ПРОЄКТ
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
Відгуки, зауваження й пропозиції просимо надсилати гарантові освітньо-професійної програми Йоні Л.Г. до 01 червня 2024 року на електронну адресу: yonalarisa66@gmail.com

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

«ПРИЙНЯТО»
Вченою радою
Міжнародного гуманітарного університету
Протокол № __ __
від «____»_____ 20___

Введено в дію наказом ректора
Міжнародного гуманітарного університету від _____ №___

Ректор _____ К.В. Громовенко

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Галузь знань – 12 Інформаційні технології

Спеціальність – 125 Кібербезпека та захист інформації

Освітній рівень – Магістр

Одеса – 2023

ЛИСТ ПОГОДЖЕННЯ
Освітньо-професійної програми «Кібербезпека»
зі спеціальності 125 Кібербезпека та захист інформації
за другим (магістерським) рівнем вищої освіти

Перший проректор _____ **Василь ЛЕФТЕРОВ**

Начальник навчального відділу _____ **Лариса РАЙЧЕВА**

Декан факультету кібербезпеки, програмної інженерії та комп'ютерних наук _____ **Ірина Стрелковська**

Завідувач кафедри Комп'ютерної інженерії та інноваційних технологій _____ **Лариса Йона**

Гарант програми _____ **Лариса Йона**

Передмова

Освітньо-професійна програма «Кібербезпека» визначає вимоги до рівня освіти осіб, які можуть розпочати навчання за цією програмою; перелік навчальних дисциплін і логічну послідовність їх вивчення (структурно-логічна схема); кількість кредитів Європейської кредитної трансферно-накопичувальної системи (ЄКТС), необхідних для виконання цієї програми; очікувані результати навчання (компетентності), якими повинен оволодіти здобувач відповідного ступеня вищої освіти.

Освітньо-професійна програма розроблена на основі Стандарту вищої освіти за спеціальністю 125 Кібербезпека та захист інформації галузі знань 12 Інформаційні технології для другого (магістерського) рівня вищої освіти. Освітньо-професійна програма «Кібербезпека» поширюється на кафедри університету, які беруть участь у підготовці фахівців другого (магістерського) рівня вищої освіти спеціальності 125 Кібербезпека та захист інформації.

Розроблено проектною групою у складі:

1. ***Йона Лариса Григорівна,*** кандидат технічних наук, доцент кафедри комп'ютерної інженерії та інноваційних технологій Міжнародного гуманітарного університету, *керівник проектної групи (гарант освітньої програми).*
2. ***Стрелковська Ірина Вікторівна,*** доктор технічних наук, професор, декан факультету кібербезпеки, програмної інженерії та комп'ютерних наук Міжнародного гуманітарного університету, *член проектної групи зі складу викладачів групи забезпечення.*
3. ***Григор'єва Тетяна Ігорівна,*** кандидат технічних наук, доцент, завідувач кафедри Інформаційних технологій МГУ, *член проектної групи зі складу викладачів групи забезпечення.*
4. ***Мішин Михаїл Миколайович***, директор Одеського Науково-дослідного інституту зв'язку, *член проектної групи зі складу викладачів групи забезпечення.*
5. ***Севрюков Олександр Володимирович,*** здобувач 2 року навчання другого (магістерського) рівня вищої освіти, член студентського самоврядування за спеціальністю 125 Кібербезпека Міжнародного гуманітарного університету, *член проєктної групи зі складу здобувачів вищої освіти.*

Рецензії-відгуки зовнішніх стейкхолдерів:

1. **Кобозева А. А.,** заступник голови підкомісії 125 Кібербезпека науково-методичної комісії (НМК 7) з інформаційних технологій, автоматизації та телекомунікацій, доктор технічних наук, професор, завідувач кафедри кібербезпеки та програмного забезпечення Одеського національного політехнічного університету.
2. **Лефтеров Л. В.,** Старший науковий співробітник НДЛ з проблемних питань кримінального аналізу Одеського державного університету внутрішніх справ. Начальник 5-го відділу 3-го управління Департаменту кіберполіції Національної поліції України, кандидат юридичних наук.
3. **Мачуський Є. А.,** Д.т.н., професор кафедри інформаційної безпеки Національного технічного університету «Київський політехнічний інститут ім. Ігоря Сікорського, фаховий експерт.
4. **Мішин М. М.,** директор Одеського Науково-дослідного інституту зв'язку.
5. **Плахотнюк О. В.,** Заступник начальника управління, начальник 1-го відділу Управління протидії кіберзлочинам в Одеській області Департаменту кіберполіції Національної поліції України.

Освітньо-професійну програму «Кібербезпека»
розроблено відповідно до:

- Закону України «Про вищу освіту» від 01 липня 2014 р. № 1556-VII (в редакції від 12 травня 2022 р),
- Закону України «Про освіту» від 05 вересня 2017 р. № 2145VIII (в редакції від 06 квітня 2022 р),
- Постанови Кабінету Міністрів України від 30 грудня 2015 р. № 1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності» (в редакції постанови Кабінету Міністрів України від 24 березня 2021 р. № 365),
- Постанови Кабінету Міністрів України від 23 листопада 2011 р. № 1341 «Про затвердження Національної рамки кваліфікацій» (в редакції постанови Кабінету Міністрів України від 25 червня 2020 р. № 519),
- Постанови Кабінету Міністрів України від 29 квітня 2015 р. №266 «Про особливості запровадження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» (із змінами, внесеними згідно з наказом МОН від 12 квітня 2016 р. № 419),
- Листа МОН України від 28.04.2017 р. №1/9-239.
- Національний Класифікатор професій ДК 003:2010. URL: http://dovidnyk.in.ua/directories/profesii
- Національна рамка кваліфікацій. URL: http://zakon3.rada.gov.ua/laws/show/ 1341-2011-п.
- Стандарту вищої освіти зі спеціальності 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для другого (магістерського) рівня вищої освіти (Наказ МОН України від 18.03.2021 № 332.

І. Профіль освітньо-професійної програми
«Кібербезпека»
за спеціальністю 125 Кібербезпека та захист інформації

1.1. Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Міжнародний гуманітарний університет, Факультет кібербезпеки, програмної інженерії та комп'ютерних наук, кафедра комп'ютерної інженерії та інноваційних технологій.
Рівень вищої освіти	Другий (магістерський) рівень
Ступінь вищої освіти	Магістр
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Офіційна назва освітньої програми	Кібербезпека
Освітня кваліфікація	Магістр з кібербезпеки та захисту інформації
Кваліфікація в дипломі	Ступень вищої освіти – Магістр Спеціальність – 125 Кібербезпека та захист інформації Освітня програма – Кібербезпека Кваліфікація: Магістр з кібербезпеки та захисту інформації
Тип диплому та обсяг освітньо-професійної програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 р. 4 місяці
Форма навчання	Денна, заочна
Наявність акредитації	Первинна акредитація у 2023 році
Цикл/рівень	НРК України – 7 рівень, FQ-EHEA – другий цикл, EQF-LLL – 7 рівень
Передумови	Наявність першого (бакалаврського) рівня вищої освіти. Особливості вступу визначаються Правилами прийому до МГУ. Наявність ступеня бакалавра; спеціаліста, магістра (за іншою спеціальністю).
Обмеження щодо форм навчання	Обмеження відсутні
Мова(и) викладання	Українська
Термін дії освітньої програми	1 рік 4 місяці
Інтернет-адреса постійного розміщення опису освітньої програми	https://mgu.edu.ua/
1.2. Мета освітньо-професійної програми	
Підготовка висококваліфікованих фахівців на принципах академічної доброчесності зі здобуттям професійних компетентностей у сфері кібербезпеки, які володіють теоретичними та практичними знаннями та вміннями, мають навички та компетенції з кібербезпеки, володіють сучасними науковими досягненнями, вміють формулювати, розв'язувати практичні задачі у професійній діяльності у системі державних та комерційних підприємств, що пов'язані з наданням послуг щодо захисту інформації на об'єктах інформаційної діяльності з використанням фундаментальних та спеціальних прикладних методів захисту інформації та технологій, мають навички науково-дослідницького та інноваційного характеру у сфері інформаційної та/або кібербезпеки.	

1.3. Характеристика освітньо-професійної програми	
Предметна область	Галузь знань: 12 Інформаційні технології, Спеціальність: 125 Кібербезпека та захист інформації Освітня програма: Кібербезпека. *Об'єкти вивчення та діяльності:* – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; – інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою; – технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. *Цілі навчання* – Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. *Теоретичний зміст предметної області:* Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки, базові математичні, інфологічні, лінгвістичні, економічні концептуальні положення щодо методів захисту інформації. *Методи, методики та технології:* Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. *Інструменти та обладнання:* Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне

	забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
Орієнтація освітньої програми	Освітньо-професійна програма базується на загальновідомих положеннях та результатах сучасних наукових досліджень в IT-галузі та орієнтована на формування фахівця, здатного розв'язувати завдання, акцент програми зроблений на формуванні та розвитку професійних компетентностей щодо захисту інформації на об'єктах інформаційної діяльності; вивченні теоретичних та методичних положень, організаційних та практичних інструментів зі спеціальності кібербезпеки та захисту інформації; методики та технології забезпечення безпеки інформації.
Основний фокус освітньо-професійної програми	Спеціальна освіта в галузі 12 «Інформаційні технології» спеціальності 125 Кібербезпека та захист інформації поглиблені теоретичні та практичні знання в галузі інформаціних технологій з акцентом на формування та розвитку професійних компетентностей щодо захисту інформації на об'єктах інформаційної діяльності; вивчення теоретичних та методичних положень, організаційних та практичних інструментів зі спеціальності кібербезпеки; методики та технології забезпечення безпеки інформації. Передбачається можливість здобувачам вищої освіти самостійно обирати навчальні дисципліни для опанування нових технологій та наукових знань. **Ключові слова:** кібербезпека, захист інформації, комп'ютерні мережі, архітектура безпеки, криптографічний захист, керування доступом, безпека розробки додатків, безпека хмарних технологій, комплексна система захисту.
Особливості програми	Враховує особливості розвитку спеціальності та ринку праці шляхом залучення роботодавців в якості зовнішніх аудиторів навчальних програм та професіоналів, які працюють в системі професійної освіти та на підприємствах в галузі інформаційних технологій, зокрема захисту інформації, а також представники бізнесу, з метою передачі передового досвіду майбутньому фахівцю, висвітлення в навчальному процесі останніх досягнень науки і техніки, правил ведення успішного бізнесу. Передбачає виробничу практику з метою забезпечення умов підготовки фахівця в реальному середовищі майбутньої професійної діяльності. Забезпечує процес навчання здобувачів можливістю застосовувати і використовувати професійні компетентності, які поглиблюють дослідницькі та практичні компетентності. Надає можливість отримання знань спеціальних розділів фундаментальних та професійно-орієнтованих дисциплін, що готують випускника як фахівця з кібербезпеки в інформаційних і комунікаційних системах. Здобувачі 125 спеціальності приймають участь у Проекті USAID «Кібербезпека критично важливої інфраструктури України», зокрема у вебінарах, які відбуваються в онлайн форматі на платформі ZOOM. Також за Проектом USAID проводяться навчання здобувачів на платформі RangeForce з отриманням відповідних ліцензій.

1.4. Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Назви професій згідно Національного класифікатора України: Випускник є придатним для працевлаштування на підприємствах, в організаціях та установах, на яких обробляєтеся інформація з обмеженим доступом, що займаються розробкою та супроводом програмного забезпечення захисту інформації, в державних та банківських установах, інформаційних центрах на посадах відповідно до Національного класифікатора України (Класифікатор професій – ДК 003:2010): 3121 Фахівець з інформаційних технологій 3121 Фахівець з розробки та тестування програмного забезпечення 3439 Фахівець із організації інформаційної безпеки 3439 Фахівець із організації захисту інформації з обмеженим доступом.
Подальше навчання	Можливість продовження підготовки на наступному рівні вищої освіти (доктора філософії): НРК України – 8 рівень, FQ-EHEA – третій цикл, EQFLLL – 8 рівень.
1.5. Викладання та оцінювання	
Викладання та навчання	Лекції, практичні заняття, лабораторні роботи, самостійна робота, консультації з викладачами, практична підготовка, виконання кваліфікаційної роботи.
Оцінювання	Оцінювання включає весь спектр контрольних процедур у залежності від компетентністних характеристик (знання, уміння/навички, комунікація, автономія і відповідальність) результатів навчання, досягнення яких контролюється. Результати навчання студента, що відображають досягнутий ним рівень компетентностей відносно очікуваних, ідентифікуються та вимірюються під час контрольних заходів за допомогою критеріїв, що корелюються з вимогами Національної рамки кваліфікацій і характеризують співвідношення вимог до рівня компетентностей і показників оцінки за рейтинговою шкалою. Оцінювання навчальних досягнень студентів здійснюється за національною шкалою (відмінно, добре, задовільно, незадовільно; зараховано, незараховано); 100-бальною шкалою та шкалою ECTS (A, B, C, D, E, FX, F). Порядок та процедура оцінювання здійснюються відповідно до: «Положення про систему оцінювання навчальних досягнень здобувачів вищої освіти».
1.6. Перелік компетентностей випускника	
Інтегральна компетентність (ІК)	ІК. Здатність розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності (ЗК)	КЗ-1. Здатність застосовувати знання у практичних ситуаціях. КЗ-2. Здатність проводити дослідження на відповідному рівні. КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Фахові компетентності	КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та

	використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ7. Здатність 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. КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки. **Додатково для освітньо-наукових програм** КФ11. Здатність здійснювати наукові та/або прикладні дослідження у галузі інформаційної безпеки та/або кібербезпеки із застосуванням сучасних експериментальних і теоретичних методів моделювання процесів, формувати науково-технічну звітність.

1.7. Програмні результати навчання	
	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. РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. 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. РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. 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. РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. 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. 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.

	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. 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. РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. 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. РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. 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. РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. 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. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації. **Додатково для освітньо-наукових програм** РН24. Планувати та виконувати наукові та прикладні дослідження у сфері інформаційної безпеки та/або кібербезпеки із застосуванням сучасних технологій, експериментальних і теоретичних методів і моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики. РН25. Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.

1.8. Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Кадрове забезпечення відповідає вимогам щодо забезпечення провадження освітньої діяльності для другого рівня вищої освіти відповідно до Ліцензійних умов провадження освітньої діяльності.
Матеріально-технічне забезпечення	Матеріально-технічне забезпечення відповідає вимогам щодо забезпечення провадження освітньої діяльності для другого рівня вищої освіти відповідно до Ліцензійних умов провадження освітньої діяльності. Міжнародний гуманітарний університет має в розпорядженні необхідні для провадження освітньої діяльності за спеціальністю 125 «Кібербезпека та захист інформації » матеріально - технічні ресурси. Здобувачі набувають практичного досвіду при роботі з різноманітним програмним забезпеченням, яке функціонує в навчальних лабораторіях, Міжнародний гуманітарний університет має сучасну соціально-побутову інфраструктуру, забезпечує здобувачів вищої освіти гуртожитками.
Інформаційне та навчально-методичне забезпечення	Наявність офіційного веб-сайту закладу освіти, на якому розміщена основна інформація про його діяльність (структура, ліцензії та сертифікати про акредитацію, освітня/освітньо-наукова/ видавнича/атестаційна (наукових кадрів) діяльність, навчальні та наукові структурні підрозділи та їх склад, перелік навчальних дисциплін, правила прийому, контактна інформація). Фонд бібліотеки універсальний за змістом та складається з підручників, посібників, монографій, довідників, брошур, періодичних видань, дисертацій, авторефератів, навчально-методичної літератури, патентно-ліцензійних документів, нормативно-технічної документації. Єдиний бібліотечний фонд становить 695 478 примірників. З 2022 року фахові періодичні видання надходять в електронному форматі . З 2023 року забезпечено доступ до наступних баз даних : Web of Science (триває з 01.08.2017); Scopus (триває з 01.12.2018); Science Direct (триває з 15 лютого 2021) ; ORCID-ID (триває з 2022); Research 4 lite(триває з 21.09.2023); Наукометрична база index Copernicus; Наукометрична база Google Schalar . У навчальному процесі використовуються такі системи як LMS, Moodle та Google Classroom. Книгозабезпеченність за спеціальністю 125 «Кібербезпека та захист інформації» на одного здобувача освіти з розрахунку 1:5 складає 100%.
1.9. Академічна мобільність	
Національна кредитна мобільність	Студенти, що навчаються за даною освітньою програмою, мають право на перехресний вступ на інші спеціальності, в тому числі із зарахуванням кредитів за суміжними дисциплінами.
Міжнародна кредитна мобільність	Студенти, що навчаються за даною освітньою програмою, мають право на здійснення міжнародної академічної мобільності у термін та на умовах передбачених законодавством України, як в межах укладених договорів та міжнародних програм, так і в особистому порядку.
Навчання іноземних здобувачів вищої освіти	Можливе, за умови володіння українською мовою на рівні, достатньому для навчання.

2. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Форма атестації здобувачів вищої освіти за освітньою програмою «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації – захист кваліфікаційної роботи з отриманням документу встановленого зразка про присудження здобувачеві ступеня магістра з кібербезпеки та захисту інформації. Атестація здійснюється у формі публічного захисту кваліфікаційної роботи.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має розв'язувати складну задачу або проблему з захисту інформації і передбачати проведення досліджень та/або здійснення інновацій. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації. Кваліфікаційна робота має бути оприлюднена на офіційному сайті закладу вищої освіти або його підрозділу, або у репозитарії закладу вищої освіти.
Та з Вимоги до публічного захисту	Публічний захист кваліфікаційної роботи проводиться екзаменаційною комісією, згідно затвердженого графіку закладу вищої освіти.

3. Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

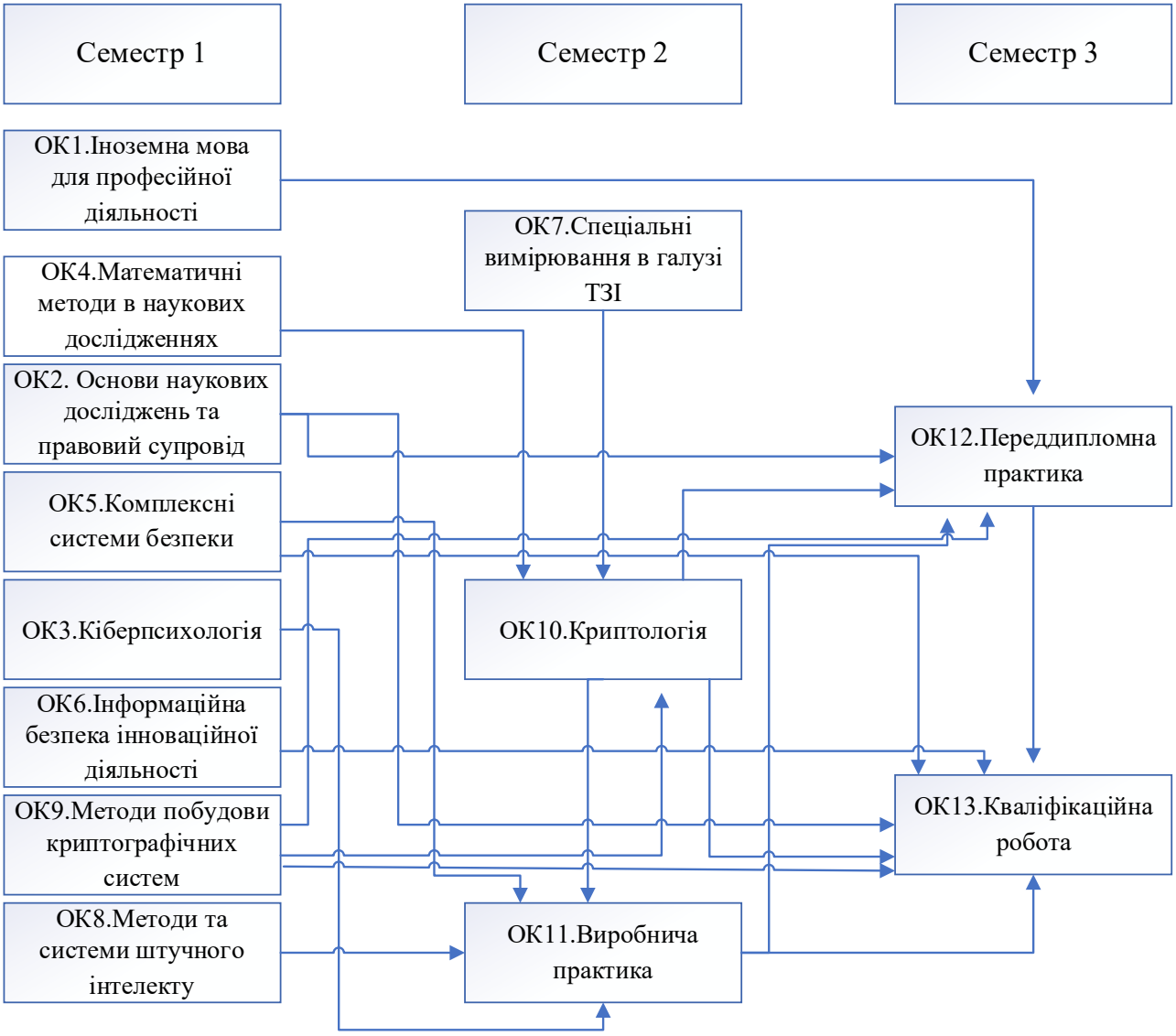
У Міжнародному гуманітарному університеті функціонує центр забезпечення якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості), яка передбачає здійснення таких процедур і заходів:

1. Забезпечення внутрішнього контролю якості освіти у Міжнародному гуманітарному університеті.
2. Online-опитування студентів, випускників, працедавців та викладачів.
3. Постійне удосконалення освітнього процесу з метою забезпечення підготовки фахівців, які відповідали б вимогам світових стандартів і потребам споживача на ринку праці.
4. Участь у покращенні освітніх програм та бізнес-процесів у Міжнародному гуманітарному університеті.
5. Забезпечення принципів академічної доброчесності.
6. Спільно з навчальним відділом Міжнародного гуманітарного університету створення умов для підвищення кваліфікації викладачів.
7. Інших процедур і заходів.

Перелік компонент освітньо-професійної програми
та їх логічна послідовність
Перелік компонент освітньо-професійної програми

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Семестр	Форма підсумк. контролю
1	2	3	4	5
	Обов'язкові компоненти ОП			
І. Навчальні дисципліни фундаментальної, гуманітарної та соціально-економічної підготовки		**15**		
ОК 1	Іноземна мова для професійної діяльності	3	1	Залік
ОК 2	Основи наукових досліджень та правовий супровід	3	1	Екзамен
ОК 3	Кіберпсихологія	3	1	Екзамен
ОК 4	Математичні методи в наукових дослідженнях	6	1	Екзамен
ІІ. Навчальні дисципліни професійної підготовки		**23**		
ОК 5	Комплексні системи безпеки	3	1	Залік
ОК 6	Інформаційна безпека інноваційної діяльності	4	1	Залік
ОК 7	Спеціальні вимірювання в галузі ТЗІ	4	2	Екзамен
ОК 8	Методи та системи штучного інтелекту	4	1	Залік
ОК 9	Методи побудови криптографічних систем	4	1	Залік
ОК 10	Криптологія	4	2	Екзамен
ІІІ. Навчальні дисципліни практичної підготовки		**28**		
ОК 11	Виробнича практика	6	2	Залік
ОК 12	Переддипломна практика	6	3	Залік
ОК 13	Кваліфікаційна робота	16	3	Екзамен
Загальний обсяг обов'язкових компонент:		**66**		
	Вибіркові компоненти ОП			
Загальний обсяг вибіркових компонент:		**24**		
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**90**		

Структурно-логічна схема компонентів ОП



Матриця відповідності програмних компетентностей навчання освітнім компонентам освітньої програми підготовки здобувачів за другим (магістерським) рівнем вищої освіти у Міжнародному гуманітарному університеті з галузі знань 12 Інформаційні технології спеціальність 125 Кібербезпека та захист інформації.

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13
ІК1		+	+	+	+	+	+	+	+	+		+	+
КЗ-1	+	+	+	+	+	+	+		+	+	+	+	+
КЗ-2		+	+	+	+	+	+	+	+	+	+		+
КЗ-3		+		+				+		+	+	+	+
КЗ-4		+		+	+		+			+	+		+
КЗ-5	+	+		+				+			+	+	+
КФ1		+	+	+	+	+	+	+	+	+	+	+	+
КФ2	+	+	+		+		+				+	+	+
КФ3			+			+		+	+	+	+	+	+
КФ4		+	+							+	+		+
КФ5				+							+	+	+
КФ6		+									+		+
КФ7		+									+	+	+
КФ8				+	+	+	+	+	+	+	+		+
КФ 9											+		+
КФ10			+								+	+	+
КФ11				+									+

Матриця відповідності програмних результатів навчання освітнім компонентам освітньої програми підготовки здобувачів за другим (магістерським) рівнем вищої освіти у Міжнародному гуманітарному університеті з галузі знань 12 Інформаційні технології спеціальність 125 Кібербезпека та захист інформації.

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13
РН1	+	+	+			+			+	+	+	+	+
РН2		+	+	+				+			+	+	+
РН3				+	+	+	+	+	+	+	+	+	+
РН4				+				+			+		+
РН5				+	+		+	+		+	+		+
РН6				+	+		+				+	+	+
РН7					+		+	+			+		+
РН8						+			+		+	+	+
РН9						+					+		+
РН10				+							+		+
РН11						+						+	+
РН12			+								+	+	+
РН13					+	+	+		+	+	+		+
РН14						+					+		+
РН15	+										+		+
РН16		+						+			+	+	+
РН17						+					+	+	+
РН18		+	+								+		+
РН19				+							+		+
РН20				+				+			+	+	+
РН21						+					+		+
РН22				+		+			+		+		+
РН23		+			+		+			+	+		+