МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ТЕХНОЛОГІЙ ТА ДИЗАЙНУ

ЗАТВЕРДЖЕНО ВЧЕНОЮ РАДОЮ
Голова Вченої ради КНУТД

_____ Іван ГРИЩЕНКО

(протокол № __ від «__» ____ 2021 р. № 5)

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

ІНЖЕНЕРІЯ КІБЕРБЕЗПЕКИ

Рівень вищої освіти перший бакалаврський

Ступінь вищої освіти бакалавр

Галузь знань 12 Інформаційні технології

Спеціальність 125 Кібербезпека

Кваліфікація бакалавр з кібербезпеки

Київ 2021

ЛИСТ ПОГОДЖЕННЯ

Освітньо-професійної програми

Інженерія кібербезпеки

Рівень вищої освіти перший бакалаврський

Ступінь вищої освіти бакалавр

Галузь знань 12 Інформаційні технології

Спеціальність 125 Кібербезпека

Проректор з науково-педагогічної діяльності (освітня діяльність)

08.12.2021 _____ **Оксана МОРГУЛЕЦЬ**
(дата) (підпис)

Схвалено Вченою радою факультету мехатроніки та комп'ютерних технологій

Протокол від «03» грудня 2021 року № 5

Декан факультету мехатроніки та комп'ютерних технологій

08.12.2021 _____ **Володимир ПАВЛЕНКО**
(дата) (підпис)

Обговорено та рекомендовано на засіданні кафедри комп'ютерних наук

Протокол від «01» грудня 2021 року № 5

Завідувач кафедри комп'ютерних наук

01.12.2021 _____ **Володимир ЩЕРБАНЬ**
(дата) (підпис)

Гарант освітньої програми

01/12/2021 _____ **Тетяна ДЕМКІВСЬКА**
(дата) (підпис)

Введено в дію наказом КНУТД від «23» 12 2021 року № 404.

ПЕРЕДМОВА

РОЗРОБЛЕНО: Київський національний університет технологій та дизайну

РОЗРОБНИКИ:

Група забезпечення освітньої програми	ПІБ, науковий ступінь, вчене звання, посада	Підпис	Дата
1	2	3	4
Гарант освітньої програми	Демківська Тетяна Іванівна, к.т.н., доцент, доцент кафедри комп'ютерних наук, Київський національний університет технологій та дизайну		14.06. 2023
Робоча група	Яхно Володимир Михайлович інженерії, к.т.н., доцент, старший викладач кафедри комп'ютерних наук, Київський національний університет технологій та дизайну		14.06 2023
	Резанова Вікторія Георгіївна, к.т.н., доцент, доцент кафедри комп'ютерних наук, Київський національний університет технологій та дизайну		14.06 2023

РЕЦЕНЗІЇ ЗОВНІШНІХ СТЕЙКХОЛДЕРІВ:

1) Панасок І.В., доктор технічних наук, професор, академік Академії інженерних наук України та Української технологічної академії, директор Навчально-наукового інституту інженерії та інформаційних технологій Київського національного університету технологій та дизайну.

2) Кривий С.Л., доктор фізико-математичних наук, професор, професор кафедри інтелектуальних програмних систем факультету кібернетики КНУ імені Тараса Шевченка.

3) Опанасенко В.М., провідний науковий співробітник інституту кібернетики ім. В.М. Глушкова НАН України, лауреат Державної премії України в галузі науки і техніки, доктор технічних наук, професор.

4) Мельник Г.В., кандидат технічних наук, доцент, директор товариства з обмеженою відповідальністю «Данн консалтинг».

5) Сніцар В.Д., заступник директора департаменту реагування на надзвичайні ситуації апарату Державної служби України з надзвичайних ситуацій у сферах захисту населення і територій від надзвичайних ситуацій.

1. Профіль освітньо-професійної програми Інженерія кібербезпеки

1.1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Київський національний університет технологій та дизайну Кафедра комп'ютерних наук
Рівень вищої освіти	перший (бакалаврський)
Освітня кваліфікація	бакалавр з кібербезпеки та захисту інформації
Кваліфікація в дипломі	Ступінь вищої освіти – бакалавр Спеціальність – 125 Кібербезпека та захист інформації Освітня програма – Інженерія кібербезпеки
Тип диплома та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС
Наявність акредитації	–
Цикл/рівень	Національна рамка кваліфікацій України – 6 рівень
Передумови	Повна загальна середня освіта, ступінь «фаховий молодший бакалавр» або ступінь «молодший бакалавр» (освітньо-кваліфікаційний рівень «молодший спеціаліст»). Відповідно до Стандарту вищої освіти за спеціальністю на базі ступеня «молодший бакалавр» (освітньо-кваліфікаційного рівня «молодший спеціаліст») Університет визнає та перезараховує кредити ЄКТС, отримані в межах попередньої освітньої програми підготовки молодшого бакалавра (молодшого спеціаліста). На основі ступеня «фаховий молодший бакалавр» Університет визнає та перезараховує кредити ЄКТС, отримані за попередньою освітньою програмою фахової передвищої освіти.
Мова(и) викладання	Українська
Строк дії сертифіката про акредитацію освітньої програми	
Інтернет-адреса постійного розміщення опису освітньої програми	https://knutd.edu.ua/ekts/

1.2 – Мета освітньої програми
Підготовка фахівців, які володіють глибокими знаннями, а також базовими й професійними компетентностями в сфері інформаційної та кібернетичної безпеки, що направлені на здобуття студентом здатності працювати з об'єктами інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології. Основними цілями програми є: формування здатності використовувати і впроваджувати технології інформаційної та/або кібербезпеки, а також новітні технології та математичні методи; проводити інноваційну діяльність в галузі захисту інформації і кібернетичної безпеки; орієнтація на міжнародні вимоги в сфері кібербезпеки; орієнтація на вимоги ринку праці.

1.3 – Характеристика освітньої програми	
Предметна область	*Об'єкти професійної діяльності випускників:* – об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту.

	Цілі навчання підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. *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. Програма орієнтована на формування у здобувачів компетентностей щодо набуття глибоких знань, умінь та навичок зі спеціальності. Обов'язкові навчальні освітні компоненти – 75%, з них: практична підготовка – 10%, вивчення іноземної мови – 10%. Дисципліни вільного вибору студента – 25% обираються із загальноуніверситетського каталогу відповідно до затвердженої процедури в Університеті.
Орієнтація освітньої програми	Освітньо-професійна для підготовки бакалавра.
Основний фокус освітньої програми	Програма орієнтована на формування фундаментальних знань та фахових навичок в сфері інформаційних технологій, експлуатації інформаційних систем (сервісів), забезпечення їх кібербезпеки. Програма забезпечує ґрунтовну фундаментальну підготовку у поєднанні із сучасною професійною підготовкою, яка дозволяє проводити інноваційну діяльність і працювати з наукоємними технологіями кібербезпеки;
Особливості освітньої програми	Акцент робиться на використанні сучасних апаратних та програмних засобів, форм та методів навчання і викладання, що сприяють отриманню актуальних знань з інформаційної та кібернетичної безпеки, вмінь обґрунтовано вибирати ефективні засоби для вирішення поставлених задач, проводити аналіз програмних систем, використовувати сучасні засоби інформаційної безпеки.

1.4 – Придатність випускників до працевлаштування та подальшого навчання		
Придатність до працевлаштування	Випускники можуть працювати фахівцями із захисту інформації та кібербезпеки в складі відповідних департаментів організацій, підприємств та банків, розробниками та тестувальниками застосунків, що потребують виконання особливих вимог щодо інформаційної та кібернетичної безпеки; співробітниками служб захисту інформації; адміністраторами інформаційної та кібернетичної безпеки, проектувальниками систем захисту в кіберпросторі; розробниками програмних та програмно-апаратних засобів захисту інформації в кіберпросторі, консультантами-інструкторами з кібербезпеки, спеціалістами в галузі кібербезпеки в складі правоохоронних органів, спеціалістами з забезпечення кібербезпеки в кіберпросторі (зокрема, об'єктах критичної інфраструктури).	
Академічні права випускників	Можливість навчання за освітньо-науковою та/або освітньо-професійною програмою другого (магістерського) рівня вищої освіти.	
1.5 – Викладання та оцінювання		
Викладання та навчання	Використовується студентоцентроване та проблемноорієнтоване навчання, навчання через навчальну, виробничу практику та самонавчання. Система методів навчання базується на принципах цілеспрямованості, бінарності – активної безпосередньої участі науково-педагогічного працівника і здобувача вищої освіти. Форми організації освітнього процесу: лекція, семінарське, практичне, лабораторне заняття, практична підготовка, самостійна робота, консультація.	
Оцінювання	Екзамени, заліки, тести, есе, проєктні роботи, презентації, звіти, портфоліо.	
1.6 – Програмні компетентності		
Інтегральна компетентність (ІК)	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)	**ЗК 1**	Здатність застосовувати знання у практичних ситуаціях.
	ЗК 2	Знання та розуміння предметної області та розуміння професії.
	ЗК 3	Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
	ЗК 4	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
	ЗК 5	Здатність до пошуку, оброблення та аналізу інформації.
	ЗК 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.
	ЗК 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.
	ЗК 8	Здатність до абстрактного мислення, аналізу та синтезу.

Фахові компетентності (ФК)	**ФК 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.
	ФК 2	Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
	ФК 3	Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
	ФК 4	Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
	ФК 5	Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
	ФК 6	Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
	ФК 7	Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)
	ФК 8	Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
	ФК 9	Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.
	ФК 10	Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.
	ФК 11	Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
	ФК 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.
	ФК 13	Здатність до логічного мислення, побудови логічних висновків, використання формальних мов і моделей алгоритмічних обчислень, проектування, розроблення й аналізу алгоритмів, оцінювання їх ефективності та складності, розв’язності та нерозв’язності алгоритмічних проблем для адекватного моделювання предметних областей і створення програмних та інформаційних систем.
	ФК 14	Здатність до виявлення статистичних закономірностей недетермінованих явищ, застосування методів обчислювального інтелекту, зокрема статистичної, нейромережевої та нечіткої обробки даних, методів машинного навчання та генетичного програмування тощо.

	ФК 15	Здатність проєктувати та розробляти програмне забезпечення із застосуванням різних парадигм програмування: узагальненого, об’єктно-орієнтованого, функціонального, логічного, з відповідними моделями, методами й алгоритмами обчислень, структурами даних і механізмами управління
	ФК 16	Здатність до розробки мережевого програмного забезпечення, що функціонує на основі різних топологій структурованих кабельних систем, використовує комп’ютерні системи і мережі передачі даних та аналізує якість роботи комп’ютерних мереж.
1.7 – Програмні результати навчання		
ПРН 1	Знати основні форми і закони абстрактно-логічного мислення, основ логіки, норм критичного підходу, основ методології наукового пізнання, методів аналізу та синтезу.	
ПРН 2	Знати методи навчання, організації та здійснення, стимулювання та мотивації навчально-пізнавальної діяльності, розуміння предметної області комп'ютерних наук.	
ПРН 3	Розуміти принципи моделювання організаційно-технічних систем і операцій.	
ПРН 4	Розуміти концепцію інформаційної безпеки, принципи безпечного проєктування програмного забезпечення, забезпечувати безпеку комп’ютерних мереж в умовах неповноти та невизначеності вихідних даних.	
ПРН 5	Розуміти відповідальність за власні рішення та результати професійної діяльності.	
ПРН 6	Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.	
ПРН 7	Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.	
ПРН 8	Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.	
ПРН 9	Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.	
ПРН 10	Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.	
ПРН 11	Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.	
ПРН 12	Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.	
ПРН 13	Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.	
ПРН 14	Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах.	
ПРН 15	Розробляти моделі загроз та порушника.	
ПРН 16	Аналізувати проєкти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних.	
ПРН 17	Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.	
ПРН 18	Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.	
ПРН 19	Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.	

ПРН 20	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.
ПРН 21	Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
ПРН 22	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
ПРН 23	Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
ПРН 24	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.
ПРН 25	Вирішувати задачі управління процедурами ідентифікації автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
ПРН 26	Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН 27	Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
ПРН 28	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.
ПРН 29	Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
ПРН 30	Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН 31	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.
ПРН 32	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.
ПРН 33	Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
ПРН 34	Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
ПРН 35	Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
ПРН 36	Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.
ПРН 37	Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

ПРН 38	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.
ПРН 39	Виявляти небезпечні сигнали технічних засобів.
ПРН 40	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.
ПРН 41	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН 42	Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
ПРН 43	Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
ПРН 44	Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
ПРН 45	Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.
ПРН 46	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.
ПРН 47	Застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
ПРН 48	Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.
ПРН 49	Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
ПРН 50	Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
ПРН 51	Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
ПРН 52	Забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
ПРН 53	Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.
ПРН 54	Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.
ПРН 55	Вирішувати задачі аналізу програмного коду на наявність можливих загроз.
ПРН 56	Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
ПРН 57	Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.
ПРН 58	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.

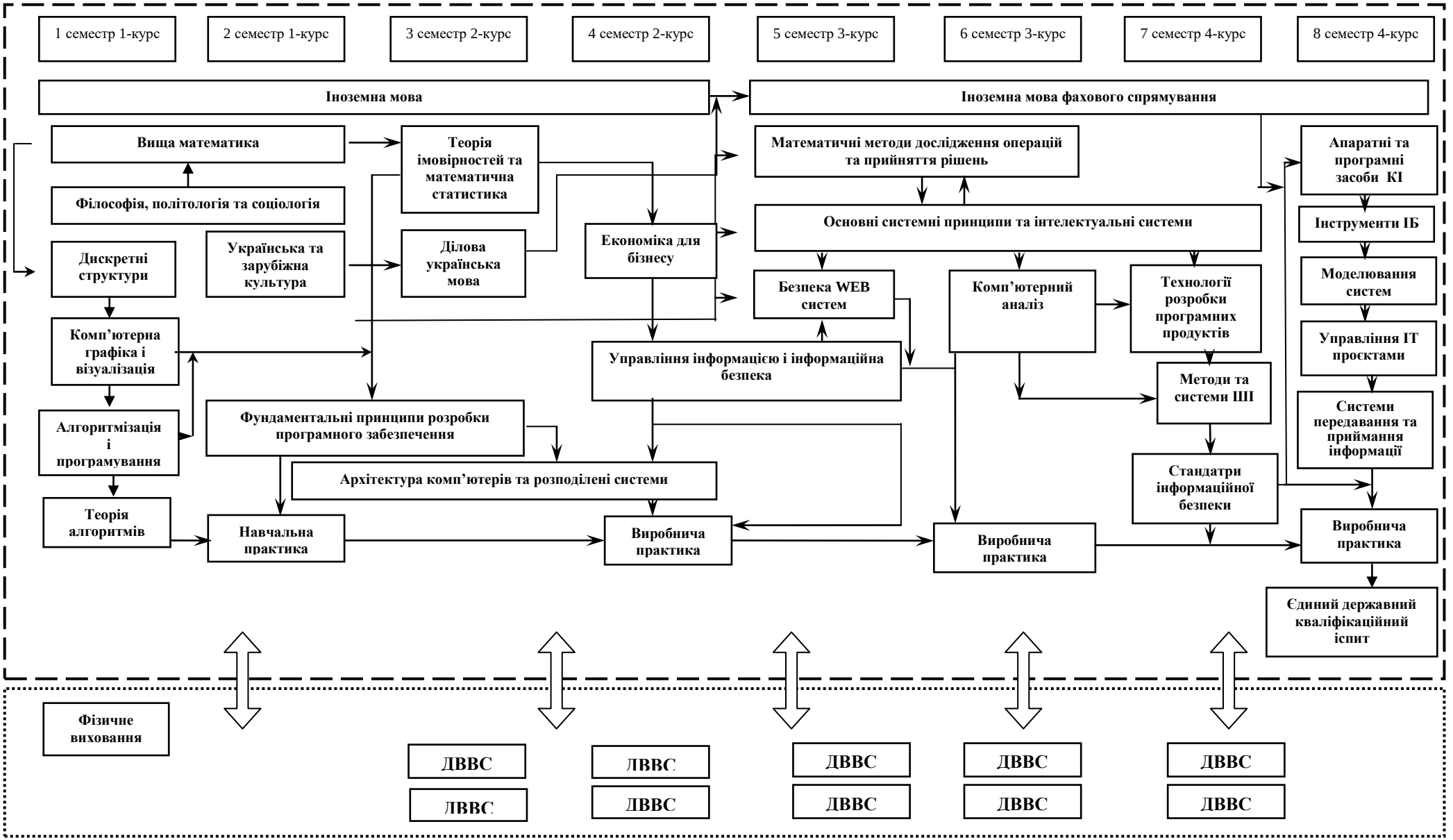
1.8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Всі науково-педагогічні працівники, що забезпечують освітньо-професійну програму за кваліфікацією, відповідають профілю і напряму дисциплін, що викладаються; мають необхідний стаж педагогічної роботи та досвід практичної роботи. В процесі організації навчання залучаються професіонали з досвідом дослідницької / управлінської / інноваційної / творчої роботи та/або роботи за фахом.
Матеріально-технічне забезпечення	Матеріально-технічне забезпечення дозволяє повністю забезпечити освітній процес протягом всього циклу підготовки за освітньою програмою. Стан приміщень засвідчено санітарно-технічними паспортами, що відповідають чинним нормативним актам.
Інформаційне та навчально-методичне забезпечення	Програма повністю забезпечена навчально-методичним комплексом з усіх компонентів освітньої програми, наявність яких представлена у модульному середовищі освітнього процесу Університету.
1.9 – Академічна мобільність	
Внутрішня академічна мобільність	Передбачає можливість академічної мобільності за деякими компонентами освітньої програми, що забезпечують набуття загальних або фахових компетентностей.
Міжнародна академічна мобільність	Програма розвиває перспективи участі та стажування у науково-дослідних проєктах та програмах академічної мобільності.
Навчання іноземних здобувачів вищої освіти	Навчання іноземних здобувачів вищої освіти здійснюється за акредитованими освітніми програмами. Виконується в активному дослідницькому середовищі. Підписана угода про співпрацю між КНУТД і Університетом прикладних наук (Латвія).

2. Перелік компонентів освітньо-професійної програми Інженерія кібербезпеки та їх логічна послідовність

2.1 Перелік освітніх компонентів освітньо-професійної програми першого (бакалаврського) рівня вищої освіти

Код	Компоненти освітньої програми (навчальні дисципліни, курсові роботи (проєкти), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
Обов'язкові компоненти ОП			
ОК 1	Українська та зарубіжна культура	3	Залік
ОК 2	Іноземна мова (англійська, німецька, французька)	12	Екзамен
ОК 3	Ділова українська мова	3	Залік
ОК 4	Філософія, політологія та соціологія	6	Екзамен
ОК 5	Іноземна мова фахового спрямування (англійська)	12	Екзамен
ОК 6	Фізичне виховання	3	Залік
ОК 7	Вища математика	12	Екзамен
ОК 8	Дискретні структури	3	Екзамен
ОК 9	Комп'ютерна графіка і візуалізація	3	Залік
ОК 10	Комп'ютерний аналіз	3	Екзамен
ОК 11	Економіка для бізнесу	3	Залік
ОК 12	Теорія ймовірностей та математична статистика	3	Екзамен
ОК 13	Теорія алгоритмів	3	Екзамен
ОК 14	Алгоритмізація і програмування	6	Екзамен
ОК 15	Безпека WEB систем	3	Екзамен
ОК 16	Апаратні та програмні засоби комп'ютерної інженерії	3	Екзамен
ОК 17	Технології розробки програмних продуктів	6	Екзамен
ОК 18	Фундаментальні принципи розробки програмного забезпечення	12	Екзамен
ОК 19	Управління інформацією і інформаційна безпека	8	Екзамен
	Курсовий проект	1	Захист
ОК 20	Інструменти інформаційної безпеки	3	Залік
ОК 21	Основні системні принципи та інтелектуальні системи	11	Екзамен
	Курсовий проект	1	Захист
ОК 22	Методи та системи штучного інтелекту	3	Екзамен
ОК 23	Архітектура комп'ютерів та розподілені системи	9	Екзамен
ОК 24	Моделювання систем	3	Екзамен
ОК 25	Стандарти інформаційної безпеки	3	Екзамен
ОК 26	Управління ІТ проєктами	3	Залік
ОК 27	Системи передавання та приймання інформації	6	Екзамен
ОК 28	Математичні методи дослідження операцій та прийняття рішень	6	Екзамен
ОК 29	Навчальна практика	6	Залік
ОК 30	Виробнича практика	18	Залік
ОК 31	Єдиний державний кваліфікаційний іспит	-	Іспит
Загальний обсяг обов'язкових освітніх компонентів		**180**	
Вибіркові компоненти освітньої програми			
ДВВС	Дисципліни вільного вибору здобувача вищої освіти	60	Залік
Загальний обсяг вибіркових компонентів		60	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

2.2 Структурно-логічна схема підготовки бакалавра за освітньо-професійною програмою Інженерія кібербезпеки зі спеціальності 125 Кібербезпека та захист інформації



3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту.
Вимоги до кваліфікаційної роботи/проєкту	Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених цим стандартом та освітньою програмою.

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

	ЗК 1	ЗК 2	ЗК 3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ФК1	ФК2	ФК3	ФК 4	ФК 5	ФК 6	ФК 7	ФК 8	ФК 9	ФК 10	ФК 11	ФК 12	ФК 13	ФК 14	ФК 15	ФК 16
ОК1	*						*																	
ОК2			*		*																			
ОК3	*		*				*																	
ОК4	*					*		*																
ОК5			*	*																				
ОК6							*																	
ОК7		*						*																
ОК8	*	*		*						*							*	*						
ОК9	*	*								*											*			
ОК10	*							*													*		*	
ОК11			*						*			*	*						*					
ОК12	*							*		*												*		
ОК13								*													*	*		
ОК14	*	*			*					*	*										*		*	
ОК15					*	*				*									*					
ОК16		*								*														
ОК17	*							*													*		*	
ОК18	*	*		*	*			*													*		*	
ОК19	*	*			*			*													*		*	
ОК20	*	*	*						*				*					*						
ОК21	*	*			*			*													*		*	*
ОК22		*			*				*	*														
ОК23		*			*					*										*				*
ОК24	*				*	*				*											*		*	
ОК25	*	*	*						*															
ОК26		*	*		*														*		*		*	
ОК27		*			*			*			*			*				*	*					*
ОК28					*		*														*		*	
ОК29	*	*											*	*		*				*		*	*	*
ОК30	*	*		*					*	*	*	*	*	*	*	*				*		*	*	*

5. Матриця забезпечення програмних результатів навчання відповідними компонентами освітньо-професійної програми

	ОК 1	ОК 2	ОК 3	ОК 4	ОК 5	ОК 6	ОК 7	ОК 8	ОК 9	ОК 10	ОК 11	ОК 12	ОК 13	ОК 14	ОК 15	ОК 16	ОК 17	ОК 18	ОК 19	ОК 20	ОК 21	ОК 22	ОК 23	ОК 24	ОК 25	ОК 26	ОК 27	ОК 28	ОК 29	ОК 30
ПРН1				*			*	*				*	*	*										*				*		
ПРН2				*										*		*		*	*					*						
ПРН3																			*		*	*		*					*	*
ПРН4											*				*					*										*
ПРН5						*					*																	*		*
ПРН6				*		*		*	*	*								*			*			*						
ПРН7			*		*							*					*	*	*		*			*					*	*
ПРН8					*		*				*					*		*			*	*	*							*
ПРН9			*				*			*	*			*							*			*						
ПРН10															*										*					
ПРН11															*					*					*			*	*	*
ПРН12															*										*					*
ПРН13								*										*			*									
ПРН14								*													*									
ПРН15																										*				
ПРН16																									*					
ПРН17																						*								
ПРН18											*																	*		
ПРН19															*															
ПРН20																														
ПРН21															*					*										
ПРН22															*															
ПРН23											*				*															
ПРН24															*															
ПРН25																										*				
ПРН26														*																
ПРН27														*		*												*		
ПРН28																													*	*
ПРН29											*																			
ПРН30														*												*		*		
ПРН31											*																			
ПРН32																													*	*
ПРН33																										*		*		
ПРН34											*		*			*							*							
ПРН35											*																			
ПРН36																													*	*
ПРН37																												?	*	*
ПРН38																													*	*
ПРН39																											*			
ПРН40													*	*				*									*			
ПРН41									*																				*	
ПРН42														*													*	*		
ПРН43																					*								*	*
ПРН44																						*						*		
ПРН45																														
ПРН46											*																			
ПРН47											*																			
ПРН48												*														*				
ПРН49																													*	
ПРН50														*												*		*		
ПРН51												*										*								
ПРН52																		*										*		
ПРН53																											*		*	*
ПРН54																											*			*
ПРН55																														*
ПРН56																											*		*	*
ПРН57	*	*	*		*																							*		*
ПРН58	*	*	*	*	*												*			*							*	*	*	*

Хронологія перегляду освітньої програми

Зміни внесені до освітньої програми відповідно до рішення вченої ради факультету Мехатроніки та комп'ютерних технологій :

1. Від 18 травня 2022 р., протокол № 10 ОПП була переглянута та оновлена у зв’язку з наступними змінами:

1.1 вилучено ОК28 Переддипломна практика - 6 кредитів та ОК29 та Дипломна бакалаврська робота (проєкт) - 12 кредитів

1.2 Введено ОК26 Управління ІТ проєктом – 3 кредити

1.3 Введено ОК27 – Системи передавання та приймання інформації – 6 кредитів

1.4 Введено ОК28 – Економіка для бізнесу – 3 кредити

1.5 Перенесено на виробничу практику 6 кредитів.

2. Від 12 квітня 2023 р. протокол № 6 (*Зміни про переведення редакції освітніх програм внесено рішенням Вченої ради КНУТД № 8 від 26.04.2023 р. і затверджено Наказом КНУТД № 146 від 11.05.2023 р. Зміна назви спеціальності «Кібербезпека» на «Кібербезпека та захист інформації»).*

ЗАТВЕРДЖУЮ

Голова Вченої ради КНУТД

_____ Іван ГРИЩЕНКО

"30" 06 2023 року

Міністерство освіти і науки України

Київський національний університет технологій та дизайну

НАВЧАЛЬНИЙ ПЛАН

Підготовки першого (бакалаврського) рівня **з галузі знань** 12 Інформаційні технології **Кваліфікація** бакалавр з кібербезпекики

спеціальність 125 Кібербезпека **Строк навчання** 3роки 10місяців

освітня програма Інженерія кібербезпеки **на основі** повної загальної середньої освіти

Форма здобуття вищої освіти денна

Курс	Вересень				Жовтень					Листопад				Грудень				Січень					Лютий				Березень				Квітень				Травень					Червень				Липень				Серпень				
	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	41	42	43	44	45	46	47	48	49	50	51	52
1	.	.	.	.	.	.	.	.	.	.	.	.	s	s	s	s	C	C	C	K	K	K	K	H	H	H	H	.	.	.	.	.	.	.	.	.	.	.	s	s	C	C	K	K	K	K	K	K	K	K	K
2	.	.	.	.	.	.	.	.	.	.	.	.	s	s	s	s	C	C	C	K	K	K	K	B	B	B	B	.	.	.	.	.	.	.	.	.	.	.	s	s	C	C	K	K	K	K	K	K	K	K	K
3	.	.	.	.	.	.	.	.	.	.	.	.	s	s	s	s	C	C	C	K	K	K	K	B	B	B	B	.	.	.	.	.	.	.	.	.	.	.	s	s	C	C	K	K	K	K	K	K	K	K	K
4	.	.	.	.	.	.	.	.	.	.	.	.	s	s	s	s	C	C	C	K	K	K	K	B	B	B	B	.	.	.	.	.	.	.	.	.	.	.	C	C	A	A									

ПОЗНАЧЕННЯ: • – теоретичне навчання; s - індивідуальні заняття та консультації; С- екзаменаційна сесія (в т.ч. додаткова для ліквідації академзаборгованостей); Н - навчальна практика; В- виробнича практика; П - переддипломна практика; К – канікули; д- дипломне проектування; А- Атестація

II. ЗВЕДЕНІ ДАНІ ПРО БЮДЖЕТ, тижні

Курс	Теоретичне навчання, індивідуальні заняття та консультації	Екзаменаційна сесія	Практика	Атестація	Виконання дипломної роботи (проекту)	Канікули	Разом
1	30	5	4			13	52
2	30	5	4			13	52
3	30	5	4			13	52

III. ПРАКТИКА

Назва практики	Семестр	Тижні
Навчальна	2	4
Виробнича	4,6,8	12

IV. АТЕСТАЦІЯ

Форма атестації (атестаційний екзамен, дипломна робота (проєкт))	Семестр
Атестаційний екзамен	8

Шифр за ОПП	НАЗВА ОСВІТНЬОГО КОМПОНЕНТА	Розподіл за семестрами				Кількість кредитів ЄКТС	Кількість годин						Розподіл годин на тиждень за курсами і семестрами							
		Екзамени	Заліки	Курсові			Загальний обсяг	Аудиторних				Самостійна робота	I курс		II курс		III курс		IV курс	
				проєкти	роботи			Всього	у тому числі:				Семестри							
									лекції	лабораторні	практичні (семінарські)		1	2	3	4	5	6	7	8
													Кількість тижнів в семестрі							
													12	12	12	12	12	12	12	12
1. ОБОВ'ЯЗКОВІ НАВЧАЛЬНІ ДИСЦИПЛІНИ																				
1.1. Дисципліни циклу загальної підготовки																				
ОК 1	Українська та зарубіжна культура		2			3	90	24	12		12	66		2						
ОК 2	Іноземна мова	4	1,2,3			12	360	192			192	168	4	4	4	4				
ОК 3	Ділова українська мова		3			3	90	24			24	66			2					
ОК 4	Філософія, політологія та соціологія	1,2				6	180	48	24		24	132	2	2						
ОК 5	Іноземна мова фахового спрямування	8	5,6,7			12	360	96			96	264					2	2	2	2
ОК 6	Фізичне виховання		1			3	90	24			24	66	2							
ОК 7	Вища математика	2	1		КТ1, КТ2	12	360	120	60		60	240	4	6						
ОК 8	Дискретні структури	1				3	90	36	12	24		54	3							
ОК 9	Комп'ютерна графіка і візуалізація		1		1РГР	3	90	36	12	24		54	3							
ОК 10	Комп'ютерний аналіз	6				3	90	60	24	24	12	30						5		
ОК 12	Теорія ймовірностей та математична статистика	3			КТ 3	3	90	36	12		24	54			3					
ОК 13	Теорія алгоритмів	1				3	90	36	12	24		54	3							
ОК 28	Економіка для бізнесу		4			3	90	48	24		24	42				4				
Всього з циклу		**9**	**12**	**0**	**4**	**69**	**2070**	**780**	**192**	**96**	**492**	**1290**	**21**	**14**	**9**	8	**2**	**7**	**2**	**2**
1.2. Дисципліни циклу професійної підготовки																				
ОК 15	Безпека WEB-систем	5				3	90	48	24	24		42					4			
ОК 16	Апаратні та програмні засоби ком'ютерної інженерії	8				3	90	48	24	24		42								4

ОК 17	Технології розробки програмних продуктів	7				6	180	48	24	24		132							4	
ОК 18	Фундаментальні принципи розробки програмного забезпечення	2,3			2РГР	12	360	108	48	60		252		5	4					
ОК 19	Управління інформацією і інформаційна безпека	4,5		5КП		9	270	120	48	72		150				5	5			
ОК 20	Інструменти інформаційної безпеки		8			3	90	36	12	24		54								3
ОК 21	Основні системні принципи та інтелектуальні системи	6,7	5	7КПф		12	360	180	72	96	12	180					4	6	5	
ОК 22	Методи та системи штучного інтелекту	7				3	90	48	24	24		42							4	
ОК 23	Архітектура комп'ютерів та розподілені системи	2,3,4			3РГР	9	270	144	72	72		126		4	4	4				
ОК 24	Моделювання систем	8				3	90	36	12	24		54								3
ОК 25	Стандарти інформаційної безпеки та кібербезпеки	7				3	90	48	24	24		42							4	
ОК 26	Управління ІТ проектами		8			3	90	72	24	48		18								6
ОК 27	Системи передавання та приймання інформації	8				6	180	84	36	48		96								7
ОК 14	Алоритмізація і програмування	1				6	180	48	24	24		132	4							
ОК 11	Математичні методи дослідження операцій та прийняття рішень	5,6				6	180	120	48	72		60					4	6		
Всього з циклу		**19**	**3**	**2**	**2**	**87**	**2610**	**1188**	**516**	**660**	**12**	**1422**	**4**	**9**	**8**	**9**	**17**	**12**	**17**	**23**
Всього дисциплін		**28**	**18**	**2**	**6**	**156**	**4680**	**1968**	**708**	**756**	**504**	**2712**	**25**	**25**	**19**	**19**	**19**	**19**	**19**	**25**
2. ДИСЦИПЛІНИ ВІЛЬНОГО ВИБОРУ СТУДЕНТА																				
	Дисципліна 1		3			6	180	36	12		24	144			3					
	Дисципліна 2		3			6	180	36	12		24	144			3					
	Дисципліна 3		4			6	180	36	12		24	144				3				
	Дисципліна 4		4			6	180	36	12		24	144				3				
	Дисципліна 5		5			6	180	36	12		24	144					3			
	Дисципліна 6		5			6	180	36	12		24	144					3			
	Дисципліна 7		6			6	180	36	12		24	144						3		
	Дисципліна 8		6			6	180	36	12		24	144						3		
	Дисципліна 9		7			6	180	36	12		24	144							3	
	Дисципліна 10		7			6	180	36	12		24	144							3	
Всього з циклу		**0**	**10**	**0**	**0**	**60**	**1800**	**360**	**120**	**0**	**240**	**1440**	**0**	**0**	**6**	**6**	**6**	**6**	**6**	**0**
Разом варіативних дисциплін		**0**	**10**	**0**	**0**	**60**	**1800**	**360**	**120**	**0**	**240**	**1440**	**0**	**0**	**6**	**6**	**6**	**6**	**6**	**0**

3. ПРАКТИЧНА ПІДГОТОВКА																				
	Навчальна практика		2			6,0	180	0				180		Н						
	Виробнича практика		4,6,8			18,0	540	0				540				В		В		В
Всього		**0**	**4**	**0**	**0**	**24,0**	**720**	**0**				**720**								
Атестація																				
	Єдиний державний кваліфікаційний іспит																			А
Всього		**28**	**29**	**2**	**6**	**240,0**	**7200**	**2328**	**828**	**756**	**744**	**4872**	**25**	**25**	**25**	**25**	**25**	**25**	**25**	**25**
Загальна кількість кредитів													**30**	**30**	**30**	**30**	**30**	**30**	**30**	**30**
Кількість годин на тиждень													**25**	**25**	**25**	**25**	**25**	**25**	**25**	**25**
Кількість екзаменів		**28**											**4**	**4**	**3**	**4**	**3**	**3**	**3**	**4**
Кількість заліків			**29**										**4**	3	**4**	**4**	**4**	**4**	**3**	**3**
Кількість розрахункових робіт				**3**									**1**	**1**	**1**					
Кількість курсових робіт/проєктів					**2**												**1**		**1**	

Схвалено Вченою радою факультету МКТ
Протокол від "26" червня 2023 р. № 9

Погоджено

проректор
Оксана МОРГУЛЕЦЬ

Директор НМЦУПФ — Олена ГРИГОРЕВСЬКА
(підпис) (ініціали та прізвище)

Декан факультету МКТ — Володимир ПАВЛЕНКО
(підпис) (ініціали та прізвище)

Завідувач кафедри КН — Володимир ЩЕРБАНІ
(підпис) (ініціали та прізвище)

Гарант освітньої програми — Тетяна ДЕМКІВСЬКА
(підпис) (ініціали та прізвище)