МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»

ОСВІТНЯ ПРОГРАМА

«АНАЛІЗ ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНИХ СИСТЕМ»

першого (бакалаврського) рівня вищої освіти
за спеціальністю №125 «Кібербезпека та захист інформації»
галузі знань №12 «Інформаційні технології»
Кваліфікація: бакалавр з кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО
Вченою радою НаУКМА
Голова Вченої ради НаУКМА

_____ С.М. Оксамитна

(протокол № 7 від 27 квітня 2023)

Київ – 2023

ПЕРЕДМОВА

Освітньо-професійна програма «Аналіз вразливостей інформаційних систем», за якою провадиться освітня діяльність на першому (бакалаврському) рівні вищої освіти з підготовки здобувачів ступеня бакалавра за спеціальністю 125 «Кібербезпека та захист інформації», розроблена згідно з вимогами Закону України «Про вищу освіту» та відповідає Стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти, затвердженого наказом МОН України № 1074 від 04 жовтня 2018 р.

Освітньо-професійна програма «Аналіз вразливостей інформаційних систем» розроблена із врахуванням досвіду бакалаврських програм провідних західних університетів, сучасних рекомендацій та практик Європейського освітнього простору, а також врахуванням відгуків і рекомендацій стейкхолдерів.

Програма розроблена робочою групою в складі:

Гороховський Семен Самуїлович – кандидат фізико-математичних наук, доцент кафедри інформатики, завідувач кафедри інформатики, керівник робочої групи;
Глибовець Андрій Миколайович – доктор технічних наук, професор кафедри мережних технологій, декан факультету інформатики;
Глибовець Микола Миколайович – доктор фізико-математичних наук, професор кафедри інформатики, заслужений діяч науки і техніки України, лауреат Державної премії України в галузі науки і техніки;
Малашонок Геннадій Іванович – доктор фізико-математичних наук, професор кафедри мережних технологій, завідувач кафедрою мереж
них технологій;
Бублик Володимир Васильович – кандидат фізико-математичних наук, доцент кафедри мультимедійних систем;
Жежерун Олександр Петрович – кандидат фізико-математичних наук, доцент кафедри мультимедійних систем, завідувач кафедри мультимедійних систем;
Олецький Олексій Віталійович – кандидат технічних наук, доцент доцент кафедри мультимедійних систем;
Проценко Володимир Семенович – кандидат фізико-математичних наук, доцент кафедри інформатики;
Стиран Володимир Сергійович – заступник начальника Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України;
Бабич Трохим Анатолійович – аспірант, асистент кафедри інформатики;

Гарант освітньо-професійної програми:

Олецький Олексій Віталійович – кандидат технічних наук, доцент кафедри мультимедійних систем

Рецензії / відгуки стейкхолдерів:

- Олександр Потій – доктор технічних наук, професор, бригадний генерал, заступник Голови Держспецзв'язку
- Назар Тимошик – кандидат технічних наук, власник групи компаній з кібербезпеки «UnderDefense»
- Степан Веселовський – виконавчий директор Львівського ІТ Кластеру
- Роман Сологуб – генеральний директор ТОВ «ІССП Сервіс»
- Єгор Аушев – директор CyberUnit

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ
«Аналіз вразливостей інформаційних систем»
зі спеціальності №125 «Кібербезпека та захист інформації»

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Національний університет «Києво-Могилянська академія» Факультет інформатики Кафедра інформатики
Рівень вищої освіти	Перший (бакалаврський) рівень
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	ступінь вищої освіти – бакалавр спеціальність: 125 Кібербезпека та захист інформації Освітня кваліфікація: бакалавр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Аналіз вразливостей інформаційних систем / Analysis of information system vulnerabilities
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 4 академічних років, 240 кредитів ЄКТС
Тип програми	Освітньо-професійна Educational professional
Наявність акредитації	Акредитація відсутня
Передумови	Наявність атестату про повну загальну середню освіту
Цикл/рівень програми	НРК України – 6 рівень, FQ-EHEA –перший цикл, EQF-LLL – 6 рівень
Мова (и) викладання	Українська
Форма навчання	Денна
Термін дії освітньої програми	Відповідно до терміну акредитації
Інтернет адреса постійного розміщення опису освітньо-професійної програми	https://www.fin.ukma.edu.ua
2 – Мета освітньої програми	
Мета програми (з врахуванням рівня кваліфікації)	Підготовка фахівців з кібербезпеки та захисту інформації, здатних проводити теоретичні та практичні дослідження в галузі аналізу та оцінки вразливостей інформаційних технологій; застосовувати математичні методи та алгоритмічні принципи в оцінці ризиків та моделюванні потенційних загроз; здійснювати розробку та впровадження заходів зі зниження вразливості інформаційних систем; аналізувати технічні та організаційні аспекти кібербезпеки, розробляти та оцінювати ефективність заходів кібербезпеки в інформаційних системах.

3 - Характеристика освітньої програми	
Предметна область (галузь знань / спеціальність / спеціалізація програми)	*Галузь знань* - 12 Інформаційні технології *Спеціальність* - 125 Кібербезпека та захист інформації вибіркові блоки: «Аналіз загроз та аудит безпеки», «Безпека операційних систем та мереж», «Безпечна розробка програмного забезпечення та криптографія».
Орієнтація освітньої програми	Освітньо-професійна, академічна
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта за спеціальністю 125 «Кібербезпека та захист інформації». Об'єкти вивчення та/або діяльності: − вразливості інформаційних систем та мереж − методи і технології виявлення та аналізу вразливостей − математичні, інформаційні та імітаційні моделі для аналізу вразливостей інформаційних систем та мереж − методи та технології кібербезпеки інформаційних систем та мереж − методи і технології зберігання, обробки, передачі та захисту інформації. Теоретичний зміст предметної області: сучасні методи та алгоритми, необхідні для отримання, зберігання, обробки та аналізу даних в інформаційних системах з метою забезпечення кібербезпеки. Поглиблені теоретичні та практичні знання в галузі кібербезпеки та інформаційних технологій з акцентом на формування навичок оцінки вразливостей і практичної реалізації заходів щодо їх запобігання. Ключові слова: науки про кібербезпеку, оцінка вразливостей, аналіз даних, виявлення та виправлення вразливостей, безпека програмного забезпечення.
Особливості програми	Програма орієнтована на навчання студентів за фахом пошуку та експлуатації вразливостей у інформаційних системах на всіх рівнях: програмне забезпечення, веб-сайти, корпоративні мережі. Окрім цього, додатково, будуть розглядатись питання пов’язані з етичними та правовими нормами, а також будуть розвиватись навички командної роботи. Окрім фундаментального теоретичного підґрунтя студенти отримають практичні прикладні знання.

	В окремих випадках можливе навчання з елементами змішаної (дистанційної) освіти.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Професійна діяльність як фахівця з проектування та розробки математичного та програмного забезпечення інформаційних систем, застосування інформаційних технологій, адміністрування баз даних і систем. Випускники можуть працювати за професіями згідно з Національним класифікатором професій ДК 003:2010: 2139.2 аналітик з оцінки вразливостей.
Подальше навчання	Можливості продовження освіти за другим (магістерським) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти
5 – Викладання та оцінювання	
Викладання та навчання	Підходами до навчання є: компетентнісний, студентоцентрований та проблемно-орієнтований. Провідні методи навчання – проблемний, частково-пошуковий та дослідницький. Викладання та навчання проводиться у форматі лекцій, серед яких, інтерактивні та мультимедійні, практичні заняття, лабораторні роботи, самостійне навчання, курсове дослідження.
Оцінювання	Письмові та усні іспити, звіти до лабораторних робіт, усні презентації, поточний контроль, заліки, диференційовані заліки, комплексний іспит, захист кваліфікаційної роботи бакалавра.

6 – Програмні компетентності	
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 (ЗК)	**ЗК1.** Здатність застосовувати знання у практичних ситуаціях. **ЗК2.** Знання та розуміння предметної області та розуміння професії. **ЗК3.** Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. **ЗК4.** Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. **ЗК5.** Здатність до пошуку, оброблення та аналізу інформації. **ЗК6.** 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. **ЗК7.** 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.
Фахові компетентності спеціальності (СК)	**СК1.** 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. **СК2.** Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. **СК3.** Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. **СК4.** Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. **СК5.** Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. **СК6.** Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. **СК7.** Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). **СК8.** Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку **СК9.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою. **СК10.** Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. **СК11.** Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. **СК12.** Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та

	інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
7 – Програмні результати навчання	
Програмні результати навчання	**ПР1.** Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. **ПР2.** Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. **ПР3.** Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. **ПР4.** 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. **ПР5.** Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. **ПР6.** Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. **ПР7.** Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки. **ПР8.** Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки. **ПР9.** Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки. **ПР10.** Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем. **ПР11.** Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. **ПР12.** Розробляти моделі загроз та порушника. **ПР13.** Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних. **ПР14.** Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень. **ПР15.** Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

	ПР16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів. **ПР17.** 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. **ПР18.** Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. **ПР19.** Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах. **ПР20.** Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах. **ПР21.** Вирішувати задачі забезпечення та супроводу (в т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. **ПР22.** Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки. **ПР23.** Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. **ПР24.** Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових). **ПР25.** 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. **ПР26.** Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем. **ПР27.** Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

	ПР28. 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. **ПР29.** 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. **ПР30.** Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем. **ПР31.** Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем. **ПР32.** Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки. **ПР33.** Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків. **ПР34.** Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації. **ПР35.** 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. **ПР36.** Виявляти небезпечні сигнали технічних засобів. **ПР37.** 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. **ПР38.** Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. **ПР39.** Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. **ПР40.** Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного

	захисту інформації. **ПР41.** Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. **ПР42.** Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. **ПР43.** Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів. **ПР44.** 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. **ПР45.** Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів. **ПР46.** Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. **ПР47.** Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах, з використанням сучасних методів та засобів криптографічного захисту інформації. **ПР48.** Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах. **ПР49.** Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах. **ПР50.** Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних). **ПР51.** Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах. **ПР52.** Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. **ПР53.** Вирішувати задачі аналізу програмного коду на наявність можливих загроз. **ПР54.** Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
8 – Ресурсне забезпечення реалізації програми	
Специфічні характеристики	Відповідає ліцензійним умовам. Викладачі є штатними викладачами Національного університету «Києво-Могилянська академія», більшість

кадрового забезпечення	має науковий ступінь та/або вчене звання, що відповідає основному профілю дисципліни, що викладається.
Специфічні характеристики матеріально-технічного забезпечення	Забезпеченість приміщеннями для проведення навчальних занять та контрольних заходів. Забезпеченість мультимедійним обладнанням для одночасного використання в навчальних аудиторіях. Наявність соціально-побутової інфраструктури. Забезпечення здобувачів вищої освіти гуртожитком. Забезпечення комп'ютерними робочими місцями, лабораторіями, полігонами, обладнанням, устаткуванням необхідними для виконання навчальних планів.
Специфічні характеристики інформаційного та навчально-методичного забезпечення	Використання платформи електронного навчання факультету інформатики (https://distedu.ukma.edu.ua/) та авторських розробок науково-педагогічних працівників факультету. Забезпеченість бібліотеки вітчизняними та закордонними фаховими періодичними виданнями відповідного або спорідненого профілю. Наявність доступу до баз даних періодичних наукових видань англійською мовою відповідного або спорідненого профілю. Наявність офіційного веб-сайту Національного університету «Києво-Могилянська академія» на якому розміщена основна інформація про його діяльність (структура, ліцензії та сертифікати про акредитацію, освітня/освітньо-професійна/видавнича/атестаційна (наукових кадрів) діяльність, навчальні та наукові структурні підрозділи та їх склад, перелік навчальних дисциплін, правила прийому, контактна інформація). Наявність електронного ресурсу закладу освіти, який містить навчально-методичні матеріали з дисциплін навчального плану в тому числі в системі дистанційного навчання. Необмежений доступ до мережі Інтернет, друковані та Інтернет-джерела (у т.ч. Центр електронного навчання Національного університету «Києво-Могилянська академія») інформації; навчальні і робочі плани (з пояснювальними записками до них), освітні програми, робочі програми дисциплін і практик, навчально-методичні комплекси дисциплін, що включають лекційний матеріал, завдання практичних робіт, питання семінарських занять, завдання самостійної роботи, питання, задачі, завдання для поточного та підсумкового контролю. Відповідає ліцензійним умовам – 100%.
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів (угод) між Національним університетом «Києво-Могилянська академія» та закладами вищої освіти України. Можлива, за бажанням студента.
Міжнародна кредитна мобільність	На основі двосторонніх договорів (угод) між Національним університетом «Києво-Могилянська академія» та закладами вищої освіти зарубіжних країн партнерів. Можлива, за бажанням студента
Навчання іноземних здобувачів вищої освіти	Навчання іноземних студентів проводиться на загальних умовах на основі двосторонніх договорів (угод) між Національним університетом «Києво-Могилянська академія» та закладами вищої освіти іноземних країн. Громадяни інших держав приймаються на навчання на підставі міжнародних договорів на умовах, визначених цими договорами, а також договорів, укладених навчальним закладом із зарубіжними навчальними закладами, організаціями, або індивідуальних договорів, контрактів.

2. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

ВК Перелік компонент ОП

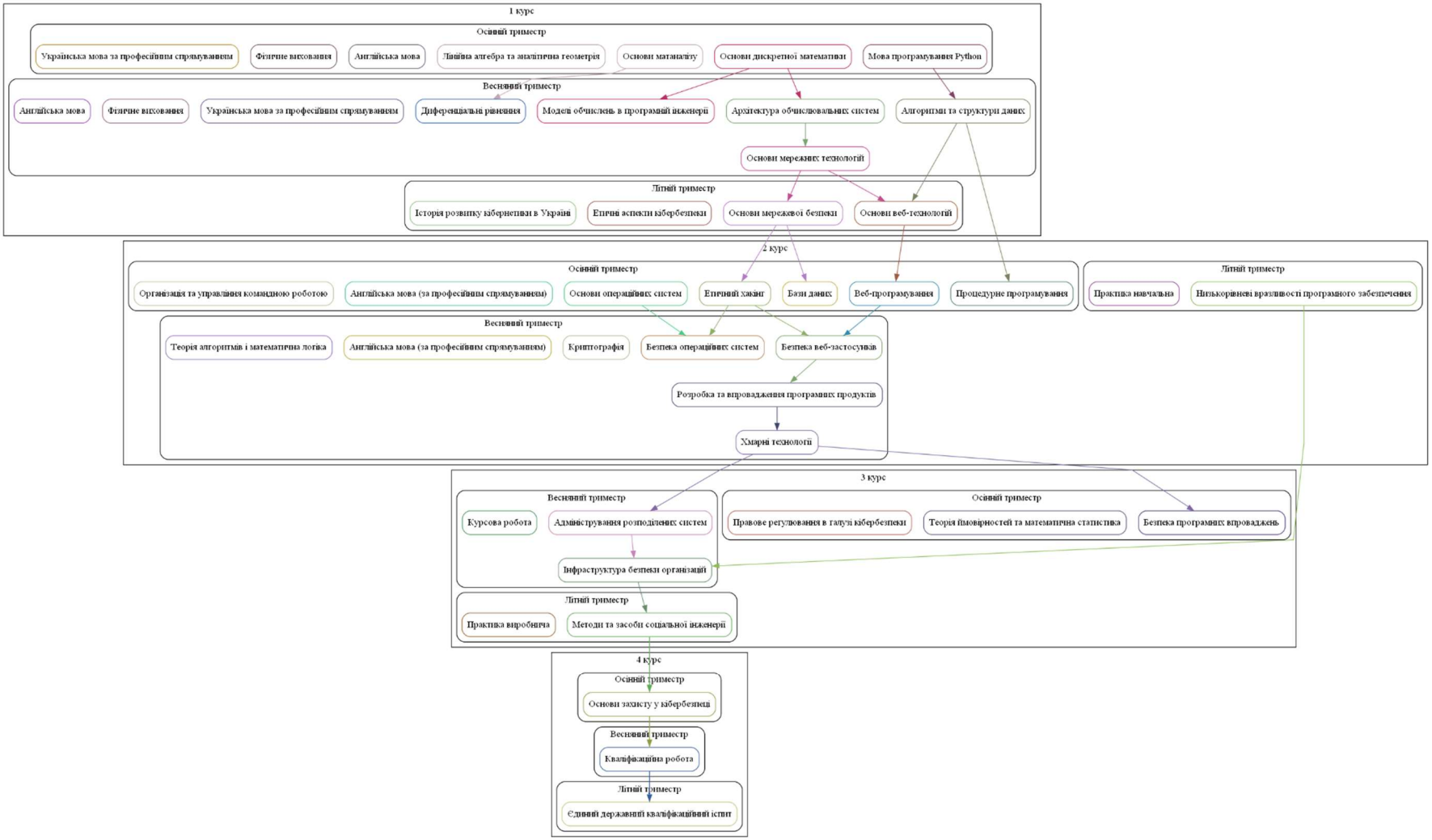
Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОП			
ОК 1.	Адміністрування розподілених систем	4,00	екзамен
ОК 2.	Алгоритми та структури даних	5,00	екзамен
ОК 3.	Англійська мова	7,00	екзамен
ОК 4.	Англійська мова (за професійним спрямуванням)	7,00	екзамен
ОК 5.	Архітектура обчислювальних систем	4,00	екзамен
ОК 6.	Бази даних	4,00	екзамен
ОК 7.	Безпека веб-застосунків	4,00	екзамен
ОК 8.	Безпека операційних систем	4,00	екзамен
ОК 9.	Безпека програмних впроваджень	4,00	екзамен
ОК 10.	Веб-програмування	4,00	екзамен
ОК 11.	Диференціальні рівняння	3,00	екзамен
ОК 12.	Етичний хакінг	4,00	екзамен
ОК 13.	Етичні аспекти кібербезпеки	2,00	екзамен
ОК 14.	Інфраструктура безпеки організацій	4,00	екзамен
ОК 15.	Історія розвитку кібернетики в Україні	2,00	екзамен
ОК 16.	Криптографія	4,00	екзамен
ОК 17.	Курсова робота	3,00	екзамен
ОК 18.	Лінійна алгебра та аналітична геометрія	4,00	екзамен
ОК 19.	Методи та засоби соціальної інженерії	2,00	екзамен
ОК 20.	Мова програмування Python	5,00	екзамен
ОК 21.	Моделі обчислень в програмній інженерії	4,00	екзамен
ОК 22.	Низькорівневі вразливості програмного забезпечення	2,00	екзамен
ОК 23.	Організація та управління командною роботою	4,00	екзамен
ОК 24.	Основи веб-технологій	3,00	екзамен
ОК 25.	Основи дискретної математики	4,00	екзамен
ОК 26.	Основи захисту у кібербезпеці	4,00	екзамен
ОК 27.	Основи математичного аналізу	4,00	екзамен
ОК 28.	Основи мережевої безпеки	2,00	екзамен
ОК 29.	Основи мережних технологій	4,00	екзамен
ОК 30.	Основи операційних систем	4,00	екзамен
ОК 31.	Правове регулювання в галузі кібербезпеки	4,00	екзамен
ОК 32.	Практика виробнича	3,00	екзамен

ОК 33.	Практика навчальна	3,00	екзамен
ОК 34.	Процедурне програмування	5,00	екзамен
ОК 35.	Розробка та впровадження програмних продуктів	4,00	екзамен
ОК 36.	Теорія алгоритмів і математична логіка	4,00	екзамен
ОК 37.	Теорія ймовірностей та математична статистика	4,00	екзамен
ОК 38.	Українська мова за професійним спрямуванням	5,00	екзамен
ОК 39.	Фізичне виховання	4,00	екзамен
ОК 40.	Хмарні технології	4,00	екзамен
Загальний обсяг обов'язкових компонент:		**155**	
Атестація			
ОК 41.	Єдиний державний кваліфікаційний іспит	3,0	екзамен
ОК 42.	Кваліфікаційна робота	12,0	теза
Загальний обсяг атестаційних компонент:		**15**	
Вибіркові компоненти ОП			
1. Професійної та практичної підготовки			
ВБ 1.1.	Електроніка та цифрова електроніка	3,0	залік
ВБ 1.2.	Мережна маршрутизація	3,0	залік
ВБ 1.3.	Локальні мережі	3,0	залік
ВБ 1.4.	Розробка клієнт серверних застосувань	3,0	залік
ВБ 1.5.	Front-end та Back-end - технології веб-застосувань	4,0	залік
ВБ 1.6.	Основи роботи з фреймворком Spring Boot	5,5	залік
ВБ 1.7.	Схематотехніка	3,5	залік
ВБ 1.8.	Мова програмування Swift	3,0	залік
ВБ 1.9.	Хмарні технології	4,0	залік
ВБ 1.10.	Методи та засоби збору чутливої інформації	2,0	залік
ВБ 1.11.	Вступ до мікросервісної архітектури з використанням Spring Boot	4,0	залік
ВБ 1.12.	Технології сучасних дата - центрів	4,0	залік
ВБ 1.13.	Адміністрування unix систем	3,0	залік
ВБ 1.14.	Розробка та експлуатація банківських комп`ютерних систем	4,5	залік
ВБ 1.15.	Прикладне програмування мобільних систем на основі ОС Android	4,0	залік
ВБ 1.16.	Технологія веб-програмування Ruby on Rails	4,0	залік
ВБ 1.17.	Основи технології блокчейн і криптовалют	4,0	залік
ВБ 1.18.	Основи фреймворку скрам	3,0	залік
ВБ 1.19.	Робота з неструктурованими даними	4,0	залік
ВБ 1.20.	Програмування мікроконтролерів та операційні системи реального часу	5,0	залік
2. Вільного вибору студента			
ВБ 2.1.	Вступ до "Могилянських" студій	2,0	залік

ВБ 2.2.	Математичні методи обробки зображень	4,0	залік
ВБ 2.3.	Обчислювальне суспільствознавство	2,5	залік
ВБ 2.4.	Вступ до ігрової розробки	4,0	залік
ВБ 2.5.	Інформаційний пошук	4,0	залік
ВБ 2.6.	Обробка зображень та мультимедіа	4,0	залік
ВБ 2.7.	Теорія чисел	4,5	залік
ВБ 2.8.	Автоматизація роботи з програмними проектами мовою Java	3,0	залік
ВБ 2.9.	Основи фотографії	2,5	залік
ВБ 2.10.	Практикум з об'єктно-орієнтованого програмування	3,0	залік
ВБ 2.11.	Базові мережні технології	4,0	залік
ВБ 2.12.	Інформаційна безпека веб-застосунків	4,0	залік
ВБ 2.13.	Математичні методи дослідження операцій	4,0	залік
ВБ 2.14.	Методи об'єктно-орієнтованого програмування	4,0	залік
ВБ 2.15.	Обчислювальна геометрія	4,5	залік
ВБ 2.16.	Спецкурс з комп`ютерної алгебри	4,0	залік
ВБ 2.17.	Технології мультимедіа	3,0	залік
ВБ 2.18.	Дані та суспільство	3,5	залік
ВБ 2.19.	Безпека комп'ютерних мереж	4,0	залік
ВБ 2.20.	Розробка iOS додатків	4,0	залік
ВБ 2.21.	Вибрані питання програмної інженерії	3,0	залік
ВБ 2.22.	Інтернет речей (Internet of Things)	4,0	залік
ВБ 2.23.	Кібербезпека	4,0	залік
ВБ 2.24.	Методи та засоби обробки інформації	3,0	залік
ВБ 2.25.	Низькорівневі вразливості програмного забезпечення	4,0	залік
ВБ 2.26.	Основи комп`ютерної алгебри	4,0	залік
ВБ 2.27.	Практичні основи роботи з базами даних в Spring Boot	3,0	залік
ВБ 2.28.	Теорія складності обчислень	4,0	залік
ВБ 2.29.	Експлуатація росподіленої хмарної інфраструктури та сервісів(DevOps)	4,0	залік
ВБ 2.30.	Веб-програмування	4,0	залік
ВБ 2.31.	Програмування в середовищі Java	4,0	залік
ВБ 2.32.	Машинне навчання та доповнена реальність на мобільних пристроях на базі iOS	2,0	залік
ВБ 2.33.	Робота в середовищі Apple	2,0	залік
ВБ 2.34.	Інформаційна безпека мереж	2,0	залік
ВБ 2.35.	Креативний дизайн програмного забезпечення	3,0	залік
ВБ 2.36.	Основи операційних систем	3,0	залік
ВБ 2.37.	Аналіз зображень та комп'ютерний зір	3,0	залік
ВБ 2.38.	Візуалізація та комп’ютерна графіка	3,0	залік

ВБ 2.39.	Нейроннні мережі	4,5	залік
ВБ 2.40.	Вибрані фреймворки для iOS	3,0	залік
ВБ 2.41.	Інформаційна безпека цільових систем	3,0	залік
ВБ 2.42.	Комп`ютерна вірусологія	4,0	залік
ВБ 2.43.	Системи кодування інформації	4,0	залік
ВБ 2.44.	Візуалізація інформації	3,0	залік
ВБ 2.45.	Аналіз даних	4,0	залік
ВБ 2.46.	Реактивне програмування в iOS	3,0	залік
Загальний обсяг вибіркових компонентів професійної та практичної підготовки:		**45**	
2. Вільного вибору студента			
Будь-які дисципліни з навчальних планів інших освітніх/освітньо-наукових програм НаУКМА			
Загальний обсяг компонентів вільного вибору студента:		**25**	
Загальний обсяг вибіркових компонент:		**70**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТЬНОЇ ПРОГРАМИ		**240**	

2.2 Структурно-логічна схема освітньо-професійної програми



3. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація здобувачів вищої освіти зі спеціальності 125 Кібербезпека та захист інформації здійснюється у формі єдиного державного кваліфікаційного іспиту та публічного захисту кваліфікаційної роботи.

Кваліфікаційна робота має передбачати теоретичне, системотехнічне або експериментальне дослідження складного спеціалізованого завдання або практичної проблеми в галузі кібербезпеки та захисту інформації, яке характеризується комплексністю та невизначеністю умов і потребує застосування теорій та методів інформаційних технологій. У кваліфікаційній роботі не має бути академічного плагіату (текстових запозичень), фальсифікації та фабрикації. Кваліфікаційна робота має бути оприлюднена на офіційному сайті університету або факультету, або на платформі електронного навчання DistEdu.

Атестація здійснюється Екзаменаційною комісією, яка затверджується наказом президента Національного університету «Києво-Могилянська академія». Екзаменаційна комісія приймає рішення про присвоєння студенту-випускнику кваліфікації бакалавра з кібербезпеки та захисту інформації та видає диплом державного зразка.

Цей диплом є юридичним документом, який дозволяє фахівцю займати первинні посади у відповідності з їх переліком та діючою в Україні відповідною номенклатурою посад.

Атестація здійснюється відкрито і публічно.

До єдиного державного кваліфікаційного іспиту та захисту кваліфікаційної роботи бакалавра допускаються студенти, які виконали всі вимоги навчального плану. Атестація має своєю метою з’ясування рівня підготовленості випускника для виконання професійних завдань, передбачених відповідними стандартами вищої освіти, і продовження освіти.

Публічний захист (демонстрація) кваліфікаційної роботи передбачає: представлення основних положень роботи у вигляді мультимедійної презентації та пояснювальної записки; відкриту форму засідання комісії; оголошення в той же день після закінчення захисту оцінки кваліфікаційної роботи та оформлення протоколу засідання комісії; ухвалення комісією рішення про присвоєння кваліфікації з кібербезпеки та захисту інформації та видачу диплома бакалавра за результатами підсумкової атестації.

4. МАТРИЦЯ ВІДПОВІДНОСТІ ЗАГАЛЬНИХ ТА СПЕЦІАЛЬНИХ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

Програмні компетентності	**Компоненти ОП**																																									
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
Загальні компетентності																																									
ЗК 1	•	•			•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•			•
ЗК 2	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•		•	•	•	•	•	•	•	•		•			•	•	•	•	•	•	•			•
ЗК 3		•	•	•	•	•	•	•	•	•	•	•	•		•	•		•	•	•	•	•	•	•	•		•			•	•	•	•	•	•	•	•		•
ЗК 4	•	•			•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•			•
ЗК 5	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•		•	•	•	•	•	•	•	•		•		•	•	•	•	•	•	•	•			•
ЗК 6													•		•																•							•		
ЗК 7															•																							•		
Спеціальні (фахові) компетентності спеціальності																																									
СК 1			•	•									•	•												•					•							•		
СК 2	•	•			•	•	•	•	•	•		•		•						•	•			•		•		•		•			•	•	•					•
СК 3	•	•				•	•	•	•	•		•		•						•				•		•			•						•	•				•
СК 4	•							•	•			•		•					•				•			•									•					•
СК 5	•	•			•	•	•	•	•	•		•							•	•	•			•				•	•					•	•				•
СК 6	•	•			•	•	•	•	•	•		•								•	•		•	•					•	•					•	•				•
СК 7	•				•	•							•	•					•		•		•			•					•	•								•
СК 8		•	•	•			•	•	•	•		•		•						•				•		•									•	•				•
СК 9		•					•	•	•	•		•							•	•				•				•		•				•	•				•
СК 10	•	•			•	•	•	•	•	•	•	•				•		•		•	•			•	•		•	•	•					•	•	•	•			•
СК 11	•	•			•	•	•	•	•	•		•		•						•	•			•		•			•	•				•	•					•
СК 12	•							•	•			•	•	•					•							•					•				•					•

5. Матриця забезпечення програмних результатів навчання (ПРН) компонентами ОПП

Програмні результати навчання	Компоненти ОП																																											
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
ПРН 1		•					•	•	•	•		•								•		•		•										•	•					•
ПРН 2						•													•				•																	
ПРН 3		•					•	•	•	•		•								•		•		•										•	•					•
ПРН 4																			•				•																	
ПРН 5		•					•	•	•	•		•								•		•		•										•	•					•
ПРН 6																																											
ПРН 7			•	•									•													•					•							•		
ПРН 8			•	•									•													•					•							•		
ПРН 9									•				•													•					•				•			•		•
ПРН 10					•				•					•							•								•						•					•
ПРН 11	•				•																•								•	•										
ПРН 12		•					•	•	•	•		•								•		•		•		•		•					•	•					•
ПРН 13			•	•	•																•								•											
ПРН 14					•																•											•								
ПРН 15	•				•			•				•									•							•	•	•		•								
ПРН 16								•			•	•	•			•		•							•		•	•			•	•				•	•	•			
ПРН 17								•	•		•	•		•		•		•							•	•	•						•			•	•	•			•

ПРН 18		•					•	•	•	•		•								•		•		•		•		•					•	•					•
ПРН 19		•					•	•	•	•	•	•				•		•		•				•	•	•	•	•					•	•	•	•			•
ПРН 20		•					•			•										•		•		•		•							•						
ПРН 21	•							•				•																•	•	•								
ПРН 22	•							•				•		•														•				•						
ПРН 23	•							•				•		•												•		•										
ПРН 24	•							•				•		•												•		•	•	•								
ПРН 25														•					•				•			•						•						
ПРН 26	•							•				•														•			•									
ПРН 27		•					•			•										•		•		•				•	•					•				
ПРН 28		•					•	•	•	•		•								•		•		•		•		•					•	•				•
ПРН 29		•					•	•	•	•		•								•		•		•		•		•					•	•				•
ПРН 30	•	•					•	•	•	•		•		•					•	•		•	•	•		•		•	•	•			•	•				•
ПРН 31					•			•			•	•				•		•			•				•		•	•	•	•					•	•		
ПРН 32	•													•															•	•								
ПРН 33		•					•	•	•	•		•							•	•			•	•				•	•					•	•			•
ПРН 34								•				•		•												•		•	•	•		•						
ПРН 35	•	•					•	•	•	•		•								•		•		•		•		•					•	•				•
ПРН 36					•																•					•		•	•								
ПРН 37					•	•							•								•					•		•	•		•					•		
ПРН 38			•	•	•	•							•								•					•		•	•		•					•		
ПРН 39																			•				•			•		•	•									
ПРН 40					•	•							•								•					•		•	•		•					•		

ПРН 41								•				•		•												•		•	•	•		•								
ПРН 42		•					•	•	•	•		•								•		•		•		•		•	•	•				•	•					•
ПРН 43													•													•					•		•					•		
ПРН 44								•				•		•												•		•	•	•		•								
ПРН 45	•							•				•		•												•			•	•										
ПРН 46		•					•	•	•	•		•								•		•		•		•		•	•	•				•	•					•
ПРН 47		•					•	•	•	•	•	•				•		•		•		•		•	•	•	•	•	•	•				•	•	•	•			•
ПРН 48		•				•	•	•	•	•	•	•		•		•		•		•		•		•	•	•	•	•	•	•				•	•	•	•			•
ПРН 49		•				•	•	•	•	•		•								•				•		•		•	•	•				•	•					•
ПРН 50	•	•				•	•	•	•	•		•								•				•		•		•	•	•				•	•					•
ПРН 51		•				•	•	•	•	•		•								•		•		•		•		•	•	•				•	•					•
ПРН 52		•					•	•	•	•		•								•		•		•		•		•	•	•				•	•					•
ПРН 53		•			•		•		•	•										•	•	•		•										•	•					•
ПРН 54													•		•																•		•					•		