



MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
NATIONAL TECHNICAL UNIVERSITY
"KHARKIV POLYTECHNIC INSTITUTE"

APPROVED



_____/ Rector of NTU "KhPI"

_____/ Yevgen SOKOL

"30" березня 2026

EDUCATIONAL AND PROFESSIONAL PROGRAM
"CYBERSECURITY"

Second (Master's) level of higher education

in specialty

F5 – Cybersecurity and information protection

fields of knowledge

F - Information technologies

qualification

Master of cybersecurity and information protection

APPROVED

ACADEMIC COUNCIL OF NTU

"Khpi"

Head of the academic council

_____/ Yevgen SOKOL

Protocol №. 4

From March, 28 2026

Kharkiv 2026

LETTER OF AGREEMENT

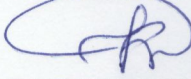
Educational and professional program «Cybersecurity»

Level of higher education	<u>Second (Master's) level</u>
Branch of knowledge	<u>F Information technologies</u>
Specialty	<u>F5 Cybersecurity and information protection</u>
Qualification	<u>Master of cybersecurity and information protection</u>

APPROVED

The EPP workgroups for the specialty
«Cybersecurity and information
protection»

Guarantor of the educational program

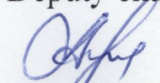

_____ Olga KOROL

Protocol №. 1

From January, 16 2026

RECOMMENDED

Methodical council of NTU “KhPI”
Deputy chairman of the methodical council



_____ Ruslan MYGUSHCHENKO

Protocol №. 3

From March, 25 2026

AGREED

Head of the Department of Cybersecurity

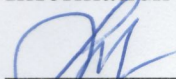

_____ Sergii YEVSEIEV

Protocol №. 12

From March, 23 2026

AGREED

Director of the Educational and Scientific
Institute of Computer Science and
Information Technology

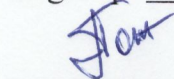

_____ Mykhailo HODLEVSKYI

« » _____ 2026

AGREED

Higher education
(member of the EPP workgroup)

№ group KH-M1125


_____ Pavlo POZHODAIEV

March, 23 2026

APPROVED AND GRANTED

By order of the rector of the National Technical University "Kharkiv Polytechnic Institute" from
April 02, 2026 No. 119 ОД.

This educational and professional program cannot be fully or partially reproduced, reproduced and distributed without the permission of the National Technical University «Kharkiv Polytechnic Institute».

REVIEWERS:

Productive remarks and feedback on the project of the educational-professional program received from:

1. OPIRSKY Ivan, Doctor of Technical Sciences, Professor, Head of the Department of Information Protection of the Institute of Computer Technology, Automation and Metrology of the National University "Lviv Polytechnic".
2. KOVTUN Vladyslav, Candidate of Technical Sciences, Associate Professor, "Syfer" LLC general director.
3. GOLOVASHYCH Serhii, Candidate of Technical Sciences, Associate Professor, LLC "Microcrypt Technologies" general director.
4. VOLOSHCHUK Olena, Candidate of Technical Sciences, Head of Educational Programs of Distributed Lab LLC.
5. SHAPOVAL Olga, Executive Director of Kharkiv Cluster of Information Technology

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.

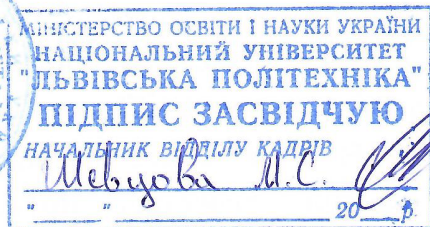
Навчальний план включає обов’язкові дисципліни загальної підготовки, такі як «Англійська мова в академічних застосунках», «Інноваційне підприємництво та управління стартапами», «Безпека Інтернет речей та сервісів» та «Етичний хакінг». Вони формують не лише технічні, а й комунікативні та управлінські 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.

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



Іван ОПІРСЬКИЙ

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 практики у рішенні завдань, які моделюють існуючі виробничі процеси та інциденти кібербезпеки.

Програма обговорювалась зі стейкхолдерами, враховує побажання здобувачів вищої освіти та спрямована на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю 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 Текнолоджіс»

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, проектування 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 Текнолоджіс»
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.

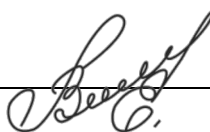
Схема підготовки фахівців за освітньо-професійною програмою, що акредитується, є правильно побудованою: врахована необхідність отримання студентами знань з дисциплін професійного змісту, які повністю покривають результати навчання, що передбачені стандартом вищої освіти зі спеціальності F5 “Кібербезпека та захист 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 сформулювати схему підготовки майбутнього фахівця, яка, з одного боку, дозволяє освітній програмі забезпечувати реалізацію результатів навчання передбачених стандартом вищої освіти в повному обсязі, а, з іншого боку, завдяки акценту на технологіях програмування випускники мають можливість працевлаштовуватися не тільки за спеціальністю, але і в ІТ сфері загалом.

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

Керівник освітніх програм
Компанії Distributed Lab,
кандидат технічних наук
2026 рік



Олена ВОЛОЩУК



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

PREFACE

Corresponds to the Standard of Higher Education of the second (Master's) level in specialty F5 "Cybersecurity and information protection", which was approved by the order of the Ministry of Education and Science of Ukraine dated 18.03.2021 No. 332.

Developed by the working group of the EPP "Cybersecurity"
Educational and Scientific Institute of Computer Sciences and Information Technologies of the National Technical University "Kharkiv Polytechnic Institute" consisting of:

Guarantor of the educational and professional program

KOROL Olga, candidate of technical sciences, associate professor, associate professor of the cybersecurity department.

Members of the workgroup EPP:

1. YEVSEIEV Sergii, doctor of technical sciences, professor, head of the cybersecurity department.
2. POHASII Serhii, doctor of technical sciences, professor, professor of the cybersecurity department.
3. MILEVSKYI Stanislav, doctor of technical sciences, professor, professor of the cybersecurity department
4. POZHDAIEV Pavlo, student, group KH- M1125.

1. PROFILE OF THE EDUCATIONAL AND PROFESSIONAL PROGRAM BY SPECIALTY F5 – CYBERSECURITY AND INFORMATION PROTECTION

1 - General information	
Higher education institution and structural unit	National Technical University "Kharkiv Polytechnic Institute", Educational and Scientific Institute <u>of Computer Sciences and Information Technologies</u> department <u>of cybersecurity</u>
The degree of higher education and the title of the qualification in the original language	The degree of higher education – Master Branch of knowledge – F Information technologies Specialty – F5 Cybersecurity and information protection Educational qualification – master of cybersecurity and information protection.
Professional qualification	There is no
Form of study	Institutional (full -time), remote)
The official name of the educational program	Cybersecurity
Names of specializations (subject specialties)	There is no
Type of diploma single, common (double) in the presence and volume of educational program	Master's Diploma, Single, 90 ECTS credits, study period 1 year 4 months
Availability of accreditation	National Higher Education Quality Agency. Accreditation certificate educational program No. 6112 Valid up to 01.07.2029
Cycle/level	second (master's) level of higher education; NRK of Ukraine – level 7, FQ-EHEA – second cycle, EQF LLL – level 7
Prerequisites	The presence of higher education first (bachelor) level.
Language of teaching	Ukrainian, English
The term of validity of the educational program	According to the validity of the certificate Reviewed annually
Link to the permanent posting of the description of the educational program	https://blogs.kpi.kharkov.ua/v2/quality/dokumenty/diyuchy-osvitni-programy/osvitnij-riven-magistr/
2 - The purpose of the educational and professional program	
Training specialists capable of solving research and/or innovative tasks in the field of information and/or cybersecurity, use and introduce technologies and use the means of protection in the safety systems of the contour of business processes.	
3 – Characteristics of the educational and professional program	
Subject area (field of knowledge, specialty,	Field of knowledge: F "Information technologies" Specialty: F5 "Cybersecurity and information protection"

specialization or subject specialty (if any)

Object of study:

- modern processes of research, analysis, creation and maintenance of information systems and technologies, other business operational processes on the objects of information activity and critical infrastructures of the field of information security and/or cybersecurity;
- information systems (information, communication, information and telecommunication, automated) and technologies;
- infrastructure of information activity and critical infrastructure;
- systems and complexes of creation, processing, transmission, storage, destruction, protection and display of data (information flows);
- information resources of different classes (including state information resources);
- software and software (means) of cyber defense;
- information safety and/or cybersecurity management systems;
- technologies, methods, models and information security and/or cybersecurity.

Training goals: training of specialists who can solve research and/or innovative problems in the field of information and/or cybersecurity.

Theoretical content of the subject area: theoretical foundations of science -intensive technologies, physical and mathematical fundamental knowledge, theories of identification and decision -making, systematic analysis, complex systems, modeling and optimization of processes, theory of mathematical statistics, cryptographic and technical protection.

Methods , techniques and technologies : methods, models, techniques and technologies of creation, processing, transmission, acceptance, destruction, protection, protection (cyber defense) of information resources in cyberspace, as well as methods and models of development and use of applied and specialized software for solving professional problems in the field of information security and/or cybersecurity.

Technologies, methods and models of research, analysis, management and provision of business/operational processes with the use of a set of regulatory and organizational and technical methods and means of protection of information resources in cyberspace.

Tools and equipment : tools, devices, network equipment and environment, applied and specialized software, automated

	systems and design complexes, modeling, operation, control, monitoring, processing, displaying and protection of data (information flows), as well as methods and models of risk theory and management of information resources in the study and supporting information security and/or cybersecurity objects.
Orientation of the educational program	Educational and professional. Professional training in cybersecurity and information protection.
The main focus of the educational program and specialization or subject specialty (if any)	An in-depth study of both external and inner audits to ensure the safety of business processes. Obtaining Cisco Academy Certificates contributes to increased competitiveness in the labor market, improving audit mechanisms and protection by peace methods. Keywords: cybersecurity, digital forensics, ethical hacking.
Features of the program	The peculiarities of the program are the formation of the skills of constructing complex information security systems for ensuring the safety of business processes on the basis of modern technologies and software applications, in the conditions of development of digital economy. Orientation to partnership with domestic and foreign educational and science institutions, private sector, scientists and practitioners, participation in international programs of joint diplomas. Ability to learn English.
4 – Eligibility of graduates to employment and academic rights of graduates	
Suitability for employment	Cybersecurity and information protection experts can work in accordance with the current version of the National Classifier of Ukraine: Classifier of Professions DK 003: 2010, namely: 2139.2 Security threats; 2139.2 Analyst of information protection systems and vulnerability assessment; 2139.2 Analyst for the safety of information and communication systems; 2139.2 Investigator (cybersecurity and information security); 2139.2 Digital forensic expert (cybersecurity and information security); 2139.2 Forensic examination expert (cybersecurity and information protection); 2139.2 Investigator of cybercrime.
Academic rights of graduates	Students who have been trained under this curriculum and received a master's degree have the right to receive education at the third (educational and scientific) level of higher education in the HUB of Ukraine and abroad in the field of

	knowledge "information technologies" or related. Acquisition of additional qualifications in the adult education system.
5 – Teaching and assessment	
Teaching and learning	The teaching process provides for the use of educational technologies such as: lectures, laboratory work, practical classes, small groups, presentations that develop communicative and leadership skills, independent work with literary sources.
Assessment	Rating system of evaluation. Current and final knowledge control (surveys, control and individual tasks, testing, etc.), tests and exams (oral and written), public protection of qualification or project. The evaluation system involves the use of the ECTS International System (with estimates A, B, C, D, E, F), the national system (with "excellent", "good", "satisfactory" and "unsatisfactory"), as well as a 100-point system of higher education institution with a established system of conformity.
6 – Software competencies	
Integral competence	The ability of a person to solve research and/or innovative problems in the field of information security and/or cybersecurity.
General competencies (GC) (defined by the standard of higher education of the specialty)	GC1. Ability to apply knowledge in practical situations. GC2. Ability to conduct research at an appropriate level. GC3. Ability to abstract thinking, analysis and synthesis. GC4. The ability to evaluate and ensure the quality of the work performed. GC5. The ability to communicate with representatives of other professional groups of different levels (with experts from other fields of knowledge / types of economic activity).
Special competences (SC) (defined by the standard of higher education of the specialty)	SC1. The ability to reasonably apply, integrate, develop and improve modern information technologies, physical and mathematical models, as well as technologies for creating and using applied and specialized software to solve professional problems in the field of information security and/or cyber security. SC2. Ability to develop, implement and analyze regulatory documents, provisions, instructions and requirements of technical and organizational direction, as well as integrate, analyze and use the best global practices, standards in professional activities in the field of information security and/or cyber security. SC3. Ability to research, develop and support methods and means of information security and/or cyber security at objects of information activity and critical infrastructure.

	<p>SC4. The ability to analyze, develop and support the information security and/or cyber security management system of the organization, to form information security strategy and policies taking into account domestic and international standards and requirements.</p> <p>SC5. The ability to research, system analysis and ensure the continuity of business/operational processes in order to determine the vulnerabilities of information systems and resources, analyze risks and determine the assessment of their impact in accordance with the established strategy and policy of information security and/or cyber security of the organization.</p> <p>SC6. The ability to analyze, control and provide a management system for access to information resources in accordance with the established strategy and policy of information security and/or cyber security of the organization.</p> <p>SC7. The ability to research, develop and implement methods and measures to counter cyber incidents, implement management, control and investigation procedures, as well as provide recommendations for the prevention and analysis of cyber incidents in general.</p> <p>SC8. The ability to research, develop, implement and support methods and means of cryptographic and technical protection of information at objects of information activity and critical infrastructure, in information systems, as well as the ability to evaluate the effectiveness of their use, according to the established strategy and policy of information security and/or cyber security of the organization.</p> <p>SC9. The ability to analyze, develop and support the system of auditing and monitoring the effectiveness of the functioning of information systems and technologies, business/operational processes in the field of information security and/or cyber security of the organization as a whole.</p> <p>SC10. The ability to conduct scientific and pedagogical activities, plan training, monitor and support work with personnel, as well as make effective decisions on information security and/or cyber security.</p>
7 - Learning outcomes	
The results of studies in the specialty (defined by the standard of higher education of the specialty)	LO1. Communicate freely in national and foreign languages, orally and in writing, to present and discuss the results of research and innovation, ensure business/operational processes and issues of professional activity in the field of information security and/or cyber security.

- LO2. Integrate fundamental and specialized knowledge to solve complex information security and/or cyber security challenges in broad or multidisciplinary contexts.
- LO3. Conduct research and/or innovation activities in the field of information security and/or cyber security, as well as in the field of technical and cryptographic protection of information in cyberspace.
- LO4. Apply, integrate, develop, implement and improve modern information technologies, physical and mathematical methods and models in the field of information security and/or cyber security.
- LO5. Critically consider the problems of information security and/or cyber security, including at the interdisciplinary and interdisciplinary level, in particular on the basis of understanding the new results of engineering and physical and mathematical sciences, as well as the development of technologies for creating and using specialized software.
- LO6. Analyze and evaluate the security of systems, complexes and means of cyber protection, technologies for creating and using specialized software.
- LO7. To justify the use, implement and analyze the best global standards, practices in order to solve complex problems of professional activity in the field of information security and/or cyber security.
- LO8. Research, develop and support systems and means of information security and/or cyber security at objects of information activity and critical infrastructure.
- LO9. Analyze, develop and support the organization's information security and/or cyber security management system based on the information security strategy and policy.
- LO10. Ensure the continuity of business/operational processes, as well as identify vulnerabilities of information systems and resources, analyze and assess risks for information security and/or cyber security of the organization.
- LO11. Analyze, control and ensure the effective functioning of the system for managing access to information resources in accordance with the established strategy and policy of information security and/or cyber security of the organization.
- LO12. Research, develop and implement methods and measures to counter cyber incidents, implement management, control and investigation procedures, as well as provide recommendations for the prevention and analysis of cyber incidents in general.
- LO13. Research, develop, implement and use methods and means of cryptographic and technical information protection of

	<p>business/operational processes, as well as analyze and provide an assessment of the effectiveness of their use in information systems, objects of information activity and critical infrastructure.</p> <p>LO14. Analyze, develop and support the system of auditing and monitoring the effectiveness of the functioning of information systems and technologies, business/operational processes in the field of information and/or cyber security as a whole.</p> <p>LO16. Make informed decisions on organizational and technical issues of information security and/or cyber security in complex and unpredictable conditions, including using modern methods and means of optimization, forecasting and decision-making.</p> <p>LO18. Plan training, as well as accompany and supervise work with personnel in the direction of information security and/or cyber security.</p> <p>LO19. Choose, analyze and develop appropriate typical analytical, calculation and experimental methods of cyber protection, develop, implement and support projects on information protection in cyberspace, innovative activities and protection of intellectual property.</p> <p>LO20. Set and solve complex applied engineering and scientific problems of information security and/or cyber security, taking into account the requirements of national and international standards and best practices.</p> <p>LO21. Use the methods of natural, physical and computer modeling to study processes related to information security and/or cyber security.</p> <p>LO22. Plan and carry out experimental and theoretical research, put forward and test hypotheses, choose suitable methods and tools for this, carry out statistical processing of data, evaluate the reliability of research results, argue conclusions.</p> <p>LO23. Justify the selection of software, equipment and tools, engineering technologies and processes, as well as their limitations in the field of information security and/or cyber security based on current knowledge in related fields, scientific, technical and reference literature and other available information.</p>
8 – Resource support for program implementation	
Personnel support	Meets the personnel requirements for ensuring educational activities in the field of higher education in accordance with the current legislation of Ukraine (Resolution of the Cabinet of Ministers of Ukraine “On Approval of Licensing Conditions

	<p>for Conducting Educational Activities of Education” of December 30, 2015 No. 1187, as amended by CMU Resolution No. 365 dated 24.03.2021. Annex 15-16).</p> <p>The composition of the working group of the educational program, the professorial teaching staff, which is involved in teaching disciplines in the specialty corresponds to the license conditions of conducting educational activities at the first (bachelor's) level of higher education.</p> <p>Teaching teachers, specialists and employees of IT companies, as well as foreign specialists are involved in teaching.</p>
Material and technical support	<p>Meets the technological requirements for the material and technical support of educational activities in the field of higher education in accordance with the current legislation of Ukraine (Resolution of the Cabinet of Ministers of Ukraine “On Approval of Licensing Conditions for Conducting Educational Activities of Education” of December 30, 2015, No. 1187, with changes made in accordance with CMU Resolution No. 365 dated 24.03.2021. Annex 17).</p> <p>Educational scientific production base in the form of: —The educational buildings, computer classes, combined by a local computer network with access to the Internet, multimedia equipment; specialized software,cyber polygon.</p>
Informational and educational and methodological support	<p>Meets the technological requirements for educational and methodological and information support of educational activities in the field of higher education in accordance with the current legislation of Ukraine (Resolution of the Cabinet of Ministers of Ukraine “On Approval of Licensing Conditions for Conducting Educational Activities of Education” of December 30, 2015, No. 1187, (as amended by CMU Resolution No. 365 of 24.03.2021. Annex 18).</p> <p>Information and educational-methodical support of the educational process is realized by the presence of the necessary educational and methodological literature: textbooks, manuals, methodological recommendations for practical classes, independent work, syabrose of educational components (https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-125-magistr/).</p> <p>Information resources are located in the funds of the scientific library of NTU "KPI", websites of graduation departments.</p> <p>The educational process uses LMS (Learning Management System).</p>
9 – Academic mobility	
National credit mobility	On the basis of bilateral agreements between the National Technical University "Kharkiv Polytechnic Institute" and

	leading technical universities of Ukraine. It is regulated by the "Regulations on academic mobility of students, graduate students, doctoral students, scientific-pedagogical and researchers of NTU" KhPI ".
International credit mobility	On the basis of bilateral agreements. On the basis of bilateral agreements between the National Technical University "Kharkiv Polytechnic Institute" and higher educational establishments of foreign partner countries.
Education of foreign students of higher education	Preparation of foreign citizens is carried out in accordance with the requirements of the current legislation, provided that the previous educational level is recognized.

2. LIST OF EDUCATIONAL COMPONENTS OF THE EDUCATIONAL AND PROFESSIONAL PROGRAM "CYBERSECURITY" AND THEIR LOGICAL SEQUENCE

2.2 List components of educational and professional program

Code n/a	Components of the educational and professional program	Credits ECTS	Final control form
1	2	3	4
1. Mandatory educational components			
1.1 General training			
<i>GT 1</i>	<i>Academic English</i>	<i>3,0</i>	<i>Test</i>
<i>GT 2</i>	<i>Innovative entrepreneurship and management</i>	<i>3,0</i>	<i>Test</i>
<i>GT 3</i>	<i>Intellectual property</i>	<i>3,0</i>	<i>Test</i>
<i>GT 4</i>	<i>Artificial intelligence-based security</i>	<i>3,0</i>	<i>Exam</i>
<i>GT 5</i>	<i>Security of the Internet of Things and Services</i>	<i>3,0</i>	<i>Test</i>
1.2 Special (professional) training			
<i>ST 1</i>	<i>Fundamentals of scientific research</i>	<i>5,0</i>	<i>Exam</i>
<i>ST 2</i>	<i>Critical Infrastructure Security</i>	<i>4,0</i>	<i>Test</i>
<i>ST 3</i>	<i>Network and cloud security</i>	<i>4,0</i>	<i>Exam</i>
<i>ST 4</i>	<i>Protection of Distributed Services and Operating Platforms</i>	<i>4,0</i>	<i>Test</i>
<i>ST 5</i>	<i>Digital forensics</i>	<i>4,0</i>	<i>Test</i>
1.3 Practical training			
<i>PT 1</i>	<i>Research and development practice</i>	<i>11,0</i>	<i>Test</i>
1.4 Certification			
	<i>Certification</i>	<i>11,0</i>	
General amount mandatory components		58	
2. Elective educational components			
2.1 Educational components of free choice of professional training of the general institutional catalog			
<i>ECPT 1</i>	<i>EC FC PT 1</i>	<i>4,0</i>	<i>Test</i>
<i>ECPT 2</i>	<i>EC FC PT 2</i>	<i>4,0</i>	<i>Test</i>
<i>ECPT 3</i>	<i>EC FC PT 3</i>	<i>4,0</i>	<i>Test</i>
<i>ECPT 4</i>	<i>EC FC PT 4</i>	<i>4,0</i>	<i>Test</i>
<i>ECPT 5</i>	<i>EC FC PT 5</i>	<i>4,0</i>	<i>Test</i>
<i>ECPT 6</i>	<i>EC FC PT 6</i>	<i>4,0</i>	<i>Test</i>
2.2 Educational components of free choice of general training			
<i>ECGT 1</i>	<i>EC FC GT 1</i>	<i>4,0</i>	<i>Test</i>
<i>ECGT 2</i>	<i>EC FC GT 2</i>	<i>4,0</i>	<i>Test</i>
Total amount for elective components:		32	
GENERAL SCOPE OF THE EDUCATIONAL AND PROFESSIONAL PROGRAM:		90	

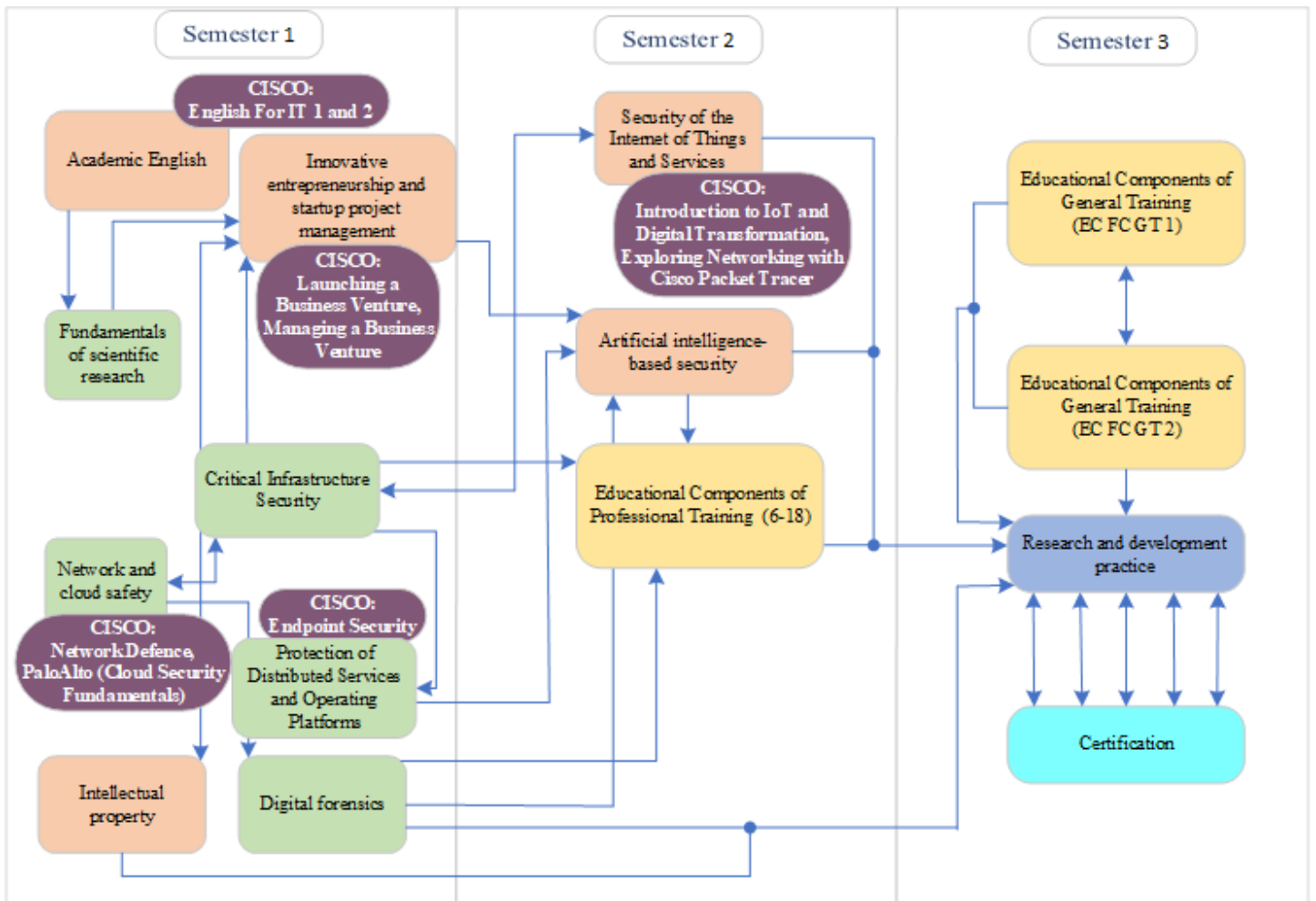
3. DISTRIBUTION CONTENT EDUCATIONAL AND PROFESSIONAL PROGRAMS BY IN GROUPS COMPONENTS AND CYCLES PREPARATION

No n/p	Cycle preparation	The amount of the applicant's educational load higher education (ECTS credits / %)		
		Mandatory components educational professional programs	Selective components educational professional programs	All in all term teaching
1	General training	15 / 16,7	-	15 / 16,7
2	Special (professional) training	21 / 23,3	-	21 / 23,3
3	Practical training	11/12,2	-	11/12,2
4	Certification	11/12,2	-	11/12,2
5	Elective educational components	-	32 / 35,6	32 / 35,6
Total for the entire term teaching		58 / 64,4	32 / 35,6	90 / 100

4. FORM CERTIFICATES EARNERS HIGHER EDUCATION

Forms of attestation of applicants of higher education	The certification is carried out in the form of public protection of qualification work.
Requirements for the unified state qualification exam	<p>Qualification work should solve the complex problem of information security and/or cybersecurity and provide research and/or innovation.</p> <p>Qualification work should not contain academic plagiarism, fabrication, falsification.</p> <p>Qualification work should be posted on the official site (or in repository) of a higher education institution or its unit.</p> <p>The publication of restricted qualification works is carried out in accordance with the requirements of the legislation.</p>

5. STRUCTURAL AND LOGICAL SCHEME



6. THE MATRIX OF COMPLIANCE OF THE COMPETENCES / LEARNING OUTCOMES DEFINED BY THE STANDARD WITH THE NQF DESCRIPTORS

Classification of competences according to NRC	Knowledge Kn1 Specialized conceptual knowledge, including modern scientific achievements in the field of professional activity or field of knowledge and is the main one for original thinking and research, critical comprehension	Skill Sk1 Specialized Skills/Skills of Problems Needed to Conduct Innovation Research and/or Pursuing Innovative Activity in order to develop new knowledge and procedures Sk2 The ability to integrate knowledge and solve complex tasks in wide or multidisciplinary contexts Sk3 The ability to solve problems in new subscribers in the presence of incomplete or limited information taking into account aspects of social and ethical responsibility	Communication C1 Clear and unambiguous communication of their own knowledge, conclusions and argumentation to specialists, in particular to persons studying	Responsibility and autonomy AB1 Management of work or educational processes that are complex, unpredictable and require new strategic approaches AB2 Responsibility for contribution to professional knowledge and practice and/or evaluation of the results of teams and teams AB3 The ability to continue learning with a high degree of autonomy
GENERAL COMPETENCES				
GC1	Kn1,	Sk1, Sk3	C1	AB1, AB2
GC2	Kn1,	Sk1, Sk2, Sk3		AB2, AB3
GC3	Kn1	Sk2, Sk3		AB1
GC4	Kn1	Sk3		AB1, AB2
GC5	Kn1	Sk2	C1	AB1
SPECIAL (PROFESSIONAL) COMPETENCES				
SC1	Kn1	Sk2		AB2
SC2	Kn1,	Sk2		AB2
SC3	Kn1	Sk, Sk2, Sk3	C1	AB1, AB2
SC4	Kn1,	Sk, Sk2	C1	AB1, AB2
SC5	Kn1,	Sk1, Sk2	C1	AB1, AB2
SC6	Kn1	Sk1, Sk2	C1	AB1
SC7	Kn1	Sk1, Sk2	C1	AB1
SC8	Kn1	Sk1, Sk2	C1	AB1
SC9	Kn1	Sk1, Sk2	C1	AB1
SC10	Kn1	Sk1, Sk2, Sk3	C1	AB1, AB2

Learning outcomes	Competences														
	Integral competence														
	General competences					Special (professional) competences									
	GC 1	GC 2	GC 3	GC 4	GC 5	SC 1	SC 2	SC 3	SC 4	SC 5	SC 6	SC 7	SC 8	SC 9	SC 10
	PT1, PT2, PT3, PT4, P1	P1		P1		P1									
LO 5			GT1, GT3, PT1, PT2, P1		GT1, GT3, GT5, PT1, PT2, PT3, P1		GT3, PT1, PT2, P1								
LO 6	GT1, GT2, GT3, GT4, GT5, PT1, PT2, PT3, PT4, P1			GT3, GT5, PT1, PT2, PT4, P1		GT1, GT2, GT5, PT3, PT4, P1		GT4, PT1, PT2, PT3, PT4, PT5, P1		GT4, GT5, PT1, PT2, PT3, PT5, P1	GT2, P1	GT4, GT5, PT1, PT2, PT3, PT5, P1		GT5, PT1, PT2, PT3, PT4, P1	
LO 7	GT1, GT2, GT3, GT4, GT5, PT1, PT2, PT3, PT4, P1		GT1, GT3, PT1, PT2, P1				GT3, PT1, PT2, P1								
LO 8	GT1, GT2,	GT1, GT5,		GT3, GT5,	GT1, GT3,			GT4, PT1,						GT5, PT1,	GT1, PT1,

Learning outcomes	Competences														
	Integral competence														
	General competences					Special (professional) competences									
	GC 1	GC 2	GC 3	GC 4	GC 5	SC 1	SC 2	SC 3	SC 4	SC 5	SC 6	SC 7	SC 8	SC 9	SC 10
	GT3, GT4, GT5, PT1, PT2, PT3, PT4, P1	PT1, PT2, PT4, P1		PT1, PT2, PT4, P1	GT5, PT1, PT2, PT3, P1			PT2, PT3, PT4, PT5, P1						PT2, PT3, PT4, P1	P1
LO 9	GT1, GT2, GT3, GT4, GT5, PT1, PT2, PT3, PT4, P1	GT1, GT5, PT1, PT2, PT4, P1	GT1, GT3, PT1, PT2, P1	GT3, GT5, PT1, PT2, PT4, P1					PT3, P1					GT5, PT1, PT2, PT3, PT4, P1	GT1, PT1, P1
LO 10	GT1, GT2, GT3, GT4, GT5, PT1, PT2, PT3, PT4, P1		GT1, GT3, PT1, PT2, P1	GT3, GT5, PT1, PT2, PT4, P1						GT4, GT5, PT1, PT2, PT3, PT5, P1				GT5, PT1, PT2, PT3, PT4, P1	
LO 11	GT1, GT2, GT3, GT4, GT5, PT1,		GT1, GT3, PT1, PT2, P1	GT3, GT5, PT1, PT2, PT4, P1							GT2, P1				GT1, PT1, P1

Learning outcomes	Competences														
	Integral competence														
	General competences					Special (professional) competences									
	GC 1	GC 2	GC 3	GC 4	GC 5	SC 1	SC 2	SC 3	SC 4	SC 5	SC 6	SC 7	SC 8	SC 9	SC 10
	PT2, PT3, PT4, P1														
LO 12	GT1, GT2, GT3, GT4, GT5, PT1, PT2, PT3, PT4, P1		GT1, GT3, PT1, PT2, P1	GT3, GT5, PT1, PT2, PT4, P1					PT3, P1			GT4, GT5, PT1, PT2, PT3, PT5, P1			GT1, PT1, P1
LO 13	GT1, GT2, GT3, GT4, GT5, PT1, PT2, PT3, PT4, P1		GT1, GT3, PT1, PT2, P1	GT3, GT5, PT1, PT2, PT4, P1									GT3, P1		GT1, PT1, P1
LO 14	GT1, GT2, GT3, GT4, GT5, PT1, PT2, PT3, PT4, P1		GT1, GT3, PT1, PT2, P1	GT3, GT5, PT1, PT2, PT4, P1					PT3, P1					GT5, PT1, PT2, PT3, PT4, P1	GT1, PT1, P1

Learning outcomes	Competences														
	Integral competence														
	General competences					Special (professional) competences									
	GC 1	GC 2	GC 3	GC 4	GC 5	SC 1	SC 2	SC 3	SC 4	SC 5	SC 6	SC 7	SC 8	SC 9	SC 10
LO 15				GT3, GT5, PT1, PT2, PT4, P1	GT1, GT3, GT5, PT1, PT2, PT3, P1										GT1, PT1, P1
LO 16	GT1, GT2, GT3, GT4, GT5, PT1, PT2, PT3, PT4, P1	GT1, GT5, PT1, PT2, PT4, P1	GT1, GT3, PT1, PT2, P1	GT3, GT5, PT1, PT2, PT4, P1				GT4, PT1, PT2, PT3, PT4, PT5, P1	PT3, P1	GT4, GT5, PT1, PT2, PT3, PT5, P1	GT2, P1	GT4, GT5, PT1, PT2, PT3, PT5, P1		GT5, PT1, PT2, PT3, PT4, P1	GT1, PT1, P1
LO 17								GT4, PT1, PT2, PT3, PT4, PT5, P1							GT1, PT1, P1
LO 18	GT1, GT2, GT3, GT4, GT5, PT1, PT2, PT3, PT4, P1			GT3, GT5, PT1, PT2, PT4, P1	GT1, GT3, GT5, PT1, PT2, PT3, P1										GT1, ST1, P1

Learning outcomes	Competences														
	Integral competence														
	General competences					Special (professional) competences									
	GC 1	GC 2	GC 3	GC 4	GC 5	SC 1	SC 2	SC 3	SC 4	SC 5	SC 6	SC 7	SC 8	SC 9	SC 10
LO 19	GT1, GT2, GT3, GT4, GT5, PT1, PT2, PT3, PT4, P1			GT3, GT5, PT1, PT2, PT4, P1	GT1, GT3, GT5, PT1, PT2, PT3, P1	GT1, GT2, GT5, PT3, PT4, P1	GT3, PT1, PT2, P1	GT4, PT1, PT2, PT3, PT4, PT5, P1	PT3, P1		GT2, P1	GT4, GT5, PT1, PT2, PT3, PT5, P1	GT3, P1	GT5, PT1, PT2, PT3, PT4, P1	
LO 20	GT1, GT2, GT3, GT4, GT5, PT1, PT2, PT3, PT4, P1	GT1, GT5, PT1, PT2, PT4, P1	GT1, GT3, PT1, PT2, P1	GT3, GT5, PT1, PT2, PT4, P1	GT1, GT3, GT5, PT1, PT2, PT3, P1	GT1, GT2, GT5, PT3, PT4, P1		GT4, PT1, PT2, PT3, PT4, PT5, P1							
LO 21	GT1, GT2, GT3, GT4, GT5, PT1, PT2, PT3, PT4, P1	GT1, GT5, PT1, PT2, PT4, P1	GT1, GT3, PT1, PT2, P1	GT3, GT5, PT1, PT2, PT4, P1		GT1, GT2, GT5, PT3, PT4, P1		GT4, PT1, PT2, PT3, PT4, PT5, P1		GT4, GT5, PT1, PT2, PT3, PT5, P1		GT4, GT5, PT1, PT2, PT3, PT5, P1	GT3, P1		
LO 22		GT1, GT5, PT1, PT2,	GT1, GT3, PT1, PT2,	GT3, GT5, PT1, PT2,		GT1, GT2, GT5, PT3,		GT4, PT1, PT2, PT3,							

Learning outcomes	Competences														
	Integral competence														
	General competences					Special (professional) competences									
	GC 1	GC 2	GC 3	GC 4	GC 5	SC 1	SC 2	SC 3	SC 4	SC 5	SC 6	SC 7	SC 8	SC 9	SC 10
		PT4, P1	P1	PT4, P1		PT4, P1		PT4, PT5, P1							
LO 23	GT1, GT2, GT3, GT4, GT5, PT1, PT2, PT3, PT4, P1		GT1, GT3, PT1, PT2, P1	GT3, GT5, PT1, PT2, PT4, P1		GT1, GT2, GT5, PT3, PT4, P1	GT3, PT1, PT2, P1	GT4, PT1, PT2, PT3, PT4, PT5, P1			GT2, P1	GT4, GT5, PT1, PT2, PT3, PT5, P1	GT3, P1	GT5, PT1, PT2, PT3, PT4, P1	

8. THE RESULTS OF DISCUSSING THE EDUCATIONAL PROGRAM

Stakeholders	Remarks / Recommendation	Taken into account / partially taken into account / not taken into account	Note
Guarantor of the EPP, Olga KOROL, candidate of technical sciences, associate professor of the cybersecurity department. Members of the EPP Working Group	Change of the specialty and field of knowledge (according to the Cabinet of Ministers of Ukraine of August 30, 2024 No 1021).	Taken into account.	Changes have been made.
Guarantor of the EPP, Olga KOROL, candidate of technical sciences, associate professor of the cybersecurity department. Members of the EPP Working Group	In order to bring it into line with modern terminology and standards of higher education, update the names of individual disciplines of the educational program.	Taken into account.	As part of the periodic review of the educational program, taking into account the recommendations of stakeholders, modern trends in the development of the industry, and updating the terminology, the names of individual academic disciplines were updated. The changes have an editorial nature and do not affect the content of disciplines, learning outcomes, the amount of ECTS credits and the structure of the educational program.
VOLOSHCHUK Olena, Candidate of Technical Sciences, Head of Educational Programs of Distributed Lab LLC.	Positive response. Without remarks.	-	-
KOVTUN Vladyslav, Candidate of Technical Sciences, Associate Professor, "Syfer" LLC general director.	Positive response. Without remarks.	-	-

GOLOVASHYCH Serhii, Candidate of Technical Sciences, Associate Professor, LLC "Microcrypt Technologies" general director.	Positive response. Without remarks.	-	-
OPIRSKY Ivan, Doctor of Technical Sciences, Professor, Head of the Department of Information Protection of the Institute of Computer Technology, Automation and Metrology of the National University "Lviv Polytechnic"	Positive response. Without remarks.	-	-

Head of the Department of Cybersecurity _____ Serhii YEVSEIEV

Guarantor of the educational program _____ Olga KOROL

9. PLAN TO TAKE INTO ACCOUNT THE COMMENTS AND FIX THE DEFICIENCIES UNDER THE EDUCATIONAL PROGRAM

Recommendations provided during the latest accreditation	The period (short - term/long - term/not appropriate to consider)	Measures aimed at taking into account the recommendations / justification as to Impracts of the recommendation	Terms of implementation of measures / responsible persons
General recommendations of the Expert Group and Sectoral Expert Council (in the department, industry, institute, university)			
<p>Recommendation 1</p> <p>To strengthen the information of applicants with regulatory documents and basic provisions of academic integrity.</p>	<p>Long -term</p>	<p>1) carrying out permanent explanatory work among teachers and education applicants to maintain a culture of academic integrity;</p> <p>2) informing the applicants about measures to cover the issues of academic integrity, which on a permanent basis are carried out by staff of the department of quality assurance of educational activity and scientific and technical library of NTU "KPI";</p> <p>3) Periodic acquaintance of interested persons with regulatory documents, which defines the policy and procedures of compliance with academic integrity at NTU "KPI":</p> <p>- “Rules of conduct of education applicants at NTU“ KPI ”;</p>	<p>The period of time to the next accreditation of OP.</p> <p>Responsible: Guarantor OP, Teachers of the Department.</p>

		<p>- "Rules of internal regulations of NTU" KPI ";</p> <p>- "Code of Ethics of Academic Relations and Integrity of NTU" KPI ".</p> <p>4) placement of motivational materials on the site of the Department of SIT.</p> <p>5) Informing the applicants is performed constantly during the lecture classes in the discipline "Fundamentals of Scientific Research".</p> <p>Considered at the meeting of the department, minutes No. 12 of 14.03.2025.</p>	
<p>Recommendation 2</p> <p>View in the next version of the APP list of approved professional standards in the field of cybersecurity in accordance with the National Classifier of Professions of Ukraine DK 003: 2010.</p>	<p>Long -term</p>	<p>Update in the OPP of the list of approved professional standards in the field of cybersecurity in accordance with the National Classifier of Professions of Ukraine DK 003: 2010.</p> <p>Considered at the meeting of the department, minutes No. 12 of 14.03.2025.</p>	<p>The period of time to the next accreditation of OP.</p> <p>Responsible: Guarantor OP.</p>
<p>Recommendation 3</p> <p>Consider the possibility of introducing a dual form of education on a given EPP.</p>	<p>Long -term</p>	<p>Consider the possibility of introducing a dual form of education on a given EPP.</p> <p>Considered at the meeting of the department, minutes No. 12 of 14.03.2025.</p>	<p>The period of time to the next accreditation of OP.</p> <p>Responsible: Guarantor OP, Head of the Department, Teachers of the department.</p>

<p>Recommendation 4</p> <p>Put information on VC in OPP in a convenient form for stakeholders with a clear indication of components available for choice (links to VC, table, etc.).</p>	<p>Long -term</p>	<p>To refine the information structure of the website. Developed, published and published on the department's website list of selective educational components with reference to Syllabus.</p> <p>Considered at the meeting of the department, minutes No. 12 of 14.03.2025.</p>	<p>The period of time to the next accreditation of OP.</p> <p>Responsible: Guarantor OP.</p>
<p>Recommendation 5</p> <p>Involvement of students in discussion and upgrade EPP</p>	<p>Long -term</p>	<p>To meet members of the working group with representatives of student self -government.</p> <p>Considered at the meeting of the department, minutes No. 1 of 26.03.2025.</p>	<p>The period of time to the next accreditation of OP.</p> <p>Responsible: Guarantor OP, Head of the Department, Teachers of the department.</p>

Director of the Educational and Scientific Institute
of Computer Science and Information Technology _____ Mykhailo HODLEVSKYI

Guarantor of the educational program _____ Olga KOROL