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

ЗАТВЕРДЖУЮ
В.о. Ректора НТУ «ХПІ»
_____ Євген СОКОЛ
«30» березня 2026 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Другого (магістерського) рівня вищої освіти

за спеціальністю **F5 – Кібербезпека та захист інформації**
галузі знань **F – Інформаційні технології**
кваліфікація **магістр з кібербезпеки та захисту інформації**

ЗАТВЕРДЖЕНО
ВЧЕНОЮ РАДОЮ НТУ «ХПІ»
Голова вченої ради
_____ / Євген СОКОЛ
Протокол № 4
від «27» березня 2026 р.

Харків 2026 р.

ЛИСТ ПОГОДЖЕННЯ

Освітньо-професійної програми Кібербезпека

Рівень вищої освіти	другий (магістерський)
Галузь знань	F Інформаційні технології
Спеціальність	F5 «Кібербезпека та захист інформації»
Кваліфікація	магістр з кібербезпеки та захисту інформації

СХВАЛЕНО
Робочою групою ОПП із спеціальності
«Кібербезпека та захист інформації»
Гарант ОПП
_____ Ольга КОРОЛЬ

Протокол № 1
« 16 » січня 2026 р.

РЕКОМЕНДОВАНО
Методичною радою НТУ «ХПІ»
Заступник голови методичної ради
_____ Руслан МИГУЩЕНКО

Протокол № 3
« 25 » березня 2026 р.

ПОГОДЖЕНО
Завідувач кафедри
кібербезпека
_____ Сергій ЄВСЕЄВ

Протокол № 12
« 23 » березня 2026 р.

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

«____»_____2026 р.

ПОГОДЖЕНО
здобувач вищої освіти
(член робочої групи ОПП)
№ групи КН-М1125
_____ Павло ПОЖИДАЄВ

« 23 » березня 2026 р.

ЗАТВЕРДЖЕНО ТА НАДАНО ЧИННОСТІ
Наказом ректора Національного технічного університету «Харківський політехнічний інститут» від « 30 » березня 2026 року № 119 ОД.

РЕЦЕНЗЕНТИ:

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

1. Іван ОПІРСЬКИЙ, доктор технічних наук, професор, завідувач кафедри захисту інформації Інституту комп'ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка»
2. Владислав КОВТУН, кандидат технічних наук, доцент, директор ТОВ "Сайфер"
3. Сергій ГОЛОВАШИЧ, кандидат технічних наук, доцент директор ТОВ "Мікрокрипт Текнолоджіс"
4. Олена ВОЛОЩУК, кандидат технічних наук, керівник освітніх програм ТОВ "Distributed Lab".
5. Ольга ШАПОВАЛ, виконавчий директор Громадської спілки «Харківський кластер інформаційних технологій»

РЕЦЕНЗІЯ-ВІДГУК
НА ОСВІТНЬО-ПРОФЕСІЙНУ ПРОГРАМУ "КІБЕРБЕЗПЕКА"
другого (магістерського) рівня вищої освіти
спеціальності F5 "Кібербезпека та захист інформації"
кафедри кібербезпеки Національного технічного університету
"Харківський політехнічний інститут"

Освітньо-професійна програма (ОПП) "Кібербезпека" для підготовки здобувачів вищої освіти другого (магістерського) рівня за спеціальністю F5 "Кібербезпека та захист інформації" галузі знань F "Інформаційні технології" розроблена науково-педагогічними працівниками Національного технічного університету "Харківський політехнічний інститут". Гарантом освітньої програми є к.т.н., доц. Король О.Г. Подана на рецензування ОПП створена на основі стандарту вищої освіти України для спеціальності F5 "Кібербезпека та захист інформації" другого (магістерського) рівня, затвердженого наказом МОН України від 18 березня 2021 р. № 332. Представлена ОПП містить профіль освітньої програми за відповідною спеціальністю, перелік компонентів освітньо-професійної програми та їхню логічну послідовність, структурно-логічну схему, а також 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 бізнес-процесів. Критичний аналіз освітньої програми показав, що її зміст повністю враховує інтегральні, загальні й фахові компетентності, передбачені стандартом. Це забезпечує досягнення здобувачами вищої освіти відповідних програмних результатів навчання.

Навчальний план включає обов'язкові дисципліни загальної підготовки, такі як «Англійська мова в академічних застосунках», «Інноваційне підприємництво та управління стартапами», «Безпека Інтернет речей та сервісів» та «Етичний хакінг». Вони формують не лише технічні, а й комунікативні та управлінські компетенції, необхідні для роботи у сучасному бізнес-середовищі.

Програмні результати ОПП корелюють із складовими професійної компетентності, що формують фундаментальні знання та фахові навички, а загальні компетентності сприяють розвитку навичок soft skills і формуванню свідомої громадянської позиції випускника з усталеними цінностями, здатністю до фахового розвитку і самовдосконалення. Фокус освітньо-професійної програми спрямований на побудову комплексних систем

захисту інформації для забезпечення безпеки бізнес-процесів із використанням сучасних технологій та програмних застосунків в умовах розвитку цифрової економіки, що додатково підкреслює актуальність програми.

Освітньо-професійна програма «Кібербезпека» магістерського рівня відповідає сучасним викликам і тенденціям у сфері кіберзахисту. Вона забезпечує всебічну підготовку спеціалістів, які володіють актуальними знаннями та практичними навичками у сфері інформаційної безпеки. Завдяки поєднанню теоретичних основ, прикладного навчання та використання новітніх технологій, випускники програми здатні ефективно працювати у сфері захисту інформаційних систем, що робить їх конкурентоспроможними на ринку праці.

ВІДДІЛ КАДРІВ 02071010

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
"ЛЬВІВСЬКА ПОЛІТЕХНІКА"
ПІДПИС ЗАСВІДЧУЮ
НАЧАЛЬНИК ВІДДІЛУ КАДРІВ
Шевцова М.С.
"____" _____ 20____ р.

Завідувач кафедри захисту інформації
Інституту комп'ютерних технологій,
автоматики та метрології Національного
університету «Львівська політехніка»,
д.т.н., професор _____ Іван ОПІРСЬКИЙ

САЙФЕР

Системи захисту інформації

ТОВ «САЙФЕР ІТ»
Адреса: 04107, Київ, вул. Нагірна, 25-27
Тел./Факс: (044) 484-46-17, 484-46-12, 483-03-22
E-mail: info@cipher.com.ua
https://cipher.com.ua

РЕЦЕНЗІЯ-ВІДГУК
НА ОСВІТНЬО-ПРОФЕСІЙНУ ПРОГРАМУ “КІБЕРБЕЗПЕКА”

другого (магістерського) рівня вищої освіти
спеціальності F5 “Кібербезпека та захист інформації”
Національного технічного університету “Харківський політехнічний інститут”

Освітньо-професійна програма “Кібербезпека” за спеціальністю F5 “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 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 F5 “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 F5 “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
2026 рік

Владислав КОВТУН

ЗАТВЕРДЖУЮ:
Генеральний директор
ТОВ «Мікрокрипт Технолоджіс»
_____ Головашич С.О.
«12» 03 2026 р.

РЕЦЕНЗІЯ-ВІДГУК
НА ОСВІТНЬО-ПРОФЕСІЙНУ ПРОГРАМУ “КІБЕРБЕЗПЕКА”
другого (магістерського) рівня вищої освіти,
спеціальності F5 “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 F5 “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. Мобільність програми забезпечує своєчасне корегування в умовах стрімкого розвитку цієї спеціальності.

Освітньо-професійна програма охоплює широкий спектр дисциплін, спрямованих на формування у студентів компетентностей, необхідних для ефективного аналізу, проєктування та впровадження технологій кіберзахисту в різних галузях діяльності. Значна увага приділяється практичним заняттям, лабораторним роботам, моделюванню загроз і управлінню ризиками.

Однією з основних проблем реалізації освітнього процесу за спеціальністю F5 “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.

Освітньо-професійна програма "Кібербезпека" магістерського рівня, що складена та запропонована кафедрою кібербезпеки Національного технічного університету “Харківський політехнічний інститут” є високоякісною та конкурентоспроможною на ринку праці. Вона надає випускникам необхідні знання та навички для роботи у сфері захисту інформації та забезпечення кібербезпеки, відповідаючи сучасним викликам цифрового суспільства.

Генеральний директор
ТОВ “Мікрокрипт Технолоджіс”,
кандидат технічних наук
2026 рік

Сергій ГОЛОВАШИЧ

РЕЦЕНЗІЯ-ВІДГУК
НА ОСВІТНЬО-ПРОФЕСІЙНУ ПРОГРАМУ “КІБЕРБЕЗПЕКА”
другого (магістерського) рівня вищої освіти
спеціальності F5 “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.

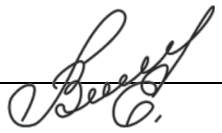
Схема підготовки фахівців за освітньо-професійною програмою, що акредитується, є правильно побудованою: врахована необхідність отримання студентами знань з дисциплін професійного змісту, які повністю покривають результати навчання, що передбачені стандартом вищої освіти зі спеціальності F5 “Кібербезпека тазахист інформації” другого (магістерського) рівня вищої освіти.

Освітньо-професійна програма охоплює широкий спектр дисциплін, спрямованих на формування у студентів компетентностей, необхідних для аналізу, проєктування та впровадження технологій кіберзахисту в різних сферах. Особливий акцент зроблено на практичну підготовку, що включає лабораторні роботи, моделювання кіберзагроз і управління ризиками.

В рамках освітньо-професійної програми “Кібербезпека”, яка складена кафедрою кібербезпеки Національного технічного університету “Харківський політехнічний інститут”, автори змогли досить органічно та логічно сформувати 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 IT 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,
кандитат технічних наук
2026 рік



Олена ВОЛОЩУК

KHARKIV IT CLUSTER

Громадська спілка "Харківський кластер інформаційних технологій"
вул.Громадянська 11/13,
м.Харків, 61057 Україна
+38 (050) 658-88-46
olga.shapoval@it-kharkiv.com
www.it-kharkiv.com

Рецензія

на освітньо-професійну програму «Кібербезпека» за спеціальністю F5 «Кібербезпека та захист інформації» другого (магістерського) рівня вищої освіти в Національному технічному університеті «Харківський політехнічний інститут»

Поглиблений аналіз освітньо-професійної програми «Кібербезпека» за спеціальністю F 5 «Кібербезпека та захист інформації» другого (магістерського) рівня вищої освіти в Національному технічному університеті «Харківський політехнічний інститут» демонструє її ключове значення для зміцнення кіберстійкості України. У ситуації, коли повний цикл функціонування інформаційних систем опирається на надійність мережевих технологій і захищеність операційних середовищ, підготовка фахівців із досконалим розумінням протоколів OSI та TCP/IP, моделей Ethernet, ARP, ICMP і адресації IPv4/IPv6 стає стратегічним завданням.

У структурі програми поєднується теоретичне вивчення сучасних мережних технологій із лабораторними вправами на кіберполігоні, де слухачі закріплюють навички комутації Ethernet і налаштування віртуальних локальних мереж із підтримкою DHCPv4. Курсова робота передбачає симуляцію створення малої мережі з функціоналом VPN та IPsec, що дозволяє студентам практично застосувати принципи безпеки LAN і WLAN, а також перевірити механізми аутентифікації, авторизації та обліку користувачів у корпоративному середовищі. Одночасно з цим у межах профільного модуля розробляються вміння налаштовувати списки контролю доступу й впроваджувати технології IPS/IDS та брандмауери другого рівня, що гарантує зменшення загроз на мережевому рівні.

Високий рівень практико-орієнтованого навчання доповнюється елементами системного адміністрування: слухачі опановують роботу в операційних системах Windows і Linux, освоюють механізми управління

дозволами, моніторингу та ведення журналів безпеки. Особлива увага приділяється оцінці вразливостей кінцевих точок і сервісів, а також захисту кінцевих пристроїв від сучасних загроз. Паралельно з технічними дисциплінами реалізовано курс із професійного англійського спілкування, який готує здобувачів до ведення переговорів з міжнародними партнерами та документування результатів аудитів англійською мовою.

Щоби додатково посилити конкурентоспроможність випускників, доцільно запровадити поглиблену аналітику загроз із використанням методів машинного навчання та штучного інтелекту, що розширить можливості проактивного реагування на аномалії. Розвиток напрямку контейнерної безпеки вимагатиме окремого циклу практичних занять із побудови захищених Kubernetes-кластерів та управління секретами в публічних хмарах. Крім того, розширення тренінгів із розвитку комунікаційних і проєктних навичок дозволить майбутнім фахівцям впевнено координувати роботу міждисциплінарних команд і шукати спільні рішення зі стейкхолдерами.

Підсумовуючи, зазначаємо, що освітньо-професійна програма «Кібербезпека» за спеціальністю F5 «Кібербезпека та захист інформації» другого (магістерського) рівня вищої освіти в Національному технічному університеті «Харківський політехнічний інститут» по своєму наповненню та кадровому забезпеченню здатна формувати необхідні мережеві та системні компетенції, покриваючи весь спектр від базових моделей OSI/TCP-IP і комутації до побудови комплексних систем безпеки з VPN, IPS/IDS, AAA та криптографічних сервісів. Завдяки сучасному кіберполігону, лабораторіям із Windows і Linux, а також тренуванню технічної англійської вона готує універсальних спеціалістів, здатних ефективно захищати інформаційні ресурси в організаціях будь-якого рівня.

Виконавчий директор
ГС «Харківський кластер
інформаційних
технологій»
2026 рік

Ольга ШАПОВАЛ

ПЕРЕДМОВА

Відповідає Стандарту вищої освіти другого (магістерського) рівня галузі знань F «Інформаційні технології», спеціальності F5 «Кібербезпека та захист інформації», затвердженого та введеного в дію наказом Міністерства освіти і науки України від 18.03.2021 р. № 332.

Розроблено робочою групою освітньо-професійної програми «Кібербезпека»
Навчально-наукового інституту комп'ютерних наук та інформаційних технолгій
Національного технічного університету «Харківський політехнічний інститут»
у складі:

Гарант освітньо-професійної програми
Ольга КОРОЛЬ, кандидат технічних наук, доцент, доцент кафедри кібербезпеки.

Члени робочої групи ОПП :

1. Сергій ЄВСЕЄВ, доктор технічних наук, професор, завідувач кафедри кібербезпеки.
2. Сергій ПОГАСІЙ, доктор технічних наук, професор, професор кафедри кібербезпеки.
3. Станіслав МІЛЕВСЬКИЙ, доктор технічних наук, професор, професор кафедри кібербезпеки.
4. Павло ПОЖИДАЄВ, студент групи КН- М1125.

1. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ 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 технолгій кафедра кібербезпеки
Ступінь вищої освіти та назва кваліфікації (освітньої, професійної) мовою оригіналу	Ступінь вищої освіти – Магістр Галузь знань - F Інформаційні технології Спеціальність – F5 Кібербезпека та захист інформації Освітня кваліфікація – магістр з кібербезпеки та захисту інформації.
Професійна кваліфікація	Відсутня
Форма навчання	Інституційна (очна (денна)), заочна.
Офіційна назва освітньо-професійної програми	Кібербезпека
Назви спеціалізацій (предметних спеціальностей)	Відсутня
Тип диплому одиничний, спільний (подвійний) за наявності та обсяг освітньої програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 рік 4 місяці
Наявність акредитації	Національне агентство забезпечення якості вищої освіти. Сертифікат про акредитацію освітньої програми № 6112. Термін дії – 01.07.2029р.
Цикл/рівень	Другий (магістерський) рівень вищої освіти; НРК України – 7 рівень, EQF LLL – 7 рівень, FQ-EHEA– другий цикл.
Передумови	Наявність ступеня вищої освіти «бакалавр»
Мова викладання	Українська мова, Англійська мова
Термін дії освітньо-професійної програми	Відповідно до терміну дії сертифікату. Переглядається щорічно
Посилання на постійне розміщення опису освітньо-професійної програми	https://blogs.kpi.kharkov.ua/v2/quality/dokumenty/diyuchy-osvitni-programy/osvitnij-riven-magistr/
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, спеціалізація або предметна спеціальність (за наявності))	**Галузь знань:** F “Інформаційні технології” **Спеціальність:** F5 “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 освітньої програми	Освітньо-професійна. Підготовка фахівців у сфері кібербезпеки та захисту інформації
Основний фокус освітньої програми та спеціалізації або предметна спеціальність (за наявності)	Спеціальна освіта у галузі інформаційних технологій зі спеціальності F5 "Кібербезпека та захист інформації". Поглиблене вивчення проведення, як зовнішнього, так й внутрішнього аудиту з метою забезпечення безпеки контуру бізнес-процесів. Отримання сертифікатів курсів академії Cisco, покращує конкурентоспроможність на ринку праці, удосконаленню механізмів аудиту та захисту за мировими методиками. Ключові слова: кібербезпека, цифрова криміналістика, етичний 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 академічні права випускників	
Придатність до працевлаштування	Фахівці з кібербезпеки та захисту інформації можуть працювати, згідно з чинною редакцією Національного класифікатора України: Класифікатор професій 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-комунікаційних систем; 2139.2 Дізнавач (сфера кібербезпеки та захисту інформації); 2139.2 Експерт з цифрової криміналістики (сфера кібербезпеки та захисту інформації); 2139.2 Експерт-криміналіст судової експертизи (сфера кібербезпеки та захисту інформації); 2139.2 Слідчий з кіберзлочинів.
Академічні права випускників	Здобувачі освіти, які пройшли підготовку за даною навчальною програмою та отримали диплом магістра, мають право на здобуття освіти на третьому (освітньо-науковому) рівні вищої освіти у ЗВО України та за кордоном в галузі знань "Інформаційні технології" або суміжних. 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	Рейтингова система оцінювання. Поточний та підсумковий контроль знань (опитування, контрольні та індивідуальні завдання, тестування тощо), заліки та іспити (усні та письмові), публічний захист кваліфікаційної роботи чи проекту. Система оцінювання передбачає застосування міжнародної системи ЄКТС (з оцінками A, B, C, D, E, F), національної системи (з оцінками «відмінно», «добре», «задовільно» та «незадовільно»), а також 100-бальної системи закладу вищої освіти зі встановленою системою відповідності.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні компетентності (визначені стандартом вищої освіти спеціальності)	КЗ1. Здатність застосовувати знання у практичних ситуаціях. КЗ2. Здатність проводити дослідження на відповідному рівні. КЗ3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Спеціальні (фахові)	КФ1. Здатність обґрунтовано застосовувати, інтегрувати,

компетентності (визначені стандартом вищої освіти спеціальності)	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. Провадити 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 напряму 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 натурного, 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.
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 КМУ № 365 від 24.03.2021. Додаток 15-16). Склад робочої групи освітньої програми, професорсько викладацький склад, що задіяний до викладання навчальних дисциплін за спеціальністю відповідають Ліцензійним умовам провадження освітньої діяльності на другому (магістерському) рівні вищої освіти. 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). Навчально-науково-виробнича база у вигляді: –навчальні корпуси, комп'ютерні класи, об'єднані локальною обчислювальною мережею з виходом до Інтернету, мультимедійне обладнання;–спеціалізоване програмне забезпечення, кіберполігон.
Інформаційне та навчально-методичне	Відповідає технологічним вимогам щодо навчально-методичного та інформаційного забезпечення освітньої

забезпечення	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 КМУ № 365 від 24.03.2021. Додаток 18). Інформаційне та навчально-методичне забезпечення навчального процесу реалізується наявністю необхідної навчальної та методичної літератури: підручники, навчальні посібники, методичні рекомендації до практичних занять, самостійної роботи, силабуси освітніх компонентів (https://cybersecurity.khpi.edu.ua/sylabusy-osvitnikh-komponentiv-125-magistr/). Інформаційні ресурси розміщені у фондах наукової бібліотеки НТУ “ХПІ”, сайтах випускових кафедр.
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. На основі двосторонніх договорів між Національним технічним університетом «Харківський політехнічний інститут» та вищими навчальними закладами зарубіжних країн-партнерів.
Навчання іноземних здобувачів вищої освіти	Підготовка іноземних громадян здійснюється згідно з вимогами чинного законодавства за умови визнання попереднього освітнього рівня.

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

2.1 Перелік компонент освітньо-професійної програми

Код н/д	Компоненти освітньо-професійної програми	Кількість кредитів	Форма підсумкового контролю
1. Обов'язкові освітні компоненти			
1.1 Загальна підготовка			
ЗП 1	*Академічна англійська мова*	*3,0*	*Залік*
ЗП 2	*Інноваційне підприємництво та управління стартап-проєктами*	*3,0*	*Залік*
ЗП 3	*Інтелектуальна власність*	*3,0*	*Залік*
ЗП 4	*Безпека на основі штучного інтелекту*	*3,0*	*Екзамен*
ЗП 5	*Безпека Інтернет-речей та сервісів*	*3,0*	*Екзамен*
1.2. Спеціальна (фахова) підготовка			
СП1	*Основи наукових досліджень*	*5,0*	*Екзамен*
СП2	*Безпека об'єктів критичної інфраструктури*	*4,0*	*Залік*
СП3	*Мережева та хмарна безпека*	*4,0*	*Екзамен*
СП4	*Захист розподілених сервісів і операційних платформ*	*4,0*	*Залік*
СП5	*Цифрова криміналістика*	*4,0*	*Залік*
1.3 Практична підготовка			
ПП 1	*Переддипломна практика*	*11,0*	*Залік*
1.4 Атестація			
	Атестація	*11,0*	*Екзамен*
Загальний обсяг обов'язкових компонентів		***58***	
2. Вибіркові освітні компоненти			
2.1 Освітні компоненти вільного вибору професійної підготовки загальноінститутського каталогу			
ОКВП 1	*ОК ВВ ПП 1*	*4,0*	*Залік*
ОКВП 2	*ОК ВВ ПП 2*	*4,0*	*Залік*
ОКВП 3	*ОК ВВ ПП 3*	*4,0*	*Залік*
ОКВП 4	*ОК ВВ ПП 4*	*4,0*	*Залік*
ОКВП 5	*ОК ВВ ПП 5*	*4,0*	*Залік*
ОКВП 6	*ОК ВВ ПП 6*	*4,0*	*Залік*
2.2 Освітні компоненти вільного вибору загальної підготовки			
ОКВЗ 1	*ОК ВВ ЗП 1*	*4,0*	*Залік*
ОКВЗ 2	*ОК ВВ ЗП 2*	*4,0*	*Залік*
Загальний обсяг вибіркових компонент:		***32***	

ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ:	***90***

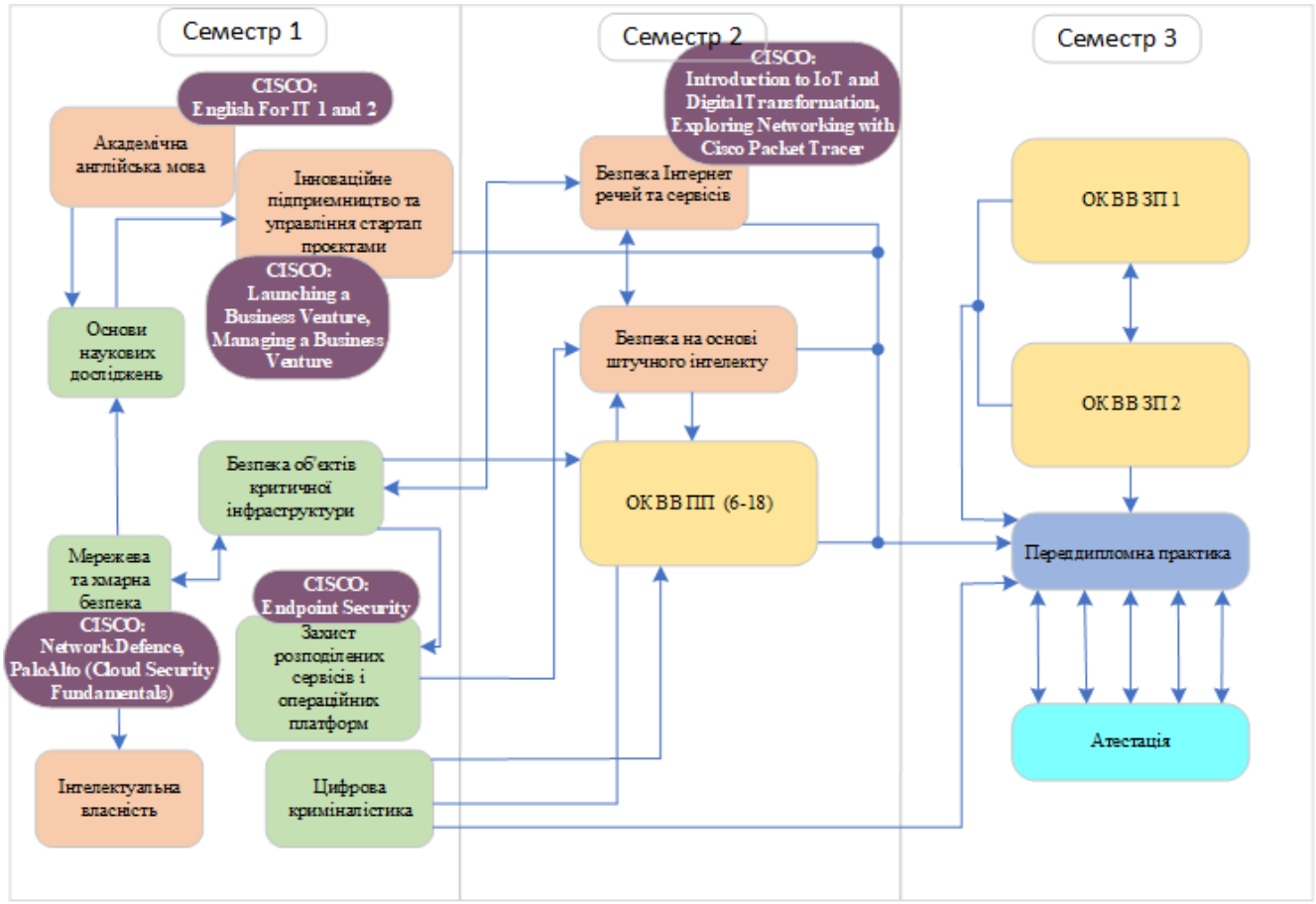
3. РОЗПОДІЛ ЗМІСТУ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ЗА ГРУПАМИ КОМПОНЕНТІВ ТА ЦИКЛАМИ ПІДГОТОВКИ

№ 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	15 / 16,7	-	**15 / 16,7**
2	Спеціальна (фахова) підготовка	21 / 23,3	-	**21 / 23,3**
3	Практична підготовка	11/12,2	-	**11/12,2**
4	Атестація	11/12,2	-	**11/12,2**
5	Компоненти вільного вибору	-	32 / 35,6	**32 / 35,6**
Всього за весь термін навчання		**58 / 64,4**	**32 / 35,6**	**90 / 100**

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. СТРУКТУРНО-ЛОГІЧНА СХЕМА



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

Класифікація компетентностей за НРК	**Знання** **Зн1** Спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері професійної діяльності або галузі знань і є основною для оригінального мислення та проведення досліджень, критичне осмислення проблем у галузі та на межі галузей знань	**Уміння** **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 мкльтидисциплінарних контекстах **Ум3** Здатність розв'язувати проблеми у нових абонезнайомих 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, 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

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

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 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП3 СП4 ПП1		ЗП1 ЗП3 СП1 СП2 ПП1			ЗП1 ЗП2 ЗП5 СП3 СП4 ПП1									
РН 2		ЗП1 ЗП5 СП1 СП2 СП4 ПП1	ЗП1 ЗП3 СП1 СП2 ПП1			ЗП1 ЗП2 ЗП4 СП3 СП4 ПП1	ЗП3 СП1 СП2 ПП1	ЗП4 СП1 СП2 СП3 СП4 СП5 ПП1							
РН 3	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП3 СП4 ПП1					ЗП1 ЗП2 ЗП4 СП3 СП4 ПП1									
РН 4	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП3 СП4 ПП1	ЗП1 ЗП5 СП1 СП2 СП4 ПП1	ЗП1 ЗП3 СП1 СП2 ПП1	ЗП3 ЗП5 СП1 СП2 СП4 ПП1		ЗП1 ЗП2 ЗП4 СП3 СП4 ПП1	ЗП3 СП1 СП2 ПП1								

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 5			ЗП1 ЗП3 СП1 СП2 ПП1		ЗП1 ЗП3 ЗП5 СП1 СП2 СП3 ПП1		ЗП3 СП1 СП2 ПП1								
РН 6	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП3 СП4 ПП1			ЗП3 ЗП5 СП1 СП2 СП4 ПП1		ЗП1 ЗП2 ЗП4 СП3 СП4 ПП1		ЗП4 СП1 СП2 СП3 СП4 СП5 ПП1		ЗП4 ЗП5 СП1 СП2 СП3 СП5 ПП1	ЗП2 ПП1	ЗП4 ЗП5 СП1 СП2 СП3 СП5 ПП1		ЗП5 СП1 СП2 СП3 СП4 ПП1	
РН 7	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП3 СП4 ПП1		ЗП1 ЗП3 СП1 СП2 ПП1				ЗП3 СП1 СП2 ПП1								
РН 8	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП3 СП4 ПП1	ЗП1 ЗП5 СП1 СП2 СП4 ПП1		ЗП3 ЗП5 СП1 СП2 СП4 ПП1	ЗП1 ЗП3 ЗП5 СП1 СП2 СП3 ПП1			ЗП4 СП1 СП2 СП3 СП4 СП5 ПП1						ЗП5 СП1 СП2 СП3 СП4 ПП1	ЗП1 СП1 ПП1

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 9	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП3 СП4 ПП1	ЗП1 ЗП5 СП1 СП2 СП4 ПП1	ЗП1 ЗП3 СП1 СП2 ПП1	ЗП3 ЗП5 СП1 СП2 СП4 ПП1					СП3 ПП1					ЗП5 СП1 СП2 СП3 СП4 ПП1	ЗП1 СП1 ПП1
РН 10	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП3 СП4 ПП1		ЗП1 ЗП3 СП1 СП2 ПП1	ЗП3 ЗП5 СП1 СП2 СП4 ПП1						ЗП4 ЗП5 СП1 СП2 СП3 СП5 ПП1				ЗП5 СП1 СП2 СП3 СП4 ПП1	
РН 11	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП3 СП4 ПП1		ЗП1 ЗП3 СП1 СП2 ПП1	ЗП3 ЗП5 СП1 СП2 СП4 ПП1							ЗП2 ПП1				ЗП1 СП1 ПП1
РН 12	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2		ЗП1 ЗП3 СП1 СП2 ПП1	ЗП3 ЗП5 СП1 СП2 СП4 ПП1					СП3 ПП1			ЗП4 ЗП5 СП1 СП2 СП3 СП5 ПП1			ЗП1 СП1 ПП1

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
	СП3 СП4 ПП1														
РН 13	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП3 СП4 ПП1		ЗП1 ЗП3 СП1 СП2 ПП1	ЗП3 ЗП5 СП1 СП2 СП4 ПП1									СП3 ПП1		ЗП1 СП1 ПП1
РН 14	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП3 СП4 ПП1		ЗП1 ЗП3 СП1 СП2 ПП1	ЗП3 ЗП5 СП1 СП2 СП4 ПП1					СП3 ПП1					ЗП5 СП1 СП2 СП3 СП4 ПП1	ЗП1 СП1 ПП1
РН 15				ЗП3 ЗП5 СП1 СП2 СП4 ПП1	ЗП1 ЗП3 ЗП5 СП1 СП2 СП3 ПП1										ЗП1 СП1 ПП1
РН 16	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2	ЗП1 ЗП5 СП1 СП2 СП4 ПП1	ЗП1 ЗП3 СП1 СП2 ПП1	ЗП3 ЗП5 СП1 СП2 СП4 ПП1				ЗП4 СП1 СП2 СП3 СП4 СП5 ПП1	СП3 ПП1	ЗП4 ЗП5 СП1 СП2 СП3 СП5 ПП1	ЗП2 ПП1	ЗП4 ЗП5 СП1 СП2 СП3 СП5 ПП1		ЗП5 СП1 СП2 СП3 СП4 ПП1	ЗП1 СП1 ПП1

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
	СП3 СП4 ПП1														
РН 17								ЗП4 СП1 СП2 СП3 СП4 СП5 ПП1							ЗП1 СП1 ПП1
РН 18	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП3 СП4 ПП1			ЗП3 ЗП5 СП1 СП2 СП4 ПП1	ЗП1 ЗП3 ЗП5 СП1 СП2 СП3 ПП1										ЗП1 СП1 ПП1
РН 19	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП3 СП4 ПП1			ЗП3 ЗП5 СП1 СП2 СП4 ПП1	ЗП1 ЗП3 ЗП5 СП1 СП2 СП3 ПП1	ЗП1 ЗП2 ЗП4 СП3 СП4 ПП1	ЗП3 СП1 СП2 ПП1	ЗП4 СП1 СП2 СП3 СП4 СП5 ПП1	СП3 ПП1		ЗП2 ПП1	ЗП4 ЗП5 СП1 СП2 СП3 СП5 ПП1	СП3 ПП1	ЗП5 СП1 СП2 СП3 СП4 ПП1	
РН 20	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2	ЗП1 ЗП5 СП1 СП2 СП4 ПП1	ЗП1 ЗП3 СП1 СП2 ПП1	ЗП3 ЗП5 СП1 СП2 СП4 ПП1	ЗП1 ЗП3 ЗП5 СП1 СП2 СП3 ПП1	ЗП1 ЗП2 ЗП4 СП3 СП4 ПП1		ЗП4 СП1 СП2 СП3 СП4 СП5 ПП1							

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
	СП3 СП4 ПП1														
РН 21	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП3 СП4 ПП1	ЗП1 ЗП5 СП1 СП2 СП4 ПП1	ЗП1 ЗП3 СП1 СП2 ПП1	ЗП3 ЗП5 СП1 СП2 СП4 ПП1		ЗП1 ЗП2 ЗП4 СП3 СП4 ПП1		ЗП4 СП1 СП2 СП3 СП4 СП5 ПП1		ЗП4 ЗП5 СП1 СП2 СП3 СП5 ПП1		ЗП3 СП1 СП2 СП3 СП5 ПП1	СП3 ПП1		
РН 22		ЗП1 ЗП5 СП1 СП2 СП4 ПП1	ЗП1 ЗП3 СП1 СП2 ПП1	ЗП3 ЗП5 СП1 СП2 СП4 ПП1		ЗП3 СП1 СП2 СП3 СП4 СП5 ПП1		ЗП4 СП1 СП2 СП3 СП4 СП5 ПП1							
РН 23	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП3 СП4 ПП1		ЗП1 ЗП3 СП1 СП2 ПП1	ЗП3 ЗП5 СП1 СП2 СП4 ПП1		ЗП3 СП1 СП2 СП3 СП4 СП5 ПП1	ЗП3 СП1 СП2 ПП1	ЗП4 СП1 СП2 СП3 СП4 СП5 ПП1			ЗП2 ПП1	ЗП3 СП1 СП2 СП3 СП5 ПП1	СП3 ПП1	ЗП5 СП1 СП2 СП3 СП4 ПП1	

8. РЕЗУЛЬТАТИ ОБГОВОРЕННЯ ОСВІТНЬОЇ ПРОГРАМИ

Стейкхолдери (вказати ПІБ та посаду, місце роботи)	Зауваження/Рекомендація	Враховано / частково враховано / не враховано	Примітка
Гарант ОПП, к.т.н., доц. Король О.Г. 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.
Гарант ОПП, к.т.н., доц. Король О.Г. завідувач кафедри, д.т.н., професор Євсеєв С.П. Члени робочої групи ОПП	З метою приведення у відповідність до сучасної термінології та стандартів вищої освіти оновити назви окремих дисциплін освітньої програми.	Враховано.	У межах періодичного перегляду освітньої програми з урахуванням рекомендацій стейкхолдерів, сучасних тенденцій розвитку галузі та актуалізації термінології було оновлено назви окремих навчальних дисциплін. Зміни мають редакційний характер і не впливають на зміст дисциплін, результати навчання, обсяг кредитів ЄКТС та структуру освітньої програми.
Волощук О. Б., к. т. н., керівник освітніх програм ТОВ “Distributed Lab”	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.	-	-
Опірський І. Р., доктор технічних наук, професор, завідувач кафедри захисту інформації Інституту комп’ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка»	Позитивний відгук. Без зауважень.	-	-

Завідувач кафедри кібербезпека _____ Сергій ЄВСЕЄВ

Гарант освітньої програми _____ Ольга КОРОЛЬ

9. ПЛАН ВРАХУВАННЯ ЗАУВАЖЕНЬ ТА ВИПРАВЛЕННЯ НЕДОЛІКІВ ЗА ОСВІТНЬОЮ ПРОГРАМОЮ

Рекомендації, надані під час останньої акредитації	Період врахування (короткостроковий/довгостроковий/ не доцільно враховувати)	Заходи, що спрямовані на врахування рекомендацій/Обгрунтування щодо недоцільності впровадження рекомендації	Терміни впровадження заходів/відповідальні особи
Загальні рекомендації Експертної групи та Галузевої експертної ради (по кафедрі, галузі, інституту, університету)			
Рекомендація 1 Посилити інформування здобувачів з нормативними документами та основними положеннями академічної доброчесності.	Довгостроковий	1) проведення постійної роз'яснювальної роботи серед викладачів та здобувачів освіти щодо підтримання культури академічної доброчесності; 2) інформування здобувачів про заходи з висвітлення питань академічної доброчесності, які на постійній основі проводяться співробітниками відділу забезпечення якості освітньої діяльності та науково-технічної бібліотеки НТУ «ХПІ»; 3) періодичне ознайомлення зацікавлених осіб з нормативно-правовими документами, в яких визначено політику та процедури дотримання академічної доброчесності в НТУ «ХПІ»: - «Правила поведінки здобувачів освіти в НТУ «ХПІ»; - «Правила внутрішнього розпорядку	Період часу до наступної акредитації ОП. Відповідальні: гарант ОП, викладачі кафедри.

		НТУ «ХПІ»; - «Кодекс етики академічних взаємовідносин та доброчесності НТУ «ХПІ»; - «Положення про систему запобігання та виявлення академічного плагіату у випускних кваліфікаційних роботах здобувачів вищої освіти НТУ «ХПІ»; 4) розміщення мотиваційних матеріалів на сайті кафедри САІТ. 5) інформування здобувачів проводиться постійно під час проведення лекційних занять з дисципліни «Основи наукових досліджень» Розглянуто на засіданні кафедри, протокол № 12 від 14.03.2025р.	
Рекомендація 2 Переглянути в наступній редакції ОПП перелік затверджених професійних стандартів в сфері кібербезпеки відповідно до Національного класифікатора професій України ДК 003:2010.	Довгостроковий	Оновлення у ОПП переліку затверджених професійних стандартів в сфері кібербезпеки відповідно до Національного класифікатора професій України ДК 003:2010. Розглянуто на засіданні кафедри, протокол № 9 від 16.01.2026р.	Період часу до наступної акредитації ОП. Відповідальні: гарант ОП.
Рекомендація 3 Розглянути можливість впровадження дуальної форми освіти на даній ОПП.	Довгостроковий	Розглянути можливість впровадження дуальної форми освіти на даній ОПП. Розглянуто на засіданні кафедри, протокол № 12 від 14.03.2025р.	Період часу до наступної акредитації ОП. Відповідальні: гарант ОП, завідувач кафедри, викладачі кафедри.

Рекомендація 4 Розмістити інформацію щодо вибіркових компонентів в ОПП у зручній для стейкхолдерів формі з чітким зазначенням компонент, доступних для вибору (посилання до вибіркових компонент, таблиці тощо).	Довгостроковий	Доопрацювати інформаційну структуру веб-сайту. Розроблено, опубліковано та оприлюднено на веб-сайті кафедри перелік вибіркових освітніх компонент із посиланням на Силабус. Розглянуто на засіданні кафедри, протокол № 9 від 16.01.2026р.	Період часу до наступної акредитації ОП. Відповідальні: гарант ОП.
Рекомендація 5 Залучення студентів до обговорення та оновлення ОПП.	Довгостроковий	Провести зустріч членів робочої групи з представниками студентського самоврядування. Розглянуто на засіданні кафедри, протокол № 1 від 26.03.2025р.	Період часу до наступної акредитації ОП. Відповідальні: гарант ОП, завідувач кафедри, викладачі кафедри.

Директор навчально-наукового інституту
комп’ютерних наук та інформаційних технологій_____Михайло ГОДЛЕВСЬКИЙ

Гарант освітньої програми _____Ольга КОРОЛЬ