ПРОЄКТ
Розглянуто на засіданні кафедри 30.10.2024 Протокол № 4

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

ЗАТВЕРДЖУЮ
Ректор НТУ «ХПІ»

_____ Євген СОКОЛ

«___» _____ 2025 р.

ОСВІТНЬО-НАУКОВА ПРОГРАМА “КІБЕРБЕЗПЕКА”

третього (освітньо-наукового) рівня вищої освіти

за спеціальністю **F5 – Кібербезпека та захист інформації**

галузі знань **F – Інформаційні технології**

кваліфікація **доктор філософії з кібербезпеки та захисту інформації**

ЗАТВЕРДЖЕНО
ВЧЕНОЮ РАДОЮ НТУ «ХПІ»
Голова вченої ради

_____/ Євген СОКОЛ

Протокол № _____
від «___»_____ 2025 р.

Харків 2025 р.

ПРОЄКТ
Розглянуто на засіданні кафедри 30.10.2024 Протокол № 4

ЛИСТ ПОГОДЖЕННЯ

освітньо-наукової програми «Кібербезпека»

Рівень вищої освіти	третій (освітньо-науковий)
Галузь знань	F – Інформаційні технології
Спеціальність	F5 – Кібербезпека та захист інформації
Кваліфікація	доктор філософії з кібербезпеки та захисту інформації

СХВАЛЕНО
Комісією Методичної ради «Методичне забезпечення підготовки докторів філософії»
Голова комісії

_____ Віктор ШАЙДА
«____» _____2025 р.

РЕКОМЕНДОВАНО
Методичною радою НТУ «ХПІ»
Заступник голови методичної ради

_____ Руслан МИГУЩЕНКО
«____» _____2025 р.

ПОГОДЖЕНО
Робочою групою ОНП із спеціальності «Кібербезпека та захист інформації»
Гарант ОНП

_____ Сергій ПОГАСІЙ
«____»_____2025 р.

ПОГОДЖЕНО
Директор навчально-наукового інституту комп'ютерних наук та інформаційних технолгій

_____ Михайло ГОДЛЕВСЬКИЙ
«____»_____2025 р.

ПОГОДЖЕНО
Радою молодих вчених

_____ Дмитро ДАНИЛЬЧЕНКО
«____»_____2025 р.

ПОГОДЖЕНО
Завідувач кафедри кібербезпеки

_____ Сергій ЄВСЕЄВ
«____»_____2025 р.

ПОГОДЖЕНО
здобувач вищої освіти
(член робочої групи ОНП)
№ групи _А-3523

_____ Сергій ДУНАЄВ
«____»_____2025 р.

ПРОЄКТ
Розглянуто на засіданні кафедри 30.10.2024 Протокол № 4

РЕЦЕНЗЕНТИ:

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

1. ДАНИЛЬЧЕНКО Дмитро Олексійович, голова Ради молодих вчених НТУ “ХПІ”
2. МОЛОДЕЦЬКА Катерина Валеріївна, доктор технічних наук, професор, професор кафедри менеджменту організацій Києво-Могилянської бізнес-школи Національний університет «Києво-Могилянська академія»
3. КОВТУН Владислав Юрійович, кандидат технічних наук, доцент, директор ТОВ “Сайфер”
4. ГОЛОВАШИЧ Сергій Олександрович, кандидат технічних наук, доцент директор ТОВ “Мікрокрипт Текнолоджіс”
5. ВОЛОЩУК Олена Борисівна, кандидат технічних наук, керівник освітніх програм ТОВ “Distributed Lab”.
6. ШАПОВАЛ Ольга Сергіївна, виконавчий директор Громадської спілки «Харківський кластер інформаційних технологій»

ПРОЄКТ
Розглянуто на засіданні кафедри 30.10.2024 Протокол № 4

Рецензії

ПРОЄКТ
Розглянуто на засіданні кафедри 30.10.2024 Протокол № 4

ПЕРЕДМОВА

Відповідає Стандарту вищої освіти третього (освітньо-наукового) рівня галузі знань F “Інформаційні технології”, спеціальності F5 “Кібербезпека та захист інформації”, затвердженого та введеного в дію наказом Міністерства освіти і науки України від 29.10.2024 р. № 1543, відповідає Закону України «Про вищу освіту», Закону України «Про освіту», постанови Кабінету Міністрів України від 30.08.2024 р. № 1021 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти», наказу Міністерства освіти і науки України від 06.11.2015 р. № 1151 «Про особливості запровадження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти», постанови Кабінету Міністрів України від 30.12.2015 р. № 1187 «Ліцензійні умови провадження освітньої діяльності закладів освіти» та постанови Кабінету Міністрів України від 23.03.2016 р. № 261 «Про затвердження Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових установах)», вимогам Національної рамки кваліфікації для восьмого кваліфікаційного рівня https://zakon2.rada.gov.ua/laws/show/1341-2011-%D0%BF/paran12#n12

Розроблено робочою групою ОНП «Кібербезпека»

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

Гарант освітньо-наукової програми

ПОГАСІЙ Сергій Сергійович, доктор технічних наук, доцент, професор кафедри кібербезпеки.

Члени робочої групи ОНП :

1. ЄВСЕЄВ Сергій Петрович, доктор технічних наук, професор, завідувач кафедри кібербезпеки.
2. МІЛЕВСЬКИЙ Станіслав Валерійович, доктор технічних наук, доцент, професор кафедри кібербезпеки.
3. КОРОЛЬ Ольга Григорівна, кандидат технічних наук, доцент, доцент кафедри кібербезпеки.
4. ДУНАЄВ Сергій Владиславович, студент групи А-3523

ПРОЄКТ
Розглянуто на засіданні кафедри 30.10.2024 Протокол № 4

1. ПРОФІЛЬ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ ЗА СПЕЦІАЛЬНІСТЮ F5 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	Ступінь вищої освіти – доктор філософії. Освітня кваліфікації: доктор філософії з кібербезпеки та захисту інформації
Офіційна назва освітньо-наукової програми	Освітньо-наукова програма "Кібербезпека", англійською мовою "Cyber Security"
Тип диплому та обсяг освітньо-наукової програми	Диплом доктора філософії, одиничний, 49 кредитів ЄКТС, термін навчання 4 роки
Форма навчання	Очна (денна, вечірня), заочна
Наявність акредитації	Національне агентство забезпечення якості вищої освіти. Україна. Сертифікат № 9110 термін дії до 01.07.2029р.
Цикл/рівень	Третій (освітньо-науковий) рівень вищої освіти, НРК України – 8 рівень, EQF–LLL – 8 рівень, QF–EHEA – третій цикл
Передумови	Для здобуття освітньо-наукового ступеня доктора філософії зі спеціальності F5 Кібербезпека та захист інформації можуть вступати особи, які здобули освітній ступінь магістра або спеціаліста. Програма фахових вступних випробувань повинна передбачати перевірку набуття особою компетентностей та результатів навчання, що визначені стандартом вищої освіти зі спеціальності F5 Кібербезпека та захист інформації для другого (магістерського) рівня вищої освіти.
Мова викладання	Українська, англійська
Термін дії освітньо-наукової програми	Переглядається щорічно
Посилання на постійне розміщення опису освітньо-наукової програми	https://web.kpi.kharkov.ua/phd/zanyattya/osvitno-naukovi-programi/
2 – МЕТА ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ	
Забезпечити підготовку наукових і науково-педагогічних кадрів у сфері комп'ютерних наук та кібербезпеки шляхом здобуття ними компетентностей, достатніх для виконання оригінальних наукових досліджень, результати яких мають наукову новизну, теоретичне та практичне значення, а також їх підтримку в ході підготовки та захисту дисертації в галузі інформаційних технологій за спеціальністю F5 "Кібербезпека та захист інформації".	

3 – ХАРАКТЕРИСТИКА ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ	
Предметна область (галузь знань, спеціальність, спеціалізація)	Галузь знань: F “Інформаційні технології” Спеціальність: F5 “Кібербезпека та захист інформації” ***Об’єкти вивчення та діяльності:*** – інформаційні системи і технології на об’єктах інформаційної діяльності та критичних інфраструктурах сфери кібербезпеки та захисту інформації; – новітні системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення інформації (інформаційних потоків); – сучасні інформаційні ресурси різних класів (у тому числі державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – автоматизовані системи управління інформаційною безпекою, кібербезпекою та захистом інформації; – методології, технології, методи, моделі та засоби кібербезпеки та захисту інформації. ***Цілі навчання:*** набуття здатності продукувати нові ідеї, розв’язувати комплексні проблеми професійної та дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, застосовувати методологію наукової та педагогічної діяльності, та здійснювати власні наукові дослідження, результати яких мають наукову новизну, теоретичне та практичне значення. ***Теоретичний зміст предметної області:*** Принципи, концепції, теорії захисту життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. ***Методи, методики та технології:*** Сучасні методи, моделі, методики та технології дослідження та вдосконалення процесів створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, методи статистичного аналізу даних. ***Інструменти та обладнання:*** Програмно-апаратне та програмне забезпечення, інструментальні засоби, комп’ютерна техніка, спеціальні контрольно-вимірювальні прилади, програмно-технічні засоби автоматизації та системи автоматизації проектування, виробництва, експлуатації, контролю,

	моніторингу, мережні, мобільні, хмарні, технології, 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).
Орієнтація програми	Освітньо-наукова академічна
Структура програми	Структура програми передбачає виконання освітньої та наукової складових. Наукова складова виконується під час усього терміну навчання, не переривається на освітню складову, сесію та практику. Зміст кожної складової програми орієнтується на сучасні наукові дослідження комплексних проблем в галузі захисту інформації, кібербезпеки та інформаційних технологій
Основний фокус освітньо-наукової програми та спеціалізації	Проведення досліджень в галузі F "Інформаційні технології" зі спеціальності F5 "Кібербезпека та захист інформаці" та формування необхідних дослідницьких навиків для наукової кар'єри, викладання дисциплін у галузі інформаційної безпеки та кібербезпеки. Ключові слова: кібербезпека, інформаційна безпека, безпека інформації, захист інформації.
Особливості програми	Програма передбачає вирішення комплексних проблем в галузі захисту інформації, кібербезпеки та інформаційних технологій. Орієнтовано на партнерство із вітчизняними та закордонними закладами освіти та науки, приватним сектором, науковцями та участі в програмах на отримання грантів.
Науковий напрямок програми	Наукова складова ОНП виконується увесь термін навчання в аспірантурі, не переривається на теоретичне навчання та педагогічну практику. Виконання наукової роботи, підготовка наукових публікацій та рукопису дисертації забезпечують формування інтегральної компетентності. Наукова робота проходить під керівництвом одного або двох керівників. Висвітлення результатів наукової роботи передбачає публікацію наукових статей, подачу заявок на патент, виступи на конференціях та після виконання ОНП оформлюється дисертація. Загальний план роботи над дисертацією регламентується сторінкою "**D**". Контроль за виконанням наукової роботи проводиться у рамках проміжної атестації (звітування сторінки "**E**" та річна атестація сторінка "**F**"). З науковим керівником (керівниками) аспірантом обговорюється тема дисертаційної роботи, яка може бути підтримана в напрямку наукових шкіл кафедр, що забезпечують підготовку PhD.
4 – ПРИДАТНІСТЬ ВИПУСКНИКІВ ДО ПРАЦЕВЛАШТУВАННЯ ТА ПОДАЛЬШОГО НАВЧАННЯ	
Придатність до	Працевлаштування на посадах наукових і науково-

працевлаштування	педагогічних працівників в наукових установах і закладах вищої освіти, посадах працівників найвищої кваліфікації у дослідницьких, проектних, конструкторських й т.п. установах і підрозділах підприємств. Назви професій згідно Національного класифікатора України: Класифікатор професій (ДК 003:2010) 1226.2 Начальник відділення (сфера захисту інформації); 1226.2 Керівник структурного підрозділу (сфера захисту інформації); 1229.7 Керівник (директор, начальник та ін.) підрозділу (служби, управління, департаменту та ін.) з безпеки (фінансово-економічної, інформаційної); 2149.2 Професіонал із організації захисту інформації з обмеженим доступом; 2310 Викладачі закладу вищої освіти; 2310.1 Докторант; 2310.1 Доцент закладу вищої освіти.
Академічні права випускників	Доктор філософії має право на здобуття наукового ступеня доктора наук та додаткових кваліфікацій у системі освіти дорослих.
5 – ВИКЛАДАННЯ ТА ОЦІНЮВАННЯ	
Викладання та навчання	Навчання проводиться у формі лекцій, семінарів, практичних лабораторних занять, консультацій, тренінгів, педагогічних практик, самостійного вивчення, виконання самостійного наукового дослідження на основі опрацювання підручників, посібників, монографій, періодичних наукових видань, використання мережі Інтернет тощо.
Оцінювання	Поточний та підсумковий контроль знань (опитування, контрольні та індивідуальні завдання, тестування тощо), заліки та іспити (усні та письмові), звітування, проміжна атестація, презентації, захист звіту з практики, публічний захист дисертаційної роботи.
6 – ПРОГРАМНІ КОМПЕТЕНТНОСТІ	
Інтегральна компетентність	Здатність продукувати нові ідеї, розв’язувати комплексні проблеми професійної та/або дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, застосовувати методологію наукової та педагогічної діяльності, а також проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення.
Загальні компетентності	ЗК1. Здатність до абстрактного мислення, аналізу і синтезу. ЗК2. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК3. Здатність працювати в міжнародному контексті. ЗК4. Здатність розв’язувати комплексні проблеми

	предметної області на основі системного наукового світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної доброчесності.
Спеціальні (фахові, предметні) компетентності	СК1. Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у сфері кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямах і можуть бути опубліковані у провідних наукових виданнях з кібербезпеки та захисту інформації. СК2. Здатність ініціювати, розробляти і реалізовувати комплексні наукові та інноваційні проєкти в сфері кібербезпеки та захисту інформації. СК3. Здатність розв'язувати значущі проблеми у сфері кібербезпеки та захисту інформації, розширювати та переоцінювати наявні знання і професійні практики. СК4. Здатність ефективно застосовувати методи аналізу даних, концептуального, математичного та комп'ютерного моделювання, виконувати натурні та обчислювальні експерименти при проведенні наукових і прикладних досліджень у сфері кібербезпеки та захисту інформації. СК5. Здатність генерувати нові ідеї щодо розвитку теорії та практики кібербезпеки та захисту інформації, виявляти, ставити та вирішувати проблеми дослідницького характеру, оцінювати та забезпечувати якість виконуваних досліджень. СК6. Здатність вільно спілкуватися з питань, що стосуються сфери кібербезпеки та захисту інформації, з колегами, широкою науковою спільнотою, суспільством у цілому з використанням академічної української та англійської мови. СК7. Здатність здійснювати та організовувати наукову та освітню науково-педагогічну діяльність у закладах вищої освіти.
7 – РЕЗУЛЬТАТИ НАВЧАННЯ	
Результати навчання	РН1. Мати передові концептуальні та методологічні знання з кібербезпеки та захисту інформації і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з кібербезпеки та захисту інформації, отримання нових знань та/або здійснення інновацій. РН2. Планувати і виконувати експериментальні та/або теоретичні дослідження з кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямів з використанням сучасних інструментів та дотриманням норм професійної і академічної етики.

	РН3. Критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми. РН4. Глибоко розуміти загальні принципи та методи кібербезпеки та захисту інформації, а також методологію наукових досліджень, застосувати їх у власних дослідженнях у сфері інформаційних технологій та у викладацькій практиці. РН5. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень і математичного та/або комп'ютерного моделювання, наявні літературні дані. РН6. Вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні проблеми кібербезпеки та захисту інформації державною та іноземною мовами усно та письмово, оприлюднювати результати досліджень у наукових публікаціях у провідних вітчизняних та міжнародних наукових виданнях. РН7. Застосовувати загальні принципи та методи математики, інформатики та інших наук, а також сучасні методи та інструменти, цифрові технології та спеціалізоване програмне забезпечення для провадження наукових досліджень у сфері кібербезпеки та захисту інформації. РН8. Розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямах. РН9. Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи. РН10. Організовувати і здійснювати освітній процес у сфері кібербезпеки та захисту інформації, його наукове, навчально-методичне та нормативне забезпечення, розробляти і викладати спеціальні навчальні дисципліни у закладах вищої освіти.
8 – РЕСУРСНЕ ЗАБЕЗПЕЧЕННЯ РЕАЛІЗАЦІЇ ПРОГРАМИ	
Кадрове забезпечення	Кадрове забезпечення ОНП відповідає постанові Кабінету Міністрів України від 30.12.2015 р. № 1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» (зі змінами, внесеними згідно з Постановою КМ від 24.03.2021 р. № 365, додаток 15-16).

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 (зі змінами, внесеними згідно з Постановою КМ від 24.03.2021р. № 365, додаток 17) Навчальний процес відбувається у аудиторіях та лабораторіях, обладнаних сучасними комп'ютерними та технічними засобами, в тому числі мультимедійними, а також спеціалізованим програмним забезпеченням.
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 2015р. № 1187 (зі змінами, внесеними згідно з Постановою КМ від 24.03.2021 р. № 365, додаток 18)
9 – АКАДЕМІЧНА МОБІЛЬНІСТЬ	
Національна кредитна мобільність	Внутрішню академічну мобільність (ступеневу або кредитну), що реалізується здобувачами вищої освіти за освітньо-науковою програмою у вищих навчальних закладах (наукових установах) – партнерах в межах України
Міжнародна кредитна мобільність	Академічна мобільність на основі двосторонніх договорів в рамках проєктів Еразмус КА1 між Національним технічним університетом "Харківський політехнічний інститут" та Університетом ім. Яна Длугоша в м. Ченстохові (Польща), Університетом у Бєльсько-Бялій (Польща).
Навчання іноземних здобувачів освіти	Підготовка іноземних громадян та осіб без громадянства здійснюється українською або англійською мовою відповідно до вимог Закону України «Про вищу освіту»..

ПРОЄКТ
Розглянуто на засіданні кафедри 30.10.2024 Протокол № 4

2. ПЕРЕЛІК КОМПОНЕНТІВ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ «КІБЕРБЕЗПЕКА» ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1 Перелік компонентів ОНП

Код н/д	Компоненти освітньо-наукової програми (дисципліни, проекти / роботи, практика, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
І. ОСВІТНЯ СКЛАДОВА			
1. Обов'язкові компоненти ОНП (здобувачі вищої освіти – громадяни України)			
1.1 Загальна підготовка			
ЗП 1	Світоглядні та соціокультурні основи науково-технічної діяльності	4,0	Екзамен
ЗП 2	Іноземна мова для комунікації у науково-педагогічному середовищі	8,0	Екзамен
ЗП 3	Представлення наукових результатів	3,0	Диф.залік
ЗП 4	Педагогіка і психологія вищої освіти з методикою викладання	3,0	Диф.залік
1.2 Спеціальна (фахова)			
СП 1	Математичні методи, моделі та інформаційні технології у наукових дослідженнях	4,0	Екзамен
СП 2	Методологія наукової та педагогічної діяльності в науках кіберзахисту	4,0	Екзамен
СП 3	Моделювання механізмів кібербезпеки	4,0	Екзамен
1.3 Практична підготовка			
ПП 1	Педагогічна практика	3,0	Диф.залік
Загальний обсяг обов'язкових компонентів		**33**	
2. Вибіркові компоненти ОНП			
ВП 1	Дисципліни зі спеціальності	8,0	Екзамен
ВП 2	Дисципліни науково-професійної підготовки	8,0	Диф.залік
Загальний обсяг вибіркових компонентів		**16**	
ІІ. НАУКОВА СКЛАДОВА			
1	Наукові публікації		Статті, поточна атестація
2	Кваліфікаційна наукова праця		Рукопис дисертації
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ		**49**	

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	18 / 37	–	**18 / 37**
2	Спеціальна (фахова) підготовка	15 / 30	–	**15/ 30**
3	Дисципліни вільного вибору	–	16 / 33	**16 / 33**
Всього за весь термін навчання		**33 / 67**	**16 / 33**	**49 / 100**

ПРОЄКТ
Розглянуто на засіданні кафедри 30.10.2024 Протокол № 4

3. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Форми атестації здобувачів вищої освіти	Атестація здобувачів освітнього рівня доктора філософії здійснюється у формі публічного захисту дисертації.
Вимоги до дисертації на здобуття ступеня доктора філософії	Дисертація на здобуття ступеня доктора філософії є самостійним розгорнутим дослідженням, що пропонує розв'язання комплексної проблеми в сфері кібербезпеки та захисту інформації, результати якого мають наукову новизну, теоретичне та практичне значення. Дисертація не повинна містити академічного плагіату, фальсифікації, фабрикації. Дисертація має бути розміщена на сайті закладу вищої освіти (наукової установи) (окрім робіт, які містять інформацію з обмеженим доступом).
Підсумкова атестація	Науково-дослідна робота аспіранта, яка виконується в рамках теми дисертаційної роботи, є головним елементом у підготовці за освітньо-науковою програмою. За цей час аспірант навчається самостійно виконувати науковий пошук, обрати й обґрунтувати методи дослідження та аналізувати результати своєї роботи. Науково-дослідна робота виконується під керівництвом наукового керівника, який несе повну відповідальність за підготовку аспіранта та своєчасно виконання, подачу дисертаційної роботи. Підготовка дисертаційної роботи та її захист є завершенням навчання на третьому (освітньо-науковому) рівні. Атестація випускників освітньо-наукової програми спеціальності F5 "Кібербезпека та захист інформації" проводиться у формі публічного захисту (демонстрації) кваліфікаційної роботи та завершується видачею документу встановленого зразка про присудження ступеня вищої освіти Доктор філософії з присвоєнням кваліфікації: доктор філософії з кібербезпеки та захисту інформації

ПРОЄКТ
Розглянуто на засіданні кафедри 30.10.2024 Протокол № 4

4. ВИМОГИ ДО НАЯВНОСТІ СИСТЕМИ ВНУТРІШНЬОГО ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

Принципи та процедури забезпечення якості освіти	Принципи: – відповідність європейським і національним стандартам якості вищої освіти; – автономія закладу вищої освіти, який відповідає за забезпечення якості освітньої діяльності та якості вищої освіти; – системний підхід, який передбачає управління якістю на всіх рівнях освітнього процесу; – здійснення моніторингу якості освіти; – залучення аспірантів, роботодавців та інших зацікавлених сторін до процесу забезпечення якості; – відкритість інформації на всіх етапах забезпечення якості. Процедури: – удосконалення планування освітньо-наукової діяльності; – затвердження, моніторинг і періодичний перегляд освітньо-наукових програм; – підвищення якості підготовки контингенту здобувачів вищої освіти; – посилення кадрового потенціалу Університету; – забезпечення наявності необхідних ресурсів для організації освітнього процесу та підтримки здобувачів вищої освіти; – розвиток інформаційних систем з метою підвищення ефективності управління освітнім процесом; – забезпечення публічності інформації про діяльність Університету; – створення ефективної системи запобігання та виявлення академічного плагіату в наукових працях викладачів та здобувачів вищої освіти.
Моніторинг та періодичний перегляд програм	Регулярний моніторинг, перегляд і оновлення освітньо-наукових програм мають на меті гарантувати відповідний рівень надання освітніх послуг, а також створює сприятливе й ефективне навчальне середовище для здобувачів вищої освіти. Це передбачає оцінювання: змісту програми, гарантуючи відповідність програми сучасним вимогам; потреб суспільства, що змінюються; навчального навантаження здобувачів вищої освіти, їх досягнень і результатів завершення освітньо-наукової програми; ефективності процедур оцінювання аспірантів; очікувань, потреб і задоволеності здобувачів вищої освіти змістом та процесом навчання; навчального середовища відповідності меті і змісту програми; якості сервісних послуг для здобувачів вищої освіти. Програми регулярно переглядають і оновлюють після завершення повного циклу підготовки до початку нового навчального року.
Оцінювання здобувачів вищої освіти	Оцінювання результатів навчання аспірантів здійснюється під час проведення контрольних та моніторингових заходів. Заходи передбачають поточний і семестровий контроль, звітування та атестація.

	Завданням поточного контролю є перевірка розуміння і засвоєння певного матеріалу, вироблених навичок проведення розрахункових робіт, умінь самостійно опрацьовувати тексти, публічно чи письмово представляти певний матеріал тощо. Формами поточного контролю є: виконання індивідуальних завдань; виконання тестових завдань; виконання контрольних робіт, які виконуються в аудиторії або під час самостійної роботи; написання і захист рефератів; захист лабораторних робіт. Підсумковий контроль проводиться з метою оцінки результатів навчання на відповідному освітньому рівні або на окремих його завершальних етапах. Підсумковий контроль включає семестровий контроль (екзамен, диференційований залік з конкретної навчальної дисципліни) та атестацію аспіранта. Семестровий контроль проводиться у формі семестрового екзамену або заліку з конкретної навчальної дисципліни в обсязі навчального матеріалу, визначеного навчальною програмою, і в терміни, встановлені навчальним планом. Навчальні дисципліни, з яких заплановано проведення моніторингових контрольних робіт, терміни проведення контрольних заходів визначаються графіком навчального процесу. Оцінювання результатів навчання аспірантів Університету проводиться методами, що відповідають специфіці конкретної навчальної дисципліни. Моніторинг успішності аспиранту здійснюється за допомогою 100-бальної системи оцінювання з обов'язковим переведенням оцінок до національної шкали та шкали ECTS.
Підвищення кваліфікації науково-педагогічних, педагогічних та наукових працівників	Система підвищення кваліфікації науково-педагогічних, педагогічних та наукових працівників розробляється у відповідності до діючої нормативної бази та будується на наступних принципах: обов'язковості та періодичності проходження стажування і підвищення кваліфікації; прозорості процедур організації стажування та підвищення кваліфікації; моніторингу відповідності змісту програм підвищення кваліфікації задачам професійної діяльності; обов'язковості впровадження результатів підвищення кваліфікації в наукову та педагогічну діяльність; оприлюднення результатів стажування та підвищення кваліфікації.
Наявність необхідних ресурсів для організації освітнього процесу	Наявне кадрове, матеріально-технічне, навчально-методичне та інформаційне забезпечення зі спеціальності відповідає вимогам діючих Ліцензійних умов провадження освітньої діяльності закладів освіти та забезпечує реалізацію державних вимог до фахівця з вищою освітою.

Наявність інформаційних систем для ефективного управління освітнім процесом	З метою управління освітніми процесами розроблено ефективну політику в сфері інформаційного менеджменту та відповідну інтегровану інформаційну систему управління освітнім процесом. Дана система передбачає автоматизацію основних функцій управління освітнім процесом, зокрема: забезпечення проведення вступної компанії, планування та організація навчального процесу; доступ до навчальних ресурсів; обліку та аналізу успішності здобувачів вищої освіти; адміністрування основних та допоміжних процесів забезпечення освітньої діяльності; моніторинг дотримання стандартів якості. Для управління якістю освітньої діяльності в Університеті створена інформаційна система АСУ НП.
Публічність інформації про освітньо-наукові програми, ступені вищої освіти та кваліфікації	Інформації про ОНП, ступені вищої освіти та кваліфікації розміщена у відкритому доступі на сайті НТУ «ХПІ».
Дотримання академічної доброчесності працівниками Університету та здобувачами вищої освіти	В Університеті працівниками та здобувачами вищої освіти здійснюється дотримання академічної доброчесності. Система забезпечення дотримання академічної доброчесності учасниками освітнього процесу базується на таких принципах: дотримання загальноприйнятих принципів моралі; демонстрація поваги до Конституції і законів України, дотримання їхніх норм; повага до всіх учасників освітнього процесу незалежно від їхнього світогляду, соціального стану, релігійної та національної приналежності; дотримання норм законодавства про авторське право; посилання на джерела інформації у разі запозичень ідей, тверджень, відомостей; самостійне виконання індивідуальних завдань.
Система запобігання та виявлення академічного плагіату	Здійснюється перевірка на плагіат згідно з вимогами нормативних документів Університету.

ПРОЄКТ
Розглянуто на засіданні кафедри 30.10.2024 Протокол № 4

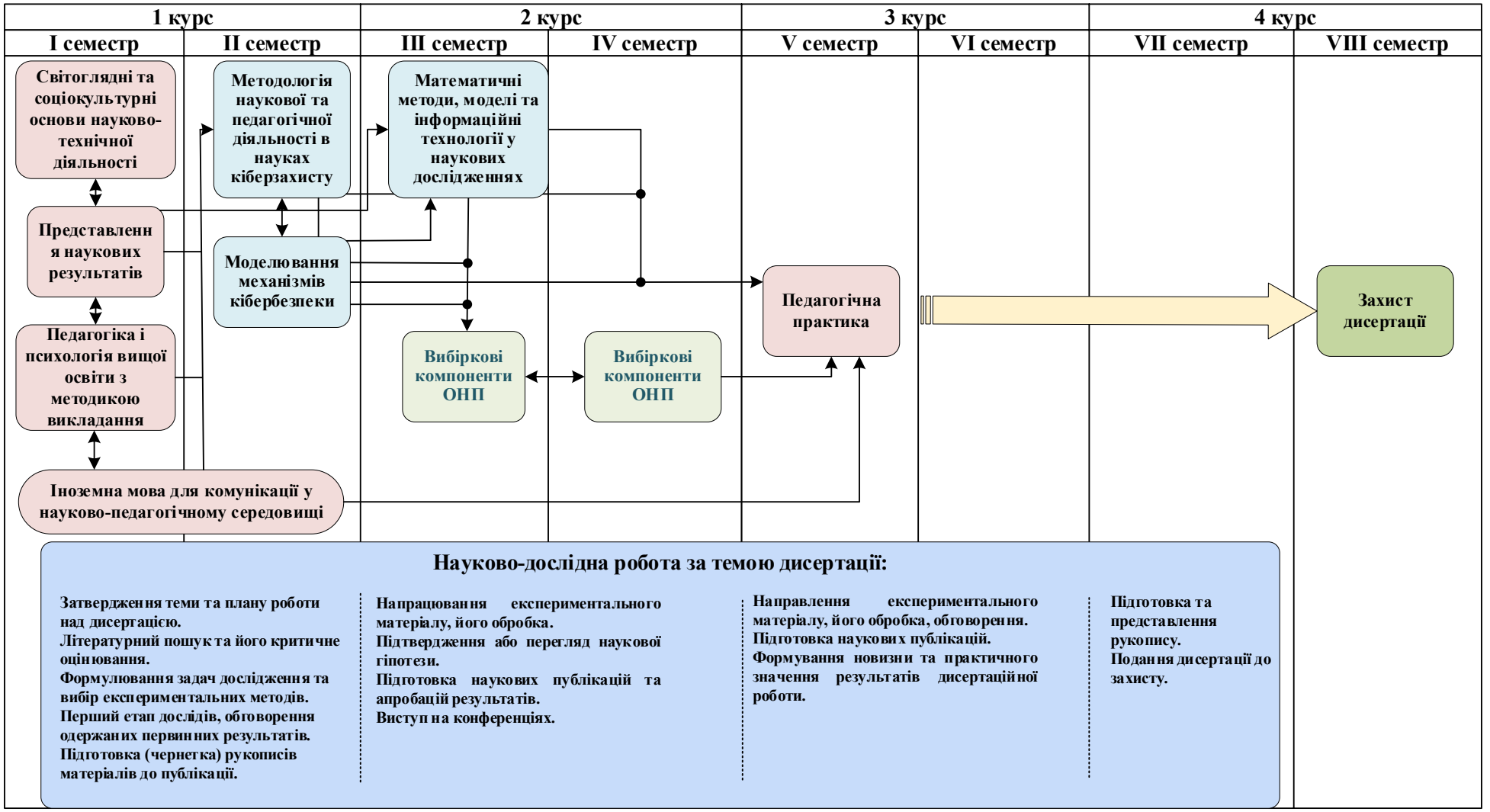
5. МАТРИЦЯ ВІДПОВІДНОСТІ ВИЗНАЧЕНИХ СТАНДАРТОМ КОМПЕТЕНТНОСТЕЙ ДЕСКРИПТОРАМ НРК

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Відповідальність і автономія
ЗАГАЛЬНІ КОМПЕТЕНТНОСТІ				
ЗК1. Здатність до абстрактного мислення, аналізу і синтезу.		+		+
ЗК2. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.	+	+	+	+
ЗК3. Здатність працювати в міжнародному контексті.			+	+
ЗК4. Здатність розв'язувати комплексні проблеми предметної області на основі системного наукового світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної доброчесності.	+	+	+	+
СПЕЦІАЛЬНІ (ФАХОВІ, ПРЕДМЕТНІ) КОМПЕТЕНТНОСТІ				
СК1. Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у сфері кібербезпеки та захисту інформації та дотичних міждисциплінарних напрямах і можуть бути опубліковані у провідних наукових виданнях з кібербезпеки та захисту інформації.	+	+	+	+
СК2. Здатність ініціювати, розробляти і реалізовувати комплексні наукові та інноваційні проєкти в сфері кібербезпеки та захисту інформації.			+	+
СК3. Здатність розв'язувати значущі проблеми у сфері кібербезпеки та захисту інформації, розширювати та переоцінювати наявні знання і професійні практики.			+	+
СК4. Здатність ефективно застосовувати методи аналізу даних, концептуального, математичного та комп'ютерного моделювання, виконувати натурні та обчислювальні експерименти при проведенні наукових і прикладних досліджень у сфері кібербезпеки та захисту	+	+		

інформації.				
СК5. Здатність генерувати нові ідеї щодо розвитку теорії та практики кібербезпеки та захисту інформації, виявляти, ставити та вирішувати проблеми дослідницького характеру, оцінювати та забезпечувати якість виконуваних досліджень.	+	+		+
СК6. Здатність вільно спілкуватися з питань, що стосуються сфери кібербезпеки та захисту інформації, з колегами, широкою науковою спільнотою, суспільством у цілому з використанням академічної української та англійської мови.		+	+	+
СК7. Здатність здійснювати та організовувати наукову та освітню науково-педагогічну діяльність у закладах вищої освіти .		+	+	+

ПРОЄКТ
Розглянуто на засіданні кафедри 30.10.2024 Протокол № 4

6. СТРУКТУРНО-ЛОГІЧНА СХЕМА



ПРОЄКТ
Розглянуто на засіданні кафедри 30.10.2024 Протокол № 4

7. ГРАФІК ОСВІТНЬОГО ПРОЦЕСУ

Місяць	Жовтень				Листопад					Грудень				Січень				Лютий					Березень				Квітень				Травень					Червень				Липень					Серпень				Вересень				
кінець тижня	06	13	20	27	03	10	17	24	01	08	15	22	29	05	12	19	26	02	09	16	23	02	09	16	23	30	06	13	20	27	04	11	18	25	01	08	15	22	29	06	13	20	27	03	10	17	24	31	07	14	21	28	29
початок тижня	30	07	14	21	28	04	11	18	25	02	09	16	23	30	06	13	20	27	03	10	17	24	03	10	17	24	31	07	14	21	28	05	12	19	26	02	09	16	23	30	07	14	21	28	04	11	18	25	01	08	15	22	29
I курс	Т	Т	Т	Т	Т	Т	Т	Т	Т	Т	С	Н	Н	Н	Н	Н	Н	Н	Н	Н	Н	Н	Т	Т	Т	Т	Т	Т	Т	Т	Т	Т	С	Н	Н	Н	Н	Н	Н	Н	К	К	К	К	К	К	К	К	Н	Н	Н	А	
	Н	Н	Н	Н	Н	Н	Н	Н	Н	Н													Н	Н	Н	Н	Н	Н	Н	З	Н	Н																				Н	
II курс	Т	Т	Т	Т	Т	Т	Т	Т	Т	Т	С	Н	Н	Н	Н	Н	Н	Н	Т	Т	Т	Т	Т	Т	Т	Т	Т	Т	С	З	Н	Н	Н	Н	Н	Н	Н	Н	Н	К	К	К	К	К	К	К	К	Н	Н	Н	А	
	Н	Н	Н	Н	Н	Н	Н	Н	Н	Н									Н	Н	Н	Н	Н	Н	Н	Н	Н	Н		Н																					Н	
III курс	П	П	П	П	П	П	П	П	П	П	Н	Н	Н	Н	Н	Н	Н	Н	Н	Н	Н	Н	П	П	П	П	П	П	П	П	П	П	Н	Н	Н	Н	Н	Н	Н	К	К	К	К	К	К	К	К	Н	Н	Н	А	
	Н	Н	Н	Н	Н	Н	Н	Н	Н	Н													Н	Н	Н	Н	Н	Н	Н	З	Н	Н																				Н	
IV курс	Н	Н	Н	Н	Н	Н	Н	Н	Н	Н	Н	А	А	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	Д	К	К	К	К	К	К	К	К	Д	Д	Д	Д	

Т	Теоретичне навчання
Н	Науково-дослідна робота
С	Екзаменаційна сесія
З	Звіт

П	Практика
Д	Підготока та захист дисертації
К	Канікули
А	Атестація

ПРОЄКТ
Розглянуто на засіданні кафедри 30.10.2024 Протокол № 4

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

Результати навчання	**Компетентності**										
	Інтегральна компетентність: Здатність розв'язувати комплексні проблеми в галузі професійної та/або дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики										
	Загальні компетентності				**Спеціальні (фахові) компетентності**						
	ЗК-1	ЗК-2	ЗК-3	ЗК-4	СК-1	СК-2	СК-3	СК-4	СК-5	СК-6	СК-7
РН-1			ЗП2, ЗП3, ЗП4, ПП1		СП1, СП3, ПП1					ЗП2, ЗП3, ЗП4, ПП1	
РН-2	ЗП1, ЗП2, ЗП3, ЗП4, СП1, СП3, ПП1	ЗП1, ЗП2, ЗП3, ЗП4, СП1, СП2, СП3, ПП1		ЗП1, СП1, СП2, СП3, ПП1	СП1, СП3, ПП1	СП2, СП3, ПП1	ЗП1, СП2, ПП1			ЗП2, ЗП3, ЗП4, СП2, ПП1	ЗП2, ЗП3, ЗП4, СП1, СП2, ПП1
РН-3			ЗП2, ЗП3, ЗП4, ПП1	ЗП1, СП1, СП2, СП3, ПП1	СП1, СП3, ПП1			СП1, СП2, СП3, ПП1			
РН-4		ЗП1, ЗП2, ЗП3, ЗП4, СП1,				СП2, СП3, ПП1		СП1, СП2, СП3, ПП1			ЗП2, ЗП3, ЗП4, СП1, СП2,

ПРОЄКТ
Розглянуто на засіданні кафедри 30.10.2024 Протокол № 4

Результати навчання	**Компетентності**										
	Інтегральна компетентність: Здатність розв'язувати комплексні проблеми в галузі професійної та/або дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики										
	Загальні компетентності				**Спеціальні (фахові) компетентності**						
	ЗК-1	ЗК-2	ЗК-3	ЗК-4	СК-1	СК-2	СК-3	СК-4	СК-5	СК-6	СК-7
		СП2, СП3, ПП1									ПП1
РН-5	ЗП1, ЗП2, ЗП3, ЗП4, СП1, СП3, ПП1			ЗП1, СП1, СП2, СП3, ПП1		СП2, СП3, ПП1					
РН-6	ЗП1, ЗП2, ЗП3, ЗП4, СП1, СП3, ПП1		ЗП2, ЗП3, ЗП4, ПП1		СП1, СП3, ПП1		ЗП1, СП2, ПП1		ЗП1, ЗП2, ЗП3, ЗП4, СП3, ПП1	ЗП2, ЗП3, ЗП4, СП2, ПП1	ЗП2, ЗП3, ЗП4, СП1, СП2, ПП1
РН-7				ЗП1, СП1, СП2, СП3, ПП1		СП2, СП3, ПП1			ЗП1, ЗП2, ЗП3, ЗП4, ПП1 СП3, ПП1		

ПРОЄКТ
Розглянуто на засіданні кафедри 30.10.2024 Протокол № 4

Результати навчання	**Компетентності**										
	Інтегральна компетентність: Здатність розв'язувати комплексні проблеми в галузі професійної та/або дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, що передбачає глибоке переосмислення наявних та створення нових цілісних знань та/або професійної практики										
	Загальні компетентності				**Спеціальні (фахові) компетентності**						
	ЗК-1	ЗК-2	ЗК-3	ЗК-4	СК-1	СК-2	СК-3	СК-4	СК-5	СК-6	СК-7
РН-8	ЗП1, ЗП2, ЗП3, ЗП4, СП1, СП3, ПП1	ЗП1, ЗП2, ЗП3, ЗП4, СП1, СП2, СП3, ПП1			СП1, СП3, ПП1		ЗП1, СП2, ПП1				ЗП2, ЗП3, ЗП4, СП1, СП2, ПП1
РН-9	ЗП1, ЗП2, ЗП3, ЗП4, СП1, СП3, ПП1	ЗП1, ЗП2, ЗП3, ЗП4, СП1, СП2, СП3, ПП1	ЗП2, ЗП3, ЗП4, ПП1					СП1, СП2, СП3, ПП1	ЗП1, ЗП2, ЗП3, ЗП4, СП3, ПП1		
РН-10	ЗП1, ЗП2, ЗП3, СП1, СП3, ПП1		ЗП2, ЗП3, ПП1					СП1, СП2, СП3, ПП1			

ПРОЄКТ
Розглянуто на засіданні кафедри 30.10.2024 Протокол № 4

9. РЕЗУЛЬТАТИ ОБГОВОРЕННЯ ОСВІТНЬОЇ ПРОГРАМИ

Стейкхолдери (вказати ПІБ та посаду, місце роботи)	Рекомендація	враховано / частково враховано / не враховано	Примітка
Зав. аспірантурою НТУ «ХПІ» к.пед.н., доц. О.М. Лапузіна, проректор з наукової роботи НТУ «ХПІ» проф. А.П. Марченко (на підставі листа Національного агентства із забезпечення якості вищої освіти за № 672 від 03.09.2021 р. «Про забезпечення володіння випускниками ОНП доктора філософії методологією педагогічної діяльності»)	До обов'язкових компонент додати нову дисципліну загальної підготовки «Педагогіка і психологія вищої освіти з методикою викладання» (3 кредити). Вилучити проходження аспірантами докторського іспиту.	Враховано. Додано дисципліну «Педагогіка і психологія вищої освіти з методикою викладання» (3 кредити).	
Гарант ОНП, д.т.н., проф. Погасій С.С. завідувач кафедри, д.т.н., професор Євсеєв С.П. Члени робочої групи ОПП	Зміна шифру спеціальності та галузі знань (згідно з постановою Кабінету Міністрів України від 30 серпня 2024 р. No 1021).	Враховано. Зміни внесено.	
Шаповал О. С., виконавчий директор Громадської спілки «Харківський кластер інформаційних технологій»	Підвищити увагу до роботи з великими даними Big Data (додати більше тем в навчальні компоненти щодо аналізу великих даних та кібербезпеки у великих IT-системах). Розширити спектр soft skills шляхом впровадження курсів з лідерства, управління проєктами, стратегічного мислення у контексті кібербезпеки	Враховано за рахунок вибіркових освітніх компонент Дисципліна «Інформаційні технології обробки великих даних» (4 кредити), «Управління науковими проєктами та дослідженнями» (4 кредити),	

		«Методологія і логіка науково-педагогічної діяльності у вищій технічній школі (4 кредити)	
Волощук О. Б., к. т. н., керівник освітніх програм ТОВ “Distributed Lab”	Позитивний відгук. Без зауважень.	-	
Молодецька К. В., доктор технічних наук, професор, професор кафедри менеджменту організацій Києво-Могилянської бізнес-школи Національний університет «Києво-Могилянська академія»	Позитивний відгук. Без зауважень.	-	
Ковтун В. Ю., кандидат технічних наук, доцент, директор ТОВ “Сайфер”	Позитивний відгук. Без зауважень.	-	
Головашич С. О., кандидат технічних наук, доцент директор ТОВ “Мікрокрипт Текнолоджіс”	Позитивний відгук. Без зауважень.	-	

ПРОЄКТ
Розглянуто на засіданні кафедри 30.10.2024 Протокол № 4

10. ПЛАН ВРАХУВАННЯ ЗАУВАЖЕНЬ ТА ВИПРАВЛЕННЯ НЕДОЛІКІВ ЗА ОСВІТНЬОЮ ПРОГРАМОЮ

Рекомендації, надані під час останньої акредитації	Період врахування (короткостроковий/довгостроковий/недоцільно враховувати)	Заходи, направлені на врахування рекомендацій	Терміни впровадження заходів
Рекомендації експертної групи та Галузевої експертної ради			
Рекомендація 1 Залучення студентів до обговорення та оновлення ОНП.	Довгостроковий	Залучення студентів до обговорення та оновлення ОПП	Березень 2025 н.р.
Рекомендація 2 Привести у відповідність кількість кредитів по кожній ОК	Довгостроковий	Переглянути збалансованість, раціональне призначення і кількість кредитів (не менше 3-х кредитів – кожна ОК) Змінено кількість кредитів ОК «Представлення наукових результатів» та «Педагогічна практика» з 2 на 3 кредити.	Щорічно під час перегляду ОНП.
Рекомендація 3 Визначити передумови вивчення дисциплін як в силабусах, так і в структурно-логічній схемі самої ОНП	Довгостроковий	Проаналізувати і виправити силабуси	Серпень 2025 н.р.
Рекомендація 4 Залучити здобувачів ВО даної ОНП до міжнародної й внутрішньої академічної мобільності	Довгостроковий	Виконати аналіз аналогічних ОНП іноземних ЗВО з метою можливості залучення аспірантів до програм академічної мобільності	Березень 2026 н.р.

Рекомендація 5 Запровадити систему особистого зобов'язання дотримання норм академічної доброчесності здобувачем ВО та НПП	Довгостроковий	Проводится постійно під час проведення лекційних занять з дисципліни «Методологія наукової та педагогічної діяльності в науках кіберзахисту»	Вересень 2025 н.р.
Рекомендація 6 Залучати до проведення лекційних занять, вітчизняних та закордонних фахівців-практиків у галузі кібербезпеки. Мотивувати та залучати НПП до участі у міжнародних проєктах (грантах) та конференціях	Довгостроковий	Участь НПП у міжнародних проєктах (грантах) та конференціях	Початок кожного навчального року

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

Гарант освітньої програми _____ Сергій ПОГАСІЙ