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

APPROVED
Rector of NTU "KhPI"
_____ Yevgen SOKOL
"28" _____03_____ 2025

EDUCATIONAL AND PROFESSIONAL PROGRAM
"CYBERSECURITY"

First (bachelor) level of higher education

in specialty **125 – Cybersecurity and information protection**
fields of knowledge **12 - Information technologies**
qualification **bachelor of cybersecurity and information protection**

APPROVED
ACADEMIC COUNCIL OF NTU
"Khpi"
Head of the academic council
_____ / Yevgen SOKOL
Protocol №. 4
From March, 28 2025

Kharkiv 2025

LETTER OF AGREEMENT

Educational and professional program «Cybersecurity»

Level of higher education	First (bachelor) level
Branch of knowledge	12 Information technologies
Specialty	125 Cybersecurity and information protection
Qualification	bachelor of cybersecurity and information protection

APPROVED
The EPP workgroups for the specialty
«Cybersecurity and information protection»
Guarantor of the educational program

_____Sergii YEVSEIEV

Protocol №. 1
From March, 26 2025

RECOMMENDED
Methodical council of NTU "KhPI"
Deputy chairman of the methodical council

_____ Ruslan MYGUSHCHENKO

Protocol №. 3
From March, 26 2025

AGREED
Head of the Department of Cybersecurity

_____ Sergii YEVSEIEV

Protocol №. 12
From March, 14 2025

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

_____ Mykhailo HODLEVSKYI

«____»_____2025

AGREED
Higher education
(member of the EPP workgroup)
№ group КН-11226

_____ Diana SIPCO

«____»_____2025

APPROVED AND GRANTED
By order of the rector of the National Technical University "Kharkiv Polytechnic Institute" from April 02, 2025 No. 111 ОД .

REVIEWERS:

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

1. Kateryna MOLODETSKA, Doctor of Technical Sciences, Professor, Professor of Management of Organizations of Kyiv-Mohyla Business School National University "Kyiv-Mohyla Academy".
2. Vladyslav KOVTUN, Candidate of Technical Sciences, Associate Professor, "Syfer" LLC general director.
3. Serhii GOLOVASHYCH, Candidate of Technical Sciences, Associate Professor, LLC "Microcrypt Technologies" general director.
4. Olena VOLOSHCHUK, Candidate of Technical Sciences, Head of Educational Programs of Distributed Lab LLC.
5. Olga SHAPOVAL, Executive Director of Kharkiv Cluster of Information Technology

РЕЦЕНЗІЯ-ВІДГУК

на освітньо-професійну програму "Кібербезпека"
першого (бакалаврського) рівня вищої освіти,
спеціальності 125 "Кібербезпека та захист інформації"
кафедри кібербезпеки Національного технічного університету
"Харківський політехнічний інститут"

У сучасному світі важливу роль відіграють інформаційні технології, включно із ними засоби забезпечення кібербезпеки підприємств будь-якої форми власності займають провідні позиції на найвищому рівні із виконанням підприємством своїх безпосередніх бізнес-завдань. Сучасний світ, фактично – це технології Індустрії 4.0 та Інтернету речей (Internet of Things), де фактичні ресурси підприємства мають свою віртуальну копію у цифровій формі та перехрещуються з традиційними підходами до документообігу та інформаційними системами супроводження бізнесу. Це безумовно сприяє щорічному збільшенню попиту у нашій країні на спеціалістів з кібербезпеки, які будуть спроможні ефективно вирішувати складні завдання щодо побудови захисту підприємства та будуть спроможні забезпечувати протидію несанкціонованому втручанню до їх інформаційної інфраструктури.

Освітньо-професійна програма "Кібербезпека" першого (бакалаврського) рівня вищої освіти, що запропонована кафедрою кібербезпеки Національного технічного університету "Харківський політехнічний інститут" має всі потрібні компоненти щодо забезпечення навчального процесу професійної підготовки фахівців, які у компаніях зможуть займати позиції: менеджера систем з інформаційної безпеки, фахівця захисту інформації, техніка захисту інформації, адміністратору бази даних, адміністратору доступу, інженера-програміста тощо.

Слід визначити, що у сучасних економічних умовах кібербезпека – це не тільки значний тренд у розвитку великих компаній та підприємств. Зараз малий та середній бізнес відкриває нові для себе ніші електронної комерції. Відповідно

стає питання щодо рішення завдань забезпечення безпеки електронних мереж не тільки корпоративного рівня, але слід вирішувати повсякденні питання кіберзахисту малого та середнього приватного бізнесу. Тому, слід вважати дуже своєчасними завдання, що розглядаються у освітньо-професійній програмі "Кібербезпека", за якою навчаються студенти Національного технічного університету "Харківський політехнічний інститут"за спеціальністю 125 "Кібербезпека та захист інформації". Випускник за цією програмою має досвід та розуміння завдань, як у масштабі потреб безпеки великих організацій та компаній, а також компаній, що мають порівняно невеликі масштаби бізнесу, та, наприклад, компаній, рівня веб-студій, що надають послуги з розроблення веб-сайтів. Запропонована програма враховує не тільки потреби компаній-роботодавців, що спрямовані тільки на рішення замовлень для закордонних компаній, так звані аутсорсингові компанії та інші, але й для компаній, що працюють виключно на внутрішньому ринку України.

Слід підвести, що освітньо-професійна програма "Кібербезпека" першого (бакалаврського) рівня вищої освіти, що запропонована кафедрою кібербезпеки Національного технічного університету "Харківський політехнічний інститут" є сучасною, ефективною та затребуваною на сучасному ринку праці у нашої країні щодо підготовки фахівців з кібербезпеки. Ця програма відповідає стандарту Міністерство освіти і науки України та узгоджується з запитами компаній роботодавців щодо наявності кваліфікованих кадрів у ІТ-галузі та напряму спеціальності 125 "Кібербезпека та захист інформації.

Керівник навчально-наукового
центру інформаційних технологій
Поліського національного університету,
доктор технічних наук, професор Катерина МОЛОДЕЦЬКА

ПІДПИС ЗАСВІДЧУЮ
Начальник відділу діловодства та контролю виконання Поліського національного університету
м. Житомир
«01» 03 2021 р.

САЙФЕР

Системи захисту інформації

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

РЕЦЕНЗІЯ-ВІДГУК

на освітньо-професійну програму "Кібербезпека",
першого (бакалаврського) рівня вищої освіти
спеціальності 125 "Кібербезпека та захист інформації"
кафедри кібербезпеки Національного технічного університету
"Харківський політехнічний інститут"

Стрімкий розвиток інформаційних технологій і швидке зростання глобальної мережі Інтернет призвели до формування інформаційного середовища, що впливає на всі сфери людської діяльності. Нові технологічні можливості полегшують поширення інформації, підвищують ефективність виробничих процесів, сприяють розширенню ділових операцій в процесі бізнесу.

Підприємства нового типу – це розгалужена мережа розподілених підрозділів, філій і груп, що взаємодіють один з одним. Розподілені корпоративні інформаційні системи стають сьогодні найважливішим засобом виробництва сучасної компанії, вони дозволяють перетворити традиційні форми бізнесу в електронний бізнес.

Електронний бізнес використовує глобальну мережу Інтернет і сучасні інформаційні технології для підвищення ефективності всіх сторін ділових відносин, включаючи продажі, маркетинг, платежі, фінансовий аналіз, пошук співробітників, підтримку клієнтів і партнерських відносин.

Однією з умов існування електронного бізнесу є інформаційна безпека, під якою розуміється захищеність інформації та підтримує інфраструктури від випадкових і навмисних впливів, здатних завдати шкоди власникам або

користувачам інформації. Збиток від порушення інформаційної безпеки може привести до ~ великим фінансовим втратам і навіть до повного закриття компанії.

Всупереч на інтенсивний розвиток комп'ютерних засобів і інформаційних технологій, вразливість сучасних інформаційних систем і комп'ютерних мереж, на жаль, не зменшується. Тому проблеми забезпечення інформаційної безпеки привертають пильну увагу як фахівців в області комп'ютерних систем і мереж, так і численних користувачів, включаючи компанії, що працюють у сфері електронного бізнесу.

Без знання і кваліфікованого застосування сучасних технологій, стандартів, протоколів і засобів захисту інформації неможливо досягти необхідного рівня інформаційної безпеки комп'ютерних систем і мереж.

Кафедрою кібербезпеки Національного технічного університету "Харківський політехнічний інститут" розроблено навчальну програму "Кібербезпека", та навчальні плани дисциплін, які пов'язані з напрямком підготовки фахівця з інформаційної безпеки широкого профілю, яка формує спектр компетентностей та забезпечує отримання результатів навчання, які передбачаються стандартом вищої освіти за спеціальністю 125 Кібербезпека та захист інформації.

Програма забезпечує підготовку фахівця, який здатен забезпечити необхідний рівень кібербезпеки систем різного призначення та природи, в першу чергу системи бізнес-процесів економічних систем, систем критичної інфраструктури, кіберфізичних систем та ін., на будь-якому рівні управлінської ієрархії, враховуючи принципи застосування криптографічних методів, сучасних технологій забезпечення кібербезпеки, інформаційної безпеки та безпеки інформації в межах національних і міжнародних стандартів й практик щодо здійснення професійної діяльності.

Навчальний процес освітньої програми організовано на базі сучасних інтегрованих середовищах розробки корпоративних додатків та систем збереження даних з санкціонованим доступом. Кожному студенту на період

навчання безплатно надається ліцензований доступ до додатків та сервісів у аккаунті у порталу Microsoft 365. Більшість лабораторних та практичних робіт, а також курсового та дипломного проєктування здійснюється з використанням апаратно-програмних засобів кіберполігону.

Вважаємо, що Освітньо-професійна програма "Кібербезпека", що запропонована та здійснюється кафедрою кібербезпеки Національного технічного університету "Харківський політехнічний інститут", має всі необхідні компоненти для підготовки кваліфікованих спеціалістів відповідно до сучасних тенденцій на попит фахівців з кібербезпеки. Випускники цієї програми отримують всі необхідні знання та навички щодо забезпечення кібербезпеки економічної діяльності підприємств корпоративного рівня, спроможні здійснювати аналіз, проєктування, програмування, розгортання та супроводження будь-яких сервісів, використовуючи сучасні технології.

Навчання за Освітньо-професійною програмою "Кібербезпека", забезпечує студентам надбання необхідних знань, компетенцій та навичок для успішної професійної діяльності у сфері впровадження та підтримки програмних рішень у корпоративному середовищі при дотриманні вимог відповідних національних і міжнародних, стандартів.

Директор ТОВ "Сайфер ІТ",
кандидат технічних наук _____ Владислав КОВТУН

ЗАТВЕРДЖУЮ:
Генеральний директор
ТОВ «Мікрокрипт Технолоджіс»
_____ Головашич С.О.
«____» _____ 2025 р.

РЕЦЕНЗІЯ-ВІДГУК

на освітню програму “Кібербезпека”
першого (бакалаврського) рівня вищої освіти,
спеціальності 125 “Кібербезпека та захист інформації”
кафедри кібербезпеки Національного технічного університету
“Харківський політехнічний інститут”

Освітня програма “Кібербезпека”, яка запропонована кафедрою кібербезпеки Національного технічного університету “Харківський політехнічний інститут” є безумовно актуальною у сучасних умовах стрімкого розвитку інформаційних технологій (ІТ) та їх глибокого проникнення до майже усіх галузей сучасного життя. Зараз у багатьох галузях народного господарства України не вистачає висококваліфікованих фахівців ІТ-напрямку, що мають досвід з кібербезпеки.

Запропонована освітня програма спрямована на надання інтегральної компетенції щодо здатності здобувача освіти розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов. Насправді, реальні сценарії кіберзагроз, характеризуються невизначеністю, синергійним характером походження та несподіваними умовами втручання. Поруч із цим, є багато сценаріїв, що можна заздалегідь передбачити та побудувати надійний контур

безпеки, наприклад, як на рівні обчислювальної мережі невеликої компанії, так й розподіленої мережі корпоративного рівня.

Об'єкт вивчення за освітньою програмою "Кібербезпека": об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; технології забезпечення безпеки інформації; процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. Це свідчить, що майбутні фахівці з кібербезпеки будуть здатні використовувати і впроваджувати технології інформаційної та/або кібербезпеки у практичних ситуаціях на виробництві або на рівні налагодження інформаційної безпеки невеликої організації.

Слід відзначити, що для забезпечення визначених компетентностей випускника та відповідних результатів навчання, кафедрою кібербезпеки Національного технічного університету "Харківський політехнічний інститут" запропоновано викладання іноземної мови (за професійним спрямуванням) як обов'язкової освітньої компоненти. Це є сучасною загальною тенденцією у IT-галузі щодо покращення комунікаційних навичок фахівців та взаємодії зі світовою спільнотою за обраним напрямом. У свою чергу аналіз структурно-логічної схеми освітньої програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти дозволяє стверджувати щодо комплексного та гармонійного формування дисциплін за спеціальністю. Студентам пропонується вивчення на першому році навчання базові дисципліни: Вступ до фаху (на базі всесвітньо відомого курсу CS50), Вища математика, Основи програмування (на базі мови Python), Введення в кібербезпеку (на основі курсу CISCO), Інформаційна безпека держави, Розробка та аналіз алгоритмів (послідовно продовжуючи вивчення за напрямом Python), Фізичні основи технічних засобів розвідки та ін., що поєднують як загальні дисципліни, якими

має оволодіти кожен ІТ-фахівець зі спеціалізованим за напрямом кібербезпеки.

На другому році навчання студентам запропоновано: Технології програмування, Основи побудови та захисту сучасних ОС, фаховий курс з мережевих технологій – CISCO CCNA Introduction to Networks, Математичні основи криптології, Теоретичні основи криптографії, Менеджмент інформаційної безпеки та ін. Що свідчить про більш цільове спрямування на вивчення особливостей напряму кіберзахисту, як з теоретичного, так й практичного характеру підбору навчальних дисциплін та рівня складності відповідних технологій.

На третьому році навчання студенти оволодівають знаннями переважно з дисциплін професійного спрямування: Інформаційні системи та Інтернет-технології (на базі мов програмування Java та Python), Основи математичного моделювання, Основи криптографічного захисту, фаховий курс з безпеки корпоративних мереж – CISCO CCNA Security, Організація та інформаційне забезпечення управлінської діяльності, Комплексні системи захисту інформації та ін. На четвертому році навчання студенти завершують цикл навчання бакалаврського рівня вивченням дисциплін: Організаційне забезпечення захисту інформації, Основи стеганографічного захисту інформації та ін., виконують Комплексний курсовий проект.

Таким чином, аналіз освітньої програми “Кібербезпека” першого (бакалаврського) рівня вищої освіти, що запропоновано кафедрою кібербезпеки Національного технічного університету “Харківський політехнічний інститут”, свідчить про її актуальність для ІТ-галузі у цілому, та сприятиме підготовці фахівців з кібербезпеки, яких зараз потребують сучасні підприємства та організації України. Також відповідна освітньо-професійна програма дозволяє студентам продовжити навчання за фахом щодо отримання освітнього ступеня магістра.

Особливістю розглянутої програми слід вважати комплексний підхід до вивчення навчальних дисциплін, який передбачає надання компетенцій майбутнім фахівцям, починаючи від особливостей побудови захищених рішень на рівні обчислювальних мереж, включно корпоративні обчислювальні мережі, застосування провідних курсів CS50, CISCO та ін., оволодіння навичок програмування з використанням мов Python та Java, поруч з вивченням технологій криптографічного захисту, технічного захисту інформації та особливостей захисту інформаційних систем і мереж.

Генеральний директор
ТОВ “Мікрокрипт Технолоджіс”,
кандидат технічних наук Голованич С.О.

РЕЦЕНЗІЯ-ВІДГУК

на освітню програму “Кібербезпека”
першого (бакалаврського) рівня вищої освіти,
спеціальності 125 “Кібербезпека та захист інформації”
кафедри кібербезпеки Національного технічного університету
“Харківський політехнічний інститут”

З урахуванням бурхливого розвитку та обчислювальних потужностей обчислювальної техніки актуальним завданням є захист життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору. У цих умовах фахівці з кібербезпеки повинні забезпечувати своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. У зв’язку із складністю і трудомісткістю бізнес-процесів і методів захисту цифрового обладнання, інформації та комп’ютерних систем від ненавмисного чи несанкціонованого доступу вразливості комп’ютерних та інформаційних систем становлять значну проблему для користувачів, підприємств.

Підготовка якісних спеціалістів у сфері захисту інформації та кібербезпеки повинна відбуватися у відповідно до поступового трансформування навчальних програм та навчальних планів дисциплін пов’язаних з напрямком “Кібербезпека”, що сформована кафедрою кібербезпеки Національного технічного університету “Харківський політехнічний інститут”, відповідно до останніх тенденцій розвитку спеціальності, повністю реалізує результати навчання передбачені стандартом вищої освіти за спеціальністю 125 “Кібербезпека та захист інформації”.

Освітня програма має чітко визначені цілі, які враховують основні її особливості – підготовки фахівця з інформаційної безпеки широкого профілю із знанням технологій автоматизації бізнес-процесів, економічних завдань та повсякденної операційної діяльності підприємств з урахуванням технологічних можливостей держави, потреб бізнес-спільноти України та перспектив розвитку цифрової трансформації на державному рівні.

Сучасним трендом розвитку технологій розробки програмних продуктів є рішення, які надають можливість вирішувати завдання

проєктування, програмування, налагодження, розгортання, супроводження, кібербезпеки, зберігання даних, організацію хмарних сервісів з мінімумом кодування. Однією з основних проблем реалізації освітнього процесу за спеціальністю 125 “Кібербезпека та захист інформації” є відсутність під час навчання можливості отримати знання та навички від професіоналів-практиків. В рамках викладання за освітньою програмою, що рецензується, залучено викладачів-практиків та вивчаються сучасні технології створення та керування безпекою у розгалужених хмарних вебдодатків для підтримання безперебійних бізнес-процесів, вчасного проведення фінансових операцій, прогнозування ланцюжків постачання сировини, надсилання готової продукції, та надання послуг клієнтам, партнерам.

Вважаємо, що освітня програма “Кібербезпека” першого (бакалаврського) рівня освіти, що складена та запропонована кафедрою кібербезпеки Національного технічного університету “Харківський політехнічний інститут”, має всі необхідні компоненти для підготовки кваліфікованих фахівців, та забезпечує надбання ними відповідних компетенцій та спроможностей щодо вирішення актуальних завдань забезпечення безпеки автоматизації бізнес-процесів, економічних завдань, питань повсякденної операційної діяльності підприємств з урахуванням технологічних можливостей держави, потреб бізнес-спільноти України та перспектив розвитку технологій на державному рівні для успішного впровадження на ринку праці.

Керівник освітніх програм
Компанії Distributed Lab,
кандидат технічних наук _____ 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 125 «Кібербезпека та захист інформації» першого (бакалаврського) рівня вищої освіти в Національному технічному університеті «Харківський політехнічний інститут».

Сучасні вимоги ринку праці та виклики, що стоять перед теперішнім суспільством, зумовлюють необхідність переорієнтації національних закладів вищої освіти на зміну структури, змісту, організації та методів навчання, а також на суттєве посилення в освітніх програмах практичної складової. Окремо слід наголосити на необхідності залучення до навчального процесу професіоналів з метою якісної підготовки випускника із вищою технічною освітою. Формування ІТ-фахівця, який поєднує теорію та практику у своїй професійній діяльності, є запорукою забезпечення інноваційного підходу до виконання ним завдань, які ставляться сьогодні перед суб'єктами господарювання в Україні та світі.

Високий попит на ІТ-спеціалістів, здатних впроваджувати та використовувати інформаційні системи та технології у різних галузях людської діяльності, особливо національної безпеки, формує конкурентний ринок освітніх програм, що започатковані останніми роками у багатьох закладах вищої освіти України та дозволяють здобувачам вищої освіти обрати сучасні професії, затребувані на ринку праці. Тому, унікальність даної ОПП, забезпечення якісної підготовки та урахування регіональних аспектів відіграє значну роль у виборі вступниками закладу вищої освіти.

Рецензована освітньо-професійна програма являє собою змістовно завершений і методологічно виважений документ з професійно обґрунтованим і логічно скомпонованим переліком компонентів; вона відповідає концепції студентоцентрованого навчання, нагальним потребам підготовки фахівців з відповідної спеціальності та здатна забезпечувати, в разі її успішного проходження здобувачами, можливість здійснення практичної фахової діяльності в галузі кібербезпеки та захисту інформації.

Результати навчання на рівні всієї програми та окремих її компонентів визначені чітко і правильно, вони сформульовані в рамках фахових (предметно-спеціальних) і загальних компетентностей, до яких входить знання, розуміння, уміння та навички, здатності та цінності. Рівень компетентностей цілком відповідає задекларованому рівню освітньої програми.

Загалом ОПП має цілком структурований і логічний вигляд. Структурно-логічна побудова викладання освітніх компонентів забезпечує здобувачам досягнення мети ОПП, а саме набуття необхідних для подальшого працевлаштування компетентностей. Освітні компоненти, як обов'язкові, так і вибіркові, підібрані з урахуванням новітніх тенденцій і здатні забезпечити якісну вищу освіту в цій галузі.

Проаналізувавши дану ОПП, експерти від IT-компаній роботодавців окреслили її наступні позитивні сторони та надали коментарі й рекомендації, а саме:

- чітко сформульовані мета, характеристики, орієнтація на основний фокус програми;
- логічно сформований перелік освітніх компонентів та їх взаємозв'язок;
- особливо хочеться відзначити, що велика увага приділяється вивченню англійської мови. Це надзвичайно важливо в сучасному світі технологій, оскільки більшість інформаційних ресурсів і документації доступні саме англійською;
- програма використовує курси мережевої академії Cisco, що охоплюють такі важливі теми, як Networking, Cybersecurity, IoT & Data Analytics, OS and IT, а також Programming Courses. Це надає учасникам міцну базу знань і практичних навичок, які є критично важливими для успіху в цій галузі;
- пропозиція приділити більше уваги опануванню принципів безпеки в базах даних. Це включає розуміння механізмів захисту даних, управління доступом та впровадження методів шифрування;
- пропозиція акцентувати увагу на вивченні хмарних технологій і DevOps, що дозволить спеціалістам інтегрувати безпекові практики на всіх етапах розробки і експлуатації ПЗ, включаючи управління конфігураціями, автоматизацію розгортання та моніторинг. Це зменшує ризики і підвищує загальну безпеку систем.

В цілому ОПП «Кібербезпека» за спеціальністю 125 «Кібербезпека та захист інформації» першого (бакалаврського) рівня вищої освіти надає позитивне враження, є сучасною, відповідає запитам ринку праці у сфері кібербезпеки та захисту інформації та забезпечує формування компетентностей, необхідних для розв’язання типових задач. Вважаємо, що рецензована ОПП може впроваджуватись в Національному технічному університеті «Харківський політехнічний інститут».

Виконавчий директор
ГС «Харківський кластер
інформаційних технологій»
2025 рік

УКРАЇНА
ГРОМАДСЬКА СПІЛКА "ХАРКІВСЬКИЙ КЛАСТЕР ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ" №39887790
місто Харків

Ольга ШАПОВАЛ

PREFACE

Corresponds to the Standard of Higher Education of the first (bachelor) level in specialty 125 "Cybersecurity and information protection", which was approved by the order of the Ministry of Education and Science of Ukraine dated 29.10.2024 No. 1547.

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
Sergii YEVSEIEV, doctor of technical sciences, professor, head of the cybersecurity department.

Members of the workgroup EPP:

1. Olga KOROL, candidate of technical sciences, associate professor, associate professor of the cybersecurity department.
2. Serhii POHASII, doctor of technical sciences, associate professor, professor of the cybersecurity department.
3. Stanislav MILEVSKYI, doctor of technical sciences, associate professor, professor of the cybersecurity department
4. Diana SIPCO, student, group КН-1122б.

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 of Computer Sciences and Information Technologies department of cybersecurity
The degree of higher education and the title of the qualification in the original language	Bachelor Educational qualification: bachelor of cybersecurity and information protection. Diploma qualification: bachelor 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	Bachelor diploma, unitary, 240 ECTS credits, study period 3 years 10 months
Availability of accreditation	National Higher Education Quality Agency. Accreditation certificate educational program No. 9111. Valid up – 01.07.2029.
Cycle/level	first (bachelor) level of higher education; NRK of Ukraine – level 6, FQ-EHEA – first cycle, EQF LLL – level 6
Prerequisites	Persons who have received a complete general secondary education may enter to obtain a bachelor's degree in the Bachelor's Degree in F5 Cybersecurity and information protection. The reception on the basis of the degree of junior bachelor, professional junior bachelor or educational qualification level of the junior specialist is carried out in the manner prescribed by law.
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-bakalavr/

2 - The purpose of the educational and professional program	
Training of specialists capable of using and implementing information and/or cyber security technologies, as well as digital economy technologies.	
3 – Characteristics of the educational and professional program	
Subject area (field of knowledge, specialty, specialization or subject specialty (if any)	**Field of knowledge:** 12 "Information technologies" **Specialty:** 125 "Cybersecurity and information protection" **Object of study:** - cybersecurity and information protection technologies; - processes of cybersecurity management and information protection; objects of information activity, including information and information and communication systems, information resources and technologies. **Training goals:** training specialists capable of using and implementing cybersecurity and information protection technologies and solving complex cybersecurity and information protection tasks. **Theoretical content of the subject area:** principles, concepts, theory of protection of vital interests of a person, society, state in the use of a cyberspace, which ensures the sustainable development of the information society and digital communicative environment, timely detection, prevention and neutralization of real and potential threats to Ukraine. **Methods , techniques and technologies :** methods, methods and technologies of solving theoretical and practical problems of cybersecurity and information protection. **Tools and equipment :** means, devices, network equipment, applied and specialized software, information systems and design complexes, modeling, control, monitoring, storage, processing, display and protection of data (information flows).
Orientation of the educational program	Educational and professional. Preparation of cybersecurity and information protection professionals.
The main focus of the educational program and specialization or subject specialty (if any)	Special education in the field of information technologies by specialty 125 "Cybersecurity and information protection". In-depth study of information technologies of information protection, information security, cyber security, and information security, development and use of software for information protection, cyber security, and information security. Keywords: cyber security , information security, information protection, information technologies.
Features of the program	The peculiarity of the program of specialty "Cybersecurity and information protection" is the focus on modern requirements for specialists in the field of information and/or cybersecurity, acquisition of higher education by higher

	education of competitive competencies based Cybersecity, Iot & Data Analytics, OS and It, Programming Courses. Ability to learn English.
4 – Eligibility of graduates to employment and academic rights of graduates	
Suitability for employment	Specialists in cybersecurity and information protection can work, according to the current version of the National classifier of Ukraine : Classifier professions DK 003:2010: 2139.2 Information security specialist; 2139.2 Safety specialist (information and communication technologies); 2139.2 Cyber defense infrastructure specialist; 2139.2 Cybersecurity Response Specialist; 2139.2 Cryptographic information specialist; 2139.2 Specialist in technical protection of information; 2139.2 Specialist in testing of security and information security systems; 2139.2 Information technology auditor (cybersecurity); 2139.2 Specialist in evaluation of information security measures (cybersecurity).
Academic rights of graduates	Students who have been trained under this curriculum and received a bachelor's degree have the right to receive education at the second (master's) higher education level in the Higher Education Institution of Ukraine and abroad in the field of knowledge "information technology" or related ones. Acquisition or improvement of education and professional training in the adult system.
5 – Teaching and assessment	
Teaching and learning	Student centered learning, problem-oriented learning, distance learning in the Microsoft 365 system, self-study, learning through project practice, learning through laboratory practice. The teaching process provides for the use of such educational technologies as: lectures, laboratory work, practical classes, small groups, seminars-discussions, Brainstorming, presentations that develop communicative and leadership skills, independent work with literary sources; Mixed forms of training using remote platforms.
Assessment	Monitoring of students' knowledge and skills is carried out in the form of current and final control. Current control - oral and written survey, assessment of work in small groups, testing, defense of group and individual research tasks. Final control - oral and written exams, assessments taking into account the accumulated points of the current control, defense

	of reports from laboratory classes, defense of coursework. State certification is a single state qualification exam. Evaluation is carried out according to the national scale ("excellent", "good", "satisfactory", "unsatisfactory"), 100-point scale and ECTS scale (A, B, C, D, E, FX, F).
6 – Software competencies	
Integral competence	The ability to solve complex specialized tasks and practical tasks in the field of cybersecurity and information protection.
General competencies (GC) (defined by the standard of higher education of the specialty)	GC1. Ability to apply knowledge in practical situations. GC2. Knowledge and understanding of the subject area and understanding of professional activity. GC3. Ability to communicate in the state language both orally and in writing. GC4. Ability to communicate in a foreign language. GC5. Ability to learn and master modern knowledge. GC6. The ability to realize own rights and responsibilities as a member of society, to realize the values of a civil (free democratic) society and the need for its sustainable development, the rule of law, the rights and freedoms of a person and a citizen in Ukraine. GC7. Ability to make decisions and act in accordance with the principle of inadmissibility of corruption and any other manifestations of dishonesty. GC8. The ability to preserve and multiply moral, cultural, scientific values and achievements of society based on an understanding of the history and patterns of development of the domain, its place in the general system of knowledge about nature and society and in the development of society, technologies, to use various types and forms of motor activity for active recreation and leading a healthy lifestyle.
Special (professional) competences (SC) (defined by the standard of higher education of the specialty)	SC1. Ability to apply the legislative and regulatory framework, as well as state and international requirements, practices and standards in order to carry out professional activities in the field of cybersecurity and information protection. SC2. Ability to use information technologies, modern methods and models of cybersecurity and information security systems. SC3. Ability to ensure the continuity of business processes according to the established cybersecurity policy and information protection. SC4. Ability to protect information in information systems according to the established cybersecurity policy and

	information protection. SC5. The ability to restore the functioning of information systems after the realization of threats, cyberattacks, failures and failures of different classes and origin. SC6. Ability to implement and ensure the functioning of complex information protection systems (complexes of regulatory, organizational and technical means and methods, procedures, practical techniques, etc.). SC7. Ability to perform professional activities based on the implemented information and cyber security management system. SC8. Ability to apply methods and means of cryptographic protection of information at objects of information activity. SC9. Ability to apply methods and means of technical protection of information at objects of information activity. SC10. The ability to monitor information processes, to analyze, identify, evaluate possible vulnerability and threats to information space and information resources in accordance with the established information security policy.
7 - Learning outcomes	
The results of studies in the specialty (defined by the standard of higher education of the specialty)	LO1. Freely speak the state language orally and in writing when performing professional duties. LO2. Communicate in a foreign language in order to ensure the effectiveness of professional communication. LO3. Apply the principle of inadmissibility of corruption and any other manifestations of dishonesty in professional activity. LO4. Organize own professional activity, choose optimal methods and ways of solving complex specialized tasks and practical problems in professional activity, evaluate their effectiveness. LO5. Analyze, argue, make decisions when solving complex specialized tasks and practical problems in professional activity, which are characterized by complexity and incomplete determination of conditions, be responsible for the decisions made. LO6. Adapt to new conditions and technologies of professional activity, predict the end result. LO7. Apply and adapt information and coding theories, mathematical statistics, numbers, cryptography and steganography, signal processing and transmission, etc., principles, methods and concepts of cybersecurity and information protection in training and professional activity. LO8. Apply knowledge and understanding of mathematics

	and physics in professional activity, formalize the objectives of the subject area of cybersecurity and protection of information, formulate their mathematical production and choose a rational method of solution. LO9. To know and apply the legislation of Ukraine and international requirements, practices and standards for the purpose of conducting professional activity in the field of cybersecurity and information protection. LO10. Be able to use modern information technologies, methods and models of cybersecurity and information security systems for professional activity. LO11. Plan preparation and ensure the continuity of processes in organizations according to the established cybersecurity policy and taking into account the requirements for information protection. LO12. Apply information security methods in information systems according to the established information security policy. LO13. To implement, adjust, accompany and maintain the functioning of software and software and software and software security and information protection systems as necessary procedures for the functioning of information systems and \ or infrastructure of the organization as a whole. LO14. To solve the problems of managing the recovery processes of information systems using reservation procedures according to the established security policy and to ensure the functioning of special software, to protect and restore information. LO15. Collect, process, store, analyze critical data to prove the implementation of cyber threats, analyze and research a cyberincident in order to promptly restore the functioning of the information system. LO16. To solve the problems of implementation and support of complex information protection systems in information systems. LO17. To ensure the functioning of the cybersecurity management system and the protection of the organization's information, including staff and managing the consequences of threats to information safety in crisis situations, on the basis of performing quantitative and qualitative risk assessment procedures. LO18. Analyze, apply the methods and means of cryptographic protection of information at information activities. LO19. To solve tasks on the organization and control of the

	state of cryptographic protection of information, in particular in accordance with the requirements of regulatory documents. LO20. Identify the threats of creation of technical channels of leakage of information on the objects of information activity; to implement the means and measures of technical protection of information from leakage by technical channels, to maintain and control the status of hardware means of information protection and complexes of technical protection of information. LO21. To implement, support, analysis of efficiency of systems for detecting unauthorized access, actions with information in the information system, vulnerability, possible threats to information space and information resources and use protection complexes to ensure the required level of information security in information systems.
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 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). 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. Teaching teachers, specialists and employees of IT companies, as well as foreign specialists are involved in teaching.
Material and technical support	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). 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.
Informational and	Meets the technological requirements for educational and

educational and methodological support	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). 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-kompontiv-125-bakalavr/). Information resources are located in the funds of the scientific library of NTU "KPI", websites of graduation departments. The educational process uses LMS (Learning Management System).
9 – Academic mobility	
National credit mobility	On the basis of bilateral agreements on academic mobility with universities of Ukraine. Agreements on cooperation regarding the implementation of programs of internal academic mobility of higher education students under the educational program specialty 125 "Cybersecurity" with Odesa National University of Technology, Chernihiv National University of Technology.
International credit mobility	On the basis of a bilateral agreement with the University named after Jan Dlugosha in Częstochowa (Poland).
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. Compulsory educational components of OPP			
1.1 General training			
ЗП 1	*History and culture of Ukraine*	*4,0*	*Exam*
ЗП 2	*Foreign Language*	*4,0*	*Test, Exam*
ЗП 3	*Ukrainian as a foreign language*	*12,0*	*Test, Exam*
ЗП 4	*Physics*	*6,0*	*Exam*
ЗП 5	*Fundamentals of humanitarian and philosophical knowledge in professional activity*	*4,0*	*Exam*
ЗП 6	*Higher mathematics*	*12,0*	*Test, Exam*
ЗП 7	*Language of professional training*	*9,0*	*Test, Exam*
ЗП	*Physical training*	*2,0*	*Test*
1.2 Special (professional) training			
СП 1	*Introduction to the specialty. Introductory practice*	*3,0*	*Test*
СП 2	*Basics of programming*	*4,0*	*Exam*
СП 3	*Information and coding theory*	*3,0*	*Exam*
СП 4	*Legal regulation of cybersecurity*	*4,0*	*Test*
СП 5	*Algorithms and data structures*	*5,0*	*Exam*
СП 6	*Physical bases of technical intelligence means*	*5,0*	*Exam*
СП 7	*Information security of the state*	*3,0*	*Test*
СП 8	*Fundamentals of social engineering*	*4,0*	*Test*
СП 9	*Mathematical foundations of cryptology*	*4,0*	*Exam*
СП 10	*Programming technologies*	*4,0*	*Exam*
СП 11	*Computer networks*	*5,0*	*Exam*
СП 12	*Operating system architecture and security*	*6,0*	*Test*
СП 13	*Programming tools*	*6,0*	*Exam*
СП 14	*Basics of cryptographic protection*	*6,0*	*Test*
СП 15	*Fundamentals of building and protecting microprocessor systems*	*4,0*	*Exam*
СП 16	*Fundamentals of mathematical modelling of security systems*	*4,0*	*Exam*
СП 17	*Basics of steganographic information protection*	*5,0*	*Test*
СП 18	*Security in information and communication systems*	*4,0*	*Test*
СП 19	*Web application development*	*6,0*	*Exam*

СП 20	*Integrated information security systems*	*4,0*	*Exam*
СП 21	*Security of Internet things*	*3,0*	*Test*
СП 22	*Web security*	*4,0*	*Test*
СП 23	*Comprehensive training*	*4,0*	*Test*
СП 24	*Antivirus protection of information*	*4,0*	*Test*
СП 25	*Machine learning basics for cybersecurity*	*3,0*	*Exam*
2. Practical training			
ПП 1	*Industrial practice*	*6,0*	*Test*
ПП 2	*Technological practice*	*6,0*	*Test*
3. Unified state qualification exam			
A1	*Preparation for the Unified State Examination*	*1,5*	
A2	*Unified state qualification exam*	*1,5*	
General amount mandatory components		***175***	
4. Selective educational components			
4.1 Profile training			
4.1.1 Profiled package of educational components 01 "Artificial Intelligence in Security Systems"			
ВП1.1	*Ethical hacking*	*3,0*	*Exam*
ВП1.2	*Date of mining*	*3,0*	*Exam*
ВП1.3	*Mathematical foundations of artificial intelligence*	*3,0*	*Exam*
ВП1.4	*Python for artificial intelligence and machine learning*	*4,0*	*Exam*
ВП1.5	*Genetic algorithms*	*3,0*	*Exam*
ВП1.6	*Python for internet things*	*3,0*	*Exam*
ВП1.7	*Systems engineering*	*3,0*	*Exam*
4.1.2 Profiled package of educational components 02 "Blockchain technology and security of banking systems"			
ВП1.1	*Decentralised systems*	*3,0*	*Exam*
ВП1.2	*Risk management*	*3,0*	*Exam*
ВП1.3	*Blockchain: basics and application examples*	*3,0*	*Exam*
ВП1.4	*Security of banking systems*	*4,0*	*Exam*
ВП1.5	*Protecting critical infrastructure facilities*	*3,0*	*Exam*
ВП1.6	*Organising document management with restricted access*	*3,0*	*Exam*
ВП1.7	*Security in social networks*	*3,0*	*Exam*
4.1.3 Profiled package of educational components в 03 "Innovation Campus"			
ВП3.1	*Basics of cybersecurity*	*3,0*	*Exam*
ВП3.2	*Development of corporate information systems (part 1)*	*3,0*	*Exam*
ВП3.3	*Development of corporate information systems (part 2)*	*3,0*	*Exam*
ВП3.4	*Databases for corporate information systems*	*4,0*	*Exam*
ВП3.5	*Architecture of corporate information*	*3,0*	*Exam*

	systems		
ВП3.6	*Security and audit of wireless and mobile networks*	*3,0*	*Exam*
ВП3.7	*Protecting critical infrastructure facilities*	*3,0*	*Exam*
4.2 Educational components of the free choice of professional training in the all-institutional catalogue			
ОКВП1	*ОК ВВ ПП 1*	*4,0*	*Test*
ОКВП2	*ОК ВВ ПП 2*	*4,0*	*Test*
ОКВП3	*ОК ВВ ПП 3*	*4,0*	*Test*
ОКВП4	*ОК ВВ ПП 4*	*4,0*	*Test*
ОКВП5	*ОК ВВ ПП 5*	*4,0*	*Test*
ОКВП6	*ОК ВВ ПП 6*	*4,0*	*Test*
ОКВП7	*ОК ВВ ПП 7*	*4,0*	*Test*
4.3 Educational components of the free choice of the university catalogue			
ОКВЗ 1	*ОК ВВ ЗП 1*	*4,0*	*Test*
ОКВЗ 2	*ОК ВВ ЗП 2*	*4,0*	*Test*
ОКВЗ 3	*ОК ВВ ЗП 3*	*4,0*	*Test*
4.4 Educational components of the special university choice			
ОКСВУ 1	*ОКСВУ*	*3,0*	*Test*
Total amount for elective components:		***65***	
GENERAL SCOPE OF THE EDUCATIONAL AND PROFESSIONAL PROGRAM:		***240***	

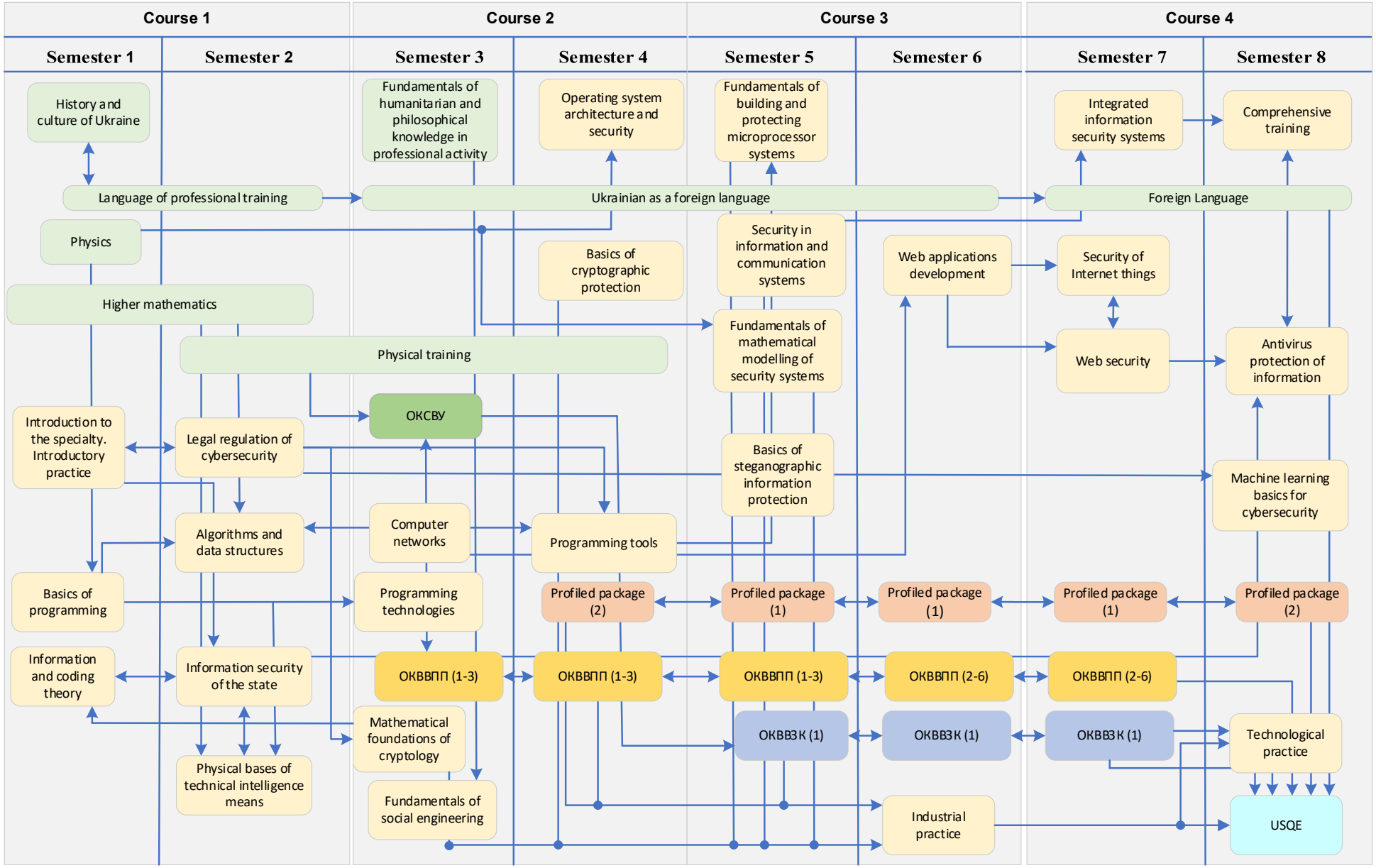
3. DISTRIBUTION CONTENT EDUCATIONAL AND PROFESSIONAL PROGRAMS BY IN GROUPS COMPONENTS AND CYCLES PREPARATION

No n/p	Cycle preparation	The amount of the applicant's educational loadhigher education (ECTS credits / %)		
		Mandatory components educational professional programs	Selective components educational professional programs	All in allterm teaching
1	General training	53 / 22,1	-	**53 / 22,1**
2	Special (professional) training	122/ 50,8	-	**122/ 50,8**
3	Components free of choice	-	65 / 27,1	**65 / 27,1**
Total for the entire term teaching		**175 / 72,9**	**65 / 27,1**	**240 / 100**

4. FORM CERTIFICATES EARNERS HIGHER EDUCATION

Forms of attestation of applicants of higher education	Attestation is carried out in the form of a state qualification exam.
Requirements for the unified state qualification exam	The only state qualification exam provides for evaluating the achievements of the learning outcomes, defined by the higher education standard of the specialty "Cybersecurity and information protection" and the educational program.

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** **Зн1.** Conceptual scientific and practical knowledge. **Зн2.** Critical understanding of theories, principles, methods and concepts in the field of professional activity and/or learning.	**Skill** **Ум1.** Deep cognitive and practical skills, skills and innovation at the level necessary to solve complex specialized tasks and practical problems in the field of professional activity or learning.	**Communication** **К1.** Reporting to experts and non -specialists of information, ideas, problems, solutions to their own experience and argumentation. **К2.** Collection, interpretation and use of data. **К3.** Communication on professional issues, including foreign language.	**Responsibility and autonomy** **АВ1.** Management of complex technical or professional activities or projects. **АВ2.** The ability to be responsible for making and making decisions in unpredictable working and/or educational contexts. **АВ3.** Formation of judgments that take into account social, scientific and ethical aspects. **АВ4.** Organization and management of professional development of persons and groups. **АВ5.** The ability to continue learning with a significant degree of autonomy.
GENERAL COMPETENCES				
ЗК1	Зн2	Ум1		
ЗК2	Зн2	Ум1	К1	
ЗК3			К1, К3	
ЗК4			К1, К3	
ЗК5	Зн1, Зн2	Ум1	К2	АВ3
ЗК6	Зн1		К1	АВ2, АВ3, АВ4
ЗК7			К1	АВ2
ЗК8	Зн2		К2	АВ3
SPECIAL (PROFESSIONAL) COMPETENCES				
СК1	Зн2	Ум1	К2	
СК2	Зн1, Зн2	Ум1	К2	
СК3		Ум1		АВ1
СК4		Ум1		АВ1
СК5		Ум1	К2	АВ1, АВ2
СК6		Ум1	К1	АВ1
СК7		Ум1	К1	АВ1
СК8	Зн2	Ум1		
СК9	Зн2	Ум1		
СК10		Ум1	К2	АВ2

7. MATRIX OF MATCHING DEFINED OF STANDARD LEARNING OUTCOMES, COMPETENCIES AND EDUCATIONAL COMPONENTS

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	CK1	CK2	CK3	CK4	CK5	CK6	CK7	CK8	CK9	CK10
LO1	СП			ЗП6 СП1 СП2 СП5 СП6 СП7 СП8 СП10 СП11 СП13 СП14 СП17 СП18 СП20 СП24 ПП5 ПП6															
LO2	СП				ЗП2 ЗП3 СП7 СП8 СП11 СП12 СП14 СП24														
LO3	СП						ЗП1 СП1 СП4 СП7	СП4 СП7											
LO4	СП	ЗП4 ЗП СП2	ЗП4 ЗП5 ЗП6																

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	CK1	CK2	CK3	CK4	CK5	CK6	CK7	CK8	CK9	CK10
		СП3 СП4 СП5 СП7 СП8 СП9 СП10 СП11 СП12 СП14 СП15 СП16 СП19 СП21 СП22 СП23 СП24 СП25 ПП5 ПП6	СП1 СП2 СП4 СП5 СП6 СП7 СП10 СП13 СП14 СП15 СП16 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП25 ПП5 ПП6																
LO5	СП	ЗП4 ЗП СП2 СП3 СП4 СП5 СП7 СП8 СП9 СП10 СП11 СП12 СП14 СП15	ЗП4 ЗП5 ЗП6 СП1 СП2 СП4 СП5 СП6 СП7 СП10 СП13 СП14 СП15 СП16																

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	CK1	CK2	CK3	CK4	CK5	CK6	CK7	CK8	CK9	CK10
		СП16 СП19 СП21 СП22 СП23 СП24 СП25 ПП5 ПП6	СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП25 ПП5 ПП6																
LO6	СП		ЗП4 ЗП5 ЗП6 СП1 СП2 СП4 СП5 СП6 СП7 СП10 СП13 СП14 СП15 СП16 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП25 ПП5 ПП6						ЗП1 ЗП4 ЗП5 ЗП СП1 СП3 СП17 СП20 СП23 СП25										
LO7	СП	ЗП4							ЗП1										

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	CK1	CK2	CK3	CK4	CK5	CK6	CK7	CK8	CK9	CK10
		ЗП СП2 СП3 СП4 СП5 СП7 СП8 СП9 СП10 СП11 СП12 СП14 СП15 СП16 СП19 СП21 СП22 СП23 СП24 СП25 ПП5 ПП6							ЗП4 ЗП5 ЗП СП1 СП3 СП17 СП20 СП23 СП25										
LO8	СП					ЗП4 ЗП6 СП1 СП2 СП3 СП4 СП5 СП6 СП7 СП9 СП10 СП11 СП12													

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	CK1	CK2	CK3	CK4	CK5	CK6	CK7	CK8	CK9	CK10
						СП14 СП15 СП16 СП23 СП25													
LO9	СП						ЗП1 СП1 СП4 СП7			СП1 СП4 СП7 СП8 СП10 СП11 СП14 СП20 СП23 СП24									
LO10	СП										СП2 СП3 СП5 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП16 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25									

Learning outcomes	Competences																			
	Integral competenc	General competences								Special (professional) competences										
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10
											ПП5								
LO11	СП											СП11 СП14 СП20 СП21 СП24							
LO12	СП												СП9 СП11 СП12 СП14 СП19 СП20 СП21 СП22 СП23 СП24 СП25						
LO13	СП												СП9 СП11 СП12 СП14 СП19 СП20 СП21 СП22 СП23 СП24 СП25						
LO14	СП													СП8 СП11 СП14 СП15 СП21 СП24					

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	CK1	CK2	CK3	CK4	CK5	CK6	CK7	CK8	CK9	CK10
														СП25					
LO15	СП													СП8 СП11 СП14 СП15 СП21 СП24 СП25					
LO16	СП														СП11 СП12 СП14 СП20 СП23 СП25 ПП6				
LO17	СП															СП7 СП16 СП23 СП25 ПП5 ПП6			
LO18	СП																СП3 СП9 СП11 СП12 СП14 СП15 СП18 СП21 СП23 СП24 ПП6		
LO19	СП																СП3 СП9		

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	CK1	CK2	CK3	CK4	CK5	CK6	CK7	CK8	CK9	CK10
																	СП11 СП12 СП14 СП15 СП18 СП21 СП23 СП24 ПП6		
LO20	СП																	СП6 СП12 СП14 СП15 СП19 СП20 СП22 СП23 ПП6	
LO21	СП																		СП8 СП11 СП14 СП16 СП18 СП23 СП24 СП25 ПП5

7. THE RESULTS OF DISCUSSING THE EDUCATIONAL PROGRAM

Stakeholders	Remarks / Recommendation	Taken into account / partially taken into account / not taken into account	Note
Olga SHAPOVAL, Executive Director of Kharkiv Cluster of Information Technology	Pay more attention to mastering security principles in databases. Emphasis on the study of cloud technologies and Devops.	Taken into account.	Due to the selective educational components: Security in Devops, databases with SQL and Python
Guarantor of the EPP, Sergii YEVSEIEV, doctor of technical sciences, professor, head of the cybersecurity department. Members of the EPP Working Group	Educational and professional program to comply with the requirements of the Higher Education Standard in the specialty 125 Cybersecurity and information protection of the first (bachelor) level of higher education, approved and put into force by the order of the Ministry of Education and Science of Ukraine dated 24.10.2024. No. 1547.	Taken into account.	Changes have been made.
Olena VOLOSHCHUK, Candidate of Technical Sciences, Head of Educational Programs of Distributed Lab LLC.	Positive response. Without remarks.	-	-
Kateryna MOLODETSKA, Doctor of Technical Sciences, Professor, Professor of Management of Organizations of Kyiv-Mohyla Business School National University "Kyiv-Mohyla	Positive response. Without remarks.	-	-

Academy"			
Vladyslav KOVTUN, Candidate of Technical Sciences, Associate Professor, "Syfer" LLC general director.	Positive response. Without remarks.	-	-
Serhii GOLOVASHYCH, Candidate of Technical Sciences, Associate Professor, LLC "Microcrypt Technologies" general director.	Positive response. Without remarks.	-	-

Head of the Department of Cybersecurity _____ Serhii YEVSEIEV

Guarantor of the educational program _____ Serhii YEVSEIEV

8. PLAN TO TAKE INTO ACCOUNT THE COMMENTS/RECOMMENDATIONS ON THE RESULTS OF THE ACCREDITATION EXAMINATION OF 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)			
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.	Long -term	Update in the EPP 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. Protocol No. 12 of 14.03.2025.	The period of time to the next accreditation of OP. Responsible: guarantor OP.
To strengthen students' awareness of internal procedures for organizing the educational process. It is recommended to review and update literature in the syllabus of educational components.	Long -term	To strengthen students' awareness of internal procedures for organizing the educational process. It is recommended to review and update literature in the syllabus of educational components. Protocol No. 12 of 14.03.2025.	The period of time to the next accreditation of OP. Responsible: guarantor OP.
Using a cyberpoligon to familiarize students with his capabilities	Long -term	Using a cyberpoligon to familiarize students with his capabilities Protocol No. 12 of 14.03.2025.	The period of time to the next accreditation of OP. Responsible: Head of the Department of KB, teachers of the department.

Provide constant updating of information on all aspects of EPP proceedings on the department's website.	Long -term	Updating information on all aspects of EPP proceedings on the department's website. Protocol No. 12 of 14.03.2025.	The period of time to the next accreditation of OP. Responsible: guarantor OP.

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

Guarantor of the educational program _____ Serhii YEVSEIEV