МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖЕНО
Протокол засідання Вченої ради
Маріупольського державного
університету
28.04.2023 № 8

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА КІБЕРБЕЗПЕКА

РІВЕНЬ ВИЩОЇ ОСВІТИ Перший (бакалаврський) рівень
(назва рівня вищої освіти)

СТУПІНЬ ВИЩОЇ ОСВІТИ Бакалавр
(назва ступеня вищої освіти)

ГАЛУЗЬ ЗНАНЬ 12 Інформаційні технології
(шифр та назва галузі знань)

СПЕЦІАЛЬНІСТЬ 125 Кібербезпека та захист інформації
(код та найменування спеціальності)

Спеціалізація (за необхідністю)

Освітня програма вводиться в дію з 01.09.2023 р.
Наказ про введення в дію
рішення Вченої ради МДУ від 28.04.2023 2023 р. № 52

І Передмова

1. Розроблено і винесено кафедрою системного аналізу та інформаційних технологій Маріупольського державного університету на підставі Стандарту вищої освіти підготовки бакалаврів спеціальності 125 Кібербезпека (наказ МОН № 1074 від 04.10.18р.).
2. Затверджено та надано чинності рішенням Вченої ради МДУ від 28.04.2023 р. протокол № 8.
3. Розробники програми:

Мартинюк Ганна Вадимівна, кандидат технічних наук, доцент, доцент кафедри системного аналізу та інформаційних технологій МДУ.

Охріменко Андрій Олександрович, кандидат технічних наук, старший викладач кафедри системного аналізу та інформаційних технологій МДУ.

Мнацаканян Марія Сергіївна, кандидат технічних наук, доцент кафедри системного аналізу та інформаційних технологій МДУ.

Міщенко Андрій Віталійович, доктор технічних наук, професор, технічний директор комунального підприємства «Міжнародний аеропорт Київ (Жуляни)», професор кафедри системного аналізу та інформаційних технологій МДУ.

Карпенко Уляна Олександрівна, студентка четвертого курсу спеціальності «Кібербезпека».

4. Рецензії-відгуки зовнішніх стейкхолдерів:

Гнатюк Сергій Олександрович, д.т.н., професор, президент громадської організації «Наукова асоціація кібербезпеки України».

Лазаренко Сергій Володимирович, д.т.н., професор, професор кафедри засобів захисту інформації Національного авіаційного університету.

Боровіков Олексій Олександрович, директор Товариства з обмеженою відповідальністю «САЙФЕР ПРО»

ІІ Профіль освітньої програми

Маріупольський державний університет
Економіко-правовий факультет
Кафедра системного аналізу та інформаційних технологій
Галузь знань 12 Інформаційні технології
Спеціальність 125 Кібербезпека та захист інформації
Назва ОПП: Кібербезпека

Ступінь вищої освіти	Бакалавр
Освітня кваліфікація	Бакалавр з кібербезпеки
Кваліфікація в дипломі	Ступінь вищої освіти – бакалавр Спеціальність 125 Кібербезпека та захист інформації Галузь знань 12 Інформаційні технології Освітня програма «Кібербезпека» Молодший адміністратор мереж і систем
Професійна кваліфікація	Молодший адміністратор мереж і систем
Тип диплому та обсяг програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, 3 роки 10 місяців
Форми здобуття вищої освіти	Денна, заочна
Заклад вищої освіти	Маріупольський державний університет, м. Київ
Акредитаційна інституція	Національне агентство із забезпечення якості вищої освіти
Період акредитації	Сертифікат про акредитацію **освітньої програми** дійсний до 21.03.2024
Рівень програми	Перший (бакалаврський) рівень FQ-EHEA- перший цикл, EQF-LLL-6 рівень, НРК- 6 рівень
Передумови	Наявність атестата про повну загальну середню освіту або диплома молодшого бакалавра та відповідних сертифікатів ЗНО/НМТ
Мови викладання	Українська
Термін дії ОПП	Відповідно до терміну акредитації
Інтернет-адреса постійного розміщення опису освітньої програми	https://mu.edu.ua/uk/educational-programs/kiberbezpeka

а	**Мета програми**	
	Підготовка кваліфікованих, конкурентоспроможних, інтегрованих у європейський та світовий науково-освітній простір фахівців з інформаційної та кібербезпеки, здатних вирішувати складні спеціалізовані задачі та практичні проблеми інформаційної безпеки, захищеності інформаційного і кіберпросторів держави в цілому та окремих суб'єктів. ОПП Кібербезпека відповідає місії МДУ, у якій наголошується щодо продукування та реалізації проривних моделей розвитку людського капіталу, зміцнення науково-освітнього та інноваційного потенціалу України.	
б	**Характеристика програми**	
1	**Предметна область**	**Об'єкти професійної діяльності випускників:** - об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси й технології; - технології забезпечення безпеки інформації; - процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. **Теоретичний зміст предметної області.** **Знання:** - законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення

		професійної діяльності; - принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; - теорії, моделей та принципів управління доступом до інформаційних ресурсів; теорії систем управління інформаційною та/або кібербезпекою; - методів та засобів виявлення, управління та ідентифікації ризиків; - методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; - методів та засобів технічного та криптографічного захисту інформації; - сучасних інформаційно-комунікаційних технологій; - сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; - автоматизованих систем проектування. Методи, методики та технології: Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/або кібербезпеки. Інструменти та обладнання: - системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/або кібербезпеки; - сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
2	***Фокус програми та спеціалізації***	Загальна Підготовка фахівців в галузі інформаційних технологій, які володіють компетентностями, необхідними для встановлення та підтримки мереж та систем, їх конкретних компонентів; адміністрування системи управління даними, що дозволяють безпечно зберігати, запитувати, захищати та використовувати дані. **Ключові слова:** кібербезпека, криптографичний захист інформації, технічний захист інформації, моделі управління доступом, ідентифікація кіберзагроз, інформаційно-комунікаційні технології.
3	***Орієнтація програми***	Освітньо-професійна
4	**Особливості та відмінності**	*Особливість (унікальність) ОП.* Особливість програми полягає у комплексному підході, який орієнтований на підготовку фахівця з потужною теоретичною та практичною базою для підготовки адміністратора мереж та систем. Освітня програма корелюється з професійним стандартом «Адміністратор мереж та систем» затвердженого Наказом Адміністрації Держспецзв'язку № 25 від 25 листопада 2022 р. https://kadrovik.isu.net.ua/news/547594-6-novykh-profesiynykh-standartiv-u-haluzi-kiberbezpeky Особливість програми досягається шляхом використання новітнього програмного забезпечення та устаткування, яке надане за підтримки компанії Rolls-Royce Power Systems та Проєкту USAID «Кібербезпека критично важливої інфраструктури України», а також за можливості використовувати в навчальному процесі матеріали Fortinet Network Security Academy Program.

в	**Працевлаштування та продовження освіти**	
1	***Працевлаштування***	Бакалавр з кібербезпеки здатний виконувати професійні види робіт згідно з Національною рамкою кваліфікацій та Національним класифікатором України, а також з професійним стандартом «Адміністратор мереж та систем» затвердженого Наказом Адміністрації Держспецзв'язку № 25 від 25 листопада 2022 р. **Основна:** 2139.2 Молодший адміністратор мереж і систем. **Додаткова:** 3121 Фахівець з інформаційних технологій. 3119 Технік (сфера захисту інформації). 3439 Фахівець з організації інформаційної безпеки. Фахівець із організації захисту інформації з обмеженим доступом.
2	***Продовження освіти***	Можливість продовжити навчання за освітньою програмою ступеня магістра
г	**Викладання та оцінювання**	
1	***Викладання та навчання***	Студентоцентроване та проблемно-орієнтоване навчання, що базується на застосуванні інноваційних підходів та інтерактивних освітніх технологій. Теоретичне навчання здійснюється на основі поєднання лекційних, семінарських (практичних) та лабораторних занять з самостійною роботою студента. Практична підготовка передбачає проходження навчальної, виробничої те переддипломної практик.
2	***Методи оцінювання***	Формами підсумкового контролю є екзамени, заліки, а також диференційовані заліки, які проводяться для оцінювання якості виконання та захисту індивідуальних проектних завдань та звітів з практики. Проміжний та поточний контроль здійснюється у формі виконання модульних контрольних робіт; підготовки та захисту проєктів, презентацій, реферативних досліджень; здійснення кейс-стаді тощо.
д	**Програмні компетентності**	
1	***Інтегральна компетентність***	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
2	***Загальні***	1. Здатність застосовувати знання у практичних ситуаціях. 2. Знання та розуміння предметної області та розуміння професії. 3.Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. 5. Здатність до пошуку, оброблення та аналізу інформації. 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. 8. Здатність до адаптації та дії у новій ситуації.

		9. Здатність до вибору стратегії спілкування, працювати в команді. 10. Здатність дотримуватися правил та норм з безпеки та охорони праці, зокрема щодо безпечної експлуатації електронного устаткування та електричного обладнання.
3	***Фахові***	1. Здатність застосовувати законодавчу та нормативно-правову бази, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та /або кібербезпеки. 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та /або кібербезпеки. 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та /або кібербезпекою. 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та /або кібербезпеки. 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та /або кібербезпеки. 13. Здатність розроблювати та документувати стандартні операційні процедури адміністрування систем щодо захисту інформації 14. Здатність підтримувати програмне та інше забезпечення систем управління базами даних 15. Здатність впроваджувати стандарти управління даними, вимоги і специфікації. 16. Здатність проводити періодичне обслуговування системи та

		мережі 17. Здатність вирішувати проблеми з апаратним /програмним інтерфейсом та проблеми сумісності.
е	**Програмні результати навчання**	
	1. застосувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; 2. організувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; 3. використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; 4. аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; 5. адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат; 6. критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. 7. діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; 8. готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; 9. впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та /або кібербезпеки; 10. виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем; 11. виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; 12 розробляти моделі загроз та порушника; 13 аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; 14 вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень; 15 використовувати сучасне програмно-апаратне забезпечення інформаційно-телекомунікаційних технологій; 16 реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; 17 забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; 18 використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів; 19 застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; 20 забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;	

	21 вирішувати задачі забезпечення та супроводу (в тому числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційно-телекомунікаційних (автоматизованих) системах; 22 вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної та /або кібербезпеки; 23 реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; 24 вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових); 25 забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту; 26 впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; 27 вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; 28 аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та /або кібербезпеки; 29 здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; 30 здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; 31 застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; 32 вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки; 33 вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; 34 приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації; 35 вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; 36 виявляти небезпечні сигнали технічних засобів; 37 вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; 38 інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;

	39 проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; 40 інтерпретувати результати проведення спеціальних вимірювань з використанням технічних-засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; 41 забезпечувати безперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур; 42 впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки; 43 застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; 44 вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; 45 застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; 46 здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах; 47 вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації; 48 виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; 49 забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах; 50 забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних); 51 підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах; 52 використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах; 53 вирішувати задачі аналізу програмного коду на наявність можливих загроз; 54 усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод і громадянина в Україні.
Академічна мобільність	
Національна кредитна мобільність	Порядок організації програм національної академічної мобільності для учасників освітнього процесу МДУ на території України визначається Положенням про порядок реалізації права на академічну мобільність учасників освітнього процесу Маріупольського державного університету
Міжнародна кредитна мобільність	Порядок організації програм міжнародної академічної мобільності для учасників освітнього процесу МДУ поза межами України та іноземних учасників освітнього процесу визначається Положенням про порядок реалізації права на академічну мобільність учасників освітнього процесу Маріупольського державного університету
Навчання іноземних здобувачів вищої освіти	Навчання іноземних здобувачів вищої освіти не здійснюється

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

Обсяг освітньої програми бакалавра становить 240 кредитів ЄКТС.

Нормативна частина – 75%, варіативна частина – 25%.

100 % обсягу освітньої програми спрямовано на забезпечення загальних та спеціальних (фахових) компетентностей, визначених стандартом вищої освіти за спеціальністю 125 «Кібербезпека» та професійного стандарту «Адміністратор мереж та систем».

У Маріупольському державному університеті визнаються та перезараховуються на базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») не більше ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста); на основі ступеня «фаховий молодший бакалавр» не більше ніж 60 кредитів ЄКТС, отриманих за попередньою освітньою програмою фахової передвищої освіти.

Тип диплома: одиничний ступінь.

Розподіл змісту освітньої складової за критеріями нормативності та вибірковості.

Обсяг освітньої складової освітньо-професійної програми підготовки бакалавра з кібербезпеки становить 240 кредитів ЄКТС.

Розподіл змісту освітньої складової програми за циклами дисциплін та критеріями нормативності і вибірковості наведено у табл. 3.1.

Таблиця 3.1

Розподіл змісту освітньої складової за критеріями нормативності та вибірковості

Цикл дисциплін	Загальна кількість кредитів	У тому числі:	
		обов'язкові дисципліни, кредитів	вибіркові дисципліни, кредитів
Загальна підготовка	**57 (23,75 %)**	**42 (17,5%)**	**15 (6,25 %)**
Професійна підготовка	**183 (76,25 %)**	**138 (57,5 %)**	**45 (18,75 %)**
Усього для ступеня бакалавра	**240 (100%)**	**180 (75%)**	**60 (25%)**

Теоретичне навчання здійснюється на основі поєднання лекційних та семінарських (практичних) занять з самостійною роботою. Практична підготовка передбачає проходження різних видів практики. Для проходження практик передбачено 18 кредитів ЄКТС.

Формами підсумкового контролю з навчальних дисциплін є екзамени, заліки, а також диференційовані заліки, які проводяться для оцінювання якості навчання (таблиця 3.2).

Таблиця 3.2

Перелік компонент ОПП

Код н/д	Шифр дисципліни за навчальним планом	Компоненти освітньої програми (навчальні дисципліни, курсові роботи, практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
Обов'язкові компоненти ОПП				
Дисципліни загальної підготовки				
ОК 1.	ОКЗП 1.1.1.	Академічне письмо	4	екзамен
ОК 2.	ОКЗП 1.1.2.	Українознавчі студії	4	екзамен
ОК 3.	ОКЗП 1.1.3.	Англійська мова	18	залік, залік, атестаційний екзамен
ОК 4.	ОКЗП 1.1.4.	Соціологія	3	екзамен
ОК 5.	ОКЗП 1.1.5.	Політико-правові студії	4	екзамен
ОК 6.	ОКЗП 1.1.6.	Психологія життєдіяльності особистості	3	екзамен
ОК 7.	ОКЗП 1.1.7.	Основи підприємництва	3	екзамен
ОК 8.	ОКЗП 1.1.8.	Безпека життєдіяльності	3	д. залік
Усього з циклу загальної підготовки			**42**	
Дисципліни професійної підготовки				
ОК 9.	ОКПП 1.2.1.	Вища математика	10	екзамен
ОК 10.	ОКПП 1.2.2.	Основи кібербезпеки	5	залік
ОК 11.	ОКПП 1.2.3.	Інформаційні технології	7	залік, екзамен
ОК 12.	ОКПП 1.2.4.	Дискретна математика	5	екзамен
ОК 13.	ОКПП 1.2.5.	Теорія ймовірностей та математична статистика	5	екзамен
ОК 14.	ОКПП 1.2.6.	Фізика	3	залік
ОК 15.	ОКПП 1.2.7.	Криптологія	6	залік
ОК 16.	ОКПП 1.2.8.	Теорія інформації та кодування	4	екзамен
ОК 17.	ОКПП 1.2.9.	Алгоритми та структури даних	5	екзамен
ОК 18.	ОКПП 1.2.10.	Нормативно-правове забезпечення інформаційної безпеки	5	екзамен
ОК 19.	ОКПП 1.2.11.	Комп'ютерні мережі	6	екзамен
ОК 20.	ОКПП 1.2.12.	Програмування	10	залік, екзамен
ОК 21.	ОКПП 1.2.13.	Сигнали та процеси у системах захисту інформації	3	екзамен
ОК 22.	ОКПП 1.2.14.	Операційні системи та технології їх захисту	4	екзамен
ОК 23.	ОКПП 1.2.15.	Бази даних та знань	3	залік
ОК 24.	ОКПП 1.2.16.	Управління інформаційною безпекою	4	залік
ОК 25	ОКПП 1.2.17.	Електроніка	5	екзамен
ОК 26.	ОКПП 1.2.18.	Архітектура комп'ютерних систем	6	екзамен
ОК 27.	ОКПП 1.2.19.	Захист інформації в комп'ютерних системах та мережах	4	екзамен
ОК 28.	ОКПП 1.2.20.	Комплексні системи захисту інформації	5	екзамен
ОК 29.	ОКПП 1.2.21.	Аудит безпеки інформаційних систем	4	залік

Код н/д	Шифр дисципліни за навчальним планом	Компоненти освітньої програми (навчальні дисципліни, курсові роботи, практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
ОК 30.	ОКПП 1.2.22.	Теорія і практика інфраструктури відкритих ключів	4	залік
ОК 31.	ОКПП 1.2.23.	Організаційне забезпечення захисту інформації	5	залік
Практична підготовка				
ОК 32.	ОКПП 1.2.24.	Навчальна практика	3	д. залік
ОК 33.	ОКПП 1.2.25.	Виробнича практика 1	6	д. залік
ОК 34.	ОКПП 1.2.26.	Виробнича практика 2	9	д. залік
Усього з циклу професійної підготовки			**138**	
Разом з нормативної частини			**180**	
Вибіркові компоненти ОПП				
Дисципліни загальної підготовки*				
ВК 1.	ВКЗП 2.1.1.	Дисц. вільного вибору №1	3	залік
ВК 2.	ВКЗП 2.1.2.	Дисц. вільного вибору №2	3	залік
ВК 3.	ВКЗП 2.1.3.	Дисц. вільного вибору №3	3	залік
ВК 4.	ВКЗП 2.1.4.	Дисц. вільного вибору №4	3	залік
ВК 5.	ВКЗП 2.1.5.	Дисц. вільного вибору №5	3	залік
Усього з циклу загальної підготовки			**15**	
Дисципліни професійної підготовки**				
ВК 6.	ВКПП 2.2.1.	Дисц. вільного вибору №1	4	екзамен
ВК 7.	ВКПП 2.2.2.	Дисц. вільного вибору №2	4	залік
ВК 8.	ВКПП 2.2.3.	Дисц. вільного вибору №3	5	екзамен
ВК 9.	ВКПП 2.2.4.	Дисц. вільного вибору №4	5	екзамен
ВК 10.	ВКПП 2.2.5.	Дисц. вільного вибору №5	3	залік
ВК 11	ВКПП 2.2.6.	Дисц. вільного вибору №6	5	екзамен
ВК 12.	ВКПП 2.2.7.	Дисц. вільного вибору №7	5	екзамен
ВК 13.	ВКПП 2.2.8.	Дисц. вільного вибору №8	4	залік
ВК 14.	ВКПП 2.2.9.	Дисц. вільного вибору №9	5	залік
ВК 15.	ВКПП 2.2.10	Дисц. вільного вибору №10	5	залік
Усього з циклу професійної підготовки			**45**	
Разом з вибіркової частини			**60**	
Разом з нормативної і вибіркової частин			**240**	

* - обираються здобувачами вищої освіти із каталогу елективних дисциплін загальної підготовки МДУ.

** - обираються здобувачами вищої освіти із каталогу дисциплін професійної підготовки кафедри САІТ або з каталогів інших кафедр університету.

Логічна послідовність вивчення компонент освітньої програми представлена у вигляді графа (рис. 3.1).

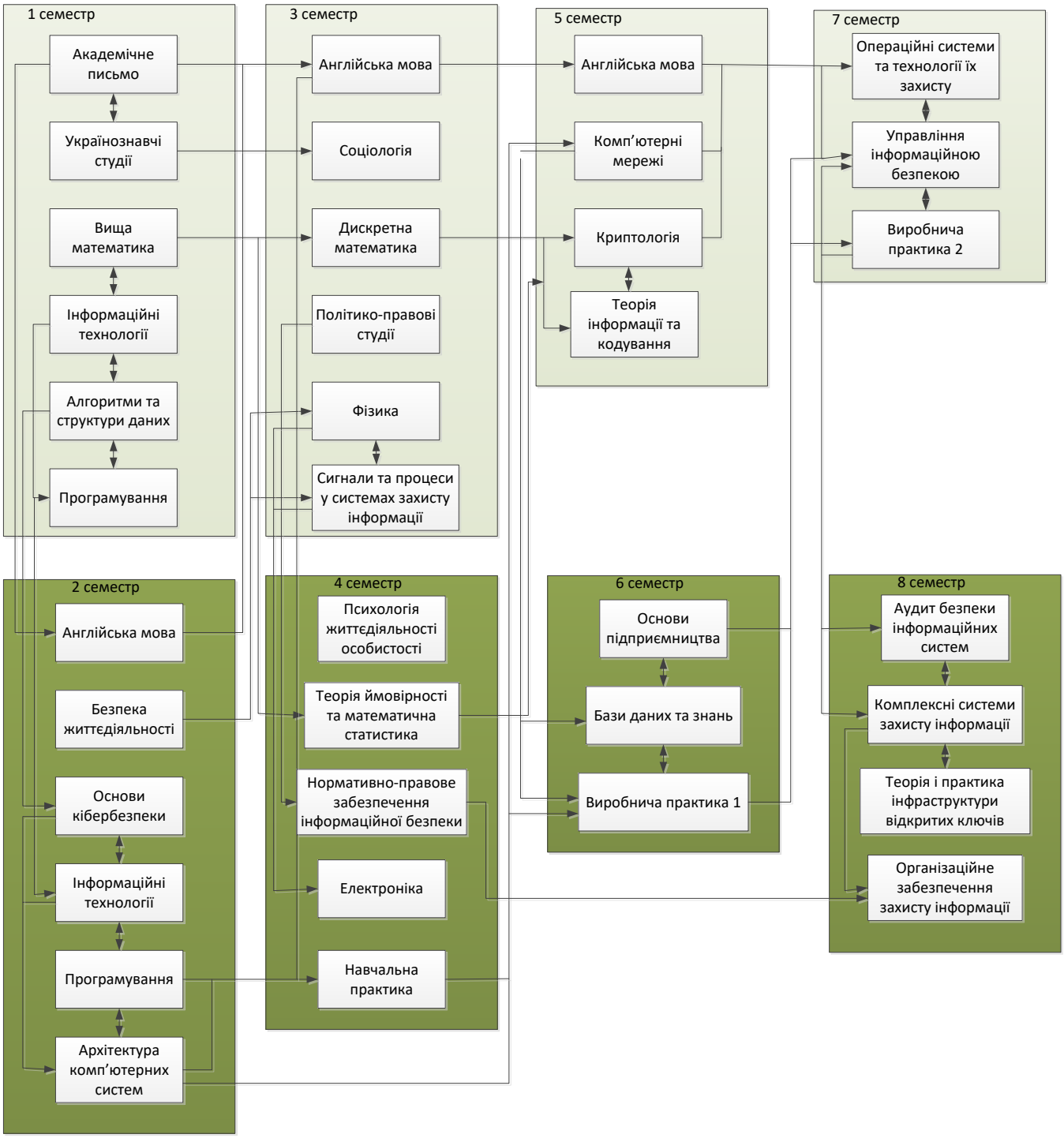
Зведена матриця відповідностей визначених Стандартом компетентностей/результатів навчання дескрипторам НРК наведено у таблиці 3.3.

Співвідношення між результатами навчання та фаховими компетентностями наведено у матриці (Таблиця 3.4), які студент набуває в результаті успішного навчання за даною освітньою програмою.

Співвідношення між результатами навчання та програмними результатами навчання наведено у матриці (Таблиця 3.5), які студент набуває в результаті успішного навчання за даною освітньою програмою.

Переліки вибіркових компонент містяться у Каталогах елективних дисциплін Маріупольського державного університету.

Структурно-логічна схема вивчення компонент освітньої програми



Таблиця 3.3.

Зведена таблиця фахових компетентностей та результатів навчання

Фахові компетентності	Результати навчання
КФ 1. Здатність застосовувати законодавчу та нормативно- правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.	- готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \або кібербезпеки; - розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем; - виконувати аналіз реалізації прийнятої політики інформаційної і /або кібербезпеки.
КФ 2. Здатність до використання інформаційно- комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки.	- здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; - розробляти та аналізувати проекти інформаційно- телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; - застосовувати в професійній діяльності знання, навички та практики, щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектур операційних систем; - здійснювати захист ресурсів і процесів в інформаційно-телекомунікаційних системах на основі моделей безпеки (кінцевих автоматів, управління потоками, Bell-LaPadula, Biba, Clarl-Wilson, та інші), а також встановлених режимів безпечного функціонування інформаційно-телекомунікаційних системах; - виконувати аналіз програмного забезпечення з метою оцінки на відповідність встановленим вимогам інформаційної і\або кібербезпеки в інформаційно- телекомунікаційних системах.
КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно- телекомунікаційних (автоматизованих) системах	- забезпечувати процеси захисту інформаційно- телекомунікаційних (автоматизованих) систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; - забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - виконувати розробку експлуатаційної документації на комплексів засобів захисту.
КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.	- вирішувати задачі супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно- телекомунікаційних (автоматизованих) системах;

	- вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);вирішувати задачі централізованого і децентралізованого адміністрування доступом до інформаційних ресурсів і процесів в інформаційних та інформаційно- телекомунікаційних (автоматизованих) системах; - забезпечувати введення підзвітності системи управління доступом інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
КФ 5 Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.	- обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної та/або кібербезпеки, та критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії захисту інформації; - вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації, користувачів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах - проектувати та реалізувати комплексні системи захисту інформації в автоматизованих системах організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації; - вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; - використовувати інструментальні засоби оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах.
КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно- телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.	- вирішувати задачі управління процесами забезпечення безперервності бізнесу з використанням процедур резервування програмного забезпечення та безпосередньо інформаційних ресурсів; - вирішувати задачі корекції цілей, стратегій, планів забезпечення безперервності бізнес процесів після здійснення кібератак, збоїв та відмов різних класів, - створювати і впроваджувати плани процесу забезпечення безперервності бізнесу; - виконувати аналіз налаштувань елементів інформаційних систем та комунікаційного обладнання;

КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)	- вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;-здійснювати оцінку рівня захищеності інформації що обробляється в інформаційно-телекомунікаційних системах використовувати інструментальні засоби оцінювання наявності потенційних вразливостей; - вирішувати задачі управління комплексною системою захисту інформації в інформаційних та інформаційно- телекомунікаційних (автоматизованих); - вирішувати задачі експертизи, випробування комплексних систем захисту інформації.
КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.	- вирішувати задачі попередження та виявлення, ідентифікації, аналізу та реагування на інциденти в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - проводити розслідування інцидентів інформаційної безпеки та/або кібербезпеки базуючись на національних та міжнародних регулюючих актах, процедурах та положеннях в сфері інформаційної безпеки та/або кібербезпеки; - забезпечувати дотримання політики ведення журналів реєстрації подій та інцидентів з встановленим рівнем деталізації;
КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.	- забезпечувати безперервність бізнес процесів організації на базі теорії ризиків та системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів; - забезпечувати функціонування системи управління інформаційною та\або кібербезпекою організації на основі керування інформаційними ризиками, здійснення процедур їх кількісного і якісного оцінки;
КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.	- аналізувати та визначати можливість застосування технологій, методів та засобів криптографічного захисту інформації; - аналізувати та визначати можливість застосування технологій, методів та засобів технічного захисту інформації; - виявляти небезпечні сигнали технічних засобів; - вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю захищеності інформації від витоку технічними каналами; - визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; - інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;

	- обґрунтовувати можливість створення технічних каналів витоку інформації на об’єктах інформаційної діяльності; - впроваджувати заходи та засоби технічного захисту інформації від витоку технічними каналами;
КФ 11. Здатність виконувати моніторинг ресурсів і процесів функціонування, інформаційно- телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	- забезпечувати процеси моніторингу доступу до ресурсів і процесів інформаційно-телекомунікаційних систем; - забезпечувати конфігурування та функціонування систем моніторингу ресурсів та процесів в інформаційно- телекомунікаційних системах;
КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно встановленої політики інформаційної та/або кібербезпеки.	- виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; - аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в інформаційно-телекомунікаційних системах; - аналізувати та впроваджувати системи захисту від зловмисних програмних кодів.
КФ 13. Здатність розроблювати та документувати стандартні операційні процедури адміністрування систем щодо захисту інформації.	- застосовувати принципи кібербезпеки і приватності при формуванні вимог організації (стосовно конфіденційності, цілісності, доступності, автентифікації і неспростовності); - налаштовувати і використовувати програмні засоби захисту комп'ютерів (наприклад, програмні фільтри, антивірусна програма й антишпигунське ПЗ); - проводити планування, управління та обслуговування систем/серверів.
КФ 14. Здатність підтримувати програмне та інше забезпечення систем управління базами даних.	- проводити запити і розробку алгоритмів аналізу структур даних; - підтримувати бази даних (резервне копіювання, відновлення, видалення даних, файли лог-журналу тощо); - оптимізовувати продуктивність бази даних.
КФ 15. Здатність впроваджувати стандарти управління даними, вимоги і специфікації.	- проводити запити і розробку алгоритмів аналізу структур даних; - створювати запити та звіти відповідного спрямування; - підтримувати бази даних (резервне копіювання, відновлення, видалення даних, файли лог-журналу тощо); - оптимізовувати продуктивність бази даних.
КФ 16. Здатність проводити періодичне обслуговування системи та мережі	- ідентифікувати та прогнозувати системну/серверну роботу, доступність, можливості або проблеми з налаштуванням; - встановлювати оновлення системи та компонентів (серверів, пристроїв, мережевих пристроїв тощо); - моніторити та оптимізувати роботу системи/сервера; - адмініструвати операційну систему (ведення облікових

	записів, резервне копіювання даних, підтримання продуктивності системи, інсталяція і налаштування нового апаратного/програмного забезпечення).
КФ 17. Здатність вирішувати проблеми з апаратним /програмним інтерфейсом та проблеми сумісності.	- виправляти фізичні та технічні проблеми, що впливають на роботу системи/сервера; - відновлювати системи/сервери після виявленого збою (програмне забезпечення для відновлення, відмовостійкі кластери, дублювання/"зеркалювання" тощо)

Таблиця 3.4

Матриця відповідності фахових компетентностей

Освітні компоненти	Компетентності																												
	ІК	Загальні										Фахові																	
		КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КЗ8	КЗ9	КЗ10	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12	КФ13	КФ14	КФ15	КФ16	КФ17
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	+	+	+			+													+		+	+	+						
ОК 14	+	+			+											+	+	+											
ОК 15	+		+		+								+	+							+								
ОК 16	+	+	+		+	+			+				+			+	+			+		+	+		+			+	
ОК 17	+	+	+										+	+		+	+												
ОК 18	+	+	+		+		+	+				+			+	+				+									
ОК 19	+	+				+			+		+		+	+		+	+	+		+		+			+			+	
ОК 20	+	+	+		+					+	+		+	+														+	
ОК 21	+	+	+		+				+		+			+			+	+											
ОК 22	+	+	+		+								+			+	+						+		+	+	+	+	
ОК 23	+	+	+		+	+																			+	+			

Освітні компоне-нти	**Компетентності**																												
	І К	Загальні										Фахові																	
		КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КЗ8	КЗ9	КЗ10	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12	КФ13	КФ14	КФ15	КФ16	КФ17
ОК 24	+	+				+	+		+	+		+	+	+	+	+		+		+				+		+	+	+
ОК 25	+	+			+											+	+	+										
ОК 26	+	+	+										+	+		+	+											
ОК 27	+	+				+			+				+			+	+			+		+	+	+	+		+	+
ОК 28	+	+	+		+	+			+		+		+	+		+	+			+		+	+	+		+	+	+
ОК 29	+	+				+			+	+														+		+	+	+
ОК 30	+	+										+			+					+								
ОК 31	+	+		+		+			+				+			+		+						+		+	+	+
ОК 32	+		+		+	+				+			+	+									+					
ОК 33	+	+	+	+	+	+	+	+		+		+	+	+	+	+	+	+	+	+	+	+	+					
ОК 34	+	+	+	+	+	+	+	+		+		+	+	+	+	+	+	+	+	+	+	+	+					

Таблиця 3.5

Перелік програмних результатів навчання

Програмні результати навчання	Освітні компоненти																																
	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	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34
РН-1	+	+	+	+																													
РН-2						+	+	+	+		+	+	+	+				+						+	+		+	+	+	+	+	+	+
РН-3						+					+																					+	+	+
РН-4						+	+		+		+	+	+			+			+									+		+		+	+	+
РН-5							+			+	+																							
РН-6										+					+																	+		
РН-7					+													+						+					+					
РН-8											+							+						+					+					
РН-9																		+						+										
РН-10											+								+													+		
РН-11																+												+		+				
РН-12																+						+					+	+						
РН-13																			+			+					+							
РН-14										+				+	+		+			+	+				+	+						+		
РН-15														+	+				+		+	+			+		+	+					+	+
РН-16															+				+									+						
РН-17																+			+									+						
РН-18										+				+	+				+		+				+			+					+	+
РН-19														+	+		+					+			+	+	+			+				
РН-20																	+			+						+					+			
РН-21																												+		+				

Програмні результати навчання	Освітні компоненти																																		
	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	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34
РН-22																			+					+			+			+				
РН-23																			+					+			+							
РН-24																														+				
РН-25																						+					+	+						
РН-26																														+				
РН-27														+	+	+	+		+	+					+	+	+	+		+				
РН-28																											+	+					+	+
РН-29										+						+			+													+		
РН-30																											+	+						
РН-31										+					+		+									+			+	+	+			
РН-32																		+						+					+					
РН-33																		+						+					+					
РН-34						+												+						+				+	+					
РН-35															+			+						+				+		+			+	+
РН-36														+											+		+						+	+
РН-37														+											+								+	+
РН-38														+											+								+	+
РН-39																		+						+					+					
РН-40																												+			+		+	+
РН-41															+			+						+			+		+				+	+
РН-42																								+			+	+					+	+
РН-43																		+									+				+			
РН-44																		+						+							+		+	+
РН-45																		+						+			+	+	+				+	+

Програмні результати навчання	Освітні компоненти																																
	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	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30	ОК 31	ОК 32	ОК 33	ОК 34
РН-46																								+						+			+	+
РН-47															+		+									+							+	+
РН-48															+												+	+		+			+	+
РН-49																						+		+			+	+					+	+
РН-50																	+	+				+				+	+						+	+
РН-51																								+			+	+	+				+	+
РН-52																											+		+				+	+
РН-53																	+			+			+	+		+	+						+	+
РН-54	+	+	+	+	+	+	+	+	+									+															+	+

IV Форми атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здобувачів вищої освіти здійснюється: 1) у формі єдиного державного кваліфікаційного іспиту за спеціальністю в установленому порядку; 2) у формі атестаційного екзамену для присудження професійної кваліфікації здобувачам.
Вимоги до кваліфікаційної роботи/проекту	1. Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених цим стандартом та освітньою програмою. 2. Атестаційний екзамен передбачає оцінювання досягнень результатів навчання, отриманих за ОК 19, ОК 22, ОК 23, ОК 24, ОК 26, ОК 27, ОК 29, які допомагають оволодіти професійними компетентностями для отримання професійної кваліфікації «Молодший адміністратор мереж і систем».
Присвоєння професійної кваліфікації	Професійна кваліфікація «Молодший адміністратор мереж і систем» присвоюється, якщо: - випускники успішно оволоділи ОК 19, ОК 22, ОК 23, ОК 24, ОК 26, ОК 27, ОК 29 з оцінками не нижче 75 балів; - проходження всіх практик, передбачених навчальним планом, з оцінкою не нижче 75 балів; - проходження підсумкової атестації з оцінками не нижче 75 балів.

V. Інформація щодо моніторингу ОП

Освітня програма вводиться в дію з 2023 р. і корелюється з професійним стандартом «Адміністратор мереж та систем» затвердженого Наказом Адміністрації Держспецзв'язку № 25 від 25 листопада 2022 р.

VI. Система внутрішнього забезпечення якості вищої освіти МДУ.

У МДУ функціонує Система внутрішнього забезпечення якості вищої освіти (https://mu.edu.ua/uk/yakist-osviti), яка складається з наступних елементів:

1) нормативне забезпечення;
2) моніторинг системи якості;
3) моніторинг освітніх програм;
4) удосконалення системи якості.

Гарант освітньої програми **Ганна МАРТИНЮК**