МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖЕНО
Протокол засідання Вченої ради
Маріупольського державного
університету
23.06. 2021 № 12

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
(код та найменування спеціальності)

Спеціалізація (за необхідністю)

Освітня програма вводиться в дію з 01.09. 2021 р.
Наказ про введення в дію
рішення Вченої ради МДУ від 24.06. 2021 р. № 208

І Преамбула

1. Розроблено і винесено кафедрою математичних методів та системного аналізу 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 23.06.2021 р. протокол № 12.

3. Розробники програми:

Неласа Ганна Вікторівна, кандидат технічних наук, доцент, професор кафедри захисту інформації Національного університету «Запорізька політехніка», професор кафедри системного аналізу та інформаційних технологій МДУ.

Мартинюк Ганна Вадимівна, кандидат технічних наук, доцент, 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.

Черновол Валерія Сергіївна, Інспектор Донецького управління кіберполіції Департаменту Національної поліції України, старший лейтенант поліції

4. Цілі ОП, особливість ОП, відповідність цілей ОП місії та стратегії МДУ.

Мета освітньої 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 практичного втілення євроінтеграційних прагнень Української держави через забезпечення зміцнення науково-освітнього та інноваційного потенціалу країни шляхом розвитку людського капіталу, продукування та поширення ідей та нових знань.

Особливість (унікальність) ОП. Особливість програми полягає у комплексному підході, який орієнтований на підготовку фахівця з потужною теоретичною та практичною базою сучасних методів та засобів ідентифікації вразливостей та загроз інформаційній безпеці, здатного адаптуватися до змін технологій та забезпечити відповідний рівень захищеності інформації згідно потреб в регіоні.

5. Рецензії-відгуки зовнішніх стейкхолдерів:

Гайдур Галина Іванівна, д.т.н., професор, завідувач кафедри інформаційної та кібернетичної безпеки Державного університету телекомунікацій (м. Київ).

Жуков Станіслав Федорович, д.т.н., професор, генеральний директор навчально-науково-виробничого центру технологій управління «Квантум».

Ціон Павло Олександрович, заступник начальника Управління – начальник відділу протидії кіберзлочинам Донецької області Донецького Управління кіберполіції Департаменту кіберполіції Національної поліції України, капітан поліції.

ІІ Профіль освітньої програми

Профіль освітньо-професійної програми ступеня вищої освіти бакалавр Галузь знань 12 Інформаційні технології Спеціальність 125 Кібербезпека Назва ОПП: Кібербезпека Кваліфікація: Бакалавр з кібербезпеки Bachelor of Cyber Security		
Тип диплому та обсяг програми		Диплом бакалавра, одиничний, 240 кредитів ЄКТС, 4 ріки
Заклад вищої освіти		Маріупольський державний університет, м. Маріуполь
Акредитаційна інституція		Національне агентство із забезпечення якості вищої освіти
Період акредитації		
Рівень програми		Перший (бакалаврський) рівень FQ-EHEA- перший цикл, EQF-LLL-6 рівень, НРК- 6 рівень / Бакалавр
Передумови		Наявність повної середньої освіти
Мови викладання		Українська
Термін дії ОПП		до 01.07.2022 року
Інтернет-адреса постійного розміщення опису освітньої програми		http://mdu.in.ua/index/opp/0-298
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 практичного втілення євроінтеграційних прагнень Української держави через забезпечення зміцнення науково-освітнього та інноваційного потенціалу країни шляхом розвитку людського капіталу, продукування та поширення ідей та нових знань.	
б	Характеристика програми	
1	Предметна область, напрям	Галузь знань - 12 Інформаційні технології Спеціальність - 125 Кібербезпека **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 інформаційнокомунікаційних технологій; - сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; - автоматизованих систем проектування. <u>Методи, методики та технології:</u> Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/або кібербезпеки. <u>Інструменти та обладнання:</u> - 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 розуміння принципів побудови захищених інформаційних систем, виявлення, управління та ідентифікації ризиків. **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 сучасних методів та засобів ідентифікації вразливостей та загроз інформаційній безпеці, здатного адаптуватися до змін технологій та забезпечити відповідний рівень захищеності інформації згідно потреб в регіоні.
в	Працевлаштування та продовження освіти	
1	*Працевлаштування*	Бакалавр з кібербезпеки здатний виконувати професійні види робіт згідно з Національною рамкою кваліфікацій та Національним класифікатором України: Класифікатор професій ДК 003:2010. **Основна:** 3439 Фахівець з організації інформаційної безпеки. Фахівець із організації захисту інформації з обмеженим доступом. **Додаткова:** 3121 Фахівець з інформаційних технологій. 3119 Технік (сфера захисту інформації).
2	*Продовження освіти*	Можливість продовжити навчання за освітньою програмою ступеня магістра
г	**Стиль та методика навчання**	
1	*Підходи до 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.
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.
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.
	Ресурсне забезпечення реалізації програми
Кадрове забезпечення	Гарант ОПП: к.т.н., доцент Мартинюк Г.В. Науково-педагогічні працівники, які залучені до викладання дисциплін, мають наукові ступені та вчені звання та високі показники наукової, методичної та організаційної діяль-ності.
Матеріально-технічне забезпечення	Забезпеченість навчальними приміщеннями, комп'ютерними робочими місцями, мультимедійним обладнанням відповідає потребі. Наявна вся необхідна соціально-побутова інфраструктура, кількість місць в гуртожитку відповідає вимогам. Навчальна лабораторія з інформаційної та кібернетичної безпеки обладнана сучасною комп'ютерною технікою. Доступ до Інтернет-мережі є відкритим.
Інформаційне та навчально-методичне забезпечення	Інформаційне забезпечення освітньої діяльності формується на основі наукової бібліотеки. Викладачі та студенти мають доступ до електронних баз (Polpred.com, електронна бібліотека видавництва «Центр учбової літератури», JoumalTOCs, електронно-бібліотечна система BiblioRossica) та мережевих електронних ресурсів вільного доступу (Наукова електронна бібліотека періодичних видань НАН України, Електронна бібліотека «Мислене древо», Тематичний інтернет-навігатор Національної бібліотеки України імені В.І. Вернадського), що цілком задовольняє інформаційні потреби учасників освітнього процесу. Комплектування бібліотеки доповнюється за рахунок спеціальної періодики з питань системного аналізу. З усіх дисциплін навчального плану підготовки бакалавра з кібербезпеки розроблено робочі програми навчальних дисциплін.
	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 у Маріупольському державному університеті.
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 у Маріупольському державному університеті.
Навчання іноземних здобувачів вищої освіти	Не передбачено

ІІІ Загальна характеристика

Рівень вищої освіти	Перший (бакалаврський) рівень
Ступінь вищої освіти	Бакалавр
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Обмеження щодо форм навчання	Денна, заочна
Освітня кваліфікація	бакалавр з кібербезпеки \ Bachelor in Cyber Security.
Професійна(і) кваліфікація(ї) (тільки для регульованих професій)	

Кваліфікація в дипломі	Ступінь вищої освіти – Бакалавр Спеціальність – 125 Кібербезпека Освітня програма - Кібербезпека
Опис предметної області	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. Цілі навчання Забезпечити підготовку висококваліфікованих бакалаврів інформаційної та кібербезпеки, здатних вирішувати складні спеціалізовані задачі та практичні проблеми інформаційної безпеки, захищеності інформаційного і кіберпросторів держави в цілому або окремих суб’єктів їх інфраструктури від ризику стороннього кібервпливу. 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.
Академічні права випускників	Можливість навчатися за програмою другого (магістерського) рівня за цією галуззю знань (що узгоджується з отриманим дипломом бакалавра) або суміжною. Набуття додаткових кваліфікацій в системі післядипломної освіти.
Працевлаштування випускників	Бакалавр з кібербезпеки здатний виконувати професійні види робіт згідно з Національною рамкою кваліфікацій та Національним класифікатором України: Класифікатор професій ДК 003:2010. **Основна:**

	3439 Фахівець з організації інформаційної безпеки. Фахівець із організації захисту інформації з обмеженим доступом. **Додаткова:** 3121 Фахівець з інформаційних технологій. 3119 Технік (сфера захисту інформації).

IV. Обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти.

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».

Для здобуття ступеня бакалавра на базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») у Маріупольському державному університеті визнаються та перезараховуються не більше ніж 120 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста).

Тип диплома: одиничний ступінь.

V. Перелік компетентностей випускника

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.	
Загальні компетентності	Здатність застосовувати знання у практичних ситуаціях.	КЗ-1
	Знання та розуміння предметної області та розуміння професії.	КЗ-2
	Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.	КЗ-3
	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.	КЗ-4
	Здатність до пошуку, оброблення та аналізу інформації.	КЗ-5
	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.	КЗ-6
	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.	КЗ-7
Фахові компетентності	Здатність використовувати 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.	КФ-1

	Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.	КФ-2
	Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.	КФ-3
	Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та /або кібербезпеки.	КФ-4
	Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та /або кібербезпеки.	КФ-5
	Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.	КФ-6
	Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).	КФ-7
	Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.	КФ-8
	Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та /або кібербезпекою.	КФ-9
	Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.	КФ-10
	Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та /або кібербезпеки.	КФ-11
	Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та /або кібербезпеки.	КФ-12

VI. Нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання

1. Результати навчання, що визначають нормативний зміст підготовки:

Результати навчання	Шифр результату навчання
застосувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;	РН1
організувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;	РН2
використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;	РН3

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;	РН4
адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;	РН5
критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.	РН6
діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;	РН7
готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;	РН8
впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та /або кібербезпеки;	РН9
виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;	РН10
виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;	РН11
розробляти моделі загроз та порушника;	РН12
аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;	РН13
вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;	РН14
використовувати сучасне програмно-апаратне забезпечення інформаційно-телекомунікаційних технологій;	РН15
реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;	РН16
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;	РН17
використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;	РН18
застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;	РН19
забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;	РН20
вирішувати задачі забезпечення та супроводу (в тому числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційно- телекомунікаційних (автоматизованих) системах;	РН21
вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної та /або кібербезпеки;	РН22
реалізовувати заходи з протидії отриманню несанкціонованого доступу до інфор-	РН23

маційних 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);	РН24
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;	РН25
впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;	РН26
вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;	РН27
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;	РН28
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;	РН29
здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;	РН30
застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;	РН31
вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;	РН32
вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;	РН33
приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;	РН34
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;	РН35
виявляти небезпечні сигнали технічних засобів;	РН36
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;	РН37
інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;	РН38
проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;	РН39
інтерпретувати результати проведення спеціальних вимірювань з використанням	РН40

технічних- засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;	
забезпечувати безперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;	РН41
впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;	РН42
застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;	РН43
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;	РН44
застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;	РН45
здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;	РН46
вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;	РН47
виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;	РН48
забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;	РН49
забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);	РН50
підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;	РН51
використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;	РН52
вирішувати задачі аналізу програмного коду на наявність можливих загроз	РН53
усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод і громадянина в Україні.	РН54

2. Стиль та методика навчання

А) *Підходи до викладання та навчання*	Лекційні курси поєднуються з практично-лабораторною діяльністю. Навчання переважно проблемно-орієнтоване, з використанням самонавчання.
Б) *Система оцінювання*	Письмові екзамени, захист практичних та лабораторних робот в обсязі, необхідному для успішного засвоєння теоретичних та прикладних питань з інформаційної безпеки. Виконання індивідуальних проектних завдань.

3. Рекомендований перелік навчальних дисциплін і практик.

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	**60 (25 %)**	**45 (18,75%)**	**15 (6,25 %)**
Професійна підготовка	**180 (75 %)**	**135 (56,25 %)**	**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 ООП

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
ОК 9.	ОКЗП 1.1.9.	Фізичне виховання	3	д. залік
Усього з циклу загальної підготовки			**45**	
Дисципліни професійної підготовки				
ОК 10.	ОКПП 1.2.1.	Вища математика	10	екзамен
ОК 11.	ОКПП 1.2.2.	Основи кібербезпеки	4	залік
ОК 12.	ОКПП 1.2.3.	Основи автоматизованої обробки інформації	4	екзамен
ОК 13.	ОКПП 1.2.4.	Дискретна математика	5	екзамен
ОК 14.	ОКПП 1.2.5.	Теорія ймовірностей та математична статистика	5	екзамен
ОК 15.	ОКПП 1.2.6.	Фізика	3	залік
ОК 16.	ОКПП 1.2.7.	Криптологія	6	залік
ОК 17.	ОКПП 1.2.8.	Теорія інформації та кодування	5	екзамен
ОК 18.	ОКПП 1.2.9.	Алгоритми та структури даних	5	екзамен
ОК 19.	ОКПП 1.2.10.	Нормативно-правове забезпечення інформаційної безпеки	5	екзамен
ОК 20.	ОКПП 1.2.11.	Комп'ютерні мережі	5	екзамен
ОК 21.	ОКПП 1.2.12.	Програмування	15	залік, екзамен, екзамен
ОК 22.	ОКПП 1.2.13.	Інформаційні технології сучасного офісу	3	залік
ОК 23.	ОКПП 1.2.14.	Основи теорії кіл, сигналів та процесів в електроніці	4	екзамен
ОК 24.	ОКПП 1.2.15.	Управління інформаційною безпекою	4	залік
ОК 25.	ОКПП 1.2.16.	Електроніка	5	екзамен
ОК 26.	ОКПП 1.2.17.	Архітектура комп'ютерних систем	5	екзамен
ОК 27.	ОКПП 1.2.18.	Захист інформації в комп'ютерних системах та мережах	5	екзамен
ОК 28.	ОКПП 1.2.19.	Комплексні системи захисту інформації	5	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 1.2.20.	Комп'ютерна графіка	4	залік
ОК 30.	ОКПП 1.2.21.	Теорія і практика інфраструктури відкритих ключів	4	залік
ОК 31.	ОКПП 1.2.22.	Курсова робота за фахом	6	д. залік
Практична підготовка				
ОК 32.	ОКПП 1.2.23.	Навчальна практика	3	д. залік
ОК 33.	ОКПП 1.2.24.	Виробнича практика 1	6	д. залік
ОК 34.	ОКПП 1.2.25.	Виробнича практика 2	9	д. залік
Усього з циклу професійної підготовки			**135**	
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	6	екзамен
ВК 12.	ВКПП 2.2.7.	Дисц. вільного вибору №7	5	екзамен
ВК 13.	ВКПП 2.2.8.	Дисц. вільного вибору №8	5	залік
ВК 14.	ВКПП 2.2.9.	Дисц. вільного вибору №9	4	залік
ВК 15.	ВКПП 2.2.10	Дисц. вільного вибору №10	4	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.

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

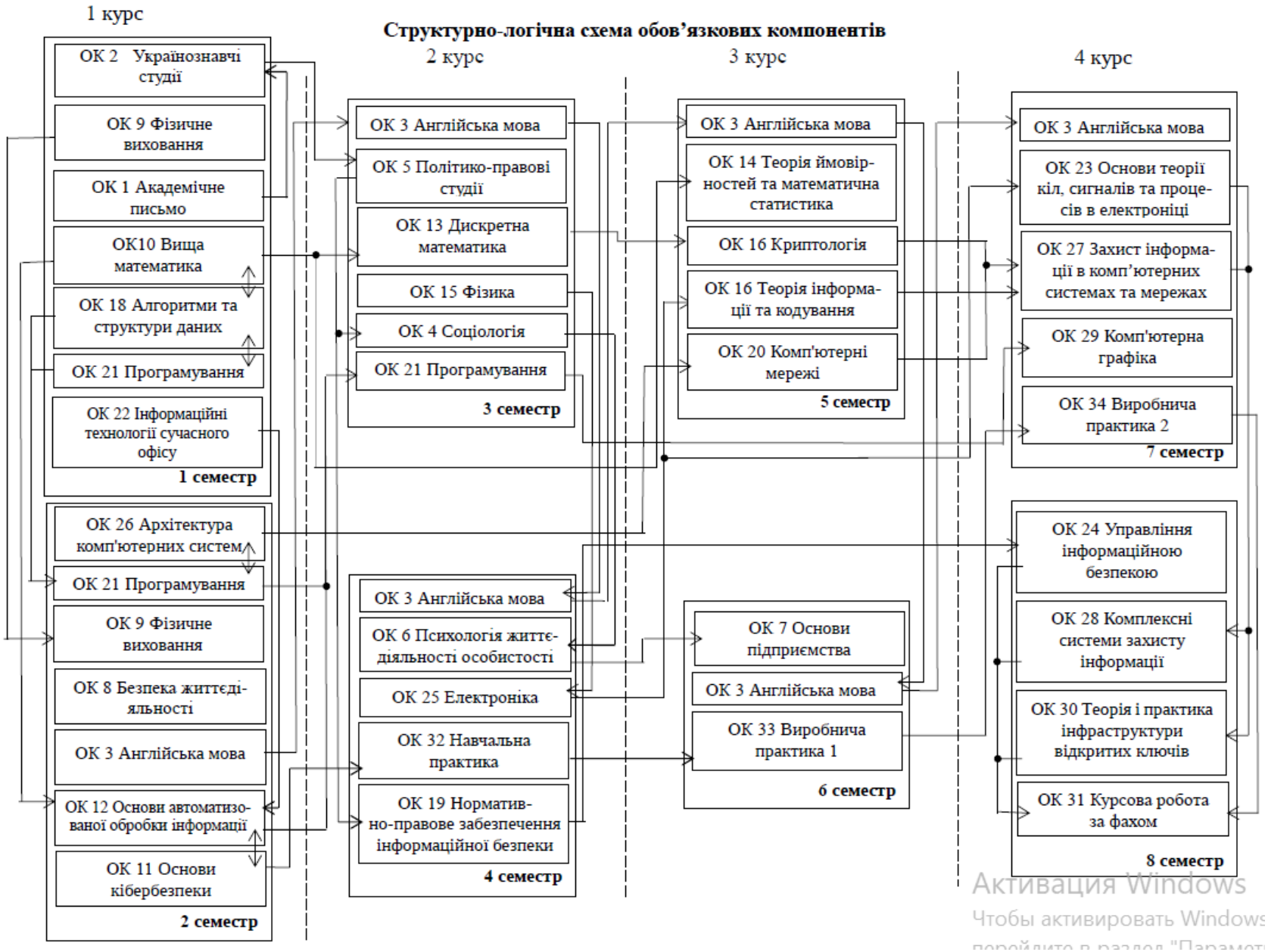
Зведена матриця відповідностей визначених Стандартом компетентностей/результатів навчання дескрипторам НРК наведено у таблиці 3.3.

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

Опис обов’язкових навчальних дисциплін наведено в Додатку А.

Переліки вибіркових компонент загальної підготовки ОП містяться у Каталозі елективних дисциплін для здобувачів вищої освіти за першим (бакалаврським) рівнями освіти та Каталозі елективних дисциплін професійної підготовки кафедри системного аналізу та інформаційних технологій МДУ.

Структурно-логічна схема обов'язкових компонентів



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.

Таблиця 3.4

Матриця відповідності фахових компетентностей та результатів навчання

Результати навчання компоненти освітньої програми (навчальні дисципліни, курсові роботи, практики, кваліфікаційна робота)	**Компетентності**																			
	ІК	Загальні							Фахові											
		КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12
РН1, РН54 ОК1. Академічне письмо ОК2. Українознавчі студії ОК3. Англійська мова	+	+		+		+	+	+												
РН2, РН3, РН4, РН34, РН54 ОК4. Соціологія ОК6. Психологія життєдіяльності особистості	+	+				+	+	+												
РН2, РН4, РН5, РН54 ОК7. Основи підприємництва		+				+	+	+												
РН2, РН54 ОК8. Безпека життєдіяльності ОК9. Фізичне виховання								+												
РН7, РН54 ОК5. Політико-правові студії		+					+	+	+											
РН2, РН7, РН8, РН9, РН32, РН33, РН34, РН35, РН39, РН41, РН43, РН44, РН45, РН50, РН54 ОК19. Нормативно-правове забезпечення інформаційної безпеки ОК24. Управління інформаційною безпекою	+	+	+		+		+		+			+	+				+			
РН6,РН14, РН15, РН16, РН18, РН19, РН24, РН26, РН27, РН31, РН35, РН41, РН47, РН48,	+		+		+					+	+							+		
РН2, РН4 ОК10. Вища математика ОК13. Дискретна математика ОК14. Теорія ймовірностей та математична статистика	+	+	+			+										+		+	+	+

Результати навчання компоненти освітньої програми (навчальні дисципліни, курсові роботи, практики, кваліфікаційна робота)	**Компетентності**																			
	ІК	Загальні							Фахові											
		КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12
РН2, РН3, РН4, РН10 ОК12. Основи автоматизованої обробки інформації	+	+	+		+	+											+			+
РН14, РН19, РН20, РН27, РН31, РН47, РН50, РН53 ОК18. Алгоритми та структури даних ОК21. Програмування ОК26. Архітектура комп'ютерних систем	+	+	+							+	+		+	+						
РН2, РН14, РН15, РН18, РН19, РН27, РН36, РН37, РН38 ОК15. Фізика ОК23. Основи теорії кіл, сигналів та процесів в електроніці ОК25. Електроніка	+	+			+								+	+	+					
РН2, РН4, РН11, РН12, РН17, РН27, РН29, РН31, РН36, РН37, РН40, РН51 ОК17. Теорія інформації та кодування	+	+	+		+					+			+	+			+		+	+
РН2, РН4, РН10, РН13, РН15, РН16, РН17, РН18, РН27, РН29, РН36, РН52 ОК20. Комп'ютерні мережі	+	+	+		+					+	+	+	+	+	+		+		+	
РН2, РН3, РН5, РН8 ОК22. Інформаційні технології сучасного офісу	+	+	+		+					+			+	+			+		+	
РН2, РН12, РН13,РН14, РН15, РН19, РН25,РН27, РН28, РН30, РН36, РН37, РН38, РН40, РН42, РН49, РН52 ОК27. Захист інформації в комп'ютерних системах та мережах	+	+	+		+	+			+	+	+			+			+			
РН2, РН4, РН11, РН19, РН21, РН22, РН24, РН26, РН27, РН31, РН35, РН46, РН48. ОК30. Теорія і практика інфраструктури відкритих ключів	+	+							+			+					+			

Результати навчання компоненти освітньої програми (навчальні дисципліни, курсові роботи, практики, кваліфікаційна робота)	**Компетентності**																			
	ІК	Загальні							Фахові											
		КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КФ1	КФ2	КФ3	КФ4	КФ5	КФ6	КФ7	КФ8	КФ9	КФ10	КФ11	КФ12
РН2, РН4, РН10, РН11, РН12, РН15, РН16, РН17, РН18, РН21, РН23, РН25, РН27,РН28, РН30, РН34, РН35, РН42, РН49, РН52. ОК28. Комплексні системи захисту інформації	+	+	+		+					+	+		+		+		+			+
РН2, РН3, РН4, РН6, РН10, РН14, РН28, РН30 ОК 32. Навчальна практика	+		+		+	+				+	+									+
РН2, РН3, РН4, РН15, РН18, РН28, РН35, РН 36, РН 37, РН 38, РН 40, РН 41, РН42, РН 44, РН 45, РН46, РН47, РН48, РН49, РН50, РН51, РН52, РН53, РН54 ОК 31. Курсова робота за фахом ОК 33. Виробнича практика 1 ОК 34. Виробнича практика 2	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
РН2, РН20, РН22, РН23 ОК29. Комп'ютерна графіка	+	+		+						+	+		+		+					+
РН5, РН6, РН 12, РН14, РН18, РН29, РН46, РН51 ОК 11. Основи кібербезпеки	+		+		+	+				+	+								+	+

VII Форми атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здобувачів вищої освіти здійснюється у формі атестаційного екзамену з англійської мови та єдиного державного кваліфікаційного іспиту за спеціальністю в установленому порядку.
Вимоги до кваліфікаційної роботи/проекту	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених цим стандартом та освітньою програмою.

VIII. Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

У МДУ функціонує система забезпечення закладом вищої освіти якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості), яка передбачає здійснення таких процедур і заходів:

1) визначення принципів та процедур забезпечення якості вищої освіти;

2) здійснення моніторингу та періодичного перегляду освітніх програм;

3) щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників вищого навчального закладу та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті закладу вищої освіти, на інформаційних стендах та в будь-який інший спосіб;

4) забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників;

5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів, за кожною освітньою програмою чи спеціальністю;

6) забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;

7) забезпечення публічності інформації про освітні програми, ступені вищої освіти та кваліфікації;

8) забезпечення ефективної системи запобігання та виявлення академічного плагіату у наукових працях працівників закладів вищої освіти і здобувачів вищої освіти;

9) інших процедур і заходів.

Гарант освітньої програми **Г.В. Мартинюк**

Додаток А

ОПИС ОБОВ'ЯЗКОВИХ НАВЧАЛЬНИХ ДИСЦИПЛІН

Обов'язкові компоненти ОПП

Дисципліни загальної підготовки

ОК 1. Академічне письмо

Мета вивчення курсу: підвищення рівня теоретичних знань та розвиток практичних навичок студентів щодо мовних умінь і навичок у професійній сфері; практичне опанування студентами умінь ділового мовлення на рівні, достатньому для професійної діяльності; формування комунікативної компетентності студентів.

Завдання курсу: підвищення загального рівня грамотності студентів; засвоєння основних відомостей про українську мову як багатоаспектну лінгвістичну систему; формування, розвиток та закріплення навичок та вмінь правильного використання усталених мовностилістичних засобів української мови; докладне вивчення зразків оформлення різних видів документів; формування вмінь культури мовлення у професійній діяльності.

ОК 2. Українознавчі студії

Мета вивчення курсу: формування знань про заселення українських земель, формування української нації та розвиток інших етнічних спільнот, історію української державності, соціально-економічні, політичні, культурні процеси, що складають змістовий пласт історії України від найдавніших часів до початку XXI ст; формування у студентів системи знань про унікальність української культури, її роль та місце в світовому культурному просторі.

Завдання курсу: виховання у студентів на фактах історії України почуття національної гідності, патріотизму, почуття відповідальності за вивчення історії України, як основи для засвоєння широкої системи історичних знань, вивчення історичного процесу за принципом історизму, об'єктивності та науковості, формування нового історичного мислення шляхом співставлення полярних точок зору і різних фактів, розвинення вміння аналізувати історичний матеріал, робити ґрунтовні висновки, використовуючи різні типи історичних джерел, навчити розрізняти історичний факт від історичного міфу, викривати стереотипи, упередженість, необ'єктивність, розвити вміння робити виважені висновки та самостійні оцінки історичних подій, явищ, толерантно сприймати багатоетнічні, полікультурні явища національної та світової історії, розглядати історію України у європейському та світовому контекстах, формувати національну самобутність і почуття патріотизму. Формування у студентів розуміння унікальності національного культурного простору на основі з'ясування проблеми культурогенезу; познайомити з основними досягненнями української культури в її діахронному вимірі; виявити детермінованість та закономірності культурного процесу, оцінити історичний розвиток культури на основі порівняння української культури з європейською та світовою; оцінити еволюцію мистецького розвитку в контексті проблеми співвідношення традиції і новаторства

ОК 3. Англійська мова

Мета вивчення курсу: формування навичок креативного усного та писемного мовлення; формування навичок монологічного і діалогічного непідготовленого мовлення на основі активно засвоєного лексичного, граматичного та стилістичного матеріалів; засвоєння лексичних одиниць та мовленнєвих моделей на матеріалі текстів підручників, розмовних тем, суспільно-політичних текстів, комунікативних ситуацій, текстів позалекційного читання; посилення самостійної пошукової, творчої роботи; підвищення рівня лінгвістичної компетенції через втілення знань стилістичних прийомів та виразних засобів в ґрунтовний аналіз англомовного те-

ксту; підвищення рівня мовної компетенції студентів, вдосконалення їхніх мовних навичок через розвиток таких вмінь як читання, аудіювання, усне та письмове мовлення, а також розвиток точності граматичної побудови мовлення.

Завдання курсу поповнити словниковий запас студентів для посилення їх висловлювальних можливостей; активізувати пасивний вокабуляр, а також поповнити активний словник, що має розширити висловлювальні можливості студентів; забезпечити знаннями практичної граматики у ході побудови монологічного та діалогічного мовлення; вдосконалити вміння студентів щодо глибокого філологічного (зокрема, лінгвостилістичного) аналізу тексту на англійській мові; покращити вміння студентів сприймати текст на слух (з опорою та без опори на друкований текст) та стимулювати активне обговорення сприйнятої інформації в аудиторії; сформувати навички письма з метою підвищення ефективності письмової комунікації; логічно структурувати та правильно виконувати словесне оформлення письмового тексту на задану тему; актуалізувати знання практичної граматики у ході побудови монологічного та діалогічного мовлення; ознайомити студентів з сучасними тенденціями англійської розмовної мови; вдосконалити навички усних доповідей/презентацій на англійській мові.

ОК 4. Соціологія

Мета вивчення курсу: полягає у виробленні у студентів правильного розуміння соціальних явищ на підставі філософських та економічних знань; формуванні соціального мислення, розуміння соціальних проблем, джерел їхнього виникнення і можливих шляхів їхньої реалізації; допомозі студентам в освоєнні соціального світу.

Завдання курсу: сформувати знання загальносоціологічних та спеціальних і галузевих соціологічних теорій, а також методів та методики проведення соціологічних досліджень.

ОК 5. Політико-правові студії

Мета вивчення курсу: складання у майбутніх фахівців глибокого та всебічного розуміння політичної реальності та її осмислення політичною наукою. Сформувати базові уявлення про взаємодію суб'єктів політики між собою та з суспільством, виокремити основні політичні інститути, процеси та явища. Застосовувати політичні знання при аналізі політичних процесів сучасності. Сформувати політичну культуру, особисту позицію. Набуття студентами ґрунтовних знань з теорії правознавства, оволодіння системою основних понять правознавства, засвоєння найважливіших положень окремих правових галузей та вироблення навичок їх застосування на практиці.

Завдання курсу: методології політичної науки; систематизація та структуризація знань про політику; понятійно-категоріального апарату; сутності політичної системи суспільства, її функціонування та взаємодію з середовищем. Вивчення теорії правознавства; закономірностей та специфіки розвитку держави та права; основних положень Конституції України, які стосуються регламентування діяльності держави та організації суспільного життя, прав і обов'язків громадянина; ознайомлення з базовими положеннями основних галузей права України та їх застосуванням у практичних завданнях; ознайомлення студентів із перспективами розвитку правової системи України у зв'язку із євроінтеграційними процесами.

ОК 6. Психологія життєдіяльності особистості

Мета вивчення: формування прагнення до самопізнання та самовдосконалення, комунікативної компетентності студентів; підвищення рівня теоретичних знань; розвиток творчого мислення і вмінь підходити до рішення професійних та життєвих задач з урахуванням основних закономірностей функціонування психіки людини.

Завдання курсу: допомога в осмисленні значущості основ психології для майбутнього професіонала в будь-який галузі життєдіяльності; ознайомлення студентів з історією, сучасним станом, основними категоріями, методами; галузями психологічної науки; формування знань про сутність, зміст, структуру, джерела психіки людини та соціальної групи; формування

професійного бачення психологічних закономірностей протікання та розвитку психічних процесів, станів та властивостей особистості; окреслення онтогенетичного шляху людини як соціального індивіда й особистості, розкриття зв'язку закономірностей психічного розвитку з вихованням і навчанням; розвиток у студентів комунікативних компетенцій, оволодіння технологіями міжособистісного спілкування; формування практичних навичок вправного застосування різних методів вивчення пізнавальної сфери особистості, психічних станів та індивідуально-типологічних особливостей особистості; заохочування студентів до пошуку зв'язків теоретичних положень науки з практикою.

ОК 7. Основи підприємництва

Мета вивчення курсу: набуття ґрунтовних економічних знань, формування логіки економічного мислення і економічної культури, навчання базовим методам пізнання і аналізу економічних процесів.

Завдання курсу: набуття навичок раціональної економічної поведінки, виходячи з концептуальних основ ринкової економіки; розуміння особливостей функціонування сучасних ринків, формування агрегованих показників, визначення чинників і наслідків макроекономічного розвитку господарських систем; формування вмінь загального аналізу основних економічних подій у своїй країні та за її межами, пошуку й використання інформації, необхідної для орієнтування в основних поточних проблемах економіки.

ОК 8. Безпека життєдіяльності

Мета вивчення курсу: набуття студентом компетенцій, знань, умінь і навичок для здійснення професійної діяльності за спеціальністю з урахуванням ризику виникнення техногенних аварій й природних небезпек, які можуть спричинити надзвичайні ситуації та привести до несприятливих наслідків на об'єктах господарювання, а також формування у студентів відповідальності за особисту та колективну безпеку; формуванні у студентів здатності творчо мислити, вирішувати складні проблеми інноваційного характеру й приймати продуктивні рішення у сфері цивільного захисту, з урахуванням особливостей майбутньої професійної діяльності випускників, а також досягнень науково-технічного прогресу; наданні знань, умінь, здатностей (компетенцій) для здійснення ефективної професійної діяльності шляхом забезпечення оптимального управління охороною праці на підприємствах (об'єктах господарської, економічної та науково-освітньої діяльності), формуванні у студентів відповідальності за особисту та колективну безпеку і усвідомлення необхідності обов'язкового виконання в повному обсязі всіх заходів гарантування безпеки праці на робочих місцях.

Завдання курсу: опанувати знання, вміння та навички вирішувати професійні завдання з обов'язковим урахуванням галузевих вимог щодо забезпечення безпеки персоналу та захисту населення в небезпечних та надзвичайних ситуаціях і формування мотивації щодо посилення особистої відповідальності за забезпечення гарантованого рівня безпеки функціонування об'єктів галузі, матеріальних та культурних цінностей в межах науково-обґрунтованих критеріїв прийнятного ризику; засвоєння студентами новітніх теорій, методів і технологій з прогнозування НС, визначення рівня ризику та обґрунтування комплексу заходів, спрямованих на відвернення НС, захисту персоналу, населення, матеріальних та культурних цінностей в умовах НС, локалізації та ліквідації їхніх наслідків; набуття студентами знань, умінь і здатностей (компетенцій) ефективно вирішувати завдання професійної діяльності з обов'язковим урахуванням вимог охорони праці та гарантуванням збереження життя, здоров'я та працездатності працівників у різних сферах професійної діяльності.

ОК 9. Фізичне виховання

Мета вивчення курсу: формування всебічно розвинених особистостей, підготовка студентів до високоякісної праці за обраних фахом, збереження та зміцнення здоров'я.

Завдання курсу: збереження та зміцнення здоров'я, загартування організму, прищеплення навичок здорового способу життя, підвищення фізичної і розумової працездатності; виховання у студентів потреби до систематичних занять фізичними вправами, прагнення до фізичного вдосконалення; оволодіння системою спеціальних знань з основ теорії і методики, організації фізичного виховання; набуття необхідних знань у галузі гігієни праці, харчування спорту; формування життєво важливих вмінь і навичок, розвиток фізичних здібностей

Дисципліни професійної підготовки

ОК 10. Вища математика

Мета вивчення курсу: формування у студентів фундаментальних понять алгебраїчного та геометричного характеру, а також умінь застосування цих понять до розв'язання практичних задач, забезпечення теоретичною підготовкою та фундаментальною базою для успішного вивчення дисциплін професійної та практичної підготовки, які передбачені навчальними планами; набуття вміння математичного формулювання завдання; оволодіння основними методами дослідження і розв'язання математичних завдань; напрацювання навичок самостійного вивчення наукової літератури, формування вміння самостійно розширювати математичні знання і проводити математичний аналіз прикладних задач, розвинення інтелекту студентів і формування вмінь аналітично мислити.

Завдання курсу: навчання студентів теоретичним основам і методам теорії лінійної алгебри, векторної алгебри, аналітичної геометрії, диференціального та інтегрального числення, теорії чисел і застосуванню цих методів для розв'язання різноманітних задач теоретичного та практичного характеру в галузі інформаційних технологій, формування у студентів ключових і міждисциплінарних компетенцій, що забезпечують успішне проходження ними дисциплін практичного, спеціального і професійного спрямування.

ОК 11. Основи кібербезпеки

Мета вивчення курсу: формування сучасного рівня культури з інформаційної безпеки; набуття практичних навичок з основ застосування сучасних методів забезпечення захисту інформації в комп'ютерних системах, починаючи з криптографічних методів захисту інформації; формуванні у студентів розуміння основ інформаційної безпеки, вміння застосовувати криптографічні методи шифрування, вміння проектувати підсистеми захисту комп'ютерних систем, вміння застосовувати методи шифрування інформації для передачі у мережі, вміння розробляти парольні захищенні системи, ознайомлення зі шляхами використовування управління доступом різними методами; ознайомлення студентів з актуальними питаннями впливу комп'ютерних вірусів і шкідливих програм на безпеку комп'ютерних систем та методам протидії цьому, ознайомлення з методами захисту мережевої інформації.

Завдання курсу: надання основних відомостей з принципів протидії спробам несанкціонованого доступу до інформації з боку сторонніх осіб; придбання знань в області захисту інформації в комп'ютерних системах та мережах з урахуванням сучасного стану та прогнозу розвитку методів; освоєння засобів аналізу погроз інформаційній безпеці; вивчення принципів використання основних методів, принципів, алгоритмів, систем та засобів здійснення захисту інформації у системах та мережах.

ОК 12. Основи автоматизованої обробки інформації

Мета вивчення курсу: формування системи теоретичних знань та практичних умінь які необхідні для розробки і виконання логічно обґрунтованих дій під час обробки інформації засобами сучасних інформаційних технологій, що є практичною основою для фахівця в галузі кібербезпеки.

Завдання курсу: ознайомлення з математичними та інформаційними аспектами вирішення завдань на обробку інформації; формування здатностей студентів самостійно робити аналіз поставленого завдання, обирати наближений метод його розв'язку; оволодіння знаннями з методів обробки і подання результатів вимірювань, методів підвищення точності результатів вимірювань; оволодіння методами складання алгоритмів та програм мовою високого рівня, отримання результату та аналіз отриманого розв'язку.

ОК 13. Дискретна математика

Мета вивчення курсу: надання майбутнім фахівцям базових знань з теорії множин, математичної логіки та теорії алгоритмів; формування системи теоретичних знань і практичних навичок побудови дискретних математичних моделей реальних об'єктів, проектування систем із застосуванням дискретного аналізу; оволодіння студентами математичною мовою і фундаментальними поняттями дискретної математики; сприяння розвитку логічного і аналітичного мислення студентів.

Завдання курсу: навчання студентів теоретичним основам і методам дискретної математики та застосуванню цих методів для розв'язання різноманітних задач теоретичного та практичного характеру в галузі інформаційних технологій.

ОК 14. Теорія ймовірностей та математична статистика

Мета вивчення курсу: формування системи теоретичних знань і практичних навичок з теорії ймовірностей, випадкових процесів та математичної статистики; оволодіння студентами основними методами кількісного вимірювання випадковості дії факторів, що впливають на будь-які процеси, засад математичної статистики, яка використовується під час прогнозування, планування інформаційної безпеки, формування аналітичного мислення та інтуїції, наукового міркування і широкого світогляду для розв'язання різноманітних задач у практичній діяльності за фахом.

Завдання курсу: навчання студентів теоретичним основам і методам теорії ймовірностей та математичної статистики, необхідних для формулювання та дослідження ймовірнісних моделей, обґрунтовування вибору ймовірнісно-статистичних методів та методів аналізу випадкових процесів для розв'язування теоретичних і прикладних задач в галузі інформацій-них технологій; застосовування статистичних методів для обробки та аналізу вихідної інформації, уміння відображати та аналізувати результати експериментів та спостережень; застосовування сучасних інформаційних технологій для обробки та аналізу статистичної інформації; розроблення відповідних висновків для наступного прийняття ефективних рішень з кібербезпеки.

ОК 13. Фізика

Мета вивчення курсу: освоєння фундаментальних фізичних законів і понять, теорій, методів класичної і сучасної фізики.

Завдання курсу: формування наукового мислення і наукового світогляду; формування навичок володіння основними прийомами і методами вирішення науково-технічних завдань; ознайомлення з сучасною науково-дослідної апаратурою і вимірювальними приладами; ознайомлення з історією фізики і її розвитком, а також з основними напрямами і тенденціями розвитку сучасної фізики; формування навичок проведення наукових досліджень; формування культури мислення, усної та письмової мови, розвиток здатності до узагальнення, аналізу, сприйняття інформації, постановці мети та вибору шляхів її досягнення.

ОК 16. Криптологія

Мета вивчення курсу: формування сучасного рівня культури з інформаційної безпеки; набуття практичних навичок з основ застосування сучасних методів забезпечення захисту інформації в комп'ютерних системах, починаючи з криптографічних методів захисту інформації;

формуванні у студентів розуміння основ інформаційної безпеки, вміння застосовувати криптографічні методи шифрування, вміння проектувати підсистеми захисту комп'ютерних систем, вміння застосовувати методи шифрування інформації для передачі у мережі, вміння розробляти парольні захищенні системи, ознайомлення зі шляхами використовування управління доступом різними методами. Формуванні у студентів розуміння основ прикладної криптології, вміння застосовувати криптографічні методи дешифрування, вміння застосовувати методи криптоаналізу.

Завдання курсу: Придбання знань в області криптології з урахуванням сучасного стану та прогнозу розвитку методів захисту за зламу; вивчення принципів використання основних методів, принципів, алгоритмів, систем та засобів здійснення захисту інформації у системах та мережах. Надання основних відомостей з принципів протидії спробам несанкціонованого доступу до інформації з боку сторонніх осіб; придбання знань в області захисту інформації в комп'ютерних системах та мережах з урахуванням сучасного стану та прогнозу розвитку методів; освоєння засобів аналізу загроз інформаційній безпеці; вивчення принципів використання основних методів, принципів, алгоритмів, систем та засобів здійснення захисту інформації у системах та мережах.

ОК 17. Теорія інформації та кодування

Мета вивчення курсу: є надання студентам знань з теорії інформації та кодування для розуміння функціонування комп'ютерних систем, а також розвитку у студентів навичок самостійної роботи для освоєння методів формування і кодування повідомлень при їх передачі по трактах зі значним рівнем завад. Формування у студентів вмінь кількісно оцінювати інформацію у повідомленнях для дискретних і неперервних ансамблів та джерел, а також кодувати повідомлення у дискретних і неперервних каналах.

Завдання курсу: придбання і закріплення основних засобів оцінки кількості інформації, освоєння сучасних методів та алгоритмів кодування для джерел повідомлень і передачі даних по каналам зв'язку; знати принципи побудови завадостійких кодів та їх використання в сучасних комп'ютерних інформаційних системах; вміти використовувати основні принципи кодування інформації з метою підвищення ефективності вводу, збереження, обробки та передачі інформації в сучасних інформаційних технологіях.

ОК 18. Алгоритми та структури даних

Мета вивчення курсу: формування системи знань в області алгоритмізації та структур даних, а також вмінь і навичок складання алгоритмів та вибору типів структур, необхідних для вирішення поставлених задач фахового спрямування.

Завдання курсу: оволодіння основами алгоритмізації на рівні, достатньому для опрацьовування задач кібербезпеки, пов'язаних з подальшою практичною діяльністю фахівця в області моделювання об'єктів і процесів, напрацювання навичок самостійної роботи з науковою літературою, розглядання методів дослідження та розв'язання прикладних задач.

ОК 19. Нормативно-правове забезпечення інформаційної безпеки

Мета вивчення курсу: вивчення сучасних понять нормативно-правового забезпечення інформаційної безпеки, як однієї з найважливіших сфер діяльності в умовах входження держави в інформаційне суспільство та алгоритмів необхідних в подальшому при розробці систем захисту інформації в комп'ютерних системах та мережах.

Завдання курсу: формування у студентів певних знань та вмінь з основ нормативно-правового забезпечення інформаційної безпеки держави. Визначити основні терміни, поняття та категорії нормативно-правового забезпечення інформаційної безпеки на рівні тлумачення та відтворення, підзаконні нормативні акти із захисту інформації, основні положення нормативно-правового забезпечення інформаційної безпеки держави для їх практичного застосування

та втілення у процесі фахової діяльності майбутнього спеціаліста з інформаційної безпеки, вільно орієнтуватися в питаннях інформаційної безпеки держави, самостійно давати характеристику стану законодавчої бази у сфері нормативно-правового забезпечення інформаційної безпеки.

ОК 20. Комп'ютерні мережі

Мета: придбання знань в області теорії комп'ютерних мереж, а також навичок проектування корпоративних комп'ютерних мереж і їхнього використання для пошуку, обробки й аналізу даних, необхідних для прийняття ефективних управлінських рішень.

Завдання: ознайомити студентів з основами побудови комп'ютерних мереж, засобами комунікаційної техніки, концепціями побудови локальних і глобальних комп'ютерних мереж; вивчити сучасні комп'ютерні технології й основні засоби забезпечення їх працездатності; ознайомитися із програмним забезпеченням мережевих технологій і тенденціями їх розвитку на сучасному етапі; надати практичних навичок проектування корпоративної комп'ютерної мережі стосовно до умов конкретного об'єкта.

ОК 21. Програмування

Мета вивчення курсу: набуття студентами знань, вмінь та навичок, необхідних для ефективного використання мов програмування при розробці прикладного і системного програмного забезпечення, розв'язування практичних обчислювальних задач за допомогою персонального комп'ютеру; ознайомлення студентів з сучасною мовою програмування C# та оволодіння основними можливостями цієї мови, навичками хорошого стилю програмування, методами проектування та створення програм згідно сучасних технологій програмування; формуванні у студентів розуміння основ теоретичних концепцій, принципів та понять сучасного, зокрема композиційного, програмування, методів формалізації мов програмування та доведення коректності програм.

Завдання курсу: набуття компетенцій, знань, умінь та навиків на рівні новітніх досягнень у теорії програмування відповідно до кваліфікації.

ОК 22. Інформаційні технології сучасного офісу

Мета вивчення курсу: формування у студентів теоретичних знань та практичних навичок, необхідних безпосередньо для проектування та використання інформаційних технологій для створення комп'ютерних систем та забезпечення їх роботи; ознайомлення студентів з теоретичними положеннями та практичними навиками, що створюють основи побудови складних корпоративних інформаційних систем та їх складових частин – автоматизованих робочих місць фахівців та керівних осіб.

Завдання курсу: надання студентам знань, щодо структури та основних методів створення і використання інформаційних технологій та систем, які містять інформацію про стан об'єктів дослідження або управління, а також економічні й технологічні показники виробничої та інших сторін діяльності підприємств та установ, функціонування технічних засобів, набуття студентами практичних навичок із створення персонального інформаційного середовища фахівця будь-якого обраного профілю на базі сучасних комп'ютерних технологій, а також вмінню використовувати інформаційні системи для вирішення прикладних задач відповідно до їх професійній спрямованості; закріплення у студентів практичних навичок роботи з складними інформаційними технологіями при вирішенні прикладних задач.

ОК 23. Основи теорії кіл, сигналів та процесів в електроніці

Мета вивчення курсу: навчити студентів методам аналізу усталених та перехідних явищ та процесів, що відбуваються в лінійних та нелінійних колах постійного та змінного струмів.

Завдання курсу: надання студентам знань щодо основних фізичних понять електромагнітних явищ; методів розрахунку та аналізу лінійних електричних та магнітних кіл; методів розрахунку нелінійних кіл постійного та змінного струму; суті процесів, що відбуваються при перехідних режимах роботи схеми та методи розрахунку таких кіл; явищ, що відбуваються в колах з розподіленими параметрами, методи розрахунку таких кіл; методів синтезу реактивних багатополюсників.

ОК 24. Управління інформаційною безпекою

Мета вивчення курсу: надати студентам знання, основні рекомендації та загальні принципи щодо здійснення, підтримки і поліпшення системи управління інформаційною безпекою підприємства на базі міжнародних стандартів серії ISO/IEC, що забезпечують загальне керівництво безпекою інформації на загальноприйнятих показниках.

Завдання курсу: забезпечити розуміння концепції менеджменту інформаційної безпеки на базі міжнародних стандартів серії ISO/IEC; надати знань щодо порядку створення системи менеджменту інформаційної безпеки (СМІБ); загальних вимог забезпечення документацією СМІБ; обов'язків керівників СМІБ; порядку проведення внутрішніх та зовнішніх аудитів коректності реалізації СМІБ; цілей управління СМІБ; засобів управління СМІБ; основних понять і визначення моделі оцінки ризику.

ОК 25. Електроніка

Мета вивчення курсу: оволодіння студентами теоретичними навичками аналізувати, розраховувати, синтезувати та проектувати електроні аналогові та цифрові пристрої, які використовуються в системах захисту інформації

Завдання курсу: надання студентам знань щодо основних типів цифрових та аналогових електронних пристроїв, а також розумінню їх роботи та характеристик; набуття практичних навичок щодо використання елементів та пристроїв при проектуванні електронних систем.

ОК 26. Архітектура комп'ютерних систем

Мета вивчення курсу: ознайомлення студентів з побудовою апаратної частини комп'ютерів та освоєння основ програмування на низькому рівні, тобто програмування мовою ASSEMBLER.

Завдання курсу: надання студентам системного уявлення про архітектуру сучасних CPU та комп'ютерних систем, організація адресного простору пам'яті в реальному та захищеному режимах, організація низькорівневої взаємодії периферійних приладів ПК, основи мови програмування ASSEMBLER.

ОК 27. Захист інформації в комп'ютерних системах та мережах

Мета вивчення курсу: закласти термінологічний фундамент, навчити студентів правильно проводити аналіз загроз інформаційній безпеці, основним методам, принципам, алгоритмам захисту інформації в комп'ютерних системах та мережах з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення загроз зі сторони потенційних порушників.

Завдання курсу: формування у студентів певних знань та вмінь з теорії та практики захисту інформації, за результатами яких студенти повинні знати сучасні загрози безпеці інформаційним системам; технічні методи і засоби захисту інформації; програмні методи і засоби захисту; методи захисту інформації в розподілених інформаційних системах; організаційно-правове забезпечення захисту інформації; а також вміти аналізувати можливості несанкціонованого здобуття інформації потенційними порушниками; аналізувати вплив комп'ютерних вірусів і шкідливих програм на безпеку комп'ютерних систем; виявляти дії вірусу в ОС Windows

за допомогою аналізу процесів, що протікають, за допомогою аналізу кодів підозрілих програм, за допомогою антивірусних програм; організовувати та виконувати практичні дій посадових осіб відділу захисту інформації відповідно до інструкцій і обов'язків.

ОК 28. Комплексні системи захисту інформації

Мета вивчення курсу: оволодіння студентами комплексом знань у галузі захисту інформації, системами й методами визначення захищеності програмних продуктів, пристроїв; комп'ютерних мереж, їх складових та набуття на основі цих знань практичних навичок та теоретичних знань, необхідних для творчого підходу в питанні сучасного та майбутнього оперативного захисту комп'ютерної техніки й інформації; опанування концептуальними моделями розробки, розподілення, обробки, використання та зберігання конфіденціальних документів; стратегією вибору систем виявлення атак, навичками роботи з пристроями безпеки в локальних та глобальних комп'ютерних мережах із метою використання їх, можливостей для покращання показників безпеки в них.

Завдання курсу: студенти повинні здобути знань та практичних навичок щодо засобів дії загроз на об'єкти інформаційної безпеки установ, методи проведення аналізу надійності системи захисту інформації в комп'ютерних системах; основні методи, технології, принципи і правила побудови захисту комп'ютерних систем, в тому числі, персональних комп'ютерів, їх елементів і об'єктів комп'ютерних мереж; формулювати завдання щодо питань захисту інформації та, формалізуючи їх, вказувати шляхи вирішення.

ОК 29. Комп'ютерна графіка

Мета вивчення курсу: формування у майбутніх фахівців сучасного рівня інформаційної культури у галузі комп'ютерної графіки; ознайомлення з основними методами і алгоритмами теорії обробки зображень; набуття практичних навичок з основ застосування сучасних технологій обробки зображень за допомогою сучасних комп'ютерних засобів та спеціалізованих пакетів роботи із графікою; формування у студентів розуміння основ комп'ютеризації сучасних методів обробки графічної інформації, а також інформаційного забезпечення, системи знань та вмінь, зорієнтованих на проведенні інформаційної та інформаційно-аналітичної роботи з використанням спеціалізованого прикладного програмного забезпечення для роботи з зображеннями; ознайомлення студентів з актуальними питаннями використання засобів для роботи з комп'ютерною графікою та обробки зображень.

Завдання курсу: придбання і закріплення знань студентами в області використання інформаційних технологій для роботи з комп'ютерною графікою; вивчення пакетів програм; придбання знань в області обробки зображень за допомогою методів та алгоритмів комп'ютерної графіки; освоєння методики і технологій обробки зображень, зокрема фільтрації, сегментації та ін.

ОК 30. Теорія і практика інфраструктури відкритих ключів

Мета вивчення курсу: навчання студентів принципам побудови комплексних систем захисту інформації, розробки, дослідженню та застосуванню механізмів захисту інформації, що засновані на використанні алгоритмів традиційної (симетричної) криптографії та криптографії з відкритим ключем для забезпечення безпеки програмного забезпечення, вивчення студентами основ стеганографічного захисту інформації та особливості побудови інфраструктури відкритих ключів.

Завдання курсу: формування у студентів володіння принципами побудови комплексних систем захисту інформації; вміння розробляти, проводити дослідження та застосовувати механізми щодо забезпечення автентичності, цілісності та конфіденційності в програмно-апаратних, програмних засобах; володіння основами стеганографічного захисту інформації, принципами захисту програмного коду від зламу/модифікації; вміння побудови інфраструктури відкритих ключів.

Аркуш обліку змін

Для ОПП Кібербезпека першого (бакалаврського) рівня вищої освіти

на 2022-2023 н.р.

№	№ та зміст пункту, до якого вносяться зміни	Підстава внесення змін	Підпис гаранта ОП
1	І Преамбула Крівенко Сергій Вікторович, доктор технічних наук, доцент, доцент кафедри математичних методів та системного аналізу МДУ **замінити на:** Мартинюк Ганна Вадимівна, кандидат технічних наук, доцент, доцент кафедри системного аналізу та інформаційних технологій МДУ		
2	І Преамбула Ротаньова Наталя Юріївна, кандидат педагогічних наук, доцент кафедри математичних методів та системного аналізу МДУ **замінити на:** Міщенко Андрій Віталійович, доктор технічних наук, професор, технічний директор комунального підприємства «Міжнародний аеропорт Київ (Жуляни)», професор кафедри системного аналізу та інформаційних технологій МДУ.		
3	ІІ Профіль освітньої програми Кадрове забезпечення. Гарант ОПП: д.т.н., доцент Крівенко С.В. **замінити на:** Кадрове забезпечення. Гарант ОПП: к.т.н., доцент Мартинюк Г.В.		