МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний технічний університет
«Харківський політехнічний інститут»

ЗАТВЕРДЖУЮ
Ректор НТУ «ХПІ»
_____Євген СОКОЛ
«__» _____2023 р.

МІЖДИСЦИПЛІНАРНА ОСВІТНЬО-НАУКОВА ПРОГРАМА

«ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ КІБЕРБЕЗПЕКИ»

Другого рівня вищої освіти

за спеціальностями	113 «Прикладна математика» 125 «Кібербезпека та захист інформації»
галузей знань	11 «Математика і статистика» 12 «Інформаційні технології»
кваліфікація	Магістр з прикладної математики та кібербезпеки

ЗАТВЕРДЖЕНО
Вченою радою НТУ «ХПІ»
Протокол № 4 від
«05» травня 2023 р.
Голова вченої ради
_____Л. Л. Товажнянський

Харків 2023 р.

ЛИСТ ПОГОДЖЕННЯ

Освітньо-наукової програми «ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ КІБЕРБЕЗПЕКИ»

Рівень вищої освіти	Другий (магістерський)
Галузь знань	11 Математика і статистика 12 Інформаційні технології
Спеціальність	113 «Прикладна математика» 125 «Кібербезпека та захист інформації»
Освітня програма	Інтелектуальні системи кібербезпеки
Кваліфікація	Магістр з прикладної математики та кібербезпеки

СХВАЛЕНО
Робочою групою ОП зі спеціальності
«Прикладна математика»
Гарант освітньої програми
_____Юрій РЕШЕТНЯК
«___»_____20 __р.

РЕКОМЕНДОВАНО
Методичною радою НТУ «ХПІ»
Заступник голови методичної ради
_____Руслан МИГУЩЕНКО
«___»_____20 __р.

ПОГОДЖЕНО
Завідувачка кафедри Комп'ютерної
математики і аналізу даних
_____Олена АХІЄЗЕР
«__»_____2023 р.

ПОГОДЖЕНО
Завідувач кафедри Комп'ютерної
математики і аналізу даних
_____Сергій ЄВСЕЄВ
«___»_____2023 р.

ПОГОДЖЕНО
Директор ННІ комп'ютерних наук та
інформаційних технологій
_____Михайло ГОДЛЕВСЬКИЙ
«___»_____2023 р

РЕЦЕНЗІЯ

на міждисциплінарну освітньо-наукову програму «Інтелектуальні системи кібербезпеки» другого (магістерського) рівня вищої освіти за спеціальностями 113 «Прикладна математика» та 125 «Кібербезпека та захист інформації» Національного технічного університету «Харківський політехнічний інститут».

Освітньо-наукова програма орієнтована підготовку фахівців високого рівня обізнаності, здатних розв'язувати типові задачі та вирішувати проблеми, що виникають у сфері побудови інтелектуальних систем кібербезпеки. Вона повністю відповідає основним вимогам Стандарту віщої освіти. Дисципліни програми вдало розподілені за циклами.

Спеціальна підготовка орієнтована, насамперед, на вивчення сучасних чисельних методів аналізу даних, веб-безпеки, цифрової криміналістики, методів вирішення зворотних некоректних задач, методів машинного навчання.

Спеціалізована підготовка на основі блоків дисциплін вибору, включає математичні методи стеганографії, математичні методи криптографії та криптоаналізу, методи штучного інтелекту. Дисципліни вибору включають також методу обробки зображень і комп'ютерний огляд, методи глибокого навчання. Компоненти освітньої програми охоплюють усі основні напрямки аналізу великих даних за умов невизначеності.

Компоненти освітньої програми збалансовані, пов'язані з обґрунтованою структурно-логічною схемою, враховують сучасні досягнення науки про дані та кібербезпеки.

Таким чином, міждисциплінарна освітньо-наукова програма «Інтелектуальні системи кібербезпеки» другого (магістерського) рівня вищої освіти за спеціальностями 113 «Прикладна математика» та 125 «Кібербезпека та захист інформації» може бути рекомендована до впровадження і використання в освітньому процесі Національного технічного університету «Харківський політехнічний інститут».

Професорка кафедри комп'ютерних
технологій і моделювання систем
Поліського національного університету
докторка технічних наук, професорка Катерина МОЛОДЕЦЬКА

САЙФЕР

Системи захисту інформації

ТОВ «САЙФЕР ІТ» ЄДРПОУ 43305772
Адреса: 04107, Київ, вул. Нагірна, 25
Тел./Факс: (044) 484-46-17, 484-46-12, 483-03-22
E-mail: info@cipher.com.ua
https://cipher.com.ua

Вих.№ 31/23
від «16» травня 2023 року

РЕЦЕНЗІЯ

на міждисциплінарну освітньо-наукову програму «Інтелектуальні системи кібербезпеки» другого (магістерського) рівня вищої освіти за спеціальностями 113 «Прикладна математика» та 125 «Кібербезпека та захист інформації» Національного технічного університету «Харківський політехнічний інститут».

Підготовка магістрів за програмою «Інтелектуальні системи кібербезпеки» обумовлена великим попитом на дослідників, в одних з найбільш затребуваних областей сучасних інформаційних технологій - науки та інженерії даних, кібербезпеки та захисту інформації. У зв'язку з цим структура та освітнє наповнення програми передбачає, насамперед, вивчення математичних методів, моделей та алгоритмів аналізу складних неструктурованих даних в умовах невизначеності.

При цьому основна увага приділяється придбанню необхідних компетенцій, що забезпечують застосування сучасних інформаційних технологій штучного інтелекту, машинного навчання, побудови безпечної архітектурі, управління ризиками.

Ця спрямованість програми забезпечується вивченням сучасних чисельних методів аналізу даних, включаючи методи вирішення зворотних некоректних завдань. Можливість спеціалізації забезпечується набором дисциплін вибору у вигляді тематичних блоків, що дозволяють здобувачеві вищої освіти отримати спеціалізовану підготовку в галузі аналізу великих даних, захисту корпоративних мереж, блокчейн-технології та безпеки інформаційних систем.

ОНП включає всі необхідні складові, що передбачені методичними рекомендаціями з розробки освітніх програм, має чітку та зрозумілу структуру, містить загальну інформацію, мету та докладну характеристику, передбачає виконання освітньої та наукової складових. Слід зазначити, що ОНП забезпечує набуття інтегральної, загальних та спеціальних компетентностей, програмних

результатів навчання, які відповідають сучасним вимогам щодо підготовки наукових кадрів вищої кваліфікації.

ОНП є актуальною, має самостійний, творчий характер, відповідає суспільним потребам щодо підготовки сучасного спеціаліста з даної спеціальності та передбачає у разі її успішного проходження можливості працевлаштування у галузі ІТ. Освітня програма враховує сучасні досягнення науки про дані та може бути рекомендована до використання у навчальному процесі при підготовці спеціалістів – прикладних математиків в Національному технічному університеті «Харківський політехнічний інститут».

Директор ТОВ «Сайфер ІТ», ктн В.Ю. Ковтун

ТОВ «Мікрокрипт Технолоджіс»
E-mail: info@microcrypt.com.ua

«Microcrypt Technologies» LTD.
Web: www.microcrypt.com.ua

ЗАТВЕРДЖУЮ:
Генеральний директор
ТОВ «Мікрокрипт Технолоджіс»

_____ Голованов О.О.

«05» 05 2023 р.

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ * УКРАЇНА * "МІКРОКРИПТ ТЕХНОЛОДЖІС" код 38281163

РЕЦЕНЗІЯ

на міждисциплінарну освітньо-наукову програму «Інтелектуальні системи кібербезпеки» другого (магістерського) рівня вищої освіти за спеціальностями 113 «Прикладна математика» та 125 «Кібербезпека та захист інформації» Національного технічного університету «Харківський політехнічний інститут».

Стратегічною метою представленої на рецензію освітньо-наукової програми є підготовка професіоналів високого рівня, здатних розв'язувати складні задачі та вирішувати проблеми в галузі статистичного та інтелектуального аналізу даних та кібербезпеки.

Рецензована освітньо-наукова програма регламентує мету, зміст, умови і технологію реалізації освітнього процесу, очікувані результати навчання, оцінку якості підготовки магістра за даною спеціальністю і включає в себе: загальну інформацію, мету і характеристику освітньої програми, придатність випускників до працевлаштування та подальшого навчання, ресурсне забезпечення реалізації програми, академічну мобільність, перелік компонент програми та їх логічну послідовність, форму атестації здобувачів вищої освіти, матрицю відповідності програмних компетентностей компонентам освітньої програми. Оцінка силабусів навчальних дисциплін, представлених на сайті НТУ «ХПІ», дозволяє зробити висновок, що зміст навчальних дисциплін відповідає моделі необхідних компетенцій випускника. Значна увага в даній ОНП приділена фаховим компетенціям, які закріплюють за собою статус основи

освітньо-наукового простору. Добре виписаним є нормативний зміст підготовки магістрів, сформульований у термінах результатів навчання.

В цілому вважаю, що ОНП складена кваліфіковано, демонструє професіоналізм і високий рівень методичної підготовки членів проектної групи. ОНП включає навчальні дисципліни, які готують здобувача вищої освіти як експерта та науковця, що здатний до самостійної діяльності, а також як викладача, що здатний до майбутньої викладацької діяльності.

ОНП є актуальною, має самостійний, творчий характер, відповідає сучасним потребам щодо підготовки фахівця з спеціальностей 113 «Прикладна математика» та 125 «Кібербезпека та захист інформації» та передбачає успішне працевлаштування у галузі ІТ.

Генеральний директор
ТОВ «Мікрокрипт Технолоджис», к.т.н. Головашич С.О.

УКРАЇНА * ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ * Харків *
"МІКРОКРИПТ ТЕХНОЛОДЖІС"
код 38281163

ПЕРЕДМОВА

Відповідає стандарту вищої освіти другого (магістерського) рівня галузі знань 12 Інформаційні технології, спеціальності 125 «Кібербезпека та захист інформації» галузі (Затверджено та введено в дію наказом Міністерства освіти і науки України від 18.03.2021 р. № 332) та галузі знань 11 Математика і статистика, спеціальності 113 «Прикладна математика» відповідно до національної рамки кваліфікацій.

Розроблено робочою групою зі спеціальностей 113 «Прикладна математика» та 125 «Кібербезпека та захист інформації» Науково-навчального інституту комп'ютерних наук та інформаційних технологій Національного технічного університету «Харківський політехнічний інститут» у складі:

Гарант освітньої програми	
РЕШЕТНЯК Юрій Борисович	кандидат фізико-математичних наук, доцент кафедри комп'ютерної математики і аналізу даних
Члени робочої групи ОП	
ЄВСЕЄВ Сергій Петрович	доктор технічних наук, завідувач кафедри кібербезпеки
АХІЄЗЕР Олена Борисівна	кандидат технічних наук, завідувачка кафедри комп'ютерної математики і аналізу даних
МІЛОВ Олександр Володимирович	доктор технічних наук, професор кафедри кібербезпеки

1. ПРОФІЛЬ ОСВІТНЬОЇ-НАУКОВОЇ ПРОГРАМИ ЗА СПЕЦІАЛЬНОСТЯМИ

1 – Загальна інформація	
Вищий навчальний заклад та структурний підрозділ	Національний технічний університет «Харківський політехнічний інститут» Навчально-науковий інститут комп'ютерних наук та інформаційних технологій Кафедри: комп'ютерної математики і аналізу даних, кібербезпеки
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь — магістр Кваліфікація — магістр з прикладної математики та кібербезпеки
Офіційна назва освітньої програми	Інтелектуальні системи кібербезпеки
Тип диплома й обсяг освітньої програми	Диплом магістра, одиничний, 120 кредитів ЄКТС, 1 рік 9 місяців
Наявність акредитації	Програма впроваджується у 2023 р.
Цикл / рівень програми	Другий (магістерський) рівень вищої освіти, НРК України — 7 рівень, FQ-EHEA — другий цикл, QF-LLL — 7 рівень
Передумови	Наявність ступеня бакалавра
Мова(и) викладання	Українська, англійська.
Термін дії освітньої програми	Відповідно до терміну дії сертифіката про акредитацію. Переглядається щорічно
Інтернет-адреса постійного розміщення освітньої програми	https://cybersecurity.kpi.kharkov.ua http://web.kpi.kharkov.ua/kmmm/uk/

2 – Мета освітньо-наукової програми
Метою даної міждисциплінарної освітньо-наукової програми другого (магістрського) освітньо-кваліфікаційному рівня є забезпечення підготовки фахівців-дослідників у галузях прикладної математики та кібербезпеки, які здатні формулювати, розв'язувати й узагальнювати складні задачі та проблеми у своїй професійній діяльності, здійснювати професійну інноваційну діяльність для виконання наукових і проєктних робіт з використанням фундаментальних і спеціальних математичних методів для кібербезпеки та захисту інформації, розробляти математичні моделі, алгоритми, створювати й експлуатувати відповідне програмне забезпечення, а також використовувати і впроваджувати технології інформаційної безпеки та/або кібербезпеки. Освітньо-наукова програма спрямована на підготовку фахівців-дослідників, що володіють сучасними математичними методами й інформаційними технологіями інтелектуального пошуку, аналізу, обробки даних, зокрема даних вимірювань і спостережень, технологій захисту інформації, інформаційної безпеки, кібербезпеки і безпеки інформації, розробки і використання програмного забезпечення захисту інформації, кібербезпеки й інформаційної безпеки.

3 – Характеристика освітньо-наукової програми	
Предметна область (галузь знань, спеціальність, програма	Галузі знань: 11 – Математика та статистика, 12 – Інформаційні технології Спеціальність: 113 – Прикладна математика, 125 – Кібербезпека та захист інформації Об’єкт вивчення: процеси та явища, що можуть бути описані математично; сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об’єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; системи управління інформаційною безпекою та/або кібербезпекою; технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки Цілі навчання: оволодіння сучасними математичними методами та інформаційними технологіями; підготовка фахівців, здатних розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. Теоретичний зміст предметної області: інтелектуальний пошук, аналіз, обробка і візуалізація даних; теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки. Методи, методики та технології: сучасні інформаційні технології програмування. Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Інструменти та обладнання: засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проєктування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об’єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки й аналізу даних
Орієнтація освітньої програми	Професійна підготовка фахівців у сфері аналізу даних і кібербезпеки
Основний фокус освітньої програми та спеціалізації	Підготовка фахівців-дослідників, що володіють сучасними математичними методами й інформацій-ними технологіями інтелектуального пошуку, аналізу, обробки даних, зокрема даних вимірювань і спостережень, технологій захисту інформації, інформаційної безпеки, кібербезпеки і безпеки інформації, розробки

	і використання програмного забезпечення захисту інформації, кібербезпеки й інформаційної безпеки. Ключові слова: аналіз даних, обробка сигналів та зображень, інформаційний пошук, великі дані, штучний та обчислювальний інтелект, кібербезпека.
Особливості програми	Експериментальна проєктно-орієнтована освітньо-наукова програма. Проєктне навчання на основі виконання інтегрованих навчальних та реальних проєктів. Дуальне навчання на базових підприємствах (провідних ІТ-компаніях). Індивідуалізація навчання з орієнтацією на студента. Викладання ряду навчальних дисциплін англійською мовою.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Працевлаштування на підприємствах і компаніях ІТ-індустрії, в інформаційно-аналітичних відділах підприємств виробничого і банківсько-фінансового секторів, наукових установах, навчальних закладах вищої освіти тощо. Професійні можливості випускників (відповідно до Класифікатора професій ДК 003:2010): 212 – Професіонали в галузі математики і статистики; 2121 – Професіонали в галузі математики; 2121.1 – Наукові співробітники (математика) 2121.2 – Математик (прикладна математика), математик-аналітик з дослідження операцій; 2149.2 – Інженер-дослідник (прикладна математика); 213 – Професіонали в галузі обчислень; 2132 – Професіонали в галузі програмування; 2132.2 – Розробники комп'ютерних програм; 2139.2 – Аналітик загроз безпеки; 2139.2 – Аналітик систем захисту інформації та оцінки вразливостей; 2139.2 – Аналітик з безпеки інформаційно-телекомунікаційних систем; 2139.2 – Дізнавач (сфера кібербезпеки та захисту інформації); 2139.2 – Експерт-криміналіст (сфера кібербезпеки та захисту інформації); 2139.2 – Експерт-криміналіст судової експертизи (сфера кібербезпеки та захисту інформації); 2139.2 – Слідчий з кіберзлочинів. Первинні посади: науковий співробітник, математик (прикладна математика), фахівець з аналізу даних, системний аналітик, розробник програмного забезпечення.
Подальше навчання	Можливість продовження освіти на третьому (освітньо-науковому) рівні вищої освіти (8 рівень НРК) за програмами підготовки докторів філософії (PhD). Можливість післядипломної освіти для отримання професійної кваліфікації за відповідними професійними стандартами.
5 – Викладання та оцінювання	
Викладання та навчання	Лекції, лабораторні та практичні заняття, науково-практичні семінари, виконання навчальних та реальних проєктів, проблемно-орієнтоване навчання та навчання за запитами, студентоцентроване

	навчання, дуальне навчання, дистанційне та змішане навчання в системі Office 365, самостійна робота та самонавчання, практика, підготовка кваліфікаційної роботи.
Оцінювання	Рейтингова система оцінювання. Поточний та підсумковий контроль знань (опитування, контрольні та індивідуальні завдання, тестування тощо), заліки та екзамени (усні та письмові), захист навчальних та реальних проєктів з презентацією, публічний захист кваліфікаційної роботи.
6 – Програмні компетентності	
Інтегральна компетентність (113)	Здатність розв'язувати задачі дослідницького та/або інноваційного характеру у професійній діяльності або у процесі навчання, що характеризується невизначеністю умов і вимог та передбачає проведення досліджень та/або здійснення інновацій і потребує застосування математичних теорій, методів, алгоритмів, інформаційних технологій та спеціалізованого програмного забезпечення.
Інтегральна компетентність (125)	Здатність розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності (ЗК)	
Загальні компетентності (113)	ЗК 1. 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 2. 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. ЗК 3. Здатність до безперервного навчання, придбання нових знань та умінь, у тому числі в галузі, відмінній від професійної. ЗК 4. Здатність виявляти, ставити та вирішувати проблеми в професійній діяльності. ЗК 5. Здатність генерувати нові ідеї (креативність) й нестандартні підходи до їх реалізації, гнучко адаптуватися до реальних професійних ситуацій, проявляти творчий підхід, ініціативу. ЗК 6. Здатність критично оцінювати й переосмислювати накопичений досвід (власний і чужий), аналізувати свою професійну й соціальну діяльність. ЗК 7. Здатність працювати з інформацією: знаходити й використовувати інформацію з різних джерел, потрібну для розв'язання професійних завдань. ЗК 8. Здатність ефективно будувати комунікацію, виходячи з цілей і ситуації спілкування. ЗК 9. Здатність готувати та здійснювати публічні виступи з презентацією одержаних результатів, готувати науково-технічні публікації за результатами виконаних досліджень, у тому числі іноземною мовою. ЗК 10. Здатність здійснювати професійну наукову та проєктно-виробничу діяльність у міжнародному середовищі.

	ЗК 11. Здатність до соціальної й професійної взаємодії та співпраці в колективі, командної роботи.
Загальні компетентності (125)	ЗК 12. Здатність застосовувати знання у практичних ситуаціях. ЗК 13. Здатність проводити дослідження на відповідному рівні. ЗК 14. Здатність до абстрактного мислення, аналізу та синтезу. ЗК 15. Здатність оцінювати та забезпечувати якість виконуваних робіт. ЗК 16. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Спеціальне (фахове) (СК)	
Спеціальні (фахові, предметні) компетентності (113)	СК 1. Здатність формулювати математичну постановку задачі, спираючись на постановку мовою предметної галузі, перевіряти коректність постановки, в тому числі в умовах невизначеності. СК 2. Здатність обирати, розробляти та досліджувати математичний, аналітичний або чисельний метод розв'язання практичних задач, що забезпечує потрібні точність і надійність результату. СК 3. Здатність обирати, розробляти, досліджувати та застосовувати математичні методи для розв'язання практичних задач моделювання, проєктування, керування, прогнозування, прийняття рішень. СК 4. Здатність розробляти алгоритми аналізу невизначених великих даних, розробляти відповідні програмні засоби та документацію, проєктувати програмні системи, бази даних і знань. СК 5. Здатність до проведення математичного і комп'ютерного моделювання та обчислювального експерименту, збору, візуалізації, аналізу та обробки отриманих даних, розв'язання формалізованих задач за допомогою спеціалізованих програмних засобів. СК 6. Здатність організовувати роботу колективу виконавців для проведення досліджень та розробок проєктів, приймати доцільні та економічно обґрунтовані організаційні та управлінські рішення. СК 7. Здатність до пошуку, вивчення та аналізу науково-технічної інформації, вітчизняного й закордонного досвіду, пов'язаного із застосуванням математичних методів для дослідження процесів та систем. СК 8. Здатність брати участь у складанні наукових та технічних звітів із виконаних проєктних або науково-дослідних робіт та у впровадженні результатів проведених досліджень і розробок. СК 9. Здатність до ефективної професійної письмової й усної технічної та наукової комунікації в предметній галузі українською мовою та однією з поширених європейських мов. СК 10. Здатність обирати, розробляти, досліджувати та застосовувати математичні моделі та методи для інтелектуального аналізу даних в умовах невизначеності. СК 11. Здатність розробляти, досліджувати та застосовувати математичні методи й алгоритми машинного навчання, м'яких обчислень і обчислювального інтелекту для аналізу невизначених даних, прогнозування та прийняття рішень. СК 12. Здатність до розробки та експлуатації спеціалізованих програмних засобів інтелектуального аналізу даних, текстів, сигналів і зображень.

	СК 13. Здатність до розробки та експлуатації спеціалізованих програмних засобів обробки великих масивів даних на основі інформаційних технологій розподілених і хмарних обчислень. СК 14. Здатність до використання сучасних інформаційних технологій інтелектуального аналізу даних, прогнозування, прийняття рішень, інформаційного пошуку та видобування знань.
Спеціальні (фахові, предметні) компетентності (125)	СК 15. Здатність обґрунтовано застосовувати, інтегрувати, розробляти і вдосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення і використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. СК 16. Здатність розробляти, впроваджувати й аналізувати нормативні документи, положення, інструкції й вимоги технічного й організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. СК 17. Здатність досліджувати, розробляти і супроводжувати методи і засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури. СК 18. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політику інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів і вимог. СК 19. Здатність до дослідження, системного аналізу і забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем і ресурсів, аналізу ризиків і визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. СК 20. Здатність аналізувати, контролювати і забезпечувати систему управління доступом до інформаційних ресурсів згідно з встановленою стратегією і політикою інформаційної безпеки та/або кібербезпеки організації. СК 21. Здатність досліджувати, розробляти і впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження й аналізу кіберінцидентів у цілому. СК 22. Здатність досліджувати, розробляти, впроваджувати і супроводжувати методи і засоби криптографічного й технічного захисту інформації на об’єктах інформаційної діяльності й критичної інфраструктури, у інформаційних системах, а також здатність оцінювати ефективність їхнього використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. СК 23. Здатність аналізувати, розробляти і супроводжувати систему аудиту і моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів у галузі інформаційної безпеки та/або кібербезпеки організації в цілому. СК 24. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з

	персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки. СК 25. Здатність здійснювати наукові та/або прикладні дослідження у галузі інформаційної безпеки та/або кібербезпеки із застосуванням сучасних експериментальних і теоретичних методів моделювання процесів, формувати науково-технічну звітність.
7 – Результати навчання	
Результати навчання за спеціальністю за спеціальністю 113	РН 1. Демонструвати знання й розуміння основних концепцій, принципів, теорій фундаментальної та прикладної математики і використовувати їх на практиці. РН 2. Уміти формалізувати задачі, сформульовані мовою певної предметної галузі й обирати раціональний метод вирішення; розв'язувати задачі аналітичними або чисельними методами, оцінювати точність і достовірність отриманих результатів і виконувати їх інтерпретацію. РН 3. Володіти методами розробки, дослідження і застосування математичних моделей складних об'єктів і процесів, в тому числі із застосуванням методів обчислювального інтелекту. РН 4. Уміти поєднувати методи математичного та комп'ютерного моделювання з неформальними процедурами експертного аналізу для пошуку оптимальних рішень. РН 5. Будувати ефективні щодо точності обчислень, стійкості, швидкодії та витрат системних і обчислювальних ресурсів, алгоритми для чисельного дослідження математичних моделей і аналізу даних, прийняття рішень. РН 6. Уміти вибирати, розробляти і досліджувати методи й алгоритми розв'язання математичних задач оптимізації систем, дослідження операцій, оптимального керування й прийняття рішень. РН 7. Уміти застосовувати сучасні технології програмування і розроблення програмного забезпечення, програмної реалізації чисельних та символьних алгоритмів. РН 8. Уміти застосовувати в практичній роботі спеціалізовані програмні продукти і програмні системи комп'ютерної математики, аналізу великих даних тощо. РН 9. Демонструвати навички взаємодії з іншими людьми, ефективного спілкування зі спеціалістами та суспільством, уміння працювати в групах і командах, управління конфліктами та стресами. РН 10. Уміти здійснювати збір, опрацювання, аналіз, систематизацію науково-технічної інформації, уникаючи при цьому плагіату, формувати і виносити судження, розробляти презентації та публікації. РН 11. Демонструвати навички професійного спілкування, усної та письмової комунікації українською мовою і принаймні ще однією з європейських мов. РН 12. Знати та розуміти сучасні методи розв'язання математичних задач статистичного й інтелектуального аналізу даних, прогнозування тощо. РН 13. Знати і розуміти методи розв'язання математичних задач інтелектуального інформаційного пошуку та видобування знань.

	РН 14. Уміти застосовувати існуючі та розробляти нові алгоритми і програмні засоби для статистичного й інтелектуального аналізу невизначених даних. РН-15. Уміти застосовувати існуючі й розробляти нові алгоритми та програмні засоби обробки даних, текстів, сигналів і зображень. РН 16. Уміти застосовувати сучасні інформаційні технології та програмне забезпечення для обробки великих масивів даних на основі розподілених і хмарних сервісів.
Результати навчання за спеціальністю 125 (визначені стандартом вищої освіти спеціальності)	РН 17. Вільно спілкуватись державною й іноземною мовами, усно і письмово для представлення й обговорення результатів досліджень та інновацій, забезпечення бізнес/операційних процесів і питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН 18. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН 19. Провадити дослідницьку та/або інноваційну діяльність у сфері інформаційної безпеки та/або кібербезпеки, а також у сфері технічного і криптографічного захисту інформації у кіберпросторі. РН 20. Застосовувати, інтегрувати, розробляти, впроваджувати й удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. РН 21. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому і міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. РН 22. Аналізувати й оцінювати захищеність систем, комплексів і засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН 23. Обґрунтовувати використання, упроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН 24. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. РН 25. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. РН 26. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти вразливості інформаційних систем і ресурсів, аналізувати й оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. РН 27. Аналізувати, контролювати і забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. РН 28. Досліджувати, розробляти і впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління,

	контролю та розслідування, а також надавати рекомендації щодо попередження й аналізу кіберінцидентів в цілому. РН 29. Досліджувати, розробляти, упроваджувати та використовувати методи і засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їхнього використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. РН 30. Аналізувати, розробляти і супроводжувати систему аудиту і моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів у сфері інформаційної та/або кібербезпеки в цілому. РН 31. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання і пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. РН 32. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування і прийняття рішень. РН 33. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання. РН 34. Планувати навчання, а також супроводжувати і контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. РН 35. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові й експериментальні методи кіберзахисту, розробляти, реалізовувати і супроводжувати проєкти із захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН 36. Ставити та вирішувати складні інженерно-прикладні і наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів і кращих практик. РН 37. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. РН 38. Планувати і виконувати експериментальні та теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи й інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. РН 39. Обґрунтовувати вибір програмного забезпечення, устаткування й інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної і довідкової літератури та іншої доступної інформації. РН 40. Планувати і виконувати наукові та прикладні дослідження у сфері інформаційної безпеки та/або кібербезпеки із застосуванням сучасних технологій, експериментальних і теоретичних методів і

	моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики. РН 41. Оцінювати ефективність і практичну цінність результатів наукових і практичних досліджень та інновацій.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Відповідає кадровим вимогам щодо забезпечення провадження освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова кабінету міністрів України «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30 грудня 2015 р. № 1187, зі змінами, внесеними згідно з Постановою КМ № 365 від 24.03.2021, додаток 15-16).
Матеріально-технічне забезпечення	Відповідає вимогам щодо матеріально-технічного забезпечення провадження освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова кабінету міністрів України «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30 грудня 2015 р. № 1187, зі змінами, внесеними згідно з Постановою КМ № 365 від 24.03.2021, додаток 17). У наявності є аудиторний фонд та мультимедійне обладнання.
Інформаційне та навчально-методичне забезпечення	Відповідає вимогам щодо інформаційного та навчально-методичного забезпечення провадження освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова кабінету міністрів України «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30 грудня 2015 р. № 1187, зі змінами, внесеними згідно з Постановою КМ № 365 від 24.03.2021, додаток 18). У викладачів та студентів є доступ до бібліотеки НТУ «ХПІ» та її репозиторію, а також до кафедральної бібліотеки.
9 – Академічна мобільність	
Національна кредитна мобільність	Можливість укладення угод про академічну мобільність, про подвійне дипломування, тощо між Національним технічним університетом «Харківський політехнічний інститут» і вищими навчальними закладами України. Регламентується «Положенням про академічну мобільність студентів, аспірантів, докторантів, науково-педагогічних та наукових працівників НТУ «ХПІ»
Міжнародна кредитна мобільність	Можливість укладення угод про міжнародну академічну мобільність, про подвійне дипломування тощо між Національним технічним університетом «Харківський політехнічний інститут» і вищими навчальними закладами країн-партнерів.
Навчання іноземних здобувачів вищої освіти	Після отримання сертифікату про акредитацію (можуть навчатись іноземці та/або особи без громадянства після вивчення курсу української мови).

2. ПЕРЕЛІК ОСВІТНІХ КОМПОНЕНТ ОСВІТНЬОЇ-НАУКОВОЇ ПРОГРАМИ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

Код	Компоненти освітньої програми (навчальні дисципліни, курсові проєкти/курсові роботи, практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1. Обов'язкові компоненти ОП			
1.1. Загальна підготовка			
ЗП 1	Інноваційне підприємництво та управління стартап проєктами	3	Залік
ЗП 2	Захист інтелектуальної власності	3	Залік
ЗП 3	Іноземна мова за професійним спрямуванням	3	Залік
1.2. Спеціальна (фахова) підготовка			
СП 1	Нелінійні процеси і моделі	4	Екзамен
СП 2	Математичні методи машинного навчання	5	Екзамен
СП 3	Методи розв'язання зворотних задач	4	Екзамен
СП 4	Веб-безпека	5	Залік
СП 5	Цифрова криміналістика	4	Екзамен
СП 6	Тестування на проникнення та етичний хакінг	4	Залік
1.3. Наукова підготовка			
НП 1	Філософські проблеми сучасного наукового пізнання	3	Екзамен
НП 2	Основи наукових досліджень	5	Екзамен
НП 3	Сучасні проблеми інтелектуального аналізу даних в кібербезпеці	4	Залік
НП 4	Технології управління безпекою об'єктів критичної структури	5	Залік
НП 5	Науково-дослідницька практика	11	Залік
	Атестація	19	Екзамен
Загальний обсяг обов'язкових компонент		**82**	
2. Вибіркові компоненти			
2.1. Профільна підготовка			
2.1.1. Профільований пакет 01			
ВП 1.1	Математичні методи стеганографії	5	Екзамен
ВП 1.2	Математичні методи криптографії та криптоаналізу	5	Екзамен
ВП 1.3	Моделювання кіберфізичних дій	5	Екзамен
ВП 1.4	Штучний інтелект та експертні системи	5	Екзамен
Разом		20	
2.1.2. Профільований пакет 02			
ВП 2.1	Безпека інтернету-речей та сервісів	5	Екзамен

Код	Компоненти освітньої програми (навчальні дисципліни, курсові проєкти/курсові роботи, практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
ВП 2.2	Інженерія безпеки інформаційно-комунікаційних систем	5	Екзамен
ВП 2.3	Методи глибокого навчання	5	Екзамен
ВП 2.4	Штучний інтелект та системи кібербезпеки	5	Екзамен
Разом		20	
2.2. Блок вільного вибору профільної підготовки			
ВВ 1	Дисципліна вільного вибору 1 (вирівнювальна)	5	Екзамен
ВВ 2	Дисципліна вільного вибору 2 (вирівнювальна)	5	Залік
ВФ 1	Дисципліна вільного вибору 3 (фокусна)	4	Екзамен
ВФ 2	Дисципліна вільного вибору 4 (фокусна)	4	Залік
Разом		18	
Загальний обсяг вибіркових компонент		**38**	
Загальний обсяг освітньої програми		**120**	

2.2. Розподіл змісту освітньої програми за групами компонент та циклами підготовки

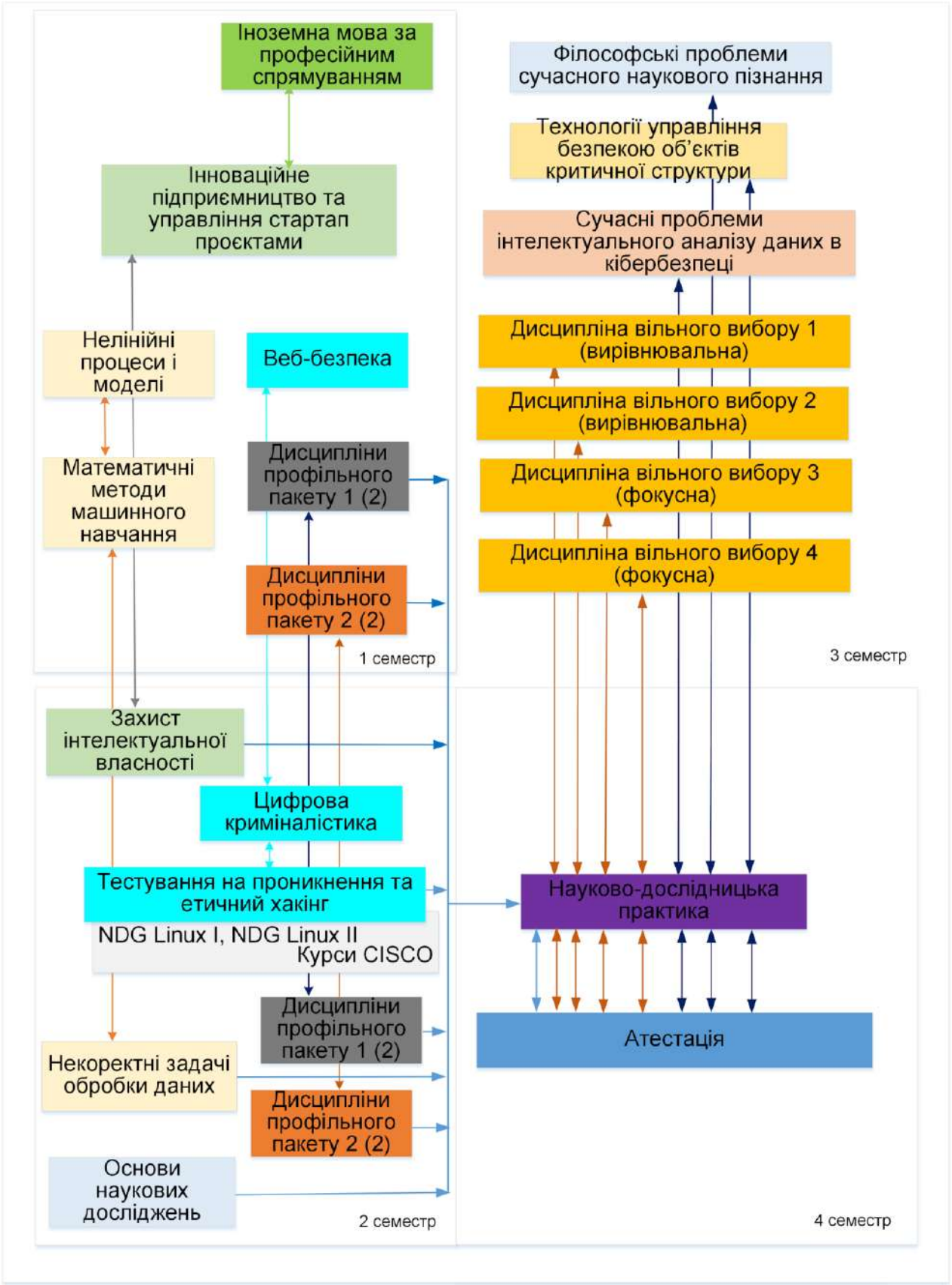
№ п/п	Цикл підготовки	Обсяг навчального навантаження здобувача вищої освіти (кредитів / %)		
		Обов'язкові компоненти освітньо-професійної програми	Вибіркові компоненти освітньо-професійної програми	Всього за весь термін навчання
1	Загальна підготовка	9 / 7,5		9 / 7,5
2	Спеціальна (фахова) підготовки	73 / 60,8		73 / 60,8
3	Дисципліни вільного вибору		38 / 31,7	38 / 31,7
Всього за весь термін навчання		82 / 68,3	38 / 31,6	**120 / 100**

2.3. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація випускників міждисциплінарної освітньої програми за спеціальностями 113 – «Прикладна математика», 125 – «Кібербезпека та захист інформації» проводиться у формі захисту кваліфікаційної магістерської роботи та завершується видачею документа встановленого зразка про присудження ступеня магістра із присвоєнням кваліфікації: «**Магістр з прикладної математики та кібербезпеки»** за освітньою програмою **«Інтелектуальні системи кібербезпеки».** Атестація здійснюється відкрито і публічно.

Кваліфікаційна робота має бути перевірена на плагіат із використанням програмно-технічних засобів, а також має бути розміщена в репозиторії вищого навчального закладу або відповідного структурного підрозділу.

3 СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬОЇ ПРОГРАМИ



Матриця відповідності визначених результатів навчання, компетентностей та освітніх компонентів (визначені стандартом вищої освіти спеціальності 113)

Результати навчання	Компетентності																								
	Загальні											Спеціальні (фахові)													
	ЗК 1	ЗК 2	ЗК 3	ЗК 4	ЗК 5	ЗК 6	ЗК 7	ЗК 8	ЗК 9	ЗК 10	ЗК 11	СК 1	СК 2	СК 3	СК 4	СК 5	СК 6	СК 7	СК 8	СК 9	СК 10	СК 11	СК 12	СК 13	СК 14
РН 1		НП3			ВП4	НП3				НП3		СП1, СП3	СП1, СП2, СП3	СП1, СП2, СП3	ВП4, НП3	ВП4, СП1, СП2, СП3		НП3	ВП4		ВП4		ВП4	ВП4, СП2	ВП4, СП2
РН 2				ВП4, СП1								ВП4, СП1, СП3	ВП4, СП1, СП2, СП3	ВП4, СП1, СП2, СП3		СП1, СП2, СП3		ВП4, СП1				ВП4, СП1			
РН 3					ВП4										ВП4	ВП4			ВП4		ВП4		ВП4	ВП4	ВП4
РН 4					ВП4										ВП4	ВП4			ВП4		ВП4		ВП4	ВП4	ВП4
РН 5				ВП4, СП1								ВП4, СП1, СП3	ВП4, СП1, СП2, СП3	ВП4, СП1, СП2, СП3		СП1, СП2, СП3		ВП4, СП1				ВП4, СП1			
РН 6				ВП4, СП1								ВП4, СП1, СП3	ВП4, СП1, СП2, СП3	ВП4, СП1, СП2, СП3		СП1, СП2, СП3		ВП4, СП1				ВП4, СП1			
РН 7					ВП4										ВП4	ВП4			ВП4		ВП4		ВП4	ВП4	ВП4
РН 8					ВП4										ВП4	ВП4			ВП4		ВП4		ВП4	ВП4	ВП4
РН 9	ЗП2		ЗП2, ЗП3	ЗП3	ЗП3			ЗП3	ЗП2, ЗП3	ЗП3	ЗП2						ЗП2, ЗП3	ЗП2	ЗП2, ЗП3	ЗП3					
РН 10		НП1, НП3	НП1, НП2		НП1	НП1, НП2, НП3	НП1		НП1	НП3					НП3			НП1, НП3							
РН 11			ЗП2	ЗП2				ЗП2	ЗП2	ЗП2							ЗП2	ЗП2	ЗП2	ЗП2					
РН 12		НП3				НП3				НП3		СП1	СП1, СП2	СП1, СП2	НП3	СП1, СП2		НП3							
РН 13				ВП4, СП1								ВП4, СП1, СП3	ВП4, СП1, СП2, СП3	ВП4, СП1, СП2, СП3		СП1, СП2, СП3		ВП4, СП1				ВП4, СП1			
РН 14				ВП4, СП1								ВП4, СП1	ВП4, СП1	ВП4, СП1				ВП4, СП1				ВП4, СП1			
РН 15					ВП4										ВП4	ВП4			ВП4		ВП4		ВП4	ВП4, СП2	ВП4, СП2
РН 16					ВП4										ВП4	ВП4			ВП4		ВП4		ВП4	ВП4	ВП4

Матриця відповідності визначених результатів навчання, компетентностей та освітніх компонентів
(визначені стандартом вищої освіти спеціальності 125)

Програмні результати навчання	Компетентності														
	Інтегральна компетентність														
	Загальні компетентності					Спеціальні (фахові) компетентності									
	ЗК 12	ЗК 13	ЗК 14	ЗК 15	ЗК 16	СК 15	СК 16	СК 17	СК 18	СК 19	СК 20	СК 21	СК 22	СК 23	СК 24
РН 17	ЗП1 ЗП3 СП4		ЗП3			ЗП3 СП4									
РН 18		ЗП3	ЗП3			ЗП3 СП4	ЗП2	СП4 СП6							
РН 19	ЗП1 ЗП3 СП4					ЗП3 СП4		СП5			НП5				
РН 20	ЗП1 ЗП3 СП4	ЗП3	ЗП3			ЗП3 СП4	ЗП2				НП5				
РН 21			ЗП3		ЗП2 ЗП3 СП4		ЗП2								
РН 22	ЗП1 ЗП3 СП4					ЗП3 СП4		СП4 СП5 СП6		СП4 СП5 СП6	НП5	СП4 СП5 СП6		СП4 НП5	
РН 23	ЗП1 ЗП3 СП4		ЗП3								НП5				
РН 24	ЗП1 ЗП3 СП4	ЗП3			ЗП2 ЗП3 СП4			СП4 СП5 СП6			НП5		НП5	СП4	ЗП3 НП5
РН 25	ЗП1 ЗП3 СП4	ЗП3	ЗП3						СП4		НП5			СП4 НП5	ЗП3 НП5
РН 26	ЗП1 ЗП3 СП4		ЗП3							СП4 СП5 СП6				СП4	
РН 27	ЗП1 ЗП3 СП4		ЗП3											НП5	ЗП3 НП5
РН 28	ЗП1 ЗП3 СП4		ЗП3						СП4			СП4 СП5 СП6	НП5		ЗП3 НП5
РН 29	ЗП1 ЗП3 СП4		ЗП3								НП5		СП4 НП5		ЗП3 НП5
РН 30	ЗП1 ЗП3 СП4		ЗП3						СП4					СП4 НП5	ЗП3 НП5
РН 31					ЗП2 ЗП СП43										ЗП3 НП5
РН 32	ЗП1 ЗП3 СП4	ЗП3	ЗП3					СП4 СП5 СП6	СП4	СП4 СП5 СП6		СП4 СП5 СП6		СП4	ЗП3 НП5
РН 33							ЗП2	СП4 СП5 СП6							ЗП3 НП5
РН 34	ЗП1 ЗП3 СП4				ЗП2 ЗП3 СП4										ЗП3 НП5
РН 35	ЗП1 ЗП3 СП4				ЗП2 ЗП3 СП4	ЗП3 СП4	ЗП2	СП4 СП5 СП6	СП4			СП4 СП5 СП6	СП4	СП4	
РН 36	ЗП1 ЗП3 ЗП3 СП4	ЗП3	ЗП3		ЗП2 ЗП3 СП4	ЗП3 СП4		СП4 СП5 СП6							

Програмні результати навчання	Компетентності														
	Інтегральна компетентність														
	Загальні компетентності					Спеціальні (фахові) компетентності									
	ЗК 12	ЗК 13	ЗК 14	ЗК 15	ЗК 16	СК 15	СК 16	СК 17	СК 18	СК 19	СК 20	СК 21	СК 22	СК 23	СК 24
РН 37	ЗП1 СП4	ЗП3	ЗП3			ЗП3 СП4		СП4 СП5 СП6		СП4 СП5 СП6	НП5	СП4 СП5 СП6	СП4		
РН 38		ЗП3	ЗП3			ЗП3		СП4 СП5 СП6			НП5				
РН 39	ЗП1 ЗП3 СП4		ЗП3			ЗП3 СП4	ЗП2	СП4 СП5 СП6				СП4 СП5 СП6	СП4	СП4	
РН 40				НП5									НП5		НП5
РН 41				НП5									НП5		НП5