

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»



ЗАТВЕРДЖУЮ
Ректор НТУ «ХПІ»

Євген СОКОЛ

04 2024 р.

**ОСВІТНЬО-НАУКОВА ПРОГРАМА
«КІБЕРБЕЗПЕКА»**

другого (магістерського) рівня вищої освіти

за спеціальністю 125 - Кібербезпека та захист інформації

галузі знань 12 - Інформаційні технології

кваліфікація магістр з кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО

Вченою радою НТУ «ХПІ»

Голова вченої ради

Леонід ТОВАЖНЯНСЬКИЙ

Протокол № 1 від «26» квітня 2024 р.

Харків 2024 р.

ЛИСТ ПОГОДЖЕННЯ

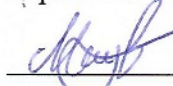
освітньо-наукової програми «Кібербезпека»

Рівень вищої освіти	другий (магістерський)
Галузь знань	12 – Інформаційні технології
Спеціальність	125 – Кібербезпека та захист інформації
Кваліфікація	магістр з кібербезпеки та захисту інформації

ПОГОДЖЕНО

Робочою групою ОНП із спеціальності
«Кібербезпека та захист інформації»

Гарант ОНП

 Станіслав МІЛЕВСЬКИЙ

« 22 » 04 2024 р.

ПОГОДЖЕНО

Завідувач кафедри
кібербезпеки

 Сергій ЄВСЕЄВ

« 22 » 04 2024 р.

ПОГОДЖЕНО

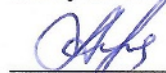
здобувач вищої освіти
(член робочої групи ОНП)
№ групи КН-М1123

 Єлизавета СОЛОВЙОВА

« 20 » 04 2024 р.

РЕКОМЕНДОВАНО

Методичною радою НТУ «ХПІ»
Заступник голови методичної ради

 Руслан МИГУЩЕНКО

« 22 » 04 2024 р.

ПОГОДЖЕНО

Директор навчально-наукового інституту
комп'ютерних наук та інформаційних
технологій

 Михайло ГОДЛЕВСЬКИЙ

« 22 » 04 2024 р.

ВЗАГОД
Нурієв Нур

РЕЦЕНЗЕНТИ:

Продуктивні зауваження та відгуки на проєкт освітньо-наукової програми одержано від:

1. Молодецька Катерина Валеріївна, доктор технічних наук, професор, Керівник навчально-наукового центру інформаційних технологій Поліського національного університету
2. Ковтун Владислав Юрійович, кандидат технічних наук, доцент, директор ТОВ “Сайфер”
3. Головашич Сергій Олександрович, кандидат технічних наук, доцент директор ТОВ “Мікрокрипт Текнолоджіс”
4. Волощук Олена Борисівна, кандидат технічних наук, керівник освітніх програм ТОВ “Distributed Lab”.

РЕЦЕНЗІЯ-ВІЩУК

на освітньо-наукову програму "Кібербезпека"
другого (магістерського) рівня вищої освіти
спеціальності 125 "Кібербезпека та захист інформації"
кафедри кібербезпеки Національного технічного університету
"Харківський політехнічний інститут"

Освітньо-наукова програма (ОНП) "Кібербезпека" підготовки здобувачів вищої освіти другого (магістерського) рівня вищої освіти спеціальності 125 "Кібербезпека та захист інформації" галузі знань 12 "Інформаційні технології" розроблена науково-педагогічними працівниками Національного технічного університету "Харківський політехнічний інститут". Керівник проектної групи - гарант освітньої програми д.т.н., проф. Мілов О. В. Подана на рецензування ОНП розроблена на основі стандарту вищої освіти України зі спеціальності 125 "Кібербезпека та захист інформації" другого (магістерського) рівня вищої освіти, затвердженого наказом МОН України від 18 березня 2021 р. N. 332. Представлена ОНП містить профіль освітньої програми за відповідною спеціальністю, перелік компонент освітньо-наукової програми та їх логічну послідовність, структурно-логічну схему, інформацію про форму атестації здобувачів вищої освіти.

Метою освітньої програми є підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки, використовувати і впроваджувати технології та застосовувати засоби захисту в системах безпеки контуру бізнес-процесів. Критичний аналіз освітньої програми показав, що зміст програми повністю враховує інтегральну, загальну й фахові компетентності, які передбачено стандартом. Це забезпечує досягнення здобувачами вищої освіти програмних результатів навчання.

Програмні результати ОНП корелюють із складовими професійної компетентності, які формують фундаментальні знання та фахові навички, а загальні компетентності забезпечують розвиток навичок soft skills та сприяють

формування свідомої громадянської позиції випускника з усталеними цінностями, здатністю до фахового розвитку і самовдосконалення. Фокус освітньо-наукової програми направлено на побудову комплексних систем захисту інформації для забезпечення безпеки контуру бізнес-процесів на основі сучасних технологій та програмних застосунків, в умовах розвитку цифрової економіки, додатково підкреслює сучасну спрямованість програми.

Вважаю, що освітньо-наукова програма підготовки здобувачів вищої освіти другого (магістерського) рівня вищої освіти галузі знань 12 "Інформаційні технології" за спеціальністю 125 "Кібербезпека та захист інформації" у Національному технічному університеті "Харківський політехнічний інститут" характеризується системністю і цільовим підходом до підготовки фахівців з кібербезпеки, відповідає сучасному рівню розвитку науки і практики освітньої діяльності та може бути рекомендована до впровадження в освітньому процесі університету.

Керівник навчально-наукового
центру інформаційних технологій

Поліського національного університету,

доктор технічних наук, професор

Катерина МОЛОДЕЦЬКА



САЙФЕР

Системи •Захисту інформації

ТОВ «САЙФЕР fГ»

Адреса: 04107, Київ, вул. Нагірна, 25-27

Тел./Факс: (044) 484-46-17, 484-46-12, 483-03-22

E-mail: info@cipler.com.ua

<https://cipler.com.ua>

РЕЦЕНЗІЯ-ВІДГУК

на освітньо-наукову програму "Кібербезпека"
другого (магістерського) рівня вищої освіти
спеціальності 125 "Кібербезпека та захист інформації"
Національного технічного університету "Харківський політехнічний
інститут"

Освітньо-наукова програма "Кібербезпека" за спеціальністю 125 "Кібербезпека та захист інформації", яку втілено до навчального процесу на другому (магістерському) рівні вищої освіти у Національному технічному університеті "Харківський політехнічний інститут", відповідає сучасним вимогам ІТ-індустрії та відповідному стандарту вищої освіти.

Програма спрямована на підготовку фахівців здатних виконувати професійні роботи та виконувати наукові дослідження у галузі забезпечення безпеки у інформаційно-комунікаційних системах та загальної безпеки інформаційних технологій. Схема навчального процесу є чіткою та зрозумілою й відбиває останні напрямки технологій кібербезпеки та досліджень у цій галузі. Навчальні дисципліни, що забезпечують освітньо-наукову програму, відповідають світовим аналогам та запитам роботодавців. Об'єкт та цілі програми є чіткими та зрозумілими. Засоби та обладнання, що застосовується у навчальному процесі повсюдню надають студентам можливості отримати не тільки теоретичні знання, але й набути практиці у рішенні завдань, які моделюють існуючі виробничі процеси та інциденти кібербезпеки.

Програма обговорювалась зі стейкхолдерами, враховує побажання здобувачів вищої освіти та спрямована на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю 125 "Кібербезпека та захист інформації". Результати навчання відповідають стандарту освіти та вимогам організацій та компаній, що зараз потребують фахівців відповідного профілю.

В цілому освітня-наукова програма "Кібербезпека" другого (магістерського) рівня вищої освіти спеціальності 125 "Кібербезпека та захист інформації" має всі необхідні складові для підготовки сучасних кваліфікованих фахівців, які будуть ефективно вирішувати теоретичні та практичні питання щодо забезпечення кібербезпеки та захисту інформації, як на рівні невеликих організацій та підприємств, так й в умовах розгортання та супроводження корпоративних рішень.

Директор ТОВ "Сайфер ІТ",
кандидат технічних наук



Владислав КОВТУН

ЗАТВЕРДЖУЮ:

Генеральний директор

ТОВ «Мікрокрипт Текнолоджіс»



І.ІСІРІТ

СЛ

«___» -----

2024 р.

РЕЦЕНЗІЯ-ВІДГУК

на освітньо-наукову програму "Кібербезпека",

другого (магістерського) рівня вищої освіти,

спеціальності 125 "Кібербезпека та захист інформації"

кафедри кібербезпеки Національного технічного університету

"Харківський політехнічний інститут"

Кібербезпека розглядає захист функціонування нової сутності – кіберпростору, середовища, що виникло в результаті взаємодії людей, програмного забезпечення, Інтернет сервісів з використанням технічних пристроїв і мережевих зв'язків.

Якщо раніше проблема безпеки в кіберпросторі стосувалася тільки окремих компаній, то з розвитком Інтернет і мобільного банкінгу, Інтернету речей та багатьох інших сучасних технологій - безпека в кіберпросторі стосується кожного з нас. Фахівці з кібербезпеки забезпечують захист життєво важливих інтересів людини та суспільства, своєчасне виявлення, запобігання і нейтралізацію реальних та потенційних загроз у сфері функціонування інформаційних, комп'ютерних та кіберфізичних систем.

Підготовка якісних спеціалістів у сфері захисту інформації (кібербезпеки) є одним з найбільших викликів сьогодення через необхідність постійного **оновлення** змісту освіти. Освітня програма "Кібербезпека" сформована кафедрою кібербезпеки Національного технічного університету

"Харківський політехнічний інститут", відповідно до останніх тенденцій розвитку спеціальності та повністю реалізує результати навчання передбачені стандартом вищої освіти за спеціальністю 125 "Кібербезпека та захист інформації". Освітньо-наукова програма має ЧПКО визначено ЦЦП, яку враховують основні її особливості - підготовки фахівця з інформаційної безпеки широкого профілю зі знанням технологій програмування. Мобільність програми забезпечує своєчасне корегування в умовах стрімкого розвитку цієї спеціальності.

Однією з основних проблем реалізації освітнього процесу за спеціальністю 125 "Кібербезпека та захист інформації" є відсутність під час навчання можливості отримати знання та навички від професіоналів-практиків. В рамках викладання за освітньою програмою, що рецензується, залучено викладачів-практиків.

Вважаємо, що Освітньо-наукова програма "Кібербезпека", що складена та запропонована кафедрою кібербезпеки Національного технічного університету "Харківський політехнічний інститут", має всі необхідні компоненти для підготовки кваліфікованих фахівців які будуть впроваджені на ринку праці.

Генеральний директор
ТОВ "Мікрокрипт Текнолоджіс",
кандидат технічних наук



The image shows a handwritten signature in blue ink over a blue circular official stamp. The stamp contains the text "ТОВ «Мікрокрипт Текнолоджіс»" (JSC "Microcrypt Technologies") and "Україна" (Ukraine). There are also some smaller, less legible markings within the stamp.

РЕЦЕНЗІЯ-ВЩГУК

на освітньо-наукову програму "Кібербезпека"
другого (магістерського) рівня вищої освіти
спеціальності 125 "Кібербезпека та захист інформації"
кафедри кібербезпеки Національного технічного університету
"Харківський політехнічний інститут"

Забезпечення безпеки в кіберпросторі є однією з найактуальніших та найскладніших проблем сьогодення у зв'язку із великими об'ємом даних, які мають бути захищені, та постійною зміною та вдосконаленням відповідних технологій. Кібербезпека та захист інформації на сьогодні є спеціальністю, яка включає в себе декілька великих напрямів: підготовки (побудова архітектури безпеки, управління ризиками, використання професійних стандартів та фреймворки криптології, технічний захист інформації тощо).

Таким чином підготовка фахівців з кібербезпеки за освітньо-науковою програмою "Кібербезпека" другого (магістерського) рівня вищої освіти є актуальним напрямом освітньої діяльності університету, що дозволяє готувати конкурентоспроможних випускників в галузі безпеки об'єктів критичної інфраструктури.

Схема підготовки фахівців за освітньо-науковою програмою, що акредитується, є правильно побудованою: врахована необхідність отримання студентами знань з дисциплін професійного змісту, які повністю покривають результати навчання, що передбачені стандартом вищої освіти зі спеціальності 125 "Кібербезпека та захист інформації" другого (магістерського) рівня вищої освіти.

В рамках освітньо-наукової програми "Кібербезпека", яка складена кафедрою кібербезпеки Національного технічного університету "Харківський політехнічний інститут", автори змогли досить органічно та логічно сформулювати схему підготовки майбутнього фахівця, яка, з одного

боку, дозволяє освітній програмі забезпечувати реалізацію результатів навчання передбачених стандартом вищої освіти в повному обсязі, а, з іншого боку, завдяки акценту на технологіях програмування випускники мають можливість працевлаштовуватися не тільки за спеціальністю, але і в ІТ сфері загалом.

Вважаємо, що освітньо-наукова програма "Кібербезпека" другого (магістерського) рівня вищої освіти, яка складена кафедрою кібербезпеки Національного технічного університету "Харківський політехнічний інститут", має всі необхідні компоненти для підготовки кваліфікованих фахівців, які будуть затребувані на ринку праці як за спеціальністю, так і в цілому на ринку інформаційних технологій.

Керівник освітніх програм
Компанії Distributed Lab,
кандидат технічних наук



Олена ВОЛОЩУК

ПЕРЕДМОВА

Відповідає Стандарту вищої освіти другого (магістерського) рівня галузі знань «Інформаційні технології», спеціальністю 125 «Кібербезпека та захист інформації», який затверджено наказом Міністерства освіти і науки України від 18.03.2021 р. № 332.

Розроблено робочою групою ОНП «Кібербезпека»

Навчально-наукового інституту комп'ютерних наук та інформаційних технологій Національного технічного університету «Харківський політехнічний інститут»

у складі:

Гарант освітньо-наукової програми

Мілевський Станіслав Валерійович, кандидат економічних наук, доцент, доцент кафедри кібербезпеки.

Члени робочої групи ОНП :

1. Євсєєв Сергій Петрович, доктор технічних наук, професор, завідувач кафедри кібербезпеки.

2. Мілов Олександр Володимирович, доктор технічних наук, професор, професор кафедри кібербезпеки.

3. Король Ольга Григорівна, кандидат технічних наук, доцент, доцент кафедри кібербезпеки.

4. Соловійова Єлизавета Олександрівна, студентка групи КН- М1123.

1. ПРОФІЛЬ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ СПЕЦІАЛЬНОСТІ 125 – КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

1 – Загальна інформація	
Вищий навчальний заклад та структурний підрозділ	Національний технічний університет «Харківський політехнічний інститут», Навчально-науковий інститут комп'ютерних наук та інформаційних технологій кафедра кібербезпеки
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр Магістр з кібербезпеки та захисту інформації
Офіційна назва освітньо-наукової програми	Освітньо-наукова програма «Кібербезпека»
Тип диплому та обсяг освітньо-наукової програми	Диплом магістра, одиничний, 120 кредитів ЄКТС, термін навчання 1 рік 9 місяців
Наявність акредитації	відсутня
Цикл/рівень	другий (магістерський) рівень вищої освіти; НРК України – 7 рівень, FQ-EHEA– другий цикл, EQF LLL – 7 рівень
Передумови	Наявність освітнього ступеня бакалавра
Мова викладання	Українська, англійська
Термін дії освітньо-наукової програми	Відповідно до терміну дії сертифікату про акредитацію. Переглядається щорічно
Посилання на постійне розміщення опису освітньо-наукової програми	Інтернет-адреса постійного розміщення опису освітньої програми https://cybersecurity.kpi.kharkov.ua
2 – Мета освітньо-наукової програми	
Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки, використовувати і впроваджувати технології та застосовувати засоби захисту в соціокіберфізичних системах (об'єктах критичної інфраструктури).	
3 – Характеристика освітньо-наукової програми	
Предметна область (галузь знань, спеціальність)	Галузь знань: 12 “Інформаційні технології” Спеціальність: 125 “Кібербезпека та захист інформації” Об'єкти вивчення: – 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; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; – інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків);

	– інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою; – технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. Цілі навчання: Підготовка фахівців, здатних розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. Теоретичний зміст предметної області 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 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. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. Інструменти та обладнання. Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, 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.
Орієнтація освітньо-наукової програми	Професійна підготовка фахівців у сфері кібербезпеки та захисту інформації.
Основний фокус освітньо-наукової програми та спеціалізації	Поглиблене вивчення механізмів та методів кіберзахисту соціокіберфізичних систем (об’єктів критичної інфраструктури) з комплексуванням з методами штучного інтелекту в умовах постквантового періоду. Отримання сертифікатів курсів академії Cisco, сприяє підвищенню конкурентноспроможності на ринку праці, удосконаленню механізмів многоконтурних систем захисту соціокіберфізичних систем (об’єктів критичної інфраструктури). Ключові слова: кібербезпека, цифрова криміналістика, етнічний

	хакінг.
Особливості програми	Особливостями програми є формування у здобувачів навичок побудови многоконтурних систем захисту в соціокіберфізичних систем (об'єктах критичної інфраструктури) для забезпечення безпеки контуру бізнес-процесів в умовах постквантового періоду (появи повномасштабного квантового комп'ютера). Орієнтація на партнерство із вітчизняними та закордонними закладами освіти та науки, приватним сектором, науковцями та практиками, участь в міжнародних програмах спільних дипломів. Можливість навчатися англійською мовою.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Фахівці з кібербезпеки та захисту інформації можуть працювати, згідно з чинною редакцією Національного класифікатора України: Класифікатор професій (Зміна № 10 до ДК 003:2010), а саме: 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;
Подальше навчання	Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі освіти дорослих.
5 – Викладання та оцінювання	
Викладання та навчання	У процесі викладання передбачено застосування таких навчальних технологій, як: лекції, лабораторні роботи, практичні заняття, робота в малих групах, презентації, що розвивають комунікативні та лідерські навички, самостійна робота з науковими та технічними джерелами.
Оцінювання	Рейтингова система оцінювання. Поточний та підсумковий контроль знань (опитування, контрольні й індивідуальні завдання, тестування тощо), заліки та іспити (усні і письмові), захист навчальних і реальних проєктів з презентацією, публічний захист кваліфікаційної роботи.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності	КЗ-1. Здатність застосовувати знання у практичних ситуаціях. КЗ-2. Здатність проводити дослідження на відповідному рівні. КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

	КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Спеціальні (фахові) компетентності	КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. КФ10. 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. КФ11. 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 (визначені стандартом вищої освіти спеціальності)	РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН3. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. РН10. Забезпечувати безперервність бізнес\операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес\операційних процесів, а також аналізувати і надавати оцінку

	ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та/або кібербезпеки в цілому. РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. РН16. 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 та прийняття рішень. РН17. 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. РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та/або кібербезпеки. РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. РН21. Використовувати методи натурального, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та 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 та довідкової літератури та іншої доступної інформації. РН24. Планувати та 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. РН25. Оцінювати ефективність та 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). До викладання залучаються викладачі-практики, фахівці та співробітники ІТ-компаній, а також закордонні фахівці.
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, кіберполігон.
Інформаційне та навчально-методичне забезпечення	Відповідає технологічним вимогам щодо навчально-методичного та інформаційного забезпечення 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). Доступ до електронного репозитарію НТУ «ХПІ» (eNTUKhPIIR) через мережу Інтернет (у тому числі університетську мережу Wi-Fi).
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між Національним технічним університетом «Харківський політехнічний інститут» та провідними технічними університетами України. Регламентується «Положенням про академічну мобільність студентів, аспірантів, докторантів, науково-педагогічних та наукових працівників НТУ «ХПІ».
Міжнародна кредитна мобільність	На основі двосторонніх договорів.
Навчання іноземних здобувачів освіти	Після отримання Сертифікату про акредитацію освітньої програми передбачається підготовка іноземців та осіб без громадянства.

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

2.1 Перелік компонент ОНП

Код н/д	Компоненти освітньо-професійної програми	Кількість кредитів	Форма підсумкового контролю
1. Обов'язкові освітні компоненти ОНП (здобувачі вищої освіти – громадяни України)			
1.1 Загальна підготовка			
ЗП 1	Англійська мова в академічних застосунках	4	Екзамен
ЗП 2	Інноваційне підприємництво та управління стартап-проектами	3	Екзамен
1.2. Спеціальна (фахова) підготовка			
СП1	Мережева та хмарна безпека	4	Екзамен
СП2	Безпека та анонімність роботи в Інтернеті	4	Екзамен
СП3	Цифрова криміналістика	4	Залік
СП4	Етичний хакінг	3	Екзамен
СП5	Основи управління в проєктах галузі кібербезпеки та захисту інформації	4	Залік
СП6	Математичні моделі управління ІТ-проектами	4	Залік
1.3. Наукова підготовка			
НП1	Основи наукових досліджень	5	Екзамен
НП2	Філософські проблеми сучасного наукового пізнання	4	Екзамен
НП3	Сучасні проблеми постквантової криптографії	4	Залік
НП4	Аналіз шкідливих програм	5	Залік
НП5	Авторське право у цифровому суспільстві	4	Залік
НП6	Виявлення вторгнень у комп'ютерні мережі (мережеві аномалії)	4	Залік
НП7	Технології управління безпекою бізнес-процесів	4	Залік
2. Практична підготовка			
ПП	Науково-дослідницька практика	19	Залік
3. Атестація			
НП	Атестація	11	
Загальний обсяг обов'язкових компонентів		90	
4. Вибіркові освітні компоненти ОНП (здобувачі вищої освіти – громадяни України)			
4.1 Освітні компоненти вільного вибору професійної підготовки згідно переліку			
ОКВП1	ОК ВВ ПП 1	4	Залік
ОКВП2	ОК ВВ ПП 2	4	Залік
ОКВП3	ОК ВВ ПП 3	4	Залік
4.2. Освітні компоненти вільного вибору загальної підготовки згідно переліку			

OKB31	OK BB 1	3	Залік
OKB32	OK BB 2	3	Залік
4.3. Освітні компоненти вільного вибору науково-професійного спрямування згідно переліку			
OKBH1	OK BB НПС 1	4	Залік
OKBH2	OK BB НПС 2	4	Залік
OKBH3	OK BB НПС 3	4	Залік
Загальний обсяг вибіркового компонента:		30	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ:		120	

2.2. Розподіл змісту освітньо-наукової програми за групами компонентів та циклами підготовки

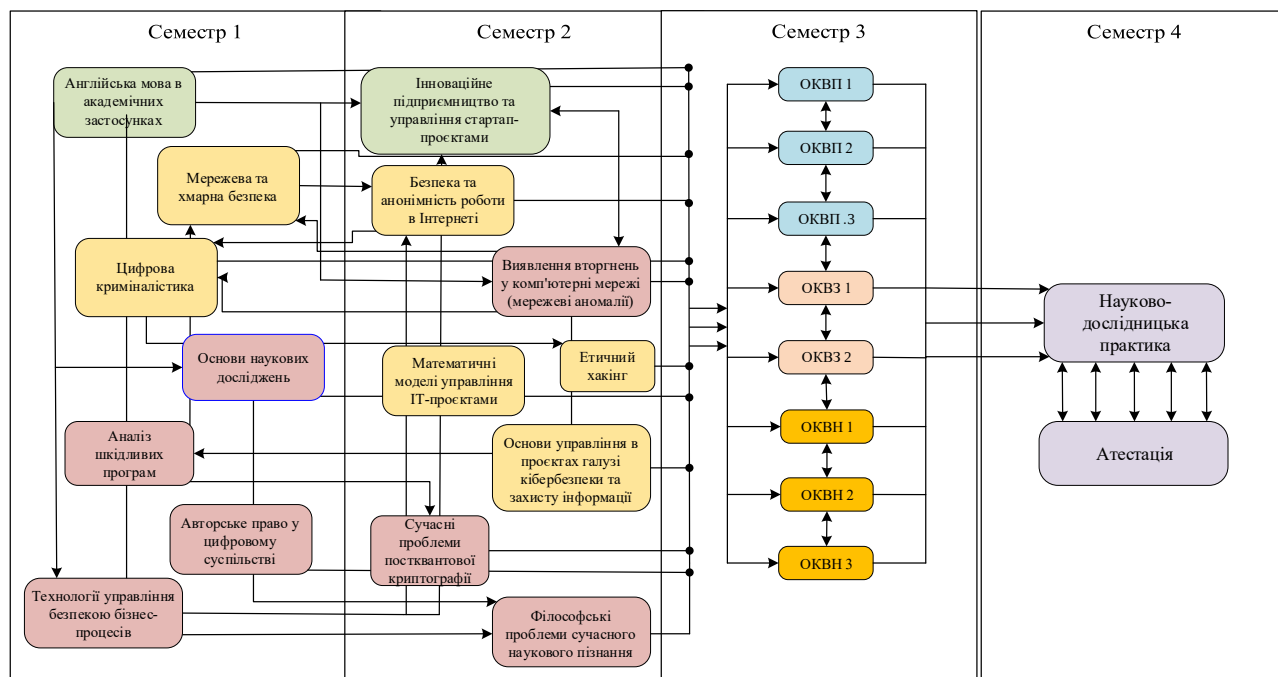
№п/п	Цикл підготовки	Обсяг навчального навантаження здобувача вищої освіти (кредитів ECTS / %)		
		Обов'язкові компоненти освітньо- наукової програми	Вибіркові компоненти освітньо- наукової програми	Всього за весь термін навчання
1	Загальна підготовка	7 / 5,8	-	7 / 5,8
2	Спеціальна (фахова) підготовка	53 / 44,2	-	53 / 44,2
3	Наукова підготовка	30/25	-	30/25
4	Дисципліни вільного вибору	-	30 / 25	30 / 25
Всього за весь термін навчання		90 / 75	30 / 25	120 / 100

3. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі публічного захисту кваліфікаційної роботи.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації. Кваліфікаційна робота має бути розміщена на офіційному сайті (або у репозитарії) закладу вищої освіти або його підрозділу. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

4. СТРУКТУРНО-ЛОГІЧНА СХЕМА

СТРУКТУРНО-ЛОГІЧНА СХЕМА



Семестр	Зміст навчальної діяльності
9	ЗП 1, ЗП 3, СП 2, СП 3
10	ЗП 2, СП 1, СП 4, НП 1
11	СП 5, НП 2, НП 3
12	ПП

5. МАТРИЦЯ ВІДПОВІДНОСТІ ВИЗНАЧЕНИХ СТАНДАРТОМ КОМПЕТЕНТНОСТЕЙ / РЕЗУЛЬТАТІВ НАВЧАННЯ ДЕСКРИПТОРАМ НРК

Класифікація компетентностей (результатів навчання) за НРК	Знання Зн1 Спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері професійної діяльності або галузі знань і є основою для оригінального мислення та проведення досліджень, критичне осмислення проблем у галузі та на межі галузей знань	Уміння/Навички Ум1 Спеціалізовані уміння/навички розв'язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур Ум2 Здатність інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах Ум3 Здатність розв'язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності	Комунікація К1 Зрозуміле і недвозначне донесення власних знань, висновків та аргументації до фахівців і нефахівців, зокрема до осіб, які навчаються	Відповідальність і автономія АВ1 Управління робочими або навчальними процесами, які є складними, непередбачуваними та потребують нових стратегічних підходів АВ2 Відповідальність за внесок до професійних знань і практики та/або оцінювання результатів діяльності команд та колективів АВ3 Здатність продовжувати навчання з високим ступенем автономії
Загальні компетентності				
КЗ1	Зн1,	Ум1, Ум3	К1	АВ1, АВ2
КЗ2	Зн1,	Ум1, Ум2, Ум3		АВ2, АВ3
КЗ3	Зн1	Ум2, Ум3		АВ1
КЗ4	Зн1	Ум3		АВ1, АВ2
КЗ5	Зн1	Ум2	К1	АВ1
Спеціальні (фахові) компетентності				
КФ1	Зн1	Ум2		АВ2
КФ2	Зн1,	Ум2		АВ2
КФ3	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2
КФ4	Зн1,	Ум1, Ум2	К1	АВ1, АВ2
КФ5	Зн1,	Ум1, Ум2	К1	АВ1, АВ2
КФ6	Зн1	Ум1, Ум2	К1	АВ1
КФ7	Зн1	Ум1, Ум2	К1	АВ1
КФ8	Зн1	Ум1, Ум2	К1	АВ1
КФ9	Зн1	Ум1, Ум2	К1	АВ1
КФ10	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2
Додатково для освітньо-наукових програм*				
КФ11*	Зн1,	Ум1, Ум2, Ум3		АВ2, АВ3

6. МАТРИЦЯ ВІДПОВІДНОСТІ ВИЗНАЧЕНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ, КОМПЕТЕНТНОСТЕЙ ТА ОСВІТНІХ КОМПОНЕНТІВ

[illegible]

Програмні результати навчання	Компетентності															
	Інтегральна компетентність															
	Загальні компетентності					Спеціальні (фахові) компетентності										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11*
	СП1, СП2, СП4, СП5, СП6, НП1, НП2, НП3, НП4, НП5, НП6, НП7, ПП НП					СП1, СП4, СП6, НП1, НП3, НП4, НП6, ПП НП										НП2, НП3, НП4, НП6, НП7, ПП НП
РН 4	ЗП1, ЗП3, СП1, СП2, СП4, СП5, СП6, НП1, НП2, НП3, НП4, НП5, НП6, НП7, ПП НП	СП5, НП1, НП3, НП5, НП7, ПП НП	СП5, СП6, НП1, НП2, НП3, НП5, НП7, ПП НП	ЗП3, СП2, СП5, СП6, НП1, НП3, НП4, НП5, НП6, НП7, ПП НП		ЗП2, ЗП3, СП1, СП4, СП6, НП1, НП3, НП4, НП6, ПП НП	ЗП3, СП3, СП5, НП1, НП2, НП3, НП4, НП5, НП6, НП7, ПП НП									
РН 5			СП5,		СП1,		ЗП3,									ЗП3,

Програмні результати навчання	Компетентності															
	Інтегральна компетентність															
	Загальні компетентності					Спеціальні (фахові) компетентності										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11*
			СП6, НП1, НП2, НП3, НП5, НП7, ПП НП		СП2, СП3, СП5, НП1, НП2, НП3, НП4, НП5, НП7, ПП НП		СП3, СП5, НП1, НП2, НП3, НП4, НП5, НП6, НП7, ПП НП									НП1, НП2, НП3, НП4, НП6, НП7, ПП НП
РН 6	ЗП1, ЗП3, СП1, СП2, СП4, СП5, СП6, НП1, НП2, НП3, НП4, НП5, НП6, НП7, ПП НП			ЗП3, СП2, СП5, СП6, НП1, НП3, НП4, НП5, НП6, НП7, ПП НП		ЗП2, ЗП3, СП1, СП2, СП4, СП6, НП1, НП3, НП4, НП6, ПП НП		ЗП3, СП1, СП2, СП4, СП5, СП6, НП1, НП3, НП4, НП6, ПП НП		ЗП2, ЗП3, СП1, СП2, СП4, СП5, НП1, НП2, НП4, НП5, НП6, НП7, ПП НП	ЗП2, ЗП3, СП6, НП1, НП3, НП4, НП5, НП6, ПП НП	ЗП3, СП1, СП2, СП4, НП1, НП3, НП4, НП6, НП7, ПП НП		ЗП3, СП1, СП6, НП1, НП4, НП5, НП6, НП7, ПП НП		
РН 7	ЗП1, ЗП3, СП1, СП2,		СП5, СП6, НП1, НП2,				ЗП3, СП3, СП5, НП1,									

Програмні результати навчання	Компетентності															
	Інтегральна компетентність															
	Загальні компетентності					Спеціальні (фахові) компетентності										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11*
	СП4, СП5, СП6, НП1, НП2, НП3, НП4, НП5, НП6, НП7, ПП НП		НП3, НП5, НП7, ПП НП				НП2, НП3, НП4, НП5, НП6, НП7, ПП НП									
РН 8	ЗП1, ЗП3, СП1, СП2, СП4, СП5, СП6, НП1, НП2, НП3, НП4, НП5, НП6, НП7, ПП НП	СП5, НП1, НП5, НП7, ПП НП		ЗП3, СП2, СП5, СП6, НП1, НП3, НП4, НП5, НП6, НП7, ПП НП	СП1, СП2, СП3, СП5, НП1, НП2, НП3, НП5, НП7, ПП НП			ЗП3, СП1, СП2, СП4, СП5, СП6, НП1, НП3, НП4, НП6, ПП НП						ЗП3, СП1, СП6, НП1, НП4, НП5, НП6, НП7, ПП НП	НП1, НП2, НП4, НП5, НП7, ПП НП	
РН 9	ЗП1, ЗП3, СП1,	СП5, НП1, НП3,	СП5, СП6, НП1,	ЗП3, СП2, СП5,					ЗП3, СП1, СП3,					ЗП3, СП1, СП6,	НП1, НП2, НП4,	

Програмні результати навчання	Компетентності															
	Інтегральна компетентність															
	Загальні компетентності					Спеціальні (фахові) компетентності										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11*
	СП2, СП4, СП5, СП6, НП1, НП2, НП3, НП4, НП5, НП6, НП7, ПП НП	НП5, НП7, ПП НП	НП2, НП3, НП5, НП7, ПП НП	СП6, НП1, НП3, НП4, НП5, НП6, НП7, ПП НП					СП4, СП5, СП6, НП1, НП3, НП4, НП5, НП6, НП7, ПП НП					НП1, НП4, НП5, НП6, НП7, ПП НП	НП5, НП7, ПП НП	
PH 10	ЗП1, ЗП3, СП1, СП2, СП4, СП5, СП6, НП1, НП2, НП3, НП4, НП5, НП6, НП7, ПП НП		СП5, СП6, НП1, НП2, НП3, НП5, НП7, ПП НП	ЗП3, СП2, СП5, СП6, НП1, НП3, НП4, НП5, НП6, НП7, ПП НП						ЗП2, ЗП3, СП1, СП2, СП4, НП1, НП2, НП4, НП5, НП6, НП7, ПП НП				ЗП3, СП1, СП6, НП1, НП4, НП5, НП6, НП7, ПП НП		
PH 11	ЗП1, ЗП3,		СП5, СП6,	ЗП3, СП2,							ЗП2, ЗП3,				НП1, НП2,	

Програмні результати навчання	Компетентності															
	Інтегральна компетентність															
	Загальні компетентності					Спеціальні (фахові) компетентності										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11*
	СП1, СП2, СП4, СП5, СП6, НП1, НП2, НП3, НП4, НП5, НП6, НП7, ПП НП		НП1, НП2, НП3, НП5, НП7, ПП НП	СП5, СП6, НП1, НП3, НП4, НП5, НП6, НП7, ПП НП							СП6, НП1, НП3, НП4, НП5, НП6, ПП НП				НП3, НП4, НП5, НП7, ПП НП	
PH 12	ЗП1, ЗП3, СП1, СП2, СП4, СП5, СП6, НП1, НП2, НП3, НП4, НП5, НП6, НП7, ПП НП		СП5, СП6, НП1, НП2, НП3, НП5, НП7, ПП НП	ЗП3, СП2, СП5, СП6, НП1, НП3, НП4, НП5, НП6, НП7, ПП НП					ЗП3, СП1, СП3, СП4, СП5, СП6, НП1, НП3, НП4, НП5, НП6, НП7, ПП НП		ЗП3, СП1, СП2, СП4, НП1, НП3, НП4, НП6, НП7, ПП НП				НП1, НП2, НП4, НП5, НП7, ПП НП	
PH 13	ЗП1,		СП5,	ЗП3,									ЗП3,		НП1,	

Програмні результати навчання	Компетентності															
	Інтегральна компетентність															
	Загальні компетентності					Спеціальні (фахові) компетентності										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11*
	ЗП3, СП1, СП2, СП4, СП5, СП6, НП1, НП2, НП3, НП4, НП5, НП6, НП7, ПП НП		СП6, НП1, НП2, НП3, НП5, НП7, ПП НП	СП2, СП5, СП6, НП1, НП3, НП4, НП5, НП6, НП7, ПП НП									СП1, НП1, НП3, НП4, НП6, НП7, ПП НП		НП2, НП4, НП5, НП7, ПП НП	
РН 14	ЗП1, ЗП3, СП1, СП2, СП4, СП5, СП6, НП1, НП2, НП3, НП4, НП5, НП6, НП7, ПП НП		СП5, СП6, НП1, НП2, НП3, НП5, НП7, ПП НП	ЗП3, СП2, СП5, СП6, НП1, НП3, НП4, НП5, НП6, НП7, ПП НП					ЗП3, СП1, СП3, СП4, СП5, СП6, НП1, НП3, НП4, НП5, НП6, НП7, ПП НП					ЗП3, СП1, СП6, НП1, НП4, НП5, НП6, НП7, ПП НП	НП1, НП2, НП4, НП5, НП7, ПП НП	

Програмні результати навчання	Компетентності															
	Інтегральна компетентність															
	Загальні компетентності					Спеціальні (фахові) компетентності										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11*
PH 15				ЗПЗ, СП2, СП5, СП6, НП1, НП3, НП4, НП5, НП6, НП7, ПП НП	СП1, СП2, СП3, СП5, НП1, НП2, НП3, НП5, ПП НП										НП1, НП2, НП4, НП5, НП7, ПП НП	
PH 16	ЗП1, ЗП3, СП1, СП2, СП4, СП5, СП6, НП1, НП2, НП3, НП4, НП5, НП6, НП7, ПП НП	СП5, НП1, НП3, НП5, НП7, ПП НП	СП5, СП6, НП1, НП2, НП3, НП5, НП7, ПП НП	ЗПЗ, СП2, СП5, СП6, НП1, НП3, НП4, НП5, НП6, НП7, ПП НП				ЗПЗ, СП1, СП2, СП4, СП5, СП6, НП1, НП3, НП4, НП6, ПП НП	ЗПЗ, СП1, СП3, СП5, СП6, НП1, НП3, НП4, НП5, НП6, НП7, ПП НП	ЗП2, ЗП3, СП1, СП2, СП4, НП1, НП1, НП2, НП4, НП5, НП6, НП7, ПП НП	ЗП2, ЗП3, СП5, СП6, НП1, НП3, НП4, НП5, НП6, ПП НП	ЗП3, СП1, СП2, СП4, НП1, НП3, НП4, НП6, НП7, ПП НП		ЗПЗ, СП1, СП6, НП1, НП4, НП5, НП6, НП7, ПП НП	НП1, НП2, НП4, НП5, НП7, ПП НП	ЗПЗ, НП1, НП2, НП3, НП4, НП6, НП7, ПП НП
PH 17								ЗПЗ, СП1, СП2,							НП1, НП2, НП4,	

Програмні результати навчання	Компетентності															
	Інтегральна компетентність															
	Загальні компетентності					Спеціальні (фахові) компетентності										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11*
								СП4, СП5, СП6, НП1, НП3, НП4, НП6, ПП НП							НП5, НП7, ПП НП	
РН 18	ЗП1, ЗП3, СП1, СП2, СП4, СП5, СП6, НП1, НП2, НП3, НП4, НП5, НП6, НП7, ПП НП			ЗП3, СП2, СП5, СП6, НП1, НП3, НП4, НП5, НП6, НП7, ПП НП	СП1, СП2, СП3, СП5, НП1, НП2, НП3, НП5, НП7, ПП НП										НП1, НП2, НП4, НП5, НП7, ПП НП	
РН 19	ЗП1, ЗП3, СП1, СП2, СП4, СП5,			ЗП3, СП2, СП5, СП6, НП1, НП3,	СП1, СП2, СП3, СП5, НП1, НП2,	ЗП2, ЗП3, СП1, СП4, СП6, НП1,	ЗП3, СП3, СП5, НП1, НП2, НП3,	ЗП3, СП1, СП2, СП4, СП5, СП6,	ЗП3, СП1, СП3, СП4, СП5, СП6,		ЗП2, ЗП3, СП5, СП6, НП1, НП3,	ЗП3, СП1, СП2, СП4, НП1, НП3,	ЗП3, СП1, НП1, НП3, НП4, НП6,	ЗП3, СП1, СП6, НП1, НП4, НП5,		

Програмні результати навчання	Компетентності																
	Інтегральна компетентність																
	Загальні компетентності					Спеціальні (фахові) компетентності											
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11*	
	СП6, НП1, НП2, НП3, НП4, НП5, НП6, НП7, ПП НП			НП4, НП5, НП6, НП7, ПП НП	НП3, НП5, НП7, ПП НП	НП3, НП4, НП6, ПП НП	НП4, НП5, НП6, НП7, ПП НП	НП1, НП3, НП4, НП6, НП5, НП6, ПП НП	НП1, НП3, НП4, НП5, НП6, НП7, ПП НП		НП4, НП5, НП6, ПП НП	НП4, НП6, НП7, ПП НП	НП7, ПП НП	НП6, НП7, ПП НП			
РН 20	ЗП1, ЗП3, СП1, СП2, СП4, СП5, СП6, НП1, НП2, НП3, НП4, НП5, НП6, НП7, ПП НП	СП5, НП1, НП3, НП5, НП7, ПП НП	СП5, СП6, НП1, НП2, НП3, НП5, НП7, ПП НП	ЗП3, СП2, СП5, СП6, НП1, НП3, НП4, НП5, НП6, НП7, ПП НП	СП1, СП2, СП3, СП5, НП1, НП2, НП3, НП5, НП7, ПП НП	ЗП2, ЗП3, СП1, СП4, СП6, НП1, НП3, НП4, НП6, ПП НП		ЗП3, СП1, СП2, СП4, СП5, СП6, НП1, НП3, НП4, НП6, ПП НП								ЗП3, НП1, НП2, НП3, НП4, НП6, НП7, ПП НП	
РН 21	ЗП1, ЗП3, СП1, СП2, СП4,	СП5, НП1, НП3, НП5, НП7,	СП5, СП6, НП1, НП2, НП3,	ЗП3, СП2, СП5, СП6, НП1,		ЗП2, ЗП3, СП1, СП4, СП6,		ЗП3, СП1, СП2, СП4, СП5,		ЗП2, ЗП3, СП1, СП2, СП4,		ЗП3, СП1, СП2, СП4, НП1,	ЗП3, СП1, НП1, НП3, НП4,				ЗП3, НП1, НП2, НП3, НП4,

Програмні результати навчання	Компетентності															
	Інтегральна компетентність															
	Загальні компетентності					Спеціальні (фахові) компетентності										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11*
	СП5, СП6, НП1, НП2, НП3, НП4, НП5, НП6, НП7, ПП НП	ПП НП	НП5, НП7, ПП НП	НП3, НП4, НП5, НП6, НП7, ПП НП		НП1, НП3, НП4, НП6, ПП НП		СП6, НП1, НП3, НП4, НП6, ПП НП		НП1, НП2, НП4, НП5, НП6, НП7, ПП НП		НП3, НП4, НП6, НП7, ПП НП	НП6, НП7, ПП НП			НП6, НП7, ПП НП
РН 22		СП5, НП1, НП3, НП5, НП7, ПП НП	СП5, СП6, НП1, НП2, НП3, НП5, НП7, ПП НП	ЗП3, СП2, СП5, СП6, НП1, НП3, НП4, НП5, НП6, НП7, ПП НП		ЗП2, ЗП3, СП1, СП4, СП6, НП1, НП3, НП4, НП6, ПП НП		ЗП3, СП1, СП2, СП4, СП5, СП6, НП1, НП3, НП4, НП6, ПП НП								ЗП3, НП1, НП2, НП3, НП4, НП6, НП7, ПП НП
РН 23	ЗП1, ЗП3, СП1, СП2, СП4, СП5, СП6, НП1,		СП5, СП6, НП1, НП2, НП3, НП5, НП7, ПП	ЗП3, СП2, СП5, СП6, НП1, НП3, НП4, НП5,		ЗП2, ЗП3, СП1, СП4, СП6, НП1, НП3, НП4,	ЗП3, СП3, СП5, НП1, НП2, НП3, НП4, НП5,	ЗП3, СП1, СП2, СП4, СП5, СП6, НП1, НП3,			ЗП2, ЗП3, СП5, СП6, НП1, НП3, НП4, НП5,	ЗП3, СП1, СП2, СП4, НП1, НП3, НП4, НП6,	ЗП3, СП1, НП1, НП3, НП4, НП7, ПП	ЗП3, СП1, СП6, НП1, НП3, НП4, НП5, НП6,		

Програмні результати навчання	Компетентності															
	Інтегральна компетентність															
	Загальні компетентності					Спеціальні (фахові) компетентності										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11*
	НП2, НП3, НП4, НП5, НП6, НП7, ПП НП		НП	НП6, НП7, ПП НП		НП6, ПП НП	НП6, НП7, ПП НП	НП4, НП6, ПП НП			НП6, ПП НП	НП7, ПП НП	НП	НП7, ПП НП		
Додатково для освітньо-наукових програм*																
РН 24		СП5, НП1, НП3, НП5, НП7, ПП НП	СП5, СП6, НП1, НП2, НП3, НП5, НП7, ПП НП	ЗП3, СП2, СП5, СП6, НП1, НП3, НП4, НП5, НП6, НП7, ПП НП	СП1, СП2, СП3, СП5, НП1, НП2, НП3, НП5, НП7, ПП НП			ЗП3, СП1, СП2, СП4, СП5, СП6, НП1, НП3, НП4, НП6, ПП НП							НП1, НП2, НП4, НП5, НП7, ПП НП	ЗП3, НП1, НП2, НП3, НП4, НП6, НП7, ПП НП
РН 25	ЗП1, ЗП3, СП1, СП2, СП4, СП5, СП6, НП1, НП2, НП3,	СП5, НП1, НП3, НП5, НП7, ПП НП	СП5, СП6, НП1, НП2, НП3, НП5, НП7, ПП НП	ЗП3, СП2, СП5, СП6, НП1, НП3, НП4, НП5, НП6, НП7,				ЗП3, СП1, СП2, СП4, СП5, СП6, НП1, НП3, НП4, НП6,								ЗП3, НП1, НП2, НП3, НП4, НП6, НП7, ПП НП

Програмні результати навчання	Компетентності															
	Інтегральна компетентність															
	Загальні компетентності					Спеціальні (фахові) компетентності										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11*
	НП4, НП5, НП6, НП7, ПП НП			ПП НП				ПП НП								