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

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

ОСВІТНЬО-НАУКОВА 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-наукової 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 ОНП із спеціальності
«Кібербезпека та захист інформації»
Гарант ОНП
_____Станіслав МІЛЕВСЬКИЙ

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 ОНП)
№ групи КН-И1125
_____ Максим РОГОЗІН

«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-наукової 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-НАУКОВУ ПРОГРАМУ "КІБЕРБЕЗПЕКА"
другого (магістерського) рівня вищої освіти
спеціальності F5 "Кібербезпека та захист інформації"
кафедри кібербезпеки Національного технічного університету
"Харківський політехнічний інститут"

Освітньо-наукова програма (ОНП) "Кібербезпека" підготовки здобувачів вищої освіти другого (магістерського) рівня вищої освіти спеціальності F5 "Кібербезпека та захист інформації" галузі знань F "Інформаційні технології" розроблена науково-педагогічними працівниками Національного технічного університету "Харківський політехнічний інститут". Керівник проектної групи — гарант освітньої програми д.т.н., проф. Мілевський С. В. Подана на рецензування ОНП розроблена на основі стандарту вищої освіти України зі спеціальності F5 "Кібербезпека та захист інформації" другого (магістерського) рівня вищої освіти, затвердженого наказом МОН України від 18 березня 2021 р. N. 332. Представлена ОНП містить профіль освітньої програми за відповідною спеціальністю, перелік компонент освітньо-наукової програми та їх логічну послідовність, структурно-логічну схему, інформацію про форму атестації здобувачів вищої освіти.

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

Навчальний план включає обов'язкові компоненти загальної підготовки, такі як «Англійська мова в академічних застосунках» та «Інноваційне підприємництво та управління стартап-проєктами». Вони формують не лише технічні, а й комунікативні та управлінські компетенції, необхідні для роботи у сучасному бізнес-середовищі. Крім того, програма включає спеціалізовані дисципліни, зокрема "Основи наукових досліджень", "Філософські проблеми сучасного наукового пізнання", "Сучасні проблеми постквантової криптографії", "Аналіз шкідливих програм", "Авторське право у цифровому суспільстві", "Виявлення вторгнень у комп'ютерні мережі (мережеві аномалії)", "Технології управління безпекою бізнес-процесів" що дозволяє студентам отримати глибокі знання та навички, необхідні для забезпечення кіберзахисту сучасних інформаційних систем.

Програмні результати ОНП корелюють із складовими професійної компетентності, які формують фундаментальні знання та фахові навички, а загальні компетентності забезпечують розвиток навичок soft skills та сприяють формуванню свідомої громадянської позиції випускника з усталеними цінностями, здатністю до фахового розвитку і самовдосконалення. Фокус освітньо-наукової програми направлено на поглиблене вивчення механізмів та методів кіберзахисту соціокіберфізичних систем (об'єктів критичної інфраструктури) з комплексуванням з методами штучного інтелекту в умовах постквантового періоду, що додатково підкреслює сучасну спрямованість програми.

Програма також передбачає активне залучення студентів до науково-дослідної діяльності, включаючи участь у міжнародних конференціях, проєктах із кібербезпеки, стажування в провідних компаніях галузі. Такий підхід сприяє розвитку аналітичного мислення, навичок проведення досліджень та практичного застосування знань у реальних умовах.

Загалом освітньо-наукова програма підготовки здобувачів вищої освіти другого (магістерського) рівня вищої освіти галузі знань F "Інформаційні технології" за спеціальністю F5 "Кібербезпека та захист інформації" у Національному технічному університеті "Харківський політехнічний інститут" характеризується системністю і цільовим підходом до підготовки фахівців з кібербезпеки, відповідає сучасному рівню розвитку науки і практики освітньої діяльності та може бути рекомендована до впровадження в освітньому процесі університету.

ВІДДІЛ КАДРІВ 02071010

ерство освіти і науки україни
ціональний університет
ьвівська 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 ОПРСЬКИЙ

CIPI-IER

ТОВ «САЙФЕР ІТ»
Адреса: 04107, Київ, вул. Нагірна, 25-27
Тел.: +38 044 484 4612, 484 46 17
E-mail: info@cipher.com.ua

Системи захисту інформації
www.cipher.com.ua

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-НАУКОВУ ПРОГРАМУ "КІБЕРБЕЗПЕКА"

другого (магістерського) рівня вищої освіти

спеціальності F5 "Кібербезпека та захист інформації"

Національного технічного університету "Харківський політехнічний інститут"

Освітньо-наукова програма "Кібербезпека", що р,еалізуєтJ:,ся в рамках спеціальності F5 "Кібербезпека та захист інформації" на другому (магістерському) рівні вищої освіти у Національному технічному університеті "Харківський політехнічний інститут", повністю відповідає сучасним викликам ІТ-індустрії та вимогам стандарту вищої освіти. Програма забезпечує студентів фундаментальними знаннями та практичними навичками, необхідними для ефективного вирішення завдань у сфері кібербезпеки.

Основною метою програми є підготовка висококваліфікованих фахівців, здатних виконувати професійні завдання та проводити наукові дослідження у сфері інформаційної безпеки. Навчальний процес структурований таким чином, щоб охоплювати актуальні технологічні тренди та методи захисту інформації в інформаційно-комунікаційних системах. Дисципліни, що входять до програми, узгоджені зі світовими стандартами та вимогами сучасного ринку праці. Завдяки використанню сучасного обладнання та програмного забезпечення, студенти мають можливість отримати не лише теоретичні знання, а й практичний досвід у вирішенні реальних кейсів, пов'язаних із кібербезпекою.

Програма розроблена з урахуванням побажань стейкхолдерів, серед яких роботодавці, науковці та самі здобувачі вищої освіти. Вона спрямована на формування загальних і спеціалізованих компетентностей, що дозволяють випускникам ефективно працювати у сфері захисту інформації. Навчальний план включає дисципліни, орієнтовані на аналіз загроз, криптографічні методи захисту, аудит інформаційної безпеки та управління ризиками, що дозволяє випускникам бути конкурентоспроможними на ринку праці.

Крім того, значна увага приділяється дослідницькій діяльності студентів, яка дозволяє їм не лише засвоїти сучасні теоретичні концепції, а й розробляти власні підходи до забезпечення кібербезпеки. Магістранти мають змогу брати участь у наукових конференціях, хакатонах, дослідницьких проєктах, що сприяє розвитку їхніх професійних навичок і підготовці до майбутньої роботи в індустрії або академічній сфері.

Загалом, освітньо-наукова програма "Кібербезпека" магістерського рівня спеціальності F5 "Кібербезпека та захист інформації" містить усі необхідні елементи для підготовки сучасних фахівців, здатних вирішувати теоретичні й практичні завдання у сфері захисту інформації. Випускники програми зможуть працювати як у невеликих організаціях, так і в масштабних корпоративних середовищах, забезпечуючи надійний захист даних та інформаційних систем.

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-НАУКОВУ 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 ІТ-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-наукова програма має чітко визначені цілі, які враховують основні її особливості - підготовку фахівця з інформаційної безпеки широкого профілю зі знанням технологій програмування. Мобільність програми забезпечує своєчасне корегування в умовах стрімкого розвитку цієї спеціальності.

Сучасний стан кібербезпеки вимагає не лише глибоких теоретичних знань, а й практичних навичок у реальних умовах. Тому важливою складовою навчального процесу є інтеграція студентів у професійне середовище через практичні заняття, лабораторні роботи та стажування у провідних компаніях галузі. Запровадження симуляційних навчальних середовищ та віртуальних лабораторій дозволяє майбутнім фахівцям розвивати навички аналізу кібератак та реагування на інциденти безпеки.

Окрім цього, особливу увагу слід приділяти етичним аспектам кібербезпеки. Студенти повинні не лише засвоїти технічні методи захисту інформації, але й усвідомлювати юридичні та етичні межі застосування своїх фахових знань та навичок. Навчальні курси мають включати питання правового регулювання кіберпростору, принципів конфіденційності та відповідальності за збереження персональних даних. Такий підхід сприяє формуванню відповідальних фахівців, здатних приймати обґрунтовані рішення у складних ситуаціях.

Раніше, однією з основних проблем реалізації освітнього процесу за спеціальністю F5 "Кібербезпека та захист інформації" була відсутність можливості (в процесі навчання) отримати знання та навички від професіоналів-практиків. Зараз, в рамках викладання за освітньою програмою, що рецензується, залучено викладачів-практиків.

Вважаємо, що освітньо-наукова програма “Кібербезпека”, розроблена кафедрою кібербезпеки Національного технічного університету “Харківський політехнічний інститут”, містить усі необхідні компоненти для якісної підготовки висококваліфікованих фахівців, які зможуть ефективно працювати у сфері кібербезпеки та успішно влаштуватися на сучасному ринку праці.

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

Сергій ГОЛОВАШИЧ

РЕЦЕНЗІЯ-ВІДГУК

НА ОСВІТНЬО-НАУКОВУ 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-науковою програмою “Кібербезпека” другого (магістерського) рівня вищої освіти є актуальним напрямом освітньої діяльності університету, що дозволяє готувати конкурентоспроможних випускників в галузі безпеки об’єктів критичної інфраструктури.

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

В рамках освітньо-наукової програми “Кібербезпека”, яка складена кафедрою кібербезпеки Національного технічного університету “Харківський політехнічний інститут”, автори змогли досить органічно та логічно 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 ІТ сфері загалом.

Крім того, освітньо-наукова програма передбачає активну науково-дослідну діяльність студентів, що дозволяє їм отримувати практичний досвід у проведенні досліджень з питань кібербезпеки. Це сприяє розвитку критичного мислення, формуванню навичок аналізу та моделювання загроз, а також підготовці до подальшої роботи у сфері безпеки інформаційних систем та мереж.

Випускники програми не лише здобувають глибокі теоретичні знання, але й проходять практичну підготовку, що включає стажування в провідних ІТ-компаніях та державних структурах, які займаються питаннями інформаційної безпеки. Це значно підвищує їхню конкурентоспроможність на ринку праці та дає можливість інтегруватися в професійне середовище ще під час навчання.

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

Керівник освітніх програм
Компанії Distributed Lab,
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-наукову програму “Кібербезпека”
другого (магістерського) рівня вищої освіти
спеціальності F5 “Кібербезпека та захист інформації”
Національного технічного університету
“Харківський політехнічний інститут”

Поглиблений аналіз освітньо-наукової програми «Кібербезпека» за спеціальністю F5 «Кібербезпека та захист інформації» другого (магістерського) рівня вищої освіти в Національному технічному університеті Національний технічний університет «Харківський політехнічний інститут» засвідчує її системну спрямованість на формування дослідницьких і практичних компетентностей у сфері сучасної кібербезпеки та захисту інформації. В умовах стрімкого розвитку мережевих технологій і зростання складності кіберзагроз особливого значення набуває підготовка фахівців, здатних не лише застосовувати наявні засоби захисту, а й здійснювати науково обґрунтований аналіз, моделювання та прогнозування кіберризиків.

Структура освітньо-наукової програми передбачає поєднання фундаментальної теоретичної підготовки з активною дослідницькою діяльністю здобувачів. Значна увага приділяється поглибленому вивченню мережевих технологій, моделей OSI та TCP/IP, принципів функціонування протоколів Ethernet, ARP, ICMP, а також особливостей адресації IPv4/IPv6. У межах науково-дослідного компонента здобувачі виконують аналітичні та експериментальні роботи, спрямовані на виявлення вразливостей у мережевій інфраструктурі та оцінювання ефективності механізмів захисту.

Практична складова програми реалізується через лабораторні роботи на кіберполігоні та дослідницькі проєкти, де слухачі моделюють складні

мережеві середовища, впроваджують VLAN, DHCPv4, VPN-рішення та механізми IPsec. Окремий акцент робиться на дослідженні політик безпеки, налаштуванні ACL, а також оцінюванні ефективності систем виявлення та запобігання вторгненням (IDS/IPS) у контексті різних сценаріїв атак. Такий підхід забезпечує не лише формування практичних навичок, а й розвиток дослідницького мислення щодо оптимізації архітектури безпечних мереж.

Важливою складовою є поглиблена підготовка з системного адміністрування та аналізу безпеки операційних систем Windows і Linux. Здобувачі опановують методології моніторингу подій безпеки, аналізу журналів, управління привілеями та оцінювання стану захищеності кінцевих вузлів. Особлива увага приділяється дослідженню сучасних атак на endpoint-рівні та розробці підходів до їх виявлення і нейтралізації.

Освітньо-наукова програма також містить компоненти, що забезпечують розвиток дослідницьких і комунікаційних компетентностей, зокрема академічне письмо, підготовку наукових публікацій і професійне спілкування англійською мовою. Це сприяє інтеграції здобувачів у міжнародний науковий простір і підвищує їхню здатність презентувати результати досліджень на міжнародному рівні.

З метою подальшого розвитку програми доцільно посилити науково-дослідний компонент шляхом впровадження методів машинного навчання та штучного інтелекту для аналізу кіберінцидентів і виявлення аномалій у великих масивах даних. Перспективним є також розвиток напряму хмарної та контейнерної безпеки, зокрема дослідження захисту Kubernetes-інфраструктур, управління секретами та політиками доступу в хмарних середовищах. Додатково варто розширити міждисциплінарні дослідницькі проєкти, спрямовані на інтеграцію технічних і управлінських аспектів кібербезпеки.

Підсумовуючи, слід зазначити, що освітньо-наукова програма «Кібербезпека» за спеціальністю F5 «Кібербезпека та захист інформації» другого (магістерського) рівня вищої освіти в НТУ «ХПІ» характеризується

високим рівнем наукової та практичної підготовки здобувачів. Вона забезпечує формування комплексних компетентностей — від глибокого розуміння мережевих технологій і криптографічного захисту до здатності здійснювати наукові дослідження у сфері кібербезпеки, моделювати загрози та розробляти інноваційні підходи до захисту інформаційних систем.

Виконавчий директор
ГС «Харківський кластер
інформаційних технологій»,
2026 рік

Ольга ШАПОВАЛ

ПЕРЕДМОВА

Відповідає Стандарту вищої освіти другого (магістерського) рівня галузі знань «Інформаційні технології», спеціальністю F5 «Кібербезпека та захист інформації», який затверджено наказом Міністерства освіти і науки України від 18.03.2021 р. № 332.

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

Гарант освітньо-наукової програми
Станіслав МІЛЕВСЬКИЙ, доктор технічних наук, професор, професор кафедри кібербезпеки.

Члени робочої групи ОНП :
1. Сергій ЄВСЕЄВ, доктор технічних наук, професор, завідувач кафедри кібербезпеки.
2. Сергій ПОГАСІЙ, доктор технічних наук, професор, професор кафедри кібербезпеки.
3. Ольга КОРОЛЬ, кандидат технічних наук, доцент, доцент кафедри кібербезпеки.
4. Максим РОГОЗІН, студент групи КН-Н1125.

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 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)).
Офіційна назва освітньо-наукової програми	Кібербезпека
Назви спеціалізацій (предметних спеціальностей)	Відсутня
Тип диплому одиничний, спільний (подвійний) за наявності та обсяг освітньої програми	Диплом магістра, одиничний, 120 кредитів ЄКТС, термін навчання 1 рік 9 місяців
Наявність акредитації	Національне агентство забезпечення якості вищої освіти. Сертифікат про акредитацію освітньої програми № 20745. Термін дії – 01.07.2031р.
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-наукової програми	Відповідно до терміну дії сертифікату. Переглядається щорічно
Посилання на постійне розміщення опису освітньо-наукової програми	https://blogs.kpi.kharkov.ua/v2/quality/dokumenty/diyuchy-osvitni-programy/osvitnij-riven-magistr/
2 – Мета освітньо-наукової програми	
Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки, використовувати і впроваджувати технології та застосовувати засоби захисту в соціокіберфізичних	

системах (об’єктах критичної інфраструктури).	
3 – Характеристика освітньо-наукової програми	
Предметна область (галузь знань, спеціальність, 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-наукова. Підготовка фахівців у сфері кібербезпеки та захисту інформації.
Основний фокус освітньої програми та спеціалізації або предметна спеціальність (за наявності)	Поглиблене вивчення механізмів та методів кіберзахисту соціокіберфізичних систем (об'єктів критичної інфраструктури) з комплексуванням з методами штучного інтелекту в умовах постквантового періоду. Отримання сертифікатів курсів академії Cisco, сприяє підвищенню конкурентноспроможності на ринке праці, удосконаленню механізмів многоконтурних систем захисту соціокіберфізичних систем (об'єктів критичної інфраструктури). Ключові слова: кібербезпека, цифрова криміналістика, етичний хакінг.
Особливості програми	Особливостями програми є підготовка професіоналів, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки, формування у здобувачів навичок побудови многоконтурних систем захисту в соціокіберфізичних систем (об'єктах критичної інфраструктури) для забезпечення безпеки контуру бізнес-процесів в умовах постквантового періоду (появи повномасштабного квантового комп'ютеру). 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	Фахівці з кібербезпеки та захисту інформації можуть

працевлаштування	працювати, згідно з чинною редакцією Національного класифікатора України: Класифікатор професій ДК 003:2010, а саме: 2131.2 Розробник програмного забезпечення; 2149.2 Інженер (у галузі обчислювальної техніки); 2139.2 Професіонал в галузі обчислювальної техніки; 2433.2 Професіонал у галузі інформації та інформаційного аналізу; 2433.1 Науковий співробітник (інформаційна аналітика); 2112.1 Молодший науковий співробітник (у галузі інформаційних технологій); 2310 Викладач закладу вищої освіти; 1495 Менеджер (управитель) систем інформаційної безпеки.
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 науковими та технічними 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)	КЗ-1. Здатність застосовувати знання у практичних ситуаціях. КЗ-2. Здатність проводити дослідження на відповідному рівні. КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.

	КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Спеціальні (фахові) компетентності (визначені стандартом вищої освіти спеціальності)	КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури. КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. КФ8. Здатність досліджувати, розробляти,

	впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки. КФ11. Здатність здійснювати наукові та/або прикладні дослідження у галузі інформаційної безпеки та/або кібербезпеки із застосуванням сучасних експериментальних і теоретичних методів моделювання процесів, формувати науково-технічну звітність.
7 – Результати навчання	
Результати навчання за спеціальністю (визначені стандартом вищої освіти спеціальності)	РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН2. Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН3. 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. РН24. Планувати та виконувати наукові та прикладні дослідження у сфері інформаційної безпеки та/або кібербезпеки із застосуванням сучасних технологій, експериментальних і теоретичних методів і моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики. РН25. Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Відповідає кадровим вимогам щодо забезпечення

	провадження освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова кабінету міністрів України «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30 грудня 2015 р. № 1187, зі змінами, внесенимизгідно з Постановою КМ № 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 забезпечення	Відповідає технологічним вимогам щодо навчально-методичного та інформаційного забезпечення освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова Кабінету Міністрів України «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30 грудня 2015 р., № 1187, зі змінами, внесеними згідно з Постановою КМ № 365 від 24.03.2021, додаток 18). 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-onp-mahistry-obovyazkovi/). 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 освіти	Підготовка іноземних громадян здійснюється згідно з вимогами чинного законодавства за умови визнання попереднього освітнього рівня.

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

2.1 Перелік компонент освітньо-наукової програми

Код н/д	Компоненти освітньо-професійної програми	Кількість кредитів	Форма підсумкового контролю
1. Обов'язкові освітні компоненти			
1.1 Загальна підготовка			
ЗП1	*Академічна англійська мова*	*3,0*	*Залік*
ЗП2	*Інноваційне підприємництво та управління стартап-проєктами*	*3,0*	*Залік*
ЗП3	*Інтелектуальна власність*	*3,0*	*Залік*
ЗП4	*Безпека на основі штучного інтелекту*	*4,0*	*Екзамен*
ЗП5	*Безпека нейронних мереж*	*3,0*	*Залік*
1.2. Спеціальна (фахова) підготовка			
СП1	*Мережева та хмарна безпека*	*4,0*	*Екзамен*
СП2	*GEOINT-безпека*	*4,0*	*Екзамен*
СП3	*Цифрова криміналістика*	*4,0*	*Залік*
СП4	*Математичні моделі управління IT-проєктами в галузі захисту інформації*	*3,0*	*Залік*
СП5	*Сучасні проблеми постквантової криптографії*	*4,0*	*Залік*
СП6	*Безпека об'єктів крітичної інфраструктури*	*4,0*	*Залік*
СП7	*Авторське право у цифровому суспільстві*	*4,0*	*Залік*
СП8	*Безпека систем штучного інтелекту*	*4,0*	*Залік*
СП9	*Розробка програмного забезпечення систем кібербезпеки*	*5,0*	*Залік*
1.3. Наукова підготовка			
НП1	*Основи наукових досліджень*	*5,0*	*Екзамен*
НП2	*Філософські проблеми сучасного наукового пізнання*	*4,0*	*Екзамен*
НП3	*Захист розподілених сервісів і операційних платформ*	*4,0*	*Залік*
2. Науково-дослідницька практика			
ПП 1	*Науково-дослідницька практика*	*11,0*	*Залік*
3. Атестація			
А1	*Атестація*	*14,0*	
Загальний обсяг обов'язкових компонентів		***90***	
4. Вибіркові освітні компоненти			
4.1 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*
4.2. Освітні компонети вільного вибору загальної підготовки			
ОКЗП 1	*ОК ВВ ЗП1*	*3,0*	*Залік*
ОКЗП 2	*ОК ВВ ЗП2*	*3,0*	*Залік*
4.3. Освітні компоненти вільного вибору науково-професійного спрямування (НПС)			
ОКНПС 1	*ОК ВВ НПС 1*	*4,0*	*Залік*
ОКНПС 2	*ОК ВВ НПС 2*	*4,0*	*Залік*
Загальний обсяг вибіркових компонент:		***30***	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ:		***120***	

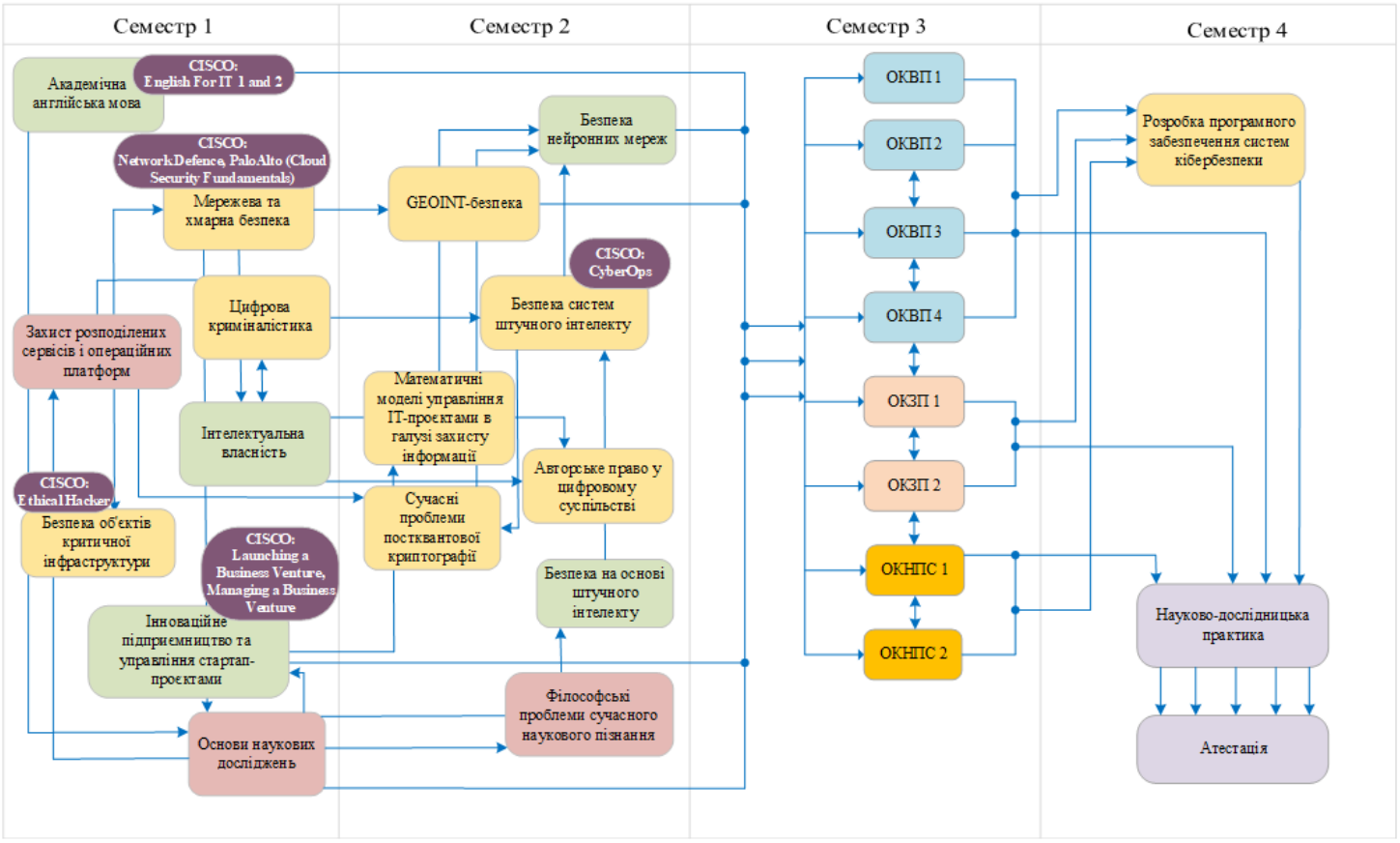
3. РОЗПОДІЛ ЗМІСТУ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ ЗА ГРУПАМИ КОМПОНЕНТІВ ТА ЦИКЛАМИ ПІДГОТОВКИ

№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	16 / 13,3	-	**16 / 13,3**
2	Спеціальна (фахова) підготовка	36 / 30	-	**36 / 30**
3	Наукова підготовка	13 / 10,8	-	**13 / 10,8**
4	Науково-дослідницька практика	11/9,2	-	**11/9,2**
5	Компоненти вільного вибору	-	30 / 25	**30 / 25**
6	Атестація	14/11,7	-	**14/11,7**
Всього за весь термін навчання		**90 / 75**	**30 / 25**	**120 / 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.

6. СТРУКТУРНО-ЛОГІЧНА СХЕМА



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

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

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**	**КФ 11***
РН 1	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП2 НП3 ПП1		ЗП3 ЗП5 СП3 СП4 СП5 СП7 СП9 НП1 НП2 НП3 ПП1			ЗП2 ЗП3 ЗП4 СП1 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП3 ПП1									
РН 2		ЗП3 ЗП5 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП3 ЗП5 СП3 СП4 СП5 СП7 СП9 НП1 НП2 НП3 ПП1			ЗП2 ЗП3 ЗП4 СП1 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП3 ПП1	ЗП2 ЗП3 ЗП4 ЗП5 СП3 СП5 СП7 СП8 СП9 НП1 НП3 ПП1	ЗП2 ЗП4 ЗП5 СП1 СП2 СП3 СП4 СП5 СП6 СП8 СП9 НП1 НП3 ПП1							ЗП2 ЗП3 ЗП4 СП5 СП8 СП9 НП1 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	КФ 11*
РН 3	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП2 НП3 ПП1					ЗП2 ЗП3 ЗП4 СП1 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП3 ПП1										ЗП2 ЗП3 ЗП4 СП5 СП8 СП9 НП1 ПП1
РН 4	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП2	ЗП3 ЗП5 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП3 ЗП5 СП3 СП4 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП2 ЗП3 ЗП5 СП2 СП4 СП5 СП7 СП8 СП9 НП1 НП2 НП3 ПП1		ЗП2 ЗП3 ЗП4 СП1 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП3 ПП1	ЗП2 ЗП3 ЗП4 ЗП5 СП3 СП5 СП7 СП8 СП9 НП1 НП3 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	КФ 11*
	НП3 ПП1															
РН 5			ЗП3 ЗП5 СП3 СП4 СП5 СП7 СП9 НП1 НП2 НП3 ПП1		ЗП3 ЗП5 СП2 СП3 СП5 СП7 СП9 НП1 НП2 НП3 ПП1		ЗП2 ЗП3 ЗП4 ЗП5 СП3 СП5 СП7 СП8 СП9 НП1 НП3 ПП1									ЗП2 ЗП3 ЗП4 СП5 СП8 СП9 НП1 ПП1
РН 6	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП2 НП3 ПП1			ЗП2 ЗП3 ЗП5 СП2 СП4 СП5 СП7 СП8 СП9 НП1 НП2 НП3 ПП1		ЗП2 ЗП3 ЗП4 СП1 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП3 ПП1		ЗП2 ЗП4 ЗП5 СП1 СП2 СП3 СП4 СП5 СП6 СП8 СП9 НП1 НП3 ПП1		ЗП2 ЗП4 ЗП5 СП1 СП2 СП3 СП6 СП7 СП8 СП9 НП1 НП3 ПП1	ЗП2 ЗП4 ЗП5 СП5 СП7 СП8 СП9 НП1 ПП1	ЗП2 ЗП4 СП1 СП2 СП3 СП5 СП6 СП8 СП9 НП1 НП3 ПП1		ЗП2 ЗП4 СП1 СП4 СП7 СП8 СП9 НП1 НП3 ПП1		
РН 7	ЗП1 ЗП2		ЗП3 ЗП5				ЗП2 ЗП3									

Результати навчання	Компетентності															
	Інтегральна компетентність															
	Загальні компетентності					Спеціальні (фахові) компетентності										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11*
	ЗП3 ЗП4 ЗП5 СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП2 НП3 ПП1		СП3 СП4 СП5 СП7 СП9 НП1 НП2 НП3 ПП1				ЗП4 ЗП5 СП3 СП5 СП7 СП8 СП9 НП1 НП3 ПП1									
РН 8	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП2 НП3 ПП1	ЗП3 ЗП5 СП5 СП7 СП9 НП1 НП2 НП3 ПП1		ЗП2 ЗП3 ЗП5 СП2 СП4 СП5 СП7 СП8 СП9 НП1 НП2 НП3 ПП1	ЗП3 ЗП5 СП2 СП3 СП5 СП7 СП9 НП1 НП2 НП3 ПП1			ЗП2 ЗП4 ЗП5 СП1 СП2 СП3 СП4 СП5 СП6 СП8 СП9 НП1 НП3 ПП1						ЗП2 ЗП4 СП1 СП4 СП7 СП8 СП9 НП1 НП3 ПП1	ЗП4 СП7 НП1 ПП1	
РН 9	ЗП1	ЗП3	ЗП3	ЗП2					ЗП2					ЗП2	ЗП4	

Результати навчання	Компетентності															
	Інтегральна компетентність															
	Загальні компетентності					Спеціальні (фахові) компетентності										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11*
	ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП2 НП3 ПП1	ЗП5 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП5 СП3 СП4 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП3 ЗП5 СП2 СП4 СП5 СП7 СП8 СП9 НП1 НП2 НП3 ПП1					ЗП4 ЗП5 СП1 СП3 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП3 ПП1					ЗП4 СП1 СП4 СП7 СП8 СП9 НП1 НП3 ПП1	СП7 НП1 ПП1	
РН 10	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП2 НП3 ПП1		ЗП3 ЗП5 СП3 СП4 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП2 ЗП3 ЗП5 СП2 СП4 СП5 СП7 СП8 СП9 НП1 НП2 НП3 ПП1						ЗП2 ЗП4 ЗП5 СП1 СП2 СП3 СП6 СП7 СП8 СП9 НП1 НП3 ПП1				ЗП2 ЗП4 СП1 СП4 СП7 СП8 СП9 НП1 НП3 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	КФ 11*
РН 11	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП2 НП3 ПП1		ЗП3 ЗП5 СП3 СП4 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП2 ЗП3 ЗП5 СП2 СП4 СП5 СП7 СП8 СП9 НП1 НП2 НП3 ПП1							ЗП2 ЗП4 ЗП5 СП5 СП7 СП8 СП9 НП1 ПП1				ЗП4 СП7 НП1 ПП1	
РН 12	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП2 НП3		ЗП3 ЗП5 СП3 СП4 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП2 ЗП3 ЗП5 СП2 СП4 СП5 СП7 СП8 СП9 НП1 НП2 НП3 ПП1					ЗП2 ЗП4 ЗП5 СП1 СП3 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП3 ПП1			ЗП2 ЗП4 СП1 СП2 СП3 СП5 СП6 СП8 СП9 НП1 НП3 ПП1			ЗП4 СП7 НП1 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	КФ 11*
	ПП1															
РН 13	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП2 НП3 ПП1		ЗП3 ЗП5 СП3 СП4 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП2 ЗП3 ЗП5 СП2 СП4 СП5 СП7 СП8 СП9 НП1 НП2 НП3 ПП1									ЗП2 ЗП4 СП1 СП5 СП9 НП1 НП3 ПП1		ЗП4 СП7 НП1 ПП1	
РН 14	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП2		ЗП3 ЗП5 СП3 СП4 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП2 ЗП3 ЗП5 СП2 СП4 СП5 СП7 СП8 СП9 НП1 НП2 НП3 ПП1					ЗП2 ЗП4 ЗП5 СП1 СП3 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП3 ПП1					ЗП2 ЗП4 СП1 СП4 СП7 СП8 СП9 НП1 НП3 ПП1	ЗП4 СП7 НП1 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	КФ 11*
	НП3 ПП1															
РН 15				ЗП2 ЗП3 ЗП5 СП2 СП4 СП5 СП7 СП8 СП9 НП1 НП2 НП3 ПП1	ЗП3 ЗП5 СП2 СП3 СП5 СП7 СП9 НП1 НП2 НП3 ПП1										ЗП4 СП7 НП1 ПП1	
РН 16	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП2 НП3 ПП1	ЗП3 ЗП5 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП3 ЗП5 СП3 СП4 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП2 ЗП3 ЗП5 СП2 СП4 СП5 СП7 СП8 СП9 НП1 НП2 НП3 ПП1				ЗП2 ЗП4 ЗП5 СП1 СП2 СП3 СП4 СП5 СП6 СП8 СП9 НП1 НП3 ПП1	ЗП2 ЗП4 ЗП5 СП1 СП3 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП3 ПП1	ЗП2 ЗП4 ЗП5 СП1 СП2 СП3 СП4 СП6 СП7 СП8 СП9 НП1 НП3 ПП1	ЗП2 ЗП4 ЗП5 СП5 СП7 СП8 СП9 НП1 ПП1	ЗП2 ЗП4 СП1 СП2 СП3 СП5 СП6 СП8 СП9 НП1 НП3 ПП1		ЗП2 ЗП4 СП1 СП4 СП7 СП8 СП9 НП1 НП3 ПП1	ЗП4 СП7 НП1 ПП1	ЗП2 ЗП3 ЗП4 СП5 СП8 СП9 НП1 ПП1
РН 17								ЗП2							ЗП4	

Результати навчання	Компетентності															
	Інтегральна компетентність															
	Загальні компетентності					Спеціальні (фахові) компетентності										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11*
								ЗП4 ЗП5 СП1 СП2 СП3 СП4 СП5 СП6 СП8 СП9 НП1 НП3 ПП1							СП7 НП1 ПП1	
РН 18	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП2 НП3 ПП1			ЗП2 ЗП3 ЗП5 СП2 СП4 СП5 СП7 СП8 СП9 НП1 НП2 НП3 ПП1	ЗП3 ЗП5 СП2 СП3 СП5 СП7 СП9 НП1 НП2 НП3 ПП1										ЗП4 СП7 НП1 ПП1	
РН 19	ЗП1 ЗП2			ЗП2 ЗП3	ЗП3 ЗП5	ЗП2 ЗП3	ЗП2 ЗП3	ЗП2 ЗП4	ЗП2 ЗП4		ЗП2 ЗП4	ЗП2 ЗП4	ЗП2 ЗП4	ЗП2 ЗП4		

Результати навчання	Компетентності															
	Інтегральна компетентність															
	Загальні компетентності					Спеціальні (фахові) компетентності										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11*
	ЗП3 ЗП4 ЗП5 СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП2 НП3 ПП1			ЗП5 СП2 СП4 СП5 СП7 СП8 СП9 НП1 НП2 НП3 ПП1	СП2 СП3 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП4 СП1 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП3 ПП1	ЗП4 ЗП5 СП3 СП5 СП7 СП8 СП9 НП1 НП3 ПП1	ЗП5 СП1 СП2 СП3 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП3 ПП1	ЗП5 СП1 СП3 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП3 ПП1		ЗП5 СП5 СП7 СП8 СП9 НП1 ПП1	СП1 СП2 СП3 СП5 СП6 СП8 СП9 НП1 НП3 ПП1	СП1 СП5 СП9 НП1 НП3 ПП1	СП1 СП4 СП7 СП8 СП9 НП1 НП3 ПП1		
РН 20	ЗП1 ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП2 НП3 ПП1	ЗП3 ЗП5 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП3 ЗП5 СП3 СП4 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП2 ЗП3 ЗП5 СП2 СП4 СП5 СП7 СП8 СП9 НП1 НП2 НП3 ПП1	ЗП3 ЗП5 СП2 СП3 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП2 ЗП3 ЗП4 СП1 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП3 ПП1		ЗП2 ЗП4 ЗП5 СП1 СП2 СП3 СП4 СП5 СП6 СП8 СП9 НП1 НП3 ПП1								ЗП2 ЗП3 ЗП4 СП5 СП8 СП9 НП1 ПП1
РН 21	ЗП1	ЗП3	ЗП3	ЗП2		ЗП2		ЗП2		ЗП2		ЗП2	ЗП2			ЗП2

Результати навчання	Компетентності															
	Інтегральна компетентність															
	Загальні компетентності					Спеціальні (фахові) компетентності										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11*
	ЗП2 ЗП3 ЗП4 ЗП5 СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП2 НП3 ПП1	ЗП5 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП5 СП3 СП4 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП3 ЗП5 СП2 СП4 СП5 СП7 СП8 СП9 НП1 НП2 НП3 ПП1		ЗП3 ЗП4 СП1 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП3 ПП1		ЗП4 ЗП5 СП1 СП2 СП3 СП4 СП5 СП6 СП8 СП9 НП1 НП3 ПП1		ЗП4 ЗП5 СП1 СП2 СП3 СП6 СП7 СП8 СП9 НП1 НП3 ПП1		ЗП4 СП1 СП2 СП3 СП5 СП6 СП8 СП9 НП1 НП3 ПП1	ЗП4 СП1 СП5 СП9 НП1 НП3 ПП1			ЗП3 ЗП4 СП5 СП8 СП9 НП1 ПП1
РН 22		ЗП3 ЗП5 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП3 ЗП5 СП3 СП4 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП2 ЗП3 ЗП5 СП2 СП4 СП5 СП7 СП8 СП9 НП1 НП2 НП3 ПП1		ЗП2 ЗП3 ЗП4 СП1 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП3 ПП1		ЗП2 ЗП4 ЗП5 СП1 СП2 СП3 СП4 СП5 СП6 СП8 СП9 НП1 НП3 ПП1								ЗП2 ЗП3 ЗП4 СП5 СП8 СП9 НП1 ПП1
РН 23	ЗП1 ЗП2		ЗП3 ЗП5	ЗП2 ЗП3		ЗП2 ЗП3	ЗП2 ЗП3	ЗП2 ЗП4			ЗП2 ЗП4	ЗП2 ЗП4	ЗП2 ЗП4	ЗП2 ЗП4		

Результати навчання	Компетентності															
	Інтегральна компетентність															
	Загальні компетентності					Спеціальні (фахові) компетентності										
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11*
	ЗП3 ЗП4 ЗП5 СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП2 НП3 ПП1		СП3 СП4 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП5 СП2 СП4 СП5 СП7 СП8 СП9 НП1 НП2 НП3 ПП1		ЗП4 СП1 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП3 ПП1	ЗП4 ЗП5 СП3 СП5 СП7 СП8 СП9 НП1 НП3 ПП1	ЗП5 СП1 СП2 СП3 СП4 СП5 СП6 СП8 СП9 НП1 НП3 ПП1			ЗП5 СП5 СП7 СП8 СП9 НП1 ПП1	СП1 СП2 СП3 СП5 СП6 СП8 СП9 НП1 НП3 ПП1	СП1 СП5 СП9 НП1 НП3 ПП1	СП1 СП4 СП7 СП8 СП9 НП1 НП3 ПП1		
Додатково для освітньо-наукових програм*																
РН 24		ЗП3 ЗП5 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП3 ЗП5 СП3 СП4 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП2 ЗП3 ЗП5 СП2 СП4 СП5 СП7 СП8 СП9 НП1 НП2 НП3 ПП1	ЗП3 ЗП5 СП2 СП3 СП5 СП7 СП9 НП1 НП2 НП3 ПП1			ЗП2 ЗП4 ЗП5 СП1 СП2 СП3 СП4 СП5 СП6 СП8 СП9 НП1 НП3 ПП1							ЗП4 СП7 НП1 ПП1	ЗП2 ЗП3 ЗП4 СП5 СП8 СП9 НП1 ПП1
РН 25	ЗП1 ЗП2	ЗП3 ЗП5	ЗП3 ЗП5	ЗП2 ЗП3				ЗП2 ЗП4								ЗП2 ЗП3

Результати навчання	Компетентності														
	Інтегральна компетентність														
	Загальні компетентності					Спеціальні (фахові) компетентності									
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10	КФ 11*
	ЗП3 ЗП4 ЗП5 СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 НП1 НП2 НП3 ПП1	СП5 СП7 СП9 НП1 НП2 НП3 ПП1	СП3 СП4 СП5 СП7 СП9 НП1 НП2 НП3 ПП1	ЗП5 СП2 СП4 СП5 СП7 СП8 СП9 НП1 НП2 НП3 ПП1				ЗП5 СП1 СП2 СП3 СП4 СП5 СП6 СП8 СП9 НП1 НП3 ПП1								ЗП4 СП5 СП8 СП9 НП1 ПП1

8. РЕЗУЛЬТАТИ ОБГОВОРЕННЯ ОСВІТНЬОЇ ПРОГРАМИ

Стейкхолдери (вказати ПІБ та посаду, місце роботи)	Рекомендація	Враховано / частково враховано / не враховано	Примітка
Гарант ОНП, д.т.н., проф. Мілевський С.В. завідувач кафедри, д.т.н., професор Євсеєв С.П. Члени робочої групи ОНП	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.	-	-
Опірський І. Р., доктор технічних наук, професор, завідувач кафедри захисту інформації Інституту комп’ютерних технологій, автоматики та метрології Національного університету	Позитивний відгук. Без зауважень.	-	-

«Львівська політехніка»			
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.	-	-

Завідувач кафедри кібербезпека _____ Сергій ЄВСЕЄВ

Гарант освітньої програми _____ Станіслав МІЛЕВСЬКИЙ

9. ПЛАН ВРАХУВАННЯ ЗАУВАЖЕНЬ ТА ВИПРАВЛЕННЯ НЕДОЛІКІВ ЗА ОСВІТНЬОЮ ПРОГРАМОЮ

Рекомендації, надані під час останньої акредитації	Період врахування (короткостроковий/довгостроковий/не доцільно враховувати)	Заходи, направлені на врахування рекомендацій	Терміни впровадження заходів
Рекомендації експертної групи та Галузевої експертної ради			
Рекомендація 1 Уточнити перелік релевантних професійних назв робіт відповідно до Національного класифікатора професій для чіткого окреслення меж професійної придатності випускників.	Довгостроковий	Уточнено перелік професійних назв робіт відповідно до Національного класифікатора професій України ДК 003:2010	Період часу до наступної акредитації ОП. Відповідальні: гарант ОП.
Рекомендація 2 Доцільним є запровадження елементів дуальної освіти з урахуванням налагодженої співпраці з роботодавцями, а також розширення міжнародної співпраці з метою активізації академічної мобільності здобувачів і науково-педагогічних працівників.	Довгостроковий	Рекомендацію враховано. З метою її реалізації в освітньо-науковій програмі передбачено впровадження елементів дуальної форми здобуття освіти шляхом залучення роботодавців до організації освітнього процесу, зокрема до проведення практичної підготовки, стажувань та виконання спільних науково-прикладних проєктів.	Період часу до наступної акредитації ОП. Відповідальні: гарант ОП, завідувач кафедри, викладачі кафедри.
Рекомендація 3 Рекомендується посилити практичну складову підготовки через залучення здобувачів до роботи з фізичним обладнанням, удосконалити процедури інформування щодо цілей і результатів навчання, забезпечити доступність	Довгостроковий	Рекомендацію щодо посилення практичної складової підготовки здобувачів буде враховано та поступово впроваджено в освітній процес. Зокрема, передбачається розширення залучення здобувачів до роботи з фізичним обладнанням у	Період часу до наступної акредитації ОП. Відповідальні: гарант ОП, завідувач кафедри, викладачі кафедри.

репозитарію кваліфікаційних робіт та врегулювати внутрішні нормативні процедури.		межах лабораторних занять та практикумів.	
Рекомендація 4 Рекомендується удосконалити механізми визнання результатів неформальної та інформальної освіти, вилучити формулювання, що обмежують такі можливості у силабусах, а також формалізувати процедури інформування здобувачів щодо освітніх компонентів.	Довгостроковий	Передбачається актуалізація положень, що регламентують процедуру визнання результатів навчання, здобутих у неформальній та інформальній освіті, відповідно до чинного законодавства. Здійснено перегляд силабусів освітніх компонентів з метою вилучення формулювань, які можуть обмежувати можливість зарахування результатів неформального навчання.	Період часу до наступної акредитації ОП. Відповідальні: гарант ОП, завідувач кафедри, викладачі кафедри.
Рекомендація 5 Також рекомендовано забезпечити повну відповідність аудиторій вимогам безпеки, підвищити рівень безбар'єрності для доступності для осіб з особливими потребами та активніше залучати здобувачів до процедур перегляду й оновлення програми.	Довгостроковий	Передбачено поетапне приведення аудиторного фонду у відповідність до вимог безпеки, посилення заходів із забезпечення безбар'єрності для осіб з особливими освітніми потребами, а також розширення залучення здобувачів вищої освіти до процедур перегляду та оновлення освітніх програм.	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 _____Станіслав МІЛЕВСЬКИЙ