої групи). Зокрема, за рекомендаціями потенційних роботодавців акцентовано необхідність підготовки здобувачів у галузі безпеки інформаційно-комунікаційних систем, що забезпечується передусім ОК8 - ОК10.

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

Збір інформації щодо кар’єрного шляху та траєкторій працевлаштування випускників освітньої програми здійснюється через моніторинг джерел у інформаційному просторі, у соціальних мережах, через особисте

спілкування. Випускники продовжують навчання в аспірантурі УжНУ; здійснюють науково-педагогічну діяльність у науково-дослідних центрах та ЗВО; успішно працюють на підприємствах, органах державної влади та в банківських структурах; у приватних фірмах або самі стають приватними підприємцями у галузі кібербезпеки. Кафедра ТЕІБ постійно підтримує зв'язок із випускниками з метою сприяння їх кар'єрному росту, залучення до роботи зі студентами в різних формах (проходження практик, семінари, круглі столи, комунікації в соцмережах). Гарант програми комунікує з випускниками і отримує цінні рекомендації щодо оновлення ОП. Вже традиційними стали мотивуючі лекції одного з кращих випускників даної ОП Павла Данилюка перед першокурсниками спеціальності 125 Кібербезпека та захист інформації (http://teib.info/?p=6141).
В УжНУ діє Міжнародна асоціація випускників ДВНЗ "УжНУ" (https://cutt.ly/JwcBRuUR), Відділ сприяння працевлаштуванню та профорієнтації (https://cutt.ly/owcBWGRB) та Центр кар'єри (https://cutt.ly/swcBEJWg), які об'єднують випускників, сприяють професійному становленню молодих спеціалістів, надають допомогу у працевлаштуванні та в реалізації власних проєктів. Ці структури безпосередньо або через роботодавців ініціюють та аналізують опитування випускників ДВНЗ "УжНУ" (http://surl.li/iubhk).

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?

Згідно з Положенням про систему внутрішнього забезпечення якості освіти ДВНЗ «УжНУ» п.4.13-4.15 (https://www.uzhnu.edu.ua/uk/infocentre/get/18747) та Положення про порядок розроблення, моніторинг та періодичний перегляд освітніх програм у ДВНЗ «УжНУ» п.3.3 (https://www.uzhnu.edu.ua/uk/infocentre/get/22968) модернізація ОП відбувається за результатами моніторингу, який здійснюється, як правило, проєктною групою та групою забезпечення. До моніторингу та перегляду ОП можуть залучаються стейкхолдери.
Під час реалізації ОП та у ході здійснення процедур внутрішнього забезпечення якості були виявлено незначний недолік. Відділом моніторингу якості освіти, методичного та інформаційного забезпечення освітнього процесу запропоновано оновити методичні рекомендації до написання кваліфікаційних робіт із врахуванням умов академічної доброчесності здобувачів та розмістити на офіційному вебсайті ДВНЗ "УжНУ", а також встановити відповідальну особу. З метою усунення недоліків представниками ЕК із захисту кваліфікаційних робіт повністю оновлено "Методичні рекомендації до виконання, оформлення та захисту кваліфікаційної роботи магістра" для здобувачів другого (магістерського) рівня вищої освіти за спеціальністю 125 Кібербезпека та захист інформації (https://www.uzhnu.edu.ua/uk/infocentre/50191), а також встановлено відповідальну особу за перевірку студентських робіт на наявність текстових запозичень - викладача даної ОП, доц. Мисло Ю.М. (https://www.uzhnu.edu.ua/uk/infocentre/get/49920).

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

За результатами акредитаційної експертизи даної ОП, що проходила впродовж 02-04.11.2022 р (наказ №597-Е від 18.10.22 р), НАЗЯВО ухвалило акредитувати ОП умовно (відкладено). На основі звіту ЕГ та висновків ГЕР було резюмовано рекомендації стосовно вдосконалення даної ОП (критерії 2,8, відносно яких встановлено рівень відповідності Е):
Кр. 2: 1) Забезпечити дотримання вимог СВО щодо обсягу ОПП, який спрямований на формування компетентностей 2) Перепроектувати структуру та зміст ОПП 3) Забезпечити відповідність змісту ОПП предметній області 4) Забезпечити формування індивідуальної освітньої траєкторії здобувача 5) Замінити ОК Педагогічна практика у ВНЗ на ОК практичної підготовки проф. спрямування 6) Передбачити в ОПП ОК або окремих тем, які забезпечують формування проф. соціальних навичок 7) Врахувати зміни до національного класифікатора професій ДК 003:2010 і опубліковані профстандарти 8) Привести у відповідність тривалість і терміни виконання та захисту кваліфікаційної роботи. Усунути комплексний державний іспит як форму атестації здобувачів.
Кр. 8: 1) Забезпечити дотримання вимог щодо розроблення та періодичного перегляду ОПП 2) Забезпечити на постійній основі залучення до процесу періодичного перегляду ОПП та інших процедур забезпечення якості ОПП здобувачів ВО з ОПП, випускників, роботодавців 3) Системі забезпечення якості ЗВО забезпечити контроль оновлення ОПП.
Під час удосконалення ОП нами проведено значну роботу з виконання цих рекомендацій:
Кр. 2: усі рекомендації враховано повністю; детальний опис змін структури і змісту даної ОП описано вище у відповідному вікні розділу 8 цих відомостей СО.
Кр. 8: 1) Забезпечено дотримання вимог згідно https://cutt.ly/8wcMcJ21 - враховано запровадження профстандартів, максимально виконано рекомендації та усунено недоліки, виявлені під час акредитаційної експертизи 2) Залучено до процесу періодичного перегляду на постійній основі здобувача ВО, представника роботодавців (члени робочої групи ОП) та випускників 3) ОП перезатверджується кожного року Вченою радою ДВНЗ "УжНУ" з обов'язковим контролем необхідності оновлення при наявності підстав визначених відповідним Положенням.
Також враховано рекомендації стосовно інших критеріїв, які передбачають підвищення якості ОП:
-Повністю забезпечено відповідність академічної та/або професійної кваліфікації НПП, задіяних до реалізації ОПП, вимогам Ліцензійних умов
-Забезпечено підвищення кваліфікації НПП, що забезпечують ОК професійного спрямування (проф. Різак В.М., проф. Пагіря М.М., доц. Чобаль О.І.).
-Проводиться інформаційна робота щодо політики та механізмів вирішення конфліктних ситуацій, порядку оскарження здобувачами результатів оцінювання та можливостей надсилання анонімних повідомлень (https://cutt.ly/7wcMvN9d), а також обговорення результатів опитування здобувачів (http://teib.info/?p=6211)
-Розроблено механізми подання пропозицій від стейкхолдерів із удосконалення ОП через інформаційні ресурси кафедри (http://teib.info/?page_id=6054)

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

Згідно «Положення про внутрішню систему забезпечення якості освіти» в ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/18747) університет сприяє залученню учасників академічної спільноти до процедур внутрішнього забезпечення якості ОП. Процес здійснюється з урахуванням всіх учасників академічної спільноти, а саме фахівців різних факультетів, які задіяні в забезпеченні ОП, роботодавців, студентів з дотриманням та реалізацією заходів: забезпечення якості; реалізація інноваційних технологій в освіті; пропагування і культивування академічної доброчесності; дотримання толерантності та недопустимість приниження гідності людини.
Робоча група ОП відповідно до існуючого "Положення про порядок розроблення, моніторинг та періодичний перегляд освітніх програм у ДВНЗ «УжНУ»", розробляє проєкт ОПП, проводить дослідження актуальності змін, а також проводить обговорення ОП із залученням учасників академічної спільноти на засіданнях кафедри ТЕІБ, на Вченій раді факультету, на щорічних конференціях професорсько-викладацького складу УжНУ та інших наукових конференціях (наприклад, XII Міжнародна науково-технічна конференція ITSEC-2023 проходила на базі ДВНЗ "УжНУ" - https://cutt.ly/kwcMUhEO). Проект даної ОП також обговорювався на зустрічі робочої групи з представниками академічної спільноти (http://teib.info/?p=6190), а рекомендації і побажання, напрацьовані в ході зустрічі, були враховані при модернізації ОП (протокол засідання робочої групи №2).

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

В ДВНЗ «УжНУ» за здійснення процесів і процедур внутрішнього забезпечення якості освіти відповідають: на рівні університету – відділ моніторингу якості освіти, методичного та інформаційного забезпечення освітнього процесу, навчальна частини університету, відділ публічного забезпечення та публічної інформації; на рівні факультету – методична комісія, Вчена рада факультету; на рівні кафедри – забезпечується викладачами кафедри, науково-методичною групою кафедри при безпосередньому керівництві завідувача кафедри (гаранта освітньої програми).
В університеті є Відділ моніторингу якості освіти, методичного та інформаційного забезпечення освітнього процесу (https://www.uzhnu.edu.ua/uk/cat/educ_dep-dep_mon_ed_qual), створений з метою посилення орієнтації управління на якісні аспекти, забезпечення всіх рівнів управління інформацією щодо якості освіти і взаємодіє із: деканатами, кафедрами з питань організації освітньої діяльності; приймальною комісією та студентським відділом із питань зарахування, відрахування студентів, своєчасного внесення інформації про рух контингенту студентів, тощо; відділом кадрового забезпечення. Навчальна частина у своїй діяльності керується чинними законодавчими й нормативно-правовими актами, Статутом, Правилами внутрішнього розпорядку ДВНЗ «УжНУ», Положенням про навчальну частину та інше. Модель внутрішньої системи забезпечення якості вищої освіти розміщена на офіційному сайті університету (https://www.uzhnu.edu.ua/uk/infocentre/get/18747).

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?

Процес розробки і затвердження внутрішніх нормативних документів ДВНЗ «УжНУ» базується на принципі дотримання рівних прав і свобод усіх учасників освітнього процесу, а також відкриває можливості для співпраці із стейкхолдерами. До основних документів ДВНЗ «УжНУ», що регулюють права та обов'язки учасників освітнього процесу і є у вільному доступі на сайті ВНЗ, належать:
1.Статут ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/9268);
2.Положення про організацію освітнього процесу в ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/31357);
3.Правила внутрішнього розпорядку ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/453);
4.Положення про академічну доброчесність в «Ужгородському національному університеті» (https://www.uzhnu.edu.ua/uk/infocentre/get/12223);
5.Положення про Наукове товариство студентів, аспірантів, докторантів і молодих вчених ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/9199);
6.Положення про студентське самоврядування ДВНЗ «УжНУ» (https://www.uzhnu.edu.ua/uk/infocentre/get/7589).
Документи, що регулюють права та обов'язки учасників освітнього процесу є чіткими, зрозумілими та доступними для усіх зацікавлених сторін. Кожного року на загальних зборах ВНЗ, засіданнях вчених рад, кафедр, студентських рад усі учасники освітнього процесу ознайомлюються із змінами в нормативно-правовому забезпеченні діяльності ДВНЗ «УжНУ», а керівники підрозділів отримують останні оновлення на офіційні корпоративні поштові адреси у домені @uzhnu.edu.ua.

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

https://www.uzhnu.edu.ua/uk/infocentre/52499
http://teib.info/?page_id=6054

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

Освітня програма "Безпека інформаційних і комунікаційних систем" розміщена на офіційному веб-сайті ДВНЗ "УжНУ" у розділі "ОСВІТНІ ПРОГРАМИ":
https://www.uzhnu.edu.ua/uk/infocentre/15072

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП?

Сильні сторони ОП "Безпека інформаційних і комунікаційних систем":
- відповідає тенденціям розвитку галузі кібербезпеки в Україні та світі;
- має чітко сформульовані цілі, що відповідають місії та стратегії ЗВО;
- висока академічна і професійна кваліфікація викладачів ОПП;
- залучення роботодавців до освітнього процесу;
- належна матеріально-технічна база для забезпечення навчальної діяльності;
- чіткість і зрозумілість політик та практик дотримання академічної доброчесності;
- дотримання правил і процедур, що регулюють права та обов'язки всіх учасників освітнього процесу;

Водночас, поруч із зазначеними сильними сторонами ОПП, існує низка аспектів, реалізація яких сприятиме покращенню освітньої програми, зокрема, введення викладання частини курсів англійською мовою, активізація участі здобувачів та викладачів у програмах міжнародної академічної мобільності, міжнародних наукових проектах.

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

Перспективи розвитку даної ОП впродовж найближчих років вбачаються у розвитку освітньої програми відповідно до вимог сучасного наукового простору; покращення матеріально-технічної бази полігону кібербезпеки кафедри ТЕІБ для комплексного навчання багаторівневого захисту від кібератак за рахунок долучення до програми «Кібербезпека для вищих навчальних закладів критичної інфраструктури» та інших донорів (USAID, DAI Global LLC і т.д.); адаптації ОПП під потреби воєнного стану і післявоєнного відновлення України; розширення участі здобувачів ВО у міжнародних проектах, грантових програмах; впровадження англомовних курсів для вивчення на ОПП. Реалізація цих заходів щодо вдосконалення ОПП сприятиме покращенню освітнього процесу за ОПП.

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: Смоланка Володимир Іванович

Дата: 22.09.2023 р.

Таблиця 1. Інформація про обов'язкові освітні компоненти ОП

Назва освітнього компонента	**Вид компонента**	**Силабус або інші навчально-методичні матеріали**		**Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього***
		Назва файла	**Хеш файла**	
Методика викладання фахових дисциплін у вищій школі	навчальна дисципліна	*ОК2.pdf*	1yv3flq3ZCyp3FKDyXUWHzJabdNnA0g/LmFk/7WVTfc=	*Аудиторія для проведення лекційних та семінарських занять, мультимедійний проектор Epson, Wi-Fi інтернет, система електронного навчання Moodle https://e-learn.uzhnu.edu.ua*
Наукові комунікації та основи наукових досліджень у сферах кіберзахисту і технічного захисту інформації	навчальна дисципліна	*ОК3.pdf*	NlOXX652wwQh8yHutMOyD7IjioEMVIluZkUEbwCgBL4=	*Аудиторія для проведення лекційних та семінарських занять, мультимедійний проектор Epson, Wi-Fi інтернет, система електронного навчання Moodle https://e-learn.uzhnu.edu.ua*
Методи побудови та аналізу криптосистем	навчальна дисципліна	*ОК4.pdf*	Ln6R5HpXcvDF4z5Zif5iTNLEwWLV7KWmBGr/86lYDeY=	*Аудиторія для проведення лекційних занять. Мультимедійний проектор. WiFi-інтернет. Комп'ютерний клас: 10 ПК Intel Core 2 Duo E8400 (ОС Windows 10 Pro for Education, Visual Studio 2019, LibreOf ice, MATLAB). Підключення до мережі Internet. Таблиці середньостатистичних частот та розподілу рівноваги для ланцюга Маркова. Система електронного навчання Moodle https://e-learn.uzhnu.edu.ua.*
Математичне моделювання процесів та систем у сфері захисту інформації	навчальна дисципліна	*ОК5.pdf*	pwqUvRaOsvApn2Oi/4S8igMKmRlA4qKe5DknAkSZG14=	*Аудиторія для проведення лекційних занять. Мультимедійний проектор Epson. Wi-Fi-інтернет. Комп'ютерний клас: 10 ПК Intel Core 2 Duo E8400 (ОС Windows 10 Pro for Education, Visual Studio 2019, LibreOffice, MATLAB). Підключення до мережі Internet. Система електронного навчання Moodle https://e-learn.uzhnu.edu.ua.*
Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки	навчальна дисципліна	*ОК6.pdf*	TTp3zK8mzDprzXE3opYCSxeIHGrfWlesJ7R7MGBhrhc=	*Аудиторія для проведення лекційних занять. Мультимедійний проектор Epson. Wi-Fi-інтернет. Комп'ютерний клас: 10 ПК Intel Core 2 Duo E8400 (Windows 10, Kali Linux, WireShark, Nessus, Metasploit). Кіберполігон кафедри ТЕІБ: маршрутизатор Cisco ISR4221, керований комутатор Cisco, міжмережевий екран Cisco, сервер Metasploitable 2. Система електронного навчання Moodle https://e-learn.uzhnu.edu.ua.*
Безпека хмарних технологій та розподілених обчислень	навчальна дисципліна	*ОК7.pdf*	Mn3w5grOAJWm5qPq6/6ZCG8GLsaoQUKFWSFkJS/tzzM=	*Аудиторія для проведення лекційних занять. Мультимедійний проектор Epson. Wi-Fi-інтернет. Комп'ютерний клас: 10 ПК Intel Core 2 Duo E8400 (Windows 10, Kali Linux, WireShark, Nessus, Metasploit). Кіберполігон кафедри ТЕІБ: маршрутизатор Cisco*

				ISR4221, керований комутатор Cisco, міжмережевий екран Cisco, сервер Metasploitable 2. Система електронного навчання Moodle https://e-learn.uzhnu.edu.ua.
Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	практика	*ОК10.pdf*	oVIJFEB6giIEUPKSXA3yGigGQq9VaUGnk4NW3Wdbt6Y=	*Комп'ютерний клас: 10 ПК Intel Core 2 Duo E8400 (Windows 10, Kali Linux, WireShark, Nessus, Metasploit, JetBrains Tools, MySQL, MongoDB, Nmap, Cisco Packet Tracer). Полігон кібербезпеки: маршрутизатор Cisco ISR4221, керований комутатор Cisco, міжмережевий екран Cisco, сервер Metasploitable 2. Лабораторія технічного захисту інформації. Мережева академія Cisco Networking Academy. Підключення до Інтернет*
Переддипломна практика	практика	*ОК11.pdf*	B5xjMIhbOHf5uqJmlrbnPdPs2cznxGFkmt/bMEc+7L8=	*Комп'ютерний клас: 10 ПК Intel Core 2 Duo E8400 (Windows 10, Kali Linux, WireShark, Nessus, Metasploit, JetBrains Tools, MySQL, MongoDB, Nmap, Cisco Packet Tracer). Полігон кібербезпеки: маршрутизатор Cisco ISR4221, керований комутатор Cisco, міжмережевий екран Cisco, сервер Metasploitable 2. Лабораторія технічного захисту інформації. Мережева академія Cisco Networking Academy. Підключення до Інтернет*
Моніторинг та аудит інформаційно-комунікаційних систем	навчальна дисципліна	*ОК9.pdf*	lpZRWQSF7pOfdDMvFWmkv82I/GIxAmXb0EnDnQb4eOY=	*Аудиторія для проведення лекційних занять. Мультимедійний проектор Epson. Wi-Fi-інтернет. Комп'ютерний клас: 10 ПК Intel Core 2 Duo E8400 (Windows 10, Kali Linux, WireShark, Nessus, Metasploit). Кіберполігон кафедри ТЕІБ: маршрутизатор Cisco ISR4221, керований комутатор Cisco, міжмережевий екран Cisco, сервер Metasploitable 2. Система електронного навчання Moodle https://e-learn.uzhnu.edu.ua.*
Іноземна мова для професійної діяльності	навчальна дисципліна	*ОК1.pdf*	wWIZFRUYM/WJrq2AY7nzOhF+I7jM7N+DqBPZ8EPMBpY=	*Аудиторія для проведення семінарських занять, комп'ютер, мультимедійні презентації, відеоматеріали, чат, аудіозаписи; офісні програми (Google Meet, Moodle), програми для перегляду файлів (pdf, .djvu), електронні перекладачі текстів, електронні словники, мультимедійне програмне забезпечення тощо.*
Виконання та захист кваліфікаційної роботи магістра	підсумкова атестація	*ОК12.pdf*	GI1LmBJSxOXsgrcQ6dfHNbti5KytGi3aXa3tQlH9+Ks=	*Комп'ютерний клас: 10 ПК Intel Core 2 Duo E8400 (Windows 10, Kali Linux, WireShark, Nessus, Metasploit, JetBrains Tools, MySQL, MongoDB, Nmap, Cisco Packet Tracer). Полігон кібербезпеки: маршрутизатор Cisco ISR4221, керований комутатор Cisco, міжмережевий екран Cisco, сервер Metasploitable 2. Лабораторія технічного захисту інформації. Мережева академія Cisco Networking Academy. Підключення до Інтернет*

Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	навчальна дисципліна	*ОК8.pdf*	i5s84nD/kT23bCOtEI3wc67kzDODCkZxZABikvI8ozU=	*Аудиторія для проведення лекційних занять. Мультимедійний проектор Epson. Wi-Fi-інтернет. Комп'ютерний клас: 10 ПК Intel Core 2 Duo E8400 (Windows 10, Kali Linux, WireShark, Nessus, Metasploit). Кіберполігон кафедри ТЕІБ: маршрутизатор Cisco ISR4221, керований комутатор Cisco, міжмережевий екран Cisco, сервер Metasploitable 2. Система електронного навчання Moodle https://e-learn.uzhnu.edu.ua.*

* 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
200340	Пагіря Михайло Михайлович	професор, Основне місце роботи	Фізичний факультет	Диплом спеціаліста, УжДУ, рік закінчення: 1981, спеціальність: математика, Диплом доктора наук ДД 008590, виданий 23.04.2019, Диплом кандидата наук КН 012313, виданий 17.10.1996, Атестат доцента ДЦ 001392, виданий 20.02.2001	40	Методи побудови та аналізу криптосистем	Досвід наукової та педагогічної роботи складає понад 40 років. Проводить дослідження з використання теорії ланцюгових дробів в різних областях. Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОП, що засвідчується виконанням підпунктів: 1,3,4,5,7,8,19 п.38 чинних Ліцензійних умов «Види та результати професійної діяльності». Автор монографії Пагіря М.М. Наближення функцій ланцюговими дробами. Ужгород, Гражда, 2016. 412 с. Має публікації, які за напрямком відповідають навчальній дисципліні: 1. Ю. Мисло, М. Пагіря Криптоаналіз асиметричних ключів алгоритмами ланцюгових дробів // ITSec: Безпека інформаційних технологій: матеріали XII Міжнар. наук.-

техн. конф., м. Ужгород, 2-4 трав. 2023 р. К.: НАУ, 2023. С. 36.

2. Ю. Мисло, М. Пагіря, В. Різак Елементи математичних методів у криптології. Навч. посіб. для студ. Спец. "Кібербезпека та захист інформації". Ужгород, Вид--во УжНУ "Говерла", 2023. 136 с.

3. Мисло Ю.М, Пагіря М.М., Різак В.М. Математичні основи криптографії, Методичний посібник до практичних занять. Ужгород, 2022, 77 с

4. Ю. Мисло, М. Пагіря Оскуляторний інтерполяційний ланцюговий дріб Тіле // Proceedings of the International Geometry Center. 2022. Vol. 15, № 2. P. 138–160.

5. M. Pahirya On zeros of the numerator and denominator polynomials of Thiele's continued fraction // Ukrainian Mathematical Journal. 2022. Vol. 74, № 1. P. 131-141.

6. M. Pahirya Continued fraction representation of the generating function of Bernoulli polynomials // Journal of Mathematical Sciences. 2022. Vol. 262, № 2. P. 194-206.

7. M. Pairya A continuant and an estimate of the remainder of the interpolating continued C-fraction // Matematychni Studii. 2020. Vol. 54, № 1. P. 32-45.

8. M. Pahirya Application of a Continuant to the Estimation of a Remainder Term of Thiele's Interpolation Continued Fraction // Journal of Mathematical Sciences. 2020. Vol. 246, № 5. P. 687-700.

9. M. Pahirya Representation of a one class functions of two variables by bicontinued fractions //

							Researches in Mathematics. 2019. Vol. 27 (2). P. 13-27. Підвищення кваліфікації в Національному авіаційному університеті. Тема: “Вдосконалення професійної підготовки, поглиблення професійних знань, умінь із дисциплін “Методи побудови та аналізу криптосистем” та “Основи наукових досліджень сферах кіберзахисту і технічного захисту інформації””, 180 год (6 кредитів ЄКТС), з 1 квітня по 30 червня 2023 р (Наказ НАУ №115/08 від 22.03.2023 р)
200340	Пагіря Михайло Михайлович	професор, Основне місце роботи	Фізичний факультет	Диплом спеціаліста, УжДУ, рік закінчення: 1981, спеціальність: математика, Диплом доктора наук ДД 008590, виданий 23.04.2019, Диплом кандидата наук КН 012313, виданий 17.10.1996, Атестат доцента ДЦ 001392, виданий 20.02.2001	40	Наукові комунікації та основи наукових досліджень у сферах кіберзахисту і технічного захисту інформації	Досвід наукової та педагогічної роботи складає понад 40 років. Доктор фізико-математичних наук, професор. Проводить дослідження з використання теорії ланцюгових дробів в різних областях. Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОП, що засвідчується виконанням підпунктів: 1,3,4,5,7,8,19 п.38 чинних Ліцензійних умов «Види та результати професійної діяльності». Підвищення кваліфікації в Національному авіаційному університеті. Тема: “Вдосконалення професійної підготовки, поглиблення професійних знань, умінь із дисциплін “Методи побудови та аналізу криптосистем” та “Основи наукових досліджень сферах кіберзахисту і технічного захисту інформації””, 180 год (6 кредитів ЄКТС), з 1 квітня по 30 червня 2023 р (Наказ НАУ №115/08 від 22.03.2023 р)
452940	Давиденко	Професор,	Фізичний	Диплом	34	Системи	Академічна та

	Анатолій Миколайович	Сумісництво	факультет	спеціаліста, Київський інститут інженерів цивільної авіації, рік закінчення: 1986, спеціальність: Автоматизовані системи управління, Диплом доктора наук ДД 011826, виданий 29.06.2021, Диплом кандидата наук КД 025625, виданий 21.11.1990, Атестат старшого наукового співробітника (старшого дослідника) АС 001853, виданий 13.06.2001		виявлення вразливостей і реагування на кіберінциденти та кібератаки	професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОП, що засвідчується виконанням підпунктів: 1,2,3,4,5,7,8,12,19 п.38 чинних Ліцензійних умов «Види та результати професійної діяльності». Має другу вищу освіту, яка відповідає навчальній дисципліні (Інформаційна безпека, НТТУ КПІ, диплом 12СПК 952747 від 22.05.2015). Має 30-річний досвід практичної та наукової роботи в галузі захисту інформації, Лауреат премії ім.С.О.Лебедева (2017 р.), захистив докторську дисертацію (13.05.2021) за тематикою, яка відповідає навчальній дисципліні «Методи та моделі адаптивного захисту та розмежування доступу до розподілених інформаційних ресурсів», спеціальність 05.13.21 – Системи захисту інформації. Має публікації, які за напрямком відповідають навчальній дисципліні, наприклад: 1. Корченко А., Давиденко А., Шабан М., Казмірчук С., Структурна модель СППР при проведенні державних експертиз КСЗІ.– Безпека інформації.– 2020.– Т.26.– № 1.–С.14-27. 2. А.М. Давиденко, С.Я. Гільгурт, М.Р. Шабан, «Апаратно-програмний комплекс підтримки прийняття рішень при проведенні державних експертиз комплексних систем захисту інформації», Патент UA 139730 U; G06F17/27. Патент опубліковано 10.01.2020, бюл. № 1 3. O. Vysotska, A. Davydenko, «Keystroke Pattern Authentication of Computer Systems

							Users as One of the Steps of Multifactor Authentication», Advances in Computer Science for Engineering and Education II. Advances in Intelligent Systems and Computing, vol. 938, pp. 356-368, 2019. 4. О. Корченко, А. Давиденко, О. Висоцька, «Метод автентифікації користувачів інформаційних систем за їх рукописним почерком з багатокроковою корекцією первинних даних», Захист інформації, Том 21, №1, С. 40-51, 2019. 5. О. Корченко, А. Давиденко, М. Шабан, «Декомпозиційна модель представлення смислових констант та змінних для реалізації експертиз у сфері ТЗІ», Захист інформації, Том 21, № 2, С. 88-96, 2019. 6. О. Корченко, А. Давиденко, М. Шабан, «Модель параметрів для ідентифікації функціонального профілю захисту в комп'ютерних системах», Безпека інформації, Том 25, № 2, С.122-126, 2019. 7. О. Корченко, А. Давиденко, М. Шабан, І. Іванченко, «Метод ідентифікації функціонального профілю захисту», Захист інформації, Том 21, № 4, С.252-258, 2019. 8. А. М. Давиденко, О. А. Суліма, «Аналіз функціональних можливостей окремих компонент засобів захисту інформаційних систем», Моделювання та інформаційні технології. Зб. наук. праць, Вип. 84, С.103-111, 2018.
127444	Різак Василь Михайлович	завідувач кафедри, Основне місце роботи	Фізичний факультет	Диплом спеціаліста, УжДУ, рік закінчення: 1985, спеціальність: 7.04020301 фізика, Диплом доктора наук ДН 002908, виданий 04.12.1996, Диплом кандидата наук	38	Методика викладання фахових дисциплін у вищій школі	Досвід наукової та педагогічної роботи складає понад 30 років. Проводить наукові дослідження в галузях методики викладання навчальних дисциплін та фізико-технологічних основ запису та захисту інформації. Академічна та професійна

				ФМ 035710, виданий 23.03.1989, Атестат доцента ДЦ 005427, виданий 29.05.1997, Атестат професора ПР 001716, виданий 25.06.1998			кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОП, що засвідчується виконанням підпунктів: 1,2,3,4,7,8,9,10,19 п.38 чинних Ліцензійних умов «Види та результати професійної діяльності». Підвищення кваліфікації в Закарпатському інституті післядипломної педагогічної освіти, "Інноваційні методи навчання у закладі вищої освіти", 6 кредитів (Наказ ЗІППО №72 від 13.09.2022 р) та Pavol Jozef Šafárik University in Kosice (17.07-21.07.23). Стажування в Департаменті кіберполіції НПУ (24.07-31.08.23) та Управлінні Держспецзв'язку в Закарпатській обл. (11.09-22.09.23); Має публікації, які за напрямком відповідають навчальній дисципліні, наприклад: 1. Yevseiev, S., Herasymov, S., Kuznietsov, O., Opirskyy, I., Volkov, A., Peleshok, Y., Sinitsyn, I., Milevskyi, S., Matovka, T., & Rizak, V. (2023). Method of assessment of frequency resolution for aircraft. Eastern-European Journal of Enterprise Technologies, 2(9 (122), 34–45. https://doi.org/10.15587/1729-4061.2023.277898 2. V.S. Bilanych, O. Shylenko, P.M. Lytvyn, V.V. Bilanych, V. Rizak, A. Feher, V. Komanicky, Electron-induced effects in Ge-Se films studied by Kelvin probe force microscopy, //J.Non-Cryst. Sol., v.601 (2023) p.121964, https://doi.org/10.1016/j.jnoncrysol.2022.121964 3. Боценюк Л.Р., Матьовка Т.В., Буковецький В.І., Різак В.М. Прихована програма для заміток

							з безпечним зберіганням даних. 2023, С. 144-158 . Розділ у колективній монографії //МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ, ЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ, НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ, ГО «АСОЦІАЦІЯ СПЕЦІАЛІСТІВ КІБЕРБЕЗПЕКИ»: АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ " 4. Програмний продукт для пошуку та виявлення програм типу Spyware/ О. Ковальов, О. Чобаль, В. Різак, М. Пригара// Захист інформації. – 2022. – Том 24, №1. – С. 37-42. 5. Trikur, I., Batori-Tartsi, Z., Sichka, M., Rizak, G., Rizak, V. (2022). Design of chemically modified bacteriorhodopsin films for information protection systems. Eastern-European Journal of Enterprise Technologies, 5 (6 (119)), 6–14. DOI: 10.15587/1729-4061.2022.265858 6. Bukovetskyi, V., & Rizak, V. (2022). Developing the algorithm and software for access token protection using request signing with temporary secret. Eastern-European Journal of Enterprise Technologies, 1(9(115), 56–62. https://doi.org/10.15587/1729-4061.2022.251570 7. Akhmetov B.S., Abuova A.K., Izbasova N.B., Zhilkishbayev A.A., Gerasymchuk N., Matovka T., Rizak V MODELS AND ALGORITHMS FOR OPTIMIZING THE RESERVE OF EQUIPMENT TO ENSURE THE CYBERSECURITY OF THE INFORMATION EDUCATIONAL ENVIRONMENT OF THE UNIVERSITY Journal of Theoretical and Applied Information Technology 30th September 2022.

							Vol.100. No 18 p. 5286-5297. 8. O.Shylenko, B.Bilanych, V.Bilanych, V.Latyshev, K.Saksl, Z.Molcanova, B.Ballokova, J.Durisin, P.Lytvyn, A.Feher, V.Rizak, V.Komanicky. Investigation of structural changes in AsxSe100-x amorphous thin films after electron beam irradiation with XAFS, XANES and Kelvin Force Microscopy. //Appl.Surf.Science, v.530 (2020) p.147266. https://doi.org/10.1016/j.apsusc.2020.147266 9. Програмний продукт типу Spyware та аналіз його стійкості до виявлення засобами захисту / О. Ковальов, О. Чобаль, В. Різак // Захист інформації. – 2020. – Том 22, №3. – С. 176-183. 10. B.V. Bilanych, O Shylenko, V.M. Latyshev, A Feher, V.S. Bilanych, V.M. Rizak, V Komanicky Interaction of Chalcogenide As4Se96 Films with Electron Beam When Used as Electronic Resists. Ukrainian Journal of Physics, Vol. 65 No. 3 (2020) DOI: https://doi.org/10.15407/ujpe65.3.247 11. V.Komanicky; V.Latyshev; O.Shylenko; V.Bilanych; V.Stamenkovic; V.Rizak; A.Feher; A.Kovalcikova. Turning catalysts on by light induced stress: When red means go. //J.ChemPubSoc Europe, v.6 (2019) p. 3264-3267. https://doi.org/10.1002/celc.201900393 12. O.Shylenko, V.Bilanych, A.Feher, V.Rizak, V.Komanicky. Evaluation of sensitivity of Ge9As9Se82 and Ge16As24Se60 thin films to irradiation with electron beam. //J. Non-Cryst.Solids, v.505 (2019) p.37–42. https://doi.org/10.1016/j.jnoncrysol.2018.10.042 13. І. І. Трикур, М. Ю. Січка, І. Й. Цьома, А. М. Потапчук, В. М. Різак Методика пошарового нанесення плівок та характеристики двошарових структур

							на основі бактеріородопсину // Науковий вісник Ужгородського університету. Серія Фізика.-2019.-Випуск46, с.48-53 https://doi.org/10.24144/2415-8038.2019.46.48-53 14. Шифрування кольорових зображень з використанням матриць Адамара/А. Фролов, О. Чобаль, В.М. Різак// Захист інформації. – 2019. – Том 21, № 4. – С. 241-246 15. В.М. Різак, С.Г. Литвинова, О.М. Соколюк, О.І. Чобаль Шкільний фізичний експеримент з використанням цифрових вимірювальних комплексів: старша школа Навчально-методичний посібник [за заг. ред. проф. В.М. Різака]. – Ужгород: Вид-во УжНУ «Говерла», 2019. – 256 с. (16 арк) 16. J. Raganová, S. Holec, M. Hruška, M. Spodniaková Pfefferová, T.Pivarči, O. Chobal, V.Rizak STEM aktivity na vyučovanie prírodovedných predmetov: fyzika, biológia, geografia. Pracovné listy k praktickým cvičeniam v slovenskom a ukrajinskom jazyku, Vydavateľ: Belianum. Vydavateľstvo UMB. 2022, 54 p. ISBN 978-80-557-1517-9 17. Мисло Ю.М, Пагіря М.М., Різак В.М. Математичні основи криптографії, Методичний посібник до практичних занять. Ужгород, 2022, 77 с 18. Ю. Мисло, М. Пагіря, В. Різак Елементи математичних методів у криптології. Навч. посіб. для студ. Спец. "Кібербезпека та захист інформації". Ужгород, Вид--во УжНУ "Говерла", 2023. 136 с. 19. Василь РІЗАК, Магдалина ОПАЧКО, Наталія ДЕШКО, Інноваційний підхід у фаховій підготовці фізиків, «Фізико-математична освіта / Physical and Mathematical

							Education», Том 38 № 4, 2023 (У друці)
283454	Чейпеш Іванна Василівна	Доцент кафедри іноземних мов, Основне місце роботи	Факультет іноземної філології	Диплом спеціаліста, -, рік закінчення: 2012, спеціальність: , Диплом спеціаліста, Державний вищий навчальний заклад "Ужгородський національний університет", рік закінчення: 2014, спеціальність: Англійська мова та література, Диплом кандидата наук ДК 003600, виданий 19.01.2012, Атестат доцента 12ДЦ 039136, виданий 25.06.2014	16	Іноземна мова для професійної діяльності	Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОП, що засвідчується виконанням підпунктів: 1,4,12,19 п.38 чинних Ліцензійних умов «Види та результати професійної діяльності». Відповідність освітньої та/або професійної кваліфікації освітньому компоненту визначається: - дипломом про вищу освіту за спеціальністю «Англійська мова та література»; - дипломом кандидата педагогічних наук ДК№003600 спеціальності 13.00.04 – теорія і методика професійної освіти; - атестатом доцента кафедри іноземних мов 12 ДЦ №039136, виданий Міністерством освіти і науки України 25 червня 2014 р. Основні публікації: 1) Чейпеш І.В., Бура І.О. Методичні рекомендації з дисципліни «Іноземна мова для професійної комунікації (для спеціальності: 125 Кібербезпека та захист інформації» / І.В.Чейпеш, І.О.Бура) – Ужгород: УжНУ, 2023. - 44с. 2) Effectiveness of the development of critical thinking in the lessons of world literature in secondary school. I. Cheypesh, O. Stepanenko, N. Bedzir, M. Demchyk/ Apuntes Universitarious, ESCI Web of Science, 398-414 3) Чейпеш І.В. Інтеграція компетентностей в іншомовній освіті сучасних фахівців. Науковий вісник Мукачівського державного університету. Збірник наукових праць. Серія «Педагогіка та психологія». Випуск 1(9). Мукачево, 2019.

							С.191 – 194. 4) Чейпеш І.В. Розвиток комунікативної компетентності студентів – майбутніх фахівців освітньої сфери. Матеріали V всеукраїнської науково-практичної конференції «Україна і Центральна Європа: історія, політика, культура». Ужгород: ТОВ «РІК-У», 2020. С. 317 –320. 5) Чейпеш І.В., Ваколя З.М., Чусова О.М. Педагогічні основи дистанційного навчання. Науковий часопис Національного педагогічного університету ім. М.П. Драгоманова. Вип. 80. Київ, 2021. С.167 – 170. Підвищення кваліфікації: 1. З 25 липня по 16 серпня 2021 р. – стажування (6 кредитів ECTS, 180 год.) за міжнародною науковою програмою «Видатні особистості: навчальний досвід і професійні досягнення у формуванні успішної особистості і світової трансформації». Інститут історичної біографії (Historical Biographical Institute): Дубай, Нью Йорк, Рим, Єрусалим, Пекін. Сертифікат № 1001 , виданий 12 серпня 2021 р. 2. З 26 липня по 2 серпня 2021 р. – стажування (1,5 кредитів ECTS, 45 год.) за міжнародною програмою «Інноваційні форми сучасної освіти з використанням програм Zoom і Moodle». Міжнародна спілка освітян і науковців (International Foundation of Educators and Scholars), Польща, Люблін. Сертифікат ESN№7210/2021, виданий 2 серпня 2021 р.
452940	Давиденко Анатолій Миколайович	Професор, Сумісництво	Фізичний факультет	Диплом спеціаліста, Київський інститут інженерів цивільної авіації, рік	34	Безпека хмарних технологій та розподілених обчислень	Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання

				закінчення: 1986, спеціальність: Автоматизовані системи управління, Диплом доктора наук ДД 011826, виданий 29.06.2021, Диплом кандидата наук КД 025625, виданий 21.11.1990, Атестат старшого наукового співробітника (старшого дослідника) АС 001853, виданий 13.06.2001			ОП, що засвідчується виконанням підпунктів: 1,2,3,4,5,7,8,12,19 п.38 чинних Ліцензійних умов «Види та результати професійної діяльності». Має другу вищу освіту, яка відповідає навчальній дисципліні (Інформаційна безпека, НТТУ КПІ, диплом 12СПК 952747 від 22.05.2015). Має 30-річний досвід практичної та наукової роботи в галузі захисту інформації, Лауреат премії ім.С.О.Лебедева (2017 р.), захистив докторську дисертацію (13.05.2021) за тематикою, яка відповідає навчальній дисципліні «Методи та моделі адаптивного захисту та розмежування доступу до розподілених інформаційних ресурсів», спеціальність 05.13.21 – Системи захисту інформації. Має публікації, які за напрямком відповідають навчальній дисципліні, наприклад: 1. Корченко А., Давиденко А., Шабан М., Казмірчук С., Структурна модель СППР при проведенні державних експертиз КСЗІ.– Безпека інформації.– 2020.– Т.26.– № 1.–С.14-27. 2. А.М. Давиденко, С.Я. Гільгурт, М.Р. Шабан, «Апаратно-програмний комплекс підтримки прийняття рішень при проведенні державних експертиз комплексних систем захисту інформації», Патент UA 139730 U; G06F17/27. Патент опубліковано 10.01.2020, бюл. № 1 3. O. Vysotska, A. Davydenko, «Keystroke Pattern Authentication of Computer Systems Users as One of the Steps of Multifactor Authentication», Advances in Computer Science for Engineering and Education II.

							Advances in Intelligent Systems and Computing, vol. 938, pp. 356-368, 2019. 4. О. Корченко, А. Давиденко, О. Висоцька, «Метод автентифікації користувачів інформаційних систем за їх рукописним почерком з багатокроковою корекцією первинних даних», Захист інформації, Том 21, №1, С. 40-51, 2019. 5. О. Корченко, А. Давиденко, М. Шабан, «Декомпозиційна модель представлення смислових констант та змінних для реалізації експертиз у сфері ТЗІ», Захист інформації, Том 21, № 2, С. 88-96, 2019. 6. О. Корченко, А. Давиденко, М. Шабан, «Модель параметрів для ідентифікації функціонального профілю захисту в комп'ютерних системах», Безпека інформації, Том 25, № 2, С.122-126, 2019. 7. О. Корченко, А. Давиденко, М. Шабан, І. Іванченко, «Метод ідентифікації функціонального профілю захисту», Захист інформації, Том 21, № 4, С.252-258, 2019. 8. А. М. Давиденко, О. А. Суліма, «Аналіз функціональних можливостей окремих компонент засобів захисту інформаційних систем», Моделювання та інформаційні технології. Зб. наук. праць, Вип. 84, С.103-111, 2018.
452813	Фролов Артем Олександрович	асистент, Основне місце роботи	Фізичний факультет	Диплом бакалавра, Державний вищий навчальний заклад "Ужгородський національний університет", рік закінчення: 2013, спеціальність: Системи технічного захисту інформації, Диплом магістра, Державний вищий навчальний	1	Моніторинг та аудит інформаційно-комунікаційних систем	Проводить практичні заняття з даної дисципліни. Магістр інформаційної безпеки (спеціальність "Системи технічного захисту інформації"). Професіонал- практик в галузі програмування та інформаційної безпеки (ФОП - 62.01 Комп'ютерне програмування з 2012 року).

				заклад "Ужгородський національний університет", рік закінчення: 2014, спеціальність: Системи технічного захисту інформації, автоматизація її обробки			
52330	Чобаль Олександр Ілліч	доцент, Основне місце роботи	Фізичний факультет	Диплом магістра, Ужгородський національний університет, рік закінчення: 2006, спеціальність: 070101 Фізика, Диплом кандидата наук ДК 019260, виданий 17.01.2014	15	Моніторинг та аудит інформаційно-комунікаційних систем	Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОП, що засвідчується виконанням підпунктів: 1,3,4,10,15,19 п.38 чинних Ліцензійних умов «Види та результати професійної діяльності». Підвищення кваліфікації: 1. Національний авіаційний університет. Тема: “Вдосконалення професійної підготовки, поглиблення професійних знань, умінь із дисциплін “Математичне моделювання процесів та систем у сфері захисту інформації” і “Моніторинг та аудит кібербезпеки””, 180 год (6 кредитів ЄКТС), з 1 квітня по 30 червня 2023 р (Наказ НАУ №115/08 від 22.03.2023 р) 2. Cisco Networking Academy, Підвищення кваліфікації з курсу CyberOps Associate (Instructor level), 23 квітня 2021 р, 70 год. (сертифікований інструктор Cisco за напрямками CyberOPS, CCNA Cybersecurity та IoT Security); 3. Курси підвищення кваліфікації “Оцінка захищеності інформації в інформаційно-комунікаційних системах”, Центр перепідготовки та підвищення кваліфікації фахівців у галузі інформаційної

							безпеки при НТУУ “КПІ ім.Сікорського”, свідоцтво № 12СПК 408732. 4. Наукове стажування в Matej Bel University in Banská Bystrica (01.04.22 - 31.07.22) Проводить наукові дослідження в галузі кібербезпеки. Основні публікації: 1. Кількісна оцінка кіберзахищеності інформації / В. Хорошко, Ю. Хохлачова, Н. Вишневська, О. Чобаль// Захист інформації. – 2023. – Т.25 (№2). – С. 70-76. 2.Метод формування параметрів функціональних обов’язків для оцінки загроз в соціотехнічних системах/ А. Корченко, С. Мацюк, О. Чобаль, О. Кручінін, Т. Паращук// Information Technology: Computer Science, Software Engineering and Cyber Security. – 2022. – №3. – С. 19-26. 3.Програмний продукт для пошуку та виявлення програм типу Spyware/ О. Ковальов, О. Чобаль, В. Різак, М. Пригара// Захист інформації. – 2022. – Том 24, №1. – С. 37-42. 4. Програмний продукт типу Spyware та аналіз його стійкості до виявлення засобами захисту / О. Ковальов, О. Чобаль, В. Різак // Захист інформації. – 2020. – Том 22, №3. – С. 176-183. 5. Шифрування кольорових зображень з використанням матриць Адамара/А. Фролов, О. Чобаль, В.М. Різак// Захист інформації. – 2019. – Том 21, № 4. – С. 241-246 6. Y. Tkach, A. Shyian, O. Vasylieva and O. Chobal. Method for Analyzing the Connection Between the Regional Population and Social Network Narratives Under of the Information Operation //Forum "Digital

							Reality" 2023. V.45 7. І. Трикур, М. Січка , О. Чобаль, Г. Різак, В. Різак. Багатофункціональні оптичні елементи на основі бактеріородопсину у системах контролю доступу та інформаційної безпеки// ITSec: Безпека інформаційних технологій: матеріали XII Міжнар. наук.-техн. конф., м. Ужгород, 2-4 трав. 2023 р. К.: НАУ, 2023. С. 58.
52330	Чобаль Олександр Ілліч	доцент, Основне місце роботи	Фізичний факультет	Диплом магістра, Ужгородський національний університет, рік закінчення: 2006, спеціальність: 070101 Фізика, Диплом кандидата наук ДК 019260, виданий 17.01.2014	15	Математичне моделювання процесів та систем у сфері захисту інформації	Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОП, що засвідчується виконанням підпунктів: 1,3,4,10,15,19 п.38 чинних Ліцензійних умов «Види та результати професійної діяльності». Проводить наукові дослідження в галузі ab initio методів математичного моделювання. Підвищення кваліфікації: 1. Національний авіаційний університет. Тема: “Вдосконалення професійної підготовки, поглиблення професійних знань, умінь із дисциплін “Математичне моделювання процесів та систем у сфері захисту інформації” і “Моніторинг та аудит кібербезпеки””, 180 год (6 кредитів ЄКТС), з 1 квітня по 30 червня 2023 р (Наказ НАУ №115/08 від 22.03.2023 р) 2. Cisco Networking Academy, Підвищення кваліфікації з курсу CyberOps Associate (Instructor level), 23 квітня 2021 р, 70 год. (сертифікований інструктор Cisco за напрямками CyberOPS, CCNA Cybersecurity та IoT Security);

							3. Курси підвищення кваліфікації “Оцінка захищеності інформації в інформаційно-комунікаційних системах”, Центр перепідготовки та підвищення кваліфікації фахівців у галузі інформаційної безпеки при НТУУ “КПІ ім.Сікорського”, свідоцтво № 12СПК 408732. 4. Наукове стажування в Matej Bel University in Banská Bystrica (01.04.22 - 31.07.22) Основні публікації: 1. Кількісна оцінка кіберзахищеності інформації / В. Хорошко, Ю. Хохлачова, Н. Вишневська, О. Чобаль// Захист інформації. – 2023. – Т.25 (№2). – С. 70-76. 2.Метод формування параметрів функціональних обов’язків для оцінки загроз в соціотехнічних системах/ А. Корченко, С. Мацюк, О. Чобаль, О. Кручінін, Т. Паращук// Information Technology: Computer Science, Software Engineering and Cyber Security. – 2022. – №3. – С. 19-26. 3.Програмний продукт для пошуку та виявлення програм типу Spyware/ О. Ковальов, О. Чобаль, В. Різак, М. Пригара// Захист інформації. – 2022. – Том 24, №1. – С. 37-42. 4. Програмний продукт типу Spyware та аналіз його стійкості до виявлення засобами захисту / О. Ковальов, О. Чобаль, В. Різак // Захист інформації. – 2020. – Том 22, №3. – С. 176-183. 5. Шифрування кольорових зображень з використанням матриць Адамара/А. Фролов, О. Чобаль, В.М. Різак// Захист інформації. – 2019. – Том 21, № 4. – С. 241-246 6. Y. Tkach, A. Shyian,

							O. Vasylieva and O. Chobal. Method for Analyzing the Connection Between the Regional Population and Social Network Narratives Under of the Information Operation //Forum "Digital Reality" 2023. V.45 7. І. Трикур, М. Січка , О. Чобаль, Г. Різак, В. Різак. Багатофункціональні оптичні елементи на основі бактеріородопсину у системах контролю доступу та інформаційної безпеки// ITSec: Безпека інформаційних технологій: матеріали XII Міжнар. наук.-техн. конф., м. Ужгород, 2-4 трав. 2023 р. К.: НАУ, 2023. С. 58.
353614	Пригара Михайло Петрович	доцента, Основне місце роботи	Інженерно-технічний факультет	Диплом спеціаліста, Київський національний університет будівництва і архітектури, рік закінчення: 2010, спеціальність: 080401 Інформаційні управляючі системи та технології, Диплом кандидата наук ДК 050146, виданий 18.12.2018	9	Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОП, що засвідчується виконанням підпунктів: 1,4,5,19 п.38 чинних Ліцензійних умов «Види та результати професійної діяльності». Захистив кандидатську дисертацію за тематикою, яка відповідає навчальній дисципліні «Захищена система технічної підтримки процесів дистанційного волевиявлення” (спеціальність 05.13.21 - „Системи захисту інформації”) Має публікації, які за напрямком відповідають навчальній дисципліні, наприклад: 1.Генерування випадкових чисел штатними засобами хостів мережі Інтернет./ В.М. Чуприн, В.М.Вишняков, М.П. Пригара // Захист інформації. – 2016. – Т. 18, №4 – С. 323-335. 2.Захист операційного середовища систем Інтернет голосування./ В.М.

							Чуприн, В.М. Вишняков, М.П. Пригара // Захист інформації. – 2017. - Т. 19, №1 – С. 56-66. 3. Доказ можливості повноцінного аудиту систем таємного Інтернет-голосування/Хлапоні н Ю. І., Вишняков В. М., Пригара М. П., Шпак О. І. //. 2023. Розділ у колективній монографії //МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ, ЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ, НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ, ГО «АСОЦІАЦІЯ СПЕЦІАЛІСТІВ КІБЕРБЕЗПЕКИ»: АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ " 4. Програмний продукт для пошуку та виявлення программ типу spyware/ Олександр Ковальов, Олександр Чобаль, Василь Різак, Михайло Пригара// Захист інформації.- 2022. – Т.24, №1 – С. 37-42.
192653	Канюк Олександра Любомирівн а	завідувач кафедри, Основне місце роботи	Факультет іноземної філології	Диплом спеціаліста, Ужгородський державний університет, рік закінчення: 1994, спеціальність: 7.02030302 мова і література(нім ецька), Диплом спеціаліста, Ужгородський державний університет, рік закінчення: 1998, спеціальність: , Диплом магістра, Державний вищий навчальний заклад "Ужгородський національний університет", рік закінчення: 2020, спеціальність: 014 Середня освіта, Диплом кандидата наук ДК 061011, виданий 01.07.2010,	27	Іноземна мова для професійної діяльності	Академічна та професійна кваліфікація забезпечує досягнення цілей та програмних результатів навчання ОП, що засвідчується виконанням підпунктів: 1,4,8,12,19 п.38 чинних Ліцензійних умов «Види та результати професійної діяльності». Відповідність освітньої та/або професійної кваліфікації освітньому компоненту визначається: - дипломом спеціаліста з відзнакою, Ужгородський державний університет за спеціальністю німецька мова та література; кваліфікація: Філолог. Викладач німецької мови та літератури, дата видачі 28 червня 1994 Серія та номер:

				Атестат доцента 12ДЦ 030366, виданий 17.02.2012			ЛК №000028; - дипломом кандидата педагогічних наук ДК № 061011, спеціальності 13.00.04 – теорія і методика професійної освіти, дата видано 01.07.2010 р. Тернопільським національним педагогічним університетом імені Володимира Гнатюка; - атестатом доцента кафедри іноземних мов, виданий рішенням Атестаційної колегії 17 лютого 2012 р., протокол №2/02 – D; 12ДЦ№030366 - стажуванням: «Підвищення мотивації до навчання засобами наукової освіти»; «Perspective Directions for the Development of Science and Practice»; «Цифрова грамотність державних службовців 1.0. на базі інструментів Google», (платформа Дія, Цифрова освіта); цикл навчальних вебінарів з наукометрії «Головні метрики сучасної науки». Scopus та Web of Science» - Компанія «Наукові публікації – Publ. Science». - (21.05.2021р.); - публікаціями у наукових виданнях: 1. Канюк О.Л., Кіш Н.В., Теличко М.І. Окремі аспекти вивчення іноземної мови у ЗВО в умовах дистанційного навчання. Актуальні питання гуманітарних наук: Міжвузівський збірник наукових праць молодих вчених Дрогобицького державного педагогічного університету імені Івана Франка. Видавничий дім «Гельветика». Вип. 36. ТОМ 1. 2021. С.302 – 307. 2. Канюк О., Кіш Н. Окремі аспекти дистанційного навчання ЗВО. Матеріали X-ї Міжнародної науково-практичної конференції «Розвиток сучасної освіти і науки: результати, проблеми, перспективи. Том X: Ефекти участі в розвитку науки та освіти на відстані.

							Конін-Ужгород-Херсон: Посвіт, 2021. С.126 – 128. 3. Канюк О.Л., Кіш Н.В. Самостійна робота як ефективна складова управління навчально – пізнавальною діяльністю у процесі навчання іноземній мові майбутніх фахівців. Збірник наукових праць. Серія: “Сучасні дослідження з іноземної філології”. 2020. Випуск 18. С.301-308. 4. Канюк О.Л., Хоминець С.І., Повідайчик О.С. Наукові підходи до формування професійної мобільності майбутніх педагогів у вищій школі. East European Scientific Journal. Warsaw, Poland. vol. 1. 05 (57) 2020. P. 9 -14. 5. Канюк О.Л. До питання визначення окремих функцій іноземної мови в процесі професійної підготовки майбутніх фахівців. Збірник наукових праць. Серія: «Сучасні дослідження з іноземної філології». 2019. Випуск 17. С.239-249. 6. Канюк О.Л., Кіш Н.В. Принципи навчання іншомовному діловому спілкуванню студентів немовних факультетів в контексті соціокультурного підходу. Науковий вісник Ужгородського університету. Серія: «Педагогіка. Соціальна робота». 2018. Вип.1(42). 2018. С.87-92.

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

Програмні результати навчання ОП	**ПРН відповідає результату навчання, визначеному стандартом вищої освіти (або охоплює його)**	**Обов’язкові освітні компоненти, що забезпечують ПРН**	**Методи навчання**	**Форми та методи оцінювання**
РН25. Надавати консультативні	☐	Виконання та захист кваліфікаційної	Практичні, проблемні, дослідницькі, навчання у	Публічний захист кваліфікаційної роботи

послуги та технічну допомогу з питань технічного та криптографічного захисту інформації та кіберзахисту.		роботи магістра	співпраці, проєктні	
		Моніторинг та аудит інформаційно-комунікаційних систем	Практичні, проблемні, інтерактивні, контекстні, навчання у співпраці, застосування інформаційно-комп'ютерних технологій	Усне опитування, тестування, захист лабораторних робіт, іспит
		Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки	Практичні, проблемні, інтерактивні, контекстні, навчання у співпраці, застосування інформаційно-комп'ютерних технологій	Усне опитування, тестування, захист лабораторних робіт, іспит
		Наукові комунікації та основи наукових досліджень у сферах кіберзахисту і технічного захисту інформації	Інформаційно-рецептивний метод; репродуктивний метод; евристичний метод; метод проблемного викладу.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні	Захист звіту з практики
		Переддипломна практика	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні	Захист звіту з практики
РН24. Володіти методиками аналізу, синтезу, оптимізації та прогнозування якості процесів функціонування інформаційних процесів та технологій в розподілених інформаційно-комунікаційних системах.	☐	Виконання та захист кваліфікаційної роботи магістра	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні, застосування інформаційно-комп'ютерних технологій	Публічний захист кваліфікаційної роботи
		Переддипломна практика	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні, застосування інформаційно-комп'ютерних технологій	Захист звіту з практики
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні, застосування інформаційно-комп'ютерних технологій	Захист звіту з практики
		Моніторинг та аудит інформаційно-комунікаційних систем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Безпека хмарних технологій та розподілених обчислень	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Математичне моделювання процесів та систем у сфері захисту інформації	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
РН23. Обґрунтовувати вибір програмного	☒	Виконання та захист кваліфікаційної роботи магістра	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні	Публічний захист кваліфікаційної роботи

забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.		Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Моніторинг та аудит інформаційно-комунікаційних систем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Переддипломна практика	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні	Захист звіту з практики
		Безпека хмарних технологій та розподілених обчислень	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Методи побудови та аналізу криптосистем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні	Захист звіту з практики
РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.	☒	Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Безпека хмарних технологій та розподілених обчислень	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Математичне моделювання процесів та систем у сфері захисту інформації	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Методи побудови та аналізу криптосистем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Наукові комунікації та основи наукових досліджень у сферах кіберзахисту і технічного захисту інформації	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
РН21. Використовувати методи натурного, фізичного і	☒	Виконання та захист кваліфікаційної роботи магістра	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні, застосування інформаційно-	Публічний захист кваліфікаційної роботи

комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.			комп'ютерних технологій	
		Переддипломна практика	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні, застосування інформаційно-комп'ютерних технологій	Захист звіту з практики
		Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Математичне моделювання процесів та систем у сфері захисту інформації	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Методи побудови та аналізу криптосистем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.	☒	Наукові комунікації та основи наукових досліджень у сферах кіберзахисту і технічного захисту інформації	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Методи побудови та аналізу криптосистем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні, застосування інформаційно-комп'ютерних технологій	Захист звіту з практики
		Переддипломна практика	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні, застосування інформаційно-комп'ютерних технологій	Захист звіту з практики
		Виконання та захист кваліфікаційної роботи магістра	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні, застосування інформаційно-комп'ютерних технологій	Публічний захист кваліфікаційної роботи
РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту	☒	Методи побудови та аналізу криптосистем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Моніторинг та аудит інформаційно-комунікаційних систем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Переддипломна	Практичні, проблемні,	Захист звіту з практики

інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.		практика	дослідницькі, навчання у співпраці, проєктні	
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні	Захист звіту з практики
		Виконання та захист кваліфікаційної роботи магістра	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні	Публічний захист кваліфікаційної роботи
		Наукові комунікації та основи наукових досліджень у сферах кіберзахисту і технічного захисту інформації	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
РН18.Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.	☒	Методика викладання фахових дисциплін у вищій школі	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; тестування; публічні виступи; залік
		Іноземна мова для професійної діяльності	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; тестування; публічні виступи
		Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Моніторинг та аудит інформаційно-комунікаційних систем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.	☒	Іноземна мова для професійної діяльності	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; тестування; публічні виступи; залік
		Методика викладання фахових дисциплін у вищій школі	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; тестування; публічні виступи; залік
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації,	☒	Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні	Захист звіту з практики
		Переддипломна практика	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні	Захист звіту з практики
		Виконання та захист кваліфікаційної роботи магістра	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні	Публічний захист кваліфікаційної роботи
		Моніторинг та аудит	Пояснювально-	Усне опитування,

прогнозування та прийняття рішень.		інформаційно-комунікаційних систем	ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	тестування, захист лабораторних робіт, іспит
		Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Математичне моделювання процесів та систем у сфері захисту інформації	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Наукові комунікації та основи наукових досліджень у сферах кіберзахисту і технічного захисту інформації	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.	☒	Переддипломна практика	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні, застосування інформаційно-комп'ютерних технологій	Захист звіту з практики
		Виконання та захист кваліфікаційної роботи магістра	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні, застосування інформаційно-комп'ютерних технологій	Публічний захист кваліфікаційної роботи
		Моніторинг та аудит інформаційно-комунікаційних систем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Методи побудови та аналізу криптосистем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.	☒	Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні, застосування інформаційно-комп'ютерних технологій	Захист звіту з практики
		Переддипломна практика	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні, застосування інформаційно-комп'ютерних технологій	Захист звіту з практики
		Виконання та захист кваліфікаційної роботи магістра	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні, застосування інформаційно-комп'ютерних технологій	Публічний захист кваліфікаційної роботи

		Моніторинг та аудит інформаційно-комунікаційних систем	Інформаційно-рецептивний метод; репродуктивний метод; евристичний метод; метод проблемного викладу.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	Інформаційно-рецептивний метод; репродуктивний метод; евристичний метод; метод проблемного викладу.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Методи побудови та аналізу криптосистем	Інформаційно-рецептивний метод; репродуктивний метод; евристичний метод; метод проблемного викладу.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Методика викладання фахових дисциплін у вищій школі	Інформаційно-рецептивний метод; репродуктивний метод; евристичний метод; метод проблемного викладу.	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; тестування; публічні виступи; іспит
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.	☒	Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	Інформаційно-рецептивний метод; репродуктивний метод; евристичний метод; метод проблемного викладу.	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; тестування; публічні виступи; іспит
		Математичне моделювання процесів та систем у сфері захисту інформації	Інформаційно-рецептивний метод; репродуктивний метод; евристичний метод; метод проблемного викладу.	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; тестування; публічні виступи; іспит
		Методи побудови та аналізу криптосистем	Інформаційно-рецептивний метод; репродуктивний метод; евристичний метод; метод проблемного викладу.	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; тестування; публічні виступи; іспит
		Наукові комунікації та основи наукових досліджень у сферах кіберзахисту і технічного захисту інформації	Інформаційно-рецептивний метод; репродуктивний метод; евристичний метод; метод проблемного викладу.	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; тестування; публічні виступи; іспит
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	☒	Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Математичне моделювання процесів та систем у сфері захисту інформації	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Методи побудови та аналізу криптосистем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Моніторинг та аудит інформаційно-комунікаційних систем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
РН11. Аналізувати,	☒	Виконання та захист	Практичні, проблемні,	Публічний захист

контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.		кваліфікаційної роботи магістра	дослідницькі, навчання у співпраці, проєктні, застосування інформаційно-комп'ютерних технологій	кваліфікаційної роботи
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні, застосування інформаційно-комп'ютерних технологій	Захист звіту з практики
		Переддипломна практика	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні, застосування інформаційно-комп'ютерних технологій	Захист звіту з практики
		Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Безпека хмарних технологій та розподілених обчислень	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Методи побудови та аналізу криптосистем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Наукові комунікації та основи наукових досліджень у сферах кіберзахисту і технічного захисту інформації	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.	☒	Безпека хмарних технологій та розподілених обчислень	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Методи побудови та аналізу криптосистем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.	☒	Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	Інформаційно-рецептивний метод; репродуктивний метод; евристичний метод; метод проблемного викладу.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Безпека хмарних технологій та розподілених обчислень	Інформаційно-рецептивний метод; репродуктивний метод; евристичний метод; метод проблемного викладу.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Методи побудови та аналізу криптосистем	Пояснювально-ілюстративні, репродуктивні, проблемний	Усне опитування, тестування, захист лабораторних робіт, іспит

			виклад, частково-пошукові, дослідницькі.	
		Наукові комунікації та основи наукових досліджень у сферах кіберзахисту і технічного захисту інформації	Інформаційно-рецептивний метод; репродуктивний метод; евристичний метод; метод проблемного викладу.	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; публічні виступи; іспит
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	☒	Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні	Захист звіту з практики
		Переддипломна практика	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні	Захист звіту з практики
		Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; тестування; публічні виступи; іспит
		Математичне моделювання процесів та систем у сфері захисту інформації	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; тестування; публічні виступи; іспит
		Методи побудови та аналізу криптосистем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; тестування; публічні виступи; іспит
		Наукові комунікації та основи наукових досліджень у сферах кіберзахисту і технічного захисту інформації	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; тестування; публічні виступи; іспит
		Виконання та захист кваліфікаційної роботи магістра	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні, застосування інформаційно-комп'ютерних технологій	Публічний захист кваліфікаційної роботи
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.	☒	Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	Інформаційно-рецептивний метод; репродуктивний метод; евристичний метод; метод проблемного викладу.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Безпека хмарних технологій та розподілених обчислень	Інформаційно-рецептивний метод; репродуктивний метод; евристичний метод; метод проблемного викладу.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Методи побудови та аналізу криптосистем	Інформаційно-рецептивний метод; репродуктивний метод; евристичний метод; метод проблемного викладу.	Усне опитування, тестування, індивідуальні завдання, іспит
		Математичне моделювання процесів та систем у сфері захисту інформації	Інформаційно-рецептивний метод; репродуктивний метод; евристичний метод; метод проблемного викладу.	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; тестування; публічні виступи; іспит

		Наукові комунікації та основи наукових досліджень у сферах кіберзахисту і технічного захисту інформації	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; тестування; публічні виступи; іспит
РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	☒	Переддипломна практика	Практичні, проблемні, інтерактивні, контекстні, навчання у співпраці, застосування інформаційно-комп'ютерних технологій	Захист звіту з практики
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	Практичні, проблемні, інтерактивні, контекстні, навчання у співпраці, застосування інформаційно-комп'ютерних технологій	Захист звіту з практики
		Методика викладання фахових дисциплін у вищій школі	Пояснювально-ілюстративні, практичні, тренінгові, репродуктивні, навчання у співпраці	Виступи на семінарських заняттях, модульна контрольна робота, залік
		Іноземна мова для професійної діяльності	Пояснювально-ілюстративні, практичні, тренінгові, репродуктивні, навчання у співпраці	Виступи на семінарських заняттях, модульна контрольна робота, залік
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	☒	Математичне моделювання процесів та систем у сфері захисту інформації	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; тестування; публічні виступи; іспит
		Методи побудови та аналізу криптосистем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; тестування; публічні виступи; іспит
		Безпека хмарних технологій та розподілених обчислень	Інформаційно-рецептивний метод; репродуктивний метод; евристичний метод; метод проблемного викладу.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	Інформаційно-рецептивний метод; репродуктивний метод; евристичний метод; метод проблемного викладу.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Переддипломна практика	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні	Захист звіту з практики
		Моніторинг та аудит інформаційно-комунікаційних систем	Інформаційно-рецептивний метод; репродуктивний метод; евристичний метод; метод проблемного викладу.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Виконання та захист кваліфікаційної роботи магістра	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні	Публічний захист кваліфікаційної роботи
		Науково-дослідна практика у сфері безпеки інформаційних і комунікаційних систем	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні	Захист звіту з практики
РН7.Обґрунтовувати використання,	☒	Безпека хмарних технологій та	Пояснювально-ілюстративні,	Усне опитування, тестування, захист

впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.		розподілених обчислень	репродуктивні, проблемний виклад, частково-пошукові, дослідницькі	лабораторних робіт, іспит
		Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі	Усне опитування, тестування, захист лабораторних робіт, іспит
		Методи побудови та аналізу криптосистем	Інформаційно-рецептивний метод; репродуктивний метод; евристичний метод; метод проблемного викладу.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Наукові комунікації та основи наукових досліджень у сферах кіберзахисту і технічного захисту інформації	Інформаційно-рецептивний метод; репродуктивний метод; евристичний метод; метод проблемного викладу.	Усне опитування, тестування, іспит
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	☒	Моніторинг та аудит інформаційно-комунікаційних систем	Практичні, проблемні, інтерактивні, контекстні, навчання у співпраці, застосування інформаційно-комп'ютерних технологій	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; тестування; публічні виступи; іспит
		Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	Практичні, проблемні, інтерактивні, контекстні, навчання у співпраці, застосування інформаційно-комп'ютерних технологій	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; тестування; публічні виступи; іспит
		Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки	Практичні, проблемні, інтерактивні, контекстні, навчання у співпраці, застосування інформаційно-комп'ютерних технологій	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; тестування; публічні виступи; іспит
		Безпека хмарних технологій та розподілених обчислень	Практичні, проблемні, інтерактивні, контекстні, навчання у співпраці, застосування інформаційно-комп'ютерних технологій	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; тестування; публічні виступи; іспит
		Методи побудови та аналізу криптосистем	Практичні, проблемні, інтерактивні, контекстні, навчання у співпраці, застосування інформаційно-комп'ютерних технологій	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; тестування; публічні виступи; іспит
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	☒	Моніторинг та аудит інформаційно-комунікаційних систем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Методи побудови та аналізу криптосистем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Наукові комунікації та основи наукових досліджень у сферах кіберзахисту і технічного захисту інформації	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, захист лабораторних робіт, іспит
РН5. Критично осмислювати проблеми	☒	Науково-дослідна практика у сфері безпеки	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні,	Захист звіту з практики

інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.		інформаційних і комунікаційних систем	застосування інформаційно-комп'ютерних технологій	
		Переддипломна практика	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні, застосування інформаційно-комп'ютерних технологій	Захист звіту з практики
		Виконання та захист кваліфікаційної роботи магістра	Практичні, проблемні, дослідницькі, навчання у співпраці, проєктні, застосування інформаційно-комп'ютерних технологій	Публічний захист кваліфікаційної роботи
		Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем	Інформаційно-рецептивний метод; репродуктивний метод; евристичний метод; метод проблемного викладу.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Безпека хмарних технологій та розподілених обчислень	Інформаційно-рецептивний метод; репродуктивний метод; евристичний метод; метод проблемного викладу.	Усне опитування, тестування, захист лабораторних робіт, іспит
		Методи побудови та аналізу криптосистем	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Усне опитування, тестування, індивідуальні завдання, іспит
		Наукові комунікації та основи наукових досліджень у сферах кіберзахисту і технічного захисту інформації	Пояснювально-ілюстративні, репродуктивні, проблемний виклад, частково-пошукові, дослідницькі.	Вибіркове усне опитування перед початком занять; фронтальне стандартизоване опитування; тестування; публічні виступи; іспит
		Методика викладання фахових дисциплін у вищій школі	Пояснювально-ілюстративні, практичні, тренінгові, репродуктивні, навчання у співпраці	Виступи на семінарських заняттях, модульна контрольна робота, залік