

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



ЗАТВЕРДЖУЮ

Ректор НТУ «ХПІ»

Євген СОКОЛ

« 29 » 04 2024 р.

**ОСВІТНЬО-ПРОФЕСІЙНА 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 № 4 від « 26 » квітня 2024 р.

Харків 2024 р.

ЛИСТ ПОГОДЖЕННЯ

Освітньо-професійної 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 ОПП із спеціальності
«Кібербезпека та захист інформації»

Гарант ОПП

Ольга КОРОЛЬ

« 29 » 04 2024 р.

ПОГОДЖЕНО

Завідувач кафедри
кібербезпеки

Сергій ЄВСЕЄВ

« 29 » 04 2024 р.

ПОГОДЖЕНО

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

Єлизавета СОЛОВЙОВА

« 29 » 04 2024 р.

РЕКОМЕНДОВАНО

Методичною радою НТУ «ХП»

Заступник голови методичної ради

Руслан МИГУЩЕНКО

« 29 » 04 2024 р.

ПОГОДЖЕНО

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

Михайло ГОДЛЕВСЬКИЙ

« 29 » 04 2024 р.

B3402
Курієв Ней

РЕЦЕНЗЕНТИ:

Продуктивні зауваження та відгуки на проєкт освітньо-професійної 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-ВІДГУК

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

Освітньо-професійна програма (ОПП) “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 ОПП 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 ОПП містить профіль освітньої програми за відповідною спеціальністю, перелік компонент освітньо-професійної 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 ОПП корелюють із складовими професійної компетентності, які формують фундаментальні знання та фахові навички, а загальні компетентності забезпечують розвиток навичок soft skills та сприяють

формуванню свідомої громадянської позиції випускника з усталеними цінностями, здатністю до фахового розвитку і самовдосконалення. Фокус освітньо-професійної 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-професійна 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



РЕЦЕНЗІЯ-ВІДГУК

на освітньо-професійну програму "Кібербезпека",
другого (магістерського) рівня вищої освіти
спеціальності 125 "Кібербезпека та захист інформації"

Національного технічного університету "Харківський політехнічний
інститут"

Освітньо-професійна програма "Кібербезпека" за спеціальністю 125 "Кібербезпека та захист інформації", яку втілено до учбового 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 повністю надають студентам можливості отримати не тільки теоретичні знання, але й набути практики 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 Освітньо-професійна 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.

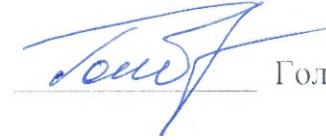
Директор ТОВ "Сайфер ІТ",
кандидат технічних наук



Владислав КОВТУН

ЗАТВЕРДЖУЮ:

Генеральний директор
ТОВ «Мікрокрипт Текнолоджіс»



Головашич С.О.

«___» _____ 2024 р.

РЕЦЕНЗІЯ-ВІДГУК

на освітньо-професійну 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-професійна програма має чітко визначені цілі, які враховують основні її особливості - підготовки фахівця з інформаційної безпеки широкого профілю зі знанням технологій програмування. Складова отримання спільних дипломів з державним Університетом у Бельсько-Бялій (Польща) підтверджує її конкурентоздатність серед програм Євросоюзу, мобільність програми забезпечує своєчасне корегування в умовах стрімкого розвитку цієї спеціальності.

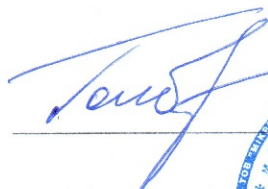
Однією з основних проблем реалізації освітнього процесу за спеціальністю 125 “Кібербезпека та захист інформації” є відсутність під час навчання можливості отримати знання та навички від професіоналів-практиків. В рамках викладання за освітньою програмою, що рецензується, залучено викладачів-практиків.

Вважаємо, що Освітньо-професійна 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




РЕЦЕНЗІЯ-ВІДГУК

на освітньо-професійну 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-професійною 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-професійною 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. Створення можливості мобільності з Університетом у Бельсько-Бялій, Польща, дозволяє отримати спільні дипломи, підтверджує якість освітніх компонент та їх відповідність вимогам Євросоюзу.

В рамках освітньо-професійної 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-професійна 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 ОПП «Кібербезпека»

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

Гарант освітньо-професійної програми

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

Члени робочої групи ОПП :

1. Євсєєв Сергій Петрович, доктор технічних наук, професор, завідувач кафедри кібербезпеки.
2. Мілов Олександр Володимирович, доктор технічних наук, професор, професор кафедри кібербезпеки.
3. Мілевський Станіслав Валерійович, кандидат економічних наук, доцент, доцент кафедри кібербезпеки.
4. Соловійова Єлизавета Олександрівна, студентка групи КН- М1123.

1. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ЗА СПЕЦІАЛЬНІСТЮ 125 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

1 – Загальна інформація	
Вищий навчальний заклад та структурний підрозділ	Національний технічний університет «Харківський політехнічний інститут», Навчально-науковий інститут <u>комп'ютерних наук та інформаційних технологій</u> кафедра <u>кібербезпеки</u>
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр Освітня кваліфікація: магістр з кібербезпеки та захисту інформації Кваліфікація в дипломі: магістр з кібербезпеки та захисту інформації
Офіційна назва освітньо-професійної програми	Кібербезпека
Тип диплому та обсяг освітньо-професійної програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання один рік 4 місяці
Наявність акредитації	Національне агентство забезпечення якості вищої освіти. Україна. Сертифікат № 6208 термін дії до 01.07.2029р.
Цикл/рівень	другий (магістерський) рівень вищої освіти; НРК України – 7 рівень, FQ-EHEA– другий цикл, EQF LLL – 7 рівень
Передумови	Набір за спеціальністю освітнього рівня «магістр» здійснюється за результатами зовнішнього незалежного оцінювання (іноземна мова) та вступного фахового випробування. Загальний конкурсний бал для вступу на основі освіти бакалавра не може бути менше 100 балів
Мова викладання	Українська, англійська
Термін дії освітньо-професійної програми	Оновлюється щорічно
Посилання на постійне розміщення опису освітньо-професійної програми	Інтернет-адреса постійного розміщення опису освітньої програми https://cybersecurity.kpi.kharkov.ua
2 – Мета освітньо-професійної 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 системах безпеки контуру бізнес-процесів.	
3 – Характеристика освітньо-професійної програми	
Предметна область (галузь знань, спеціальність)	Галузь знань: 12 “Інформаційні технології” 125 “Кібербезпека та захист інформації” Спеціальність: 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-професійної програми	Професійна підготовка фахівців у сфері кібербезпеки та захист інформації
Основний фокус	Поглиблене вивчення проведення, як зовнішнього, так й

освітньо-професійної програми та спеціалізації	внутрішнього аудиту з метою забезпечення безпеки контуру бізнес-процесів. Отримання сертифікатів курсів академії Cisco, сприяє підвищенню конкурентноспроможності на ринку праці, удосконаленню механізмів аудиту та захисту за мировими методиками. Ключові слова: кібербезпека, цифрова криміналістика, етнічний хакінг.
Особливості програми	Особливостями програми є формування у здобувачів навичок побудови комплексних систем захисту інформації для забезпечення безпеки контуру бізнес-процесів на основі сучасних технологій та програмних застосунків, в умовах розвитку цифрової економіки. 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 літературними джерелами.
Оцінювання	Моніторинг знань та умінь студентів здійснюється у формі поточного та підсумкового контролю. Поточний контроль – усне та письмове опитування, оцінка роботи в малих групах, тестування, захист групових та індивідуальних науково-дослідних завдань. Підсумковий контроль – усні та письмові екзамени, заліки з урахуванням накопичених балів поточного контролю, захист звітів з лабораторних занять. Державна атестація – підготовка та публічний захист (представлення) випускної кваліфікаційної роботи. Оцінювання здійснюється за національною шкалою (“відмінно”,

	“добре”, “задовільно”, “незадовільно”), 100-бальною шкалою та шкалою ECTS (A, B, C, D, E, FX, F).
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).
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.
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.

	кібербезпеки організації. RH11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. RH12. 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. RH13. 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. RH14. 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. RH15. 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. RH16. 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. RH17. 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. RH18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та/або кібербезпеки. RH19. 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. RH20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. RH21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. RH22. 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. RH23. 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.
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, додаток 12; зі змінами, внесеними згідно з Постановою КМУ № 365 від 24.03.2021). До викладання залучаються викладачі-практики, фахівці та співробітники ІТ-компаній, а також закордонні фахівці.
Матеріально-технічне забезпечення	Відповідає технологічним вимогам щодо матеріально-технічного 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, додаток 13)
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, додатки 14 – 15). Доступ до електронного репозитарію НТУ «ХПІ» (eNTUKhPIR) через мережу Інтернет (у тому числі університетську мережу Wi-Fi).
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів про академічну мобільність з університетами України.
Міжнародна кредитна мобільність	На основі двосторонніх договорів. Польсько-українська програма обміну та спільних дипломів для підготовки магістрів за спеціальністю «Кібербезпека та захист інформації» з Університетом у Бельсько-Бялій (м. Бельсько-Бяла, Польща).
Навчання іноземних здобувачів освіти	Після отримання Сертифікату про акредитацію освітньої програми передбачається підготовка іноземців та осіб без громадянства.

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

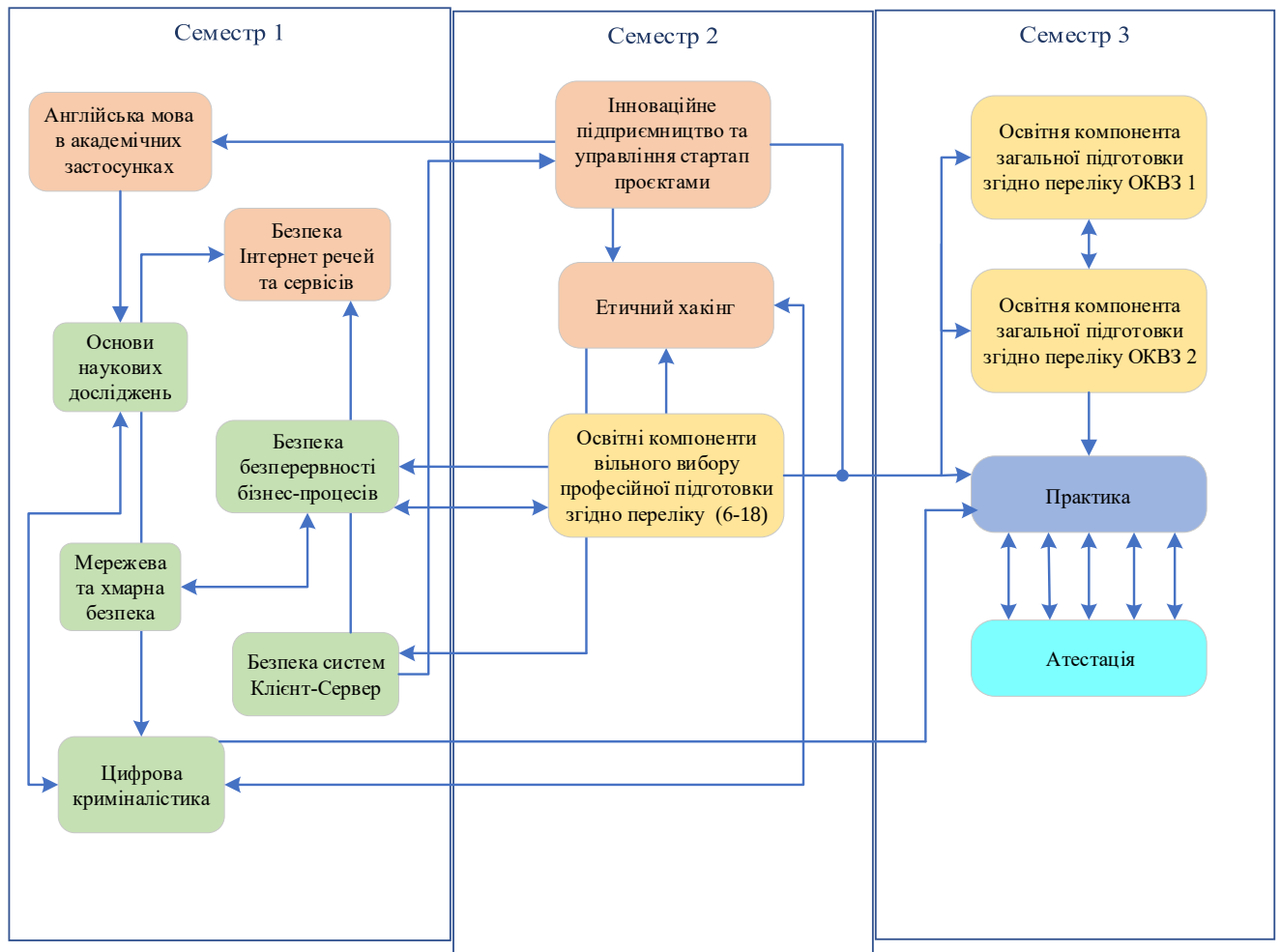
2.1 Перелік компонент ОПП

Код н/д	Компоненти освітньо-професійної програми	Кількість кредитів	Форма підсумкового контролю
1. Обов'язкові освітні компоненти (здобувачі вищої освіти – громадяни України)			
1.1 Загальна підготовка			
ЗП 1	Англійська мова в академічних застосунках	4,0	Екзамен
ЗП 2	Інноваційне підприємництво та управління стартап-проектами	3,0	Екзамен
ЗП 3	Етичний хакінг	3,0	Екзамен
ЗП 4	Безпека Інтернет-речей та сервісів	4,0	Залік
1.2. Спеціальна (фахова) підготовка			
СП1	Основи наукових досліджень	5,0	Екзамен
СП2	Безпека безперервності бізнес-процесів	5,0	Залік
СП3	Мережева та хмарна безпека	4,0	Екзамен
СП4	Безпека систем Клієнт-Сервер	4,0	Залік
СП5	Цифрова криміналістика	4,0	Залік
2. Практична підготовка			
ПП	Переддипломна практика	12,0	Залік
3. Атестація			
СП	Атестація	10,0	
Загальний обсяг обов'язкових компонентів		58	
4. Вибіркові освітні компоненти (здобувачі вищої освіти – громадяни України)			
4.1 Освітні компоненти вільного вибору професійної підготовки згідно переліку			
ОКВП1	ОК ВВ ПП 1	4,0	Залік
ОКВП2	ОК ВВ ПП 2	4,0	Залік
ОКВП3	ОК ВВ ПП 3	4,0	Залік
ОКВП4	ОК ВВ ПП 4	4,0	Залік
ОКВП5	ОК ВВ ПП 5	4,0	Залік
ОКВП6	ОК ВВ ПП 6	4,0	Залік
4.2 Освітні компоненти загальної підготовки згідно переліку			
ОКВ31	ОК ВВ ЗП 1	4,0	Залік
ОКВ32	ОК ВВ ЗП 2	4,0	Залік
Загальний обсяг вибірових компонент:		32	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ:		90	

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

№ п/п	Цикл підготовки	Обсяг навчального навантаження здобувача вищої освіти (кредитів ECTS / %)		
		Обов'язкові компоненти освітньо-професійної програми	Вибіркові компоненти освітньо-професійної програми	Всього за весь термін навчання
1	Загальна підготовка	14 / 15,5	-	14 / 15,5
2	Спеціальна (фахова) підготовка	44 / 48,9	-	44 / 48,9
3	Дисципліни вільного вибору	-	32 / 35,6	32 / 35,6
Всього за весь термін навчання		58 / 64,4	32 / 35,6	90 / 100

3. СТРУКТУРНО-ЛОГІЧНА СХЕМА



Семестр	Зміст навчальної діяльності
1	ЗП 1, ЗП 4, СП 1, СП 2, СП 3, СП 4, СП 5
2	ЗП 2, ЗП 3
3	ПП

4. 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.

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

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
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

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

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
РН 1	ЗП1, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП		СП1, ПП			ЗП2, ЗП4, СП3, СП4, ПП									
РН 2		ЗП4, СП1, ПП	СП1, ПП			ЗП2, ЗП4, СП3, СП4, ПП	СП1, СП2, СП5, ПП	СП1, СП2, СП3, ПП							
РН 3	ЗП1, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП					ЗП2, ЗП4, СП3, СП4, ПП									
РН 4	ЗП1, ЗП3, ЗП4, СП1, СП2, СП3, СП4,	ЗП4, СП1, ПП	СП1, ПП	ЗП4, СП1, ПП		ЗП2, ЗП4, СП3, СП4, ПП	СП1, СП2, СП5, ПП								

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
	ПП														
PH 5			СП1, ПП		ЗП4, СП1, СП2, СП3, СП4, СП5, ПП		СП1, СП2, СП5, ПП								
PH 6	ЗП1, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП			ЗП4, СП1, СП2, ПП		ЗП2, ЗП4, СП3, СП4, ПП		СП1, СП2, СП3, ПП		ЗП2, СП1, СП2, СП3, СП4, ПП	ЗП2, ПП	СП1, СП2, СП3, СП4, ПП		СП1, СП2, СП3, СП4, ПП	
PH 7	ЗП1, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП		СП1, СП2, ПП				СП1, СП2, СП5, ПП								
PH 8	ЗП1, ЗП3, ЗП4, СП1,	ЗП4, СП1, СП2, ПП		ЗП4, СП1, СП2, ПП	ЗП4, СП1, СП2, СП3,			СП1, СП2, СП3, ПП						СП1, СП2, СП3, СП4,	ЗП4, ПП

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
	СП2, СП3, СП4, ПП				СП4, СП5, ПП									ПП	
РН 9	ЗП1, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП	ЗП4, СП1, СП2, ПП	СП1, СП2, ПП	ЗП4, СП1, СП2, ПП					СП3, СП4, СП5, ПП					СП1, СП2, СП3, СП4, ПП	ЗП4, ПП
РН 10	ЗП1, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП		СП1, СП2, ПП	ЗП4, СП1, СП2, ПП						ЗП2, СП1, СП2, СП3, СП4, ПП				СП1, СП2, СП3, СП4, ПП	
РН 11	ЗП1, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП		СП1, СП2, ПП	ЗП4, СП1, СП2, ПП							ЗП2, ПП				ЗП4, ПП

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
PH 12	ЗП1, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП		СП1, СП2, ПП	ЗП4, СП1, СП2, ПП					СП3, СП4, СП5, ПП			СП1, СП2, СП3, СП4, ПП			ЗП4, ПП
PH 13	ЗП1, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП		СП1, СП2, ПП	ЗП4, СП1, СП2, ПП									СП3, СП4, ПП		ЗП4, ПП
PH 14	ЗП1, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП		СП1, СП2, ПП	ЗП4, СП1, СП2, ПП					СП3, СП4, СП5, ПП					СП1, СП2, СП3, СП4, ПП	ЗП4, ПП
PH 15				ЗП4, СП1, СП2, ПП	ЗП4, СП1, СП2, СП3, СП4,										ЗП4, ПП

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
					СП5, ПП										
PH 16	ЗП1, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП	ЗП4, СП1, СП2, ПП	СП1, СП2, ПП	ЗП4, СП1, СП2, ПП				СП1, СП2, СП3, ПП	СП2, СП3, СП4, СП5, ПП	ЗП2, СП1, СП2, СП3, СП4, ПП	ЗП2, ПП	СП1, СП2, СП3, СП4, ПП		СП1, СП2, СП3, СП4, ПП	ЗП4, ПП
PH 17								СП1, СП2, СП3, ПП							ЗП4, ПП
PH 18	ЗП1, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП			ЗП4, СП1, СП2, ПП	ЗП4, СП1, СП2, СП3, СП4, СП5, ПП										ЗП4, ПП
PH 19	ЗП1, ЗП3, ЗП4, СП1, СП2, СП3, СП4,			ЗП4, СП1, СП2, ПП	ЗП4, СП1, СП2, СП3, СП4, СП5, ПП	ЗП2, ЗП4, СП3, СП4, ПП	СП1, СП2, СП5, ПП	СП1, СП2, СП3, ПП	СП3, СП4, СП5, ПП		ЗП2, ПП	СП1, СП2, СП3, СП4, ПП	СП3, СП4, ПП	СП1, СП2, СП3, ПП	

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
	ПП														
PH 20	ЗП1, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП	ЗП4, СП1, СП2, ПП	СП1, СП2, ПП	ЗП4, СП1, СП2, ПП	ЗП4, СП1, СП2, СП3, СП4, СП5, ПП	ЗП2, ЗП4, СП3, СП4, ПП		СП1, СП2, ПП							
PH 21	ЗП1, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП	ЗП4, СП1, СП2, ПП	СП1, СП2, ПП	ЗП4, СП1, СП2, ПП		ЗП2, ЗП4, СП3, СП4, ПП		СП1, СП2, ПП		ЗП2, СП1, СП2, СП3, СП4, ПП		СП1, СП2, СП3, СП4, ПП	СП3, СП4, ПП		
PH 22		ЗП4, СП1, СП2, ПП	СП1, СП2, ПП	ЗП4, СП1, СП2, ПП		ЗП2, ЗП4, СП3, СП4, ПП		СП1, СП2, ПП							
PH 23	ЗП1, ЗП3, ЗП4, СП1, СП2, СП3,		СП1, СП2, ПП	ЗП4, СП1, СП2, ПП		ЗП2, ЗП4, СП3, СП4, ПП	СП1, СП2, СП5, ПП	СП1, СП2, СП3, ПП			ЗП2, ПП	СП1, СП2, СП3, СП4, ПП	СП3, СП4, ПП	СП1, СП2, СП3, СП4, ПП	

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
	СП4, ПП														