МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖЕНО
Протокол засідання Вченої ради
Маріупольського державного
університету
06.05.2025 № 9

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА КІБЕРБЕЗПЕКА

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

СТУПІНЬ ВИЩОЇ ОСВІТИ Бакалавр
(назва ступеня вищої освіти)

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

СПЕЦІАЛЬНІСТЬ F5Кібербезпека та захист інформації
(код та найменування спеціальності)

Спеціалізація (за необхідністю)

Освітня програма вводиться в дію з 01.09.2025 р.
Наказ про введення в дію
рішення Вченої ради МДУ від 06.05.2025 № 9

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 та захист інформації (наказ МОН № 1547 від 29.10.2024 р.).
2. Затверджено та надано чинності рішенням Вченої ради МДУ від 06.05.2025 протокол № 9.
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.

Дрейс Юрій Сергійович, кандидат технічних наук, доцент, доцент кафедри системного аналізу та інформаційних технологій МДУ.

Куплевацька Софія Володимирівна, 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 F Інформаційні технології
Спеціальність F5 Кібербезпека та захист інформації
Назва ОПП: Кібербезпека

Ступінь вищої освіти	Бакалавр
Освітня кваліфікація	Бакалавр з кібербезпеки та захисту інформації
Кваліфікація в дипломі	Ступінь вищої освіти – бакалавр Спеціальність F5 Кібербезпека та захист інформації Галузь знань F Інформаційні технології Освітня програма «Кібербезпека»
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 01.07.2029 р.
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/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 вивчення:** - технології кібербезпеки та захисту інформації; - - процеси управління кібербезпекою та захистом інформації; - об'єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології. **Теоретичний зміст предметної області:** Принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

		Методи, методики та технології: Методи, методики та технології розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації. **Інструменти та обладнання:** Засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).
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 навчання за програмою другого (магістерського) рівня вищої освіти.
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 і практичні завдання у галузі кібербезпеки та захисту інформації.
2	***Загальні***	1. Здатність застосовувати знання у практичних ситуаціях. 2. Знання та розуміння предметної області і розуміння професійної діяльності. 3. Здатність спілкуватися державною мовою як усно, так і письмово. 4. Здатність спілкуватися іноземною мовою. 5. Здатність вчитися і оволодівати сучасними знаннями. 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 та свобод людини і громадянина в Україні. 7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. 8. 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.
3	***Фахові***	1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності. 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. 3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. 5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження. 6. Здатність впроваджувати та забезпечувати функціонування ком-

		плексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.) 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою. 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. 9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.
е	**Програмні результати навчання**	
	1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків, 2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. 3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. 4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність. 5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. 6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат. 7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності. 8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення. 9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації'. 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. 11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації. 12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки. 13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й Інформаційно-комунікаційних систем та\або інфраструктури організації в цілому. 14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.	

	15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи. 16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах; 17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків. 18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. 19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів. 20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації. 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.
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 – 73,75%, варіативна частина – 26,25%.

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») та «фаховий молодший бакалавр» не більше ніж 60 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки.

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 %)**	**39 (16,25%)**	**18 (7,5 %)**
Професійна підготовка	**183 (76,25 %)**	**138 (57,5 %)**	**45 (18,75 %)**
Усього для ступеня бакалавра	**240 (100%)**	**177 (73,75%)**	**63 (26,25%)**

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	3	екзамен
ОК 2.	ОКЗП 1.1.2.	Українознавчі студії	3	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	3	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			**39**	
Дисципліни професійної підготовки				
ОК 9.	ОКПП 1.2.1.	Вища математика та дискретна математика	6	екзамен
ОК 10.	ОКПП 1.2.2.	Основи кібербезпеки	4	залік
ОК 11.	ОКПП 1.2.3.	Інформаційні технології	7	залік, екзамен
ОК 12.	ОКПП 1.2.4.	Адміністрування баз даних та знань	6	екзамен
ОК 13.	ОКПП 1.2.5.	Теорія ймовірностей та математична статистика	4	екзамен
ОК 14.	ОКПП 1.2.6.	Фізика	3	залік
ОК 15.	ОКПП 1.2.7.	Теорія і практика інфраструктури відкритих ключів	4	залік
ОК 16.	ОКПП 1.2.8.	Теорія інформації та кодування	4	екзамен
ОК 17.	ОКПП 1.2.9.	Алгоритми та структури даних	4	екзамен
ОК 18.	ОКПП 1.2.10.	Нормативно-правове забезпечення інформаційної безпеки	5	екзамен
ОК 19.	ОКПП 1.2.11.	Основи комп'ютерних систем та мереж	6	залік
ОК 20.	ОКПП 1.2.12.	Програмування	10	залік, екзамен
ОК 21.	ОКПП 1.2.13.	Сигнали та процеси у системах захисту інформації	4	екзамен
ОК 22.	ОКПП 1.2.14.	Технології захисту операційних систем	5	екзамен
ОК 23.	ОКПП 1.2.15.	Безпека інформаційно-комунікаційних систем	5	залік
ОК 24.	ОКПП 1.2.16.	Управління інформаційною безпекою	7	екзамен
ОК 25	ОКПП 1.2.17.	Криптографічний захист інформації	5	екзамен
ОК 26.	ОКПП 1.2.18.	Архітектура комп'ютерних систем	6	екзамен
ОК 27.	ОКПП 1.2.19.	Захист комп'ютерних мереж	5	екзамен
ОК 28.	ОКПП 1.2.20.	Комплексні системи захисту інформації	4	екзамен

Код н/д	Шифр дисципліни за навчальним планом	Компоненти освітньої програми (навчальні дисципліни, курсові роботи, практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
ОК 29.	ОКПП 1.2.21.	Технічний захист інформації	5	залік
ОК 30.	ОКПП 1.2.22.	Цифрова стеганографія	6	залік
ОК 31.	ОКПП 1.2.23.	Етичний хакінг	3	залік
ОК 32.	ОКПП 1.2.24.	CyberOps Associate	5	залік
Практична підготовка				
ОК 33.	ОКПП 1.2.25.	Навчальна практика	3	д. залік
ОК 34.	ОКПП 1.2.26.	Виробнича практика 1	6	д. залік
ОК 35.	ОКПП 1.2.27.	Виробнича практика 2	6	д. залік
Усього з циклу професійної підготовки			**138**	
Разом з нормативної частини			**177**	
Вибіркові компоненти ОПП				
Дисципліни загальної підготовки*				
ВК 1.	ВКЗП 2.1.1.	Дисципліна за вибором 1 /Базова загальновійськова підготовка***	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
ВК 6.	ВКЗП 2.1.6.	Дисц. вільного вибору №6	3	залік
Усього з циклу загальної підготовки			**18**	
Дисципліни професійної підготовки**				
ВК 6.	ВКПП 2.2.1.	Дисц. вільного вибору №1	5	залік
ВК 7.	ВКПП 2.2.2.	Дисц. вільного вибору №2	5	залік
ВК 8.	ВКПП 2.2.3.	Дисц. вільного вибору №3	5	залік
ВК 9.	ВКПП 2.2.4.	Дисц. вільного вибору №4	5	залік
ВК 10.	ВКПП 2.2.5.	Дисц. вільного вибору №5	5	залік
ВК 11	ВКПП 2.2.6.	Дисц. вільного вибору №6	5	залік
ВК 12.	ВКПП 2.2.7.	Дисц. вільного вибору №7	5	залік
ВК 13.	ВКПП 2.2.8.	Дисц. вільного вибору №8	5	залік
ВК 14.	ВКПП 2.2.9.	Дисц. вільного вибору №9	5	залік
Усього з циклу професійної підготовки			**45**	
Разом з вибіркової частини			**63**	
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.

*** - є обов'язковою навчальною дисципліною для громадян України чоловічої статі (жіночої статі - добровільно), які навчаються за денною формою здобуття освіти та досягли 18-річного віку (відповідно до Закону України «Про військовий обов'язок і військову службу)БВЗП обовязково включається в індивідуальні навчальні плани здобувачів ВО денної форми навчання на основі повної загальної середньої освіти на другому році навчання, на основі освітньо-кваліфікаційного рівня молодшого спеціаліста, освітньо-професійного ступеня фахового молодшого бакалавра та освітнього ступеня молодшого бакалавра (на основі НРК5) проходять

БЗВП на першому році навчання при вступі зі скороченим строком навчання або на другому році навчання при вступі без скорочення строку навчання.

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

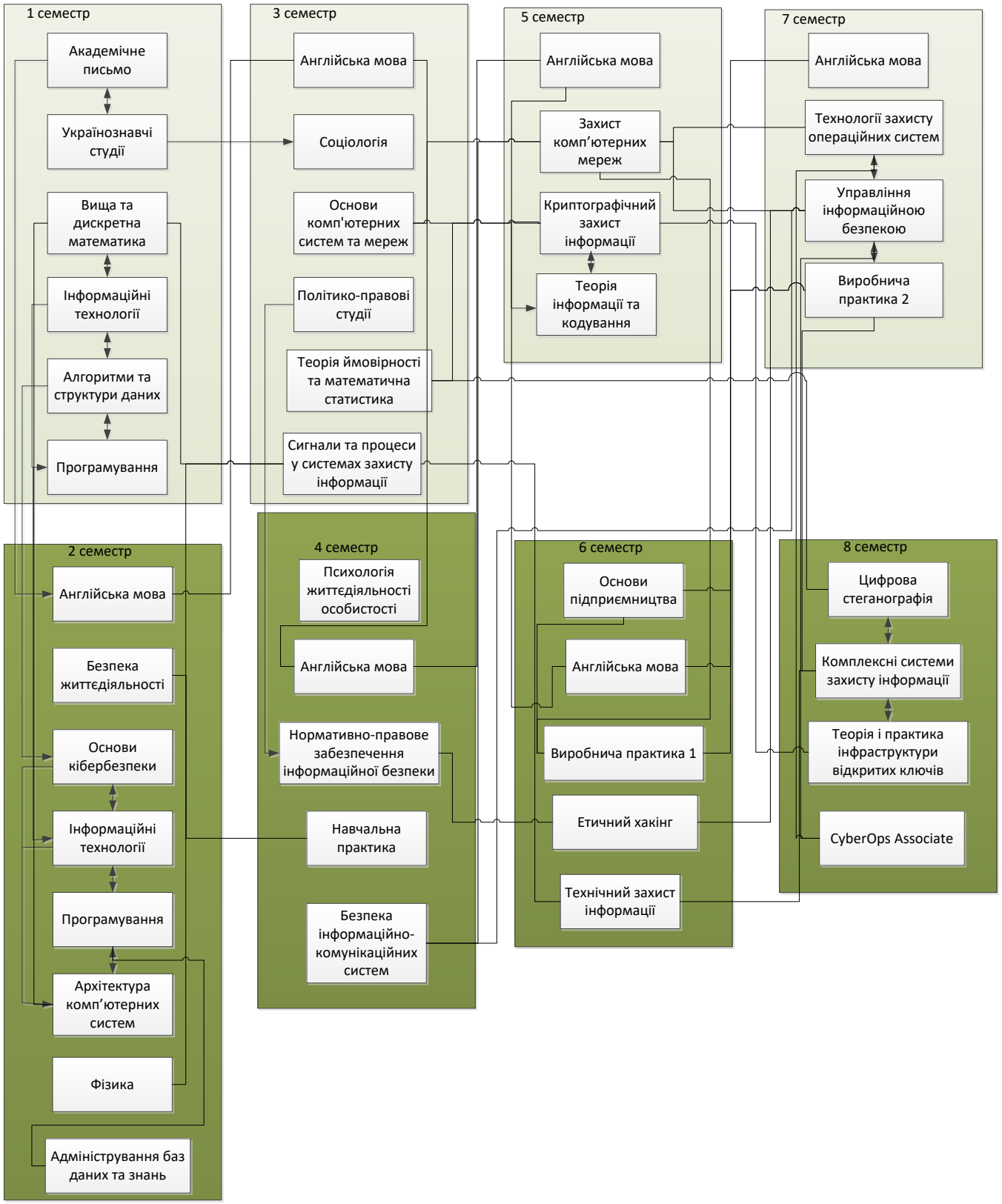
Зведена матриця відповідностей визначених Стандартом компетентностей/результатів навчання дескрипторам НРК наведено у таблиці 3.3.

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 стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.	РН 9. Вміти застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
КФ 2. Здатність до використання інформаційних технологій, сучасних методів і моделей кібербезпеки та систем захисту інформації.	РН10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
КФ 3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.	РН11. Планувати підготовку та забезпечувати неперервність процесів в організаціях згідно встановленої політики кібербезпеки та з урахування вимог до захисту інформації.
КФ 4. Здатність забезпечувати захист інформації в інформаційних системах згідно встановленої політики кібербезпеки та захисту інформації.	РН12. Застосовувати методи захисту інформації в інформаційних системах згідно встановленої політики інформаційної безпеки. РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних та програмноапаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних систем талабо інфраструктури організації в цілому.
КФ 5 Здатність відновлювати функціонування інформаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження..	РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних систем з використанням процедур резервування згідно встановленої політики безпеки та забезпечувати функціонування спеціального програмного забезпечення, щодо захисту та відновлення інформації. РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
КФ 6. Здатність забезпечувати впроваджувати та функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).	Н16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах

КФ 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.	РН17. Забезпечувати функціонування системи управління кібербезпекою та захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.
КФ 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.	РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
КФ 9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.	РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування та контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.
КФ 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, Виявляти та оцінювати можливі вразливості та загрози інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.	РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору та інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

Таблиця 3.4

Матриця відповідності фахових компетентностей

Освітні компоненти	**Компетентності**																		
	ІК	Загальні								Фахові									
		КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КЗ8	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10
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 компоненти	**Компетентності**																	
	ІК	Загальні								Фахові								
		КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КЗ8	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10
ОК 24	+									+						+			+
ОК 25	+									+							+		
ОК 26	+	+			+						+								
ОК 27	+				+							+		+					+
ОК 28	+									+					+				+
ОК 29	+									+								+	+
ОК 30	+									+							+		
ОК 31	+				+			+					+						+
ОК 32	+				+							+	+	+	+	+			
ОК 33		+	+																
ОК 34		+	+							+	+		+						
ОК 35		+	+							+	+	+	+			+	+		

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	ОК 35
ПРН 1	+	+		+																															
ПРН 2			+							+									+	+						+	+				+	+			
ПРН 3	+	+		+	+	+												+													+				
ПРН 4	+			+			+	+	+	+	+		+	+												+							+	+	+
ПРН 5	+			+			+	+	+	+	+		+	+												+							+	+	+
ПРН 6	+	+		+	+	+	+	+		+	+		+	+																			+	+	+
ПРН 7	+	+			+	+	+	+	+	+	+															+							+	+	+
ПРН 8									+				+	+								+													
ПРН 9					+	+				+		+			+	+	+	+				+	+	+	+			+	+	+			+	+
ПРН 10										+	+	+			+	+	+			+			+			+								+	+
ПРН 11												+							+				+				+					+			+
ПРН 12																			+				+									+		+	+
ПРН 13																			+				+									+		+	+
ПРН 14												+							+				+				+					+			

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	ОК 35
ПРН 15												+							+												+			
ПРН 16																		+									+				+			
ПРН 17												+			+							+		+							+			+
ПРН 18															+	+						+			+				+					+
ПРН 19															+	+						+			+				+					+
ПРН 20																					+	+						+							
ПРН 21											+								+			+		+			+	+	+						

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 2025 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**