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"

First (bachelor) level of higher education

in specialty **F5 – Cybersecurity and information protection**
fields of knowledge **F - 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 2026

Kharkiv 2026

LETTER OF AGREEMENT

Educational and professional program «Cybersecurity»

Level of higher education	First (bachelor) level
Branch of knowledge	F Information technologies
Specialty	F5 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
_____ Andrii TKACHOV
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-11226
_____ Diana SIPCO
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.

REVIEWERS:

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

1. Ivan OPIRSKY, 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. 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 освітню програму "Кібербезпека"
першого (бакалаврського) рівня вищої освіти,
спеціальності F5 "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.

Освітня 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 освітній програмі "Кібербезпека", за якою навчаються студенти Національного технічного університету "Харківський

політехнічний інститут" за спеціальністю F5 "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.

Особливої уваги заслуговує блок освітніх компонентів «Штучний інтелект в системах захисту», який є невід'ємною частиною сучасної освітньої програми. Студенти опановують методи застосування технологій штучного інтелекту для виявлення, аналізу та нейтралізації кіберзагроз. У рамках цих дисциплін розглядаються інтелектуальні системи моніторингу, машинне навчання, аналіз великих даних для виявлення аномалій у кіберпросторі, а також питання автоматизації процесів кіберзахисту. Такий підхід дозволяє майбутнім фахівцям формувати стійкі практичні навички використання інноваційних підходів до забезпечення кібербезпеки на основі інтелектуального аналізу інформації.

Слід підвести, що освітня 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 F5 "Кібербезпека та захист інформації.

ВІДДІЛ КАДРІВ 02071010

ПІДПИС ЗАСВІДЧУЮ

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

CIPI-IER

ТОВ «САЙФЕР ІТ»
Адреса: 04107, Київ, вул Напірна, 25-27
Тел.: +38 044 484 46 12, 484 4617
E-mail: 1nfo@ciphercom.ua

Системи захисту iwформзціі
www.cipher.com.ua

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

РЕЦЕНЗІЯ-ВІДГУК
НА ОСВІТНЮ ПРОГРАМУ "КІБЕРБЕЗПЕКА"

першого (бакалаврського) рівня вищої освіти
спеціальності F5 "Кібербезпека та захист інформації"
кафедри кібербезпеки Національного технічного університету
"Харківський політехнічний інститут"

Стрімкий розвиток інформаційних технологій та експоненційне зростання глобальної мережі Інтернет призвели до формування нового інформаційного середовища, що охоплює всі аспекти людської діяльності. Сучасні технології сприяють ефективному розповсюдженню даних, оптимізують виробничі процеси та розширюють можливості для ведення бізнесу.

Сучасні підприємства функціонують у форматі розподілених структур - це мережі філій, підрозділів і команд, які взаємодіють між собою. В цьому контексті ключову роль відіграють корпоративні інформаційні системи, які трансформують традиційний бізнес у цифрову площину - електронний бізнес.

Електронний бізнес базується на використанні Інтернету та сучасних ІТ-технологій, щоб підвищити продуктивність у всіх сферах: продажах, маркетингу, фінансах, кадрах, клієнтській підтримці та партнерських взаємодіях.

Одним із критично важливих факторів функціонування електронного бізнесу є інформаційна безпека. Вона передбачає захист інформації та відповідної інфраструктури від загроз, що можуть завдати шкоди користувачам чи власникам даних. Порушення інформаційної безпеки може мати серйозні фінансові наслідки, аж до повного припинення діяльності компанії.

Незважаючи на прогрес у галузі ІТ, рівень загроз не зменшується. Уразливість систем зберігається, що підвищує актуальність питань кіберзахисту. Тому інформаційна безпека є об'єктом постійної уваги як фахівців, так і широкого кола користувачів, зокрема бізнес-структур.

Останнім часом штучний інтелект (ШІ) став невід'ємною складовою систем інформаційної безпеки. Завдяки здатності аналізувати великі обсяги даних у реальному часі, ШІ дозволяє ефективно виявляти загрози, прогнозувати кібератаки, автоматизувати

реагування на інциденти та адаптувати захисні механізми. Його застосування значно підвищує надійність сучасних систем захисту.

У зв'язку з цим кафедра кібербезпеки НТУ "ХПІ" розробила освітню програму "Кібербезпека", орієнтовану на підготовку фахівців широкого профілю у сфері інформаційної безпеки. Програма охоплює як традиційні технології, так і новітні підходи, зокрема використання ШІ у системах захисту, криптографічні методи, стандарти кібербезпеки, забезпечення безпеки критичної інфраструктури тощо.

Навчання організовано з використанням інтегрованих середовищ розробки, сучасного ПЗ та апаратно-програмного комплексу кіберполігону. Студенти отримують ліцензований доступ до сервісів Microsoft 365, що сприяє формуванню практичних навичок у реальному середовищі.

Випускники освітньо-професійної програми «Кібербезпека» мають знання, необхідні для аналізу, проєктування, розгортання і супроводу ІТ-систем у корпоративному середовищі відповідно до вимог національних та міжнародних стандартів у сфері кібербезпеки. Програма формує висококваліфікованих спеціалістів, затребуваних на ринку праці, здатних ефективно впроваджувати сучасні технології захисту, зокрема інструменти на основі штучного інтелекту.

Директор ТОВ "Сайфер ІТ",
кандидат технічних наук
2026 рік

Владислав КОВТУН

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

РЕЦЕНЗІЯ-ВІДГУК

на освітню програму “Кібербезпека”
першого (бакалаврського) рівня вищої освіти,
спеціальності F5 “Кібербезпека та захист інформації”
кафедри кібербезпеки Національного технічного університету
“Харківський політехнічний інститут”

Освітня програма «Кібербезпека», запропонована кафедрою кібербезпеки Національного технічного університету «Харківський політехнічний інститут», є надзвичайно актуальною в умовах стрімкого розвитку інформаційних технологій та їх проникнення в усі сфери сучасного життя. В Україні відчувається значний дефіцит висококваліфікованих ІТ-фахівців із досвідом у сфері кібербезпеки.

Метою цієї програми є формування у студентів здатності вирішувати складні спеціалізовані завдання та практичні проблеми в галузі інформаційної взаємодії та/або кібербезпеки, які характеризуються комплексністю та неповною визначеністю умов. Сучасні сценарії реалізації кіберзагроз часто вирізняються невизначеністю можливих засобів, методів та вразливостей, що можуть бути застосовані порушником, синергетичним характером походження та несподіваними умовами втручання. Водночас існують сценарії, які можна передбачити, та побудувати надійний контур безпеки, наприклад, на рівні обчислювальної мережі невеликої компанії чи розподіленої корпоративної мережі.

Об’єктом вивчення за програмою є об’єкти інформатизації, включаючи комп’ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні та інформаційно-телекомунікаційні системи, інформаційні ресурси

та технології; технології забезпечення безпеки інформації; процеси управління інформаційною взаємодією та/або кібербезпекою об'єктів, що підлягають захисту. Це свідчить про те, що майбутні фахівці з кібербезпеки будуть здатні впроваджувати та використовувати сучасні технології інформаційної комунікації та/або кібербезпеки в практичних задачах виробництва або надання послуг.

Для забезпечення необхідних компетенцій випускників та досягнення відповідних результатів навчання, кафедра кібербезпеки НТУ «ХПІ» включила вивчення іноземної мови (за професійним спрямуванням) як обов'язковий освітній компонент. Це відповідає сучасним професійним вимогам в IT-галузі, щодо покращення комунікаційних навичок фахівців та їх взаємодії зі світовою спільнотою за обраним напрямом.

На першому курсі студенти вивчають 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» (продовження вивчення Python), «Фізичні основи технічних засобів розвідки» та інші. Ці дисципліни поєднують загальні знання, необхідні кожному IT-фахівцю, із спеціалізованими знаннями в галузі кібербезпеки.

На другому курсі студенти вивчають: «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 інші. Такий перелік курсів свідчить про більш цільове спрямування на вивчення особливостей кіберзахисту, як з теоретичної, так і з практичної точки зору.

На третьому курсі студенти опановують наступні дисципліни 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 інші.

На четвертому курсі студенти завершують бакалаврський цикл, вивчаючи дисципліни: «Організаційне забезпечення захисту інформації», «Основи стеганографічного захисту інформації» та інші, а також виконують комплексний курсовий проєкт.

Блок освітніх компонентів «Штучний інтелект в системах захисту» посідає важливе місце у структурі освітньої програми, відображаючи її сучасну спрямованість. Студенти вивчають методи використання технологій штучного інтелекту для ідентифікації, аналізу та нейтралізації кіберзагроз. Програма охоплює тематику інтелектуальних систем моніторингу, машинного навчання, обробки великих даних для виявлення аномалій у кіберпросторі, а також автоматизації процесів забезпечення кібербезпеки. Це сприяє формуванню у здобувачів освіти глибоких практичних навичок застосування інноваційних рішень у сфері кіберзахисту на основі інтелектуального аналізу даних.

Таким чином, аналіз освітньої програми «Кібербезпека» бакалаврського рівня, запропонованої кафедрою кібербезпеки НТУ «ХПІ», підтверджує її актуальність для ІТ-галузі та сприяє підготовці фахівців з кібербезпеки, які наразі дуже потрібні сучасним підприємствам та організаціям України. Крім того, ця освітньо-професійна програма дозволяє студентам продовжити навчання за фахом на рівні магістра.

Особливістю освітньо-професійної програми «Кібербезпека» для першого (бакалаврського) рівня вищої освіти є комплексний підхід до вивчення дисциплін, який передбачає надання компетенцій майбутнім фахівцям, починаючи від побудови захищених рішень на рівні локальних обчислювальних мереж, та завершуючи розподіленими гетерогенними мережами корпоративного рівня, із застосуванням зовнішніх дата-центрів.

Генеральний директор
ТОВ "Мікрокрипт Технолоджіс",
кандидат технічних наук
2026 рік

"МІКРОКРИПТ ТЕХНОЛОДЖІС" код 38281163

Сергій ГОЛОВАШИЧ

РЕЦЕНЗІЯ-ВІДГУК
НА ОСВІТНЮ ПРОГРАМУ “КІБЕРБЕЗПЕКА”
першого (бакалаврського) рівня вищої освіти,
спеціальності F5 “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 F5 “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.

Програма містить дисципліни, які формують у студентів не тільки професійні знання, а й загальні компетентності, що сприяють розвитку критичного мислення, умінь працювати в команді, приймати ефективні рішення в умовах невизначеності, що є важливими складовими діяльності у сфері кібербезпеки. Випускники володіють знаннями щодо правових, організаційних та інженерно-технічних методів забезпечення кіберзахисту інформації, навичками організації захисту комп'ютерних систем, мереж та веб-

ресурсів, а також методами аналізу ризиків та оцінки вразливостей інформаційних систем.

Освітня програма вирізняється актуальністю, оскільки орієнтована на вирішення сучасних викликів у сфері кібербезпеки, особливо в умовах гібридної війни та зростання кількості кібератак. Важливою перевагою є можливість опанування англійської мови професійного спрямування, що розширює горизонти працевлаштування як на території України, так і за її межами.

Навчальний план включає дисципліни, спрямовані не лише на формування фахових знань, а й на розвиток загальних компетентностей. Зокрема, йдеться про навички критичного мислення, командної взаємодії та прийняття рішень в умовах невизначеності — ключові якості для ефективної діяльності в галузі кібербезпеки. Випускники володіють знаннями у сфері правових, організаційних та інженерно-технічних методів захисту інформації, здатні організовувати безпеку комп’ютерних систем, мереж і веб-ресурсів, а також аналізувати ризики та виявляти вразливості в інформаційних системах.

Окреме місце в програмі займає освітній блок «Штучний інтелект у системах захисту», що є невід'ємною частиною сучасної підготовки фахівців. Студенти здобувають знання з використання технологій штучного інтелекту для ідентифікації, аналізу та нейтралізації кіберзагроз. Розглядаються інтелектуальні системи моніторингу, методи машинного навчання, обробка великих даних з метою виявлення аномалій, а також автоматизація процесів кіберзахисту. Такий підхід забезпечує майбутнім фахівцям стійкі практичні навички застосування інноваційних технологій для захисту інформаційного простору.

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 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 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,
кандитат 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» 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 ІТ-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 F5 «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»
2026 рік

Ольга ШАПОВАЛ

PREFACE

Corresponds to the Standard of Higher Education of the first (bachelor) level in specialty F5 "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
Andrii TKACHOV, Candidate of Technical Sciences, Senior Researcher, Associate Professor of the Cybersecurity Department.

Members of the workgroup EPP:
1. Sergii YEVSEIEV, Doctor of Technical Sciences, Professor, Head of the Cybersecurity Department.
2. Olga KOROL, Candidate of Technical Sciences, Professor of the Cybersecurity Department.
3. Alla HAVRYLOVA, PhD, Associate Professor of the Cybersecurity Department.
4. Stanislav MILEVSKYI, Doctor of Technical Sciences, Professor of the cybersecurity department.
5. 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:** F "Information technologies" **Specialty:** F5 "Cybersecurity and information protection" **Object of study:** – cyber security and information protection technologies; – cyber security and information protection management processes; - security of information resources, systems and technologies, artificial intelligence, objects of information activity and critical infrastructure. **Training goals:** training specialists capable of using and implementing cyber security and information protection technologies and solving complex problems in the field of cyber security and information protection. **Theoretical content of the subject area:** theories, concepts, concepts, principles of protection of the vital interests of people, society, and the state during the use of cyberspace, security of information systems and technologies, ensuring timely detection, prevention and neutralization of targeted (mixed) attacks, objects of information activity and critical infrastructure in cyberspace. **Methods , techniques and technologies :** methods, techniques and technologies, research, modeling, analysis and improvement of the processes of creation, processing, transmission, reception, destruction, display, protection (cyber protection) of information resources, solving theoretical and practical problems of cyber security and information protection in cyberspace, detection, analysis of cyber incidents and countermeasures, prevention and neutralization of real and potential threats to information resources, objects of information activity and critical infrastructure, creation, support and ensuring the effective functioning of information protection systems, research and improvement of processes of processing and protection of information resources. **Tools and equipment :** applied and specialized software, network equipment, hardware, information protection tools and devices.
Orientation of the educational program	Educational and professional. Preparation of cybersecurity and information protection professionals.
The main focus of the educational program	Special education in the field of information technologies by specialty F5 "Cybersecurity and information protection". In-

and specialization or subject specialty (if any)	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)	SC1. Ability to apply the legislative and regulatory framework, as well as state and international requirements, practices and

(defined by the standard of higher education of the specialty)	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 educational and methodological support	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). 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.khpi.edu.ua/sylabusy-osvitnikh-komponentiv-f5-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 "Cybersecurity" specialty F5 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. Mandatory educational components			
1.1 General training			
GT 1	*International Support for the National Resistance*	*5,0*	*Test*
GT 2	*The History of Ukrainian Statehood*	*4,0*	*Exam*
GT 3	*Foreign Language*	*4,0*	*Test, Exam*
GT 4	*Ukrainian as a foreign language*	*12,0*	*Test, Exam*
GT 5	*Physics*	*4,0*	*Exam*
GT 6	*Fundamentals of humanitarian and philosophical knowledge in professional activity*	*4,0*	*Exam*
GT 7	*Higher mathematics*	*5,0*	*Test*
GT 8	*Fundamentals of Higher Algebra*	*6,0*	*Exam*
GT 9	*Language of professional training*	*6,0*	*Test, Exam*
GT	*Physical education*	*8,0*	*Test*
1.2 Special (professional) training			
ST 1	*Introduction to the specialty. Introductory practice*	*3,0*	*Test*
ST 2	*Basics of programming*	*4,0*	*Exam*
ST 3	*Information and coding theory*	*4,0*	*Exam*
ST 4	*Legal Regulation of Information Security*	*3,0*	*Test*
ST 5	*Algorithms and data structures*	*4,0*	*Test*
ST 6	*Physical bases of technical intelligence means*	*3,0*	*Exam*
ST 7	*Information security of the state*	*3,0*	*Test*
ST 8	*Social Engineering Methods in Cybersecurity*	*3,0*	*Exam*
ST 9	*Mathematical foundations of cryptology*	*4,0*	*Exam*
ST 10	*Programming technologies*	*4,0*	*Exam*
ST 11	*Computer networks*	*4,0*	*Exam*
ST 12	*Security of Modern Operating Systems*	*6,0*	*Exam*
ST 13	*Cybersecurity Software Development*	*5,0*	*Exam*
ST 14	*Basics of cryptographic protection*	*5,0*	*Test*
ST 15	*Fundamentals of Microprocessor System Security*	*5,0*	*Exam*
ST 16	*Administration of information protection systems*	*4,0*	*Exam*
ST 17	*Basics of steganographic information protection*	*4,0*	*Exam*

ST 18	*Geosint-reconnaissance*	*4,0*	*Test*
ST 19	*Web application development*	*4,0*	*Exam*
ST 20	*Information security systems*	*5,0*	*Exam*
ST 21	*Web security*	*6,0*	*Exam*
ST 22	*Internet of Things security*	*4,0*	*Test*
ST 23	*Comprehensive training*	*4,0*	*Test*
ST 24	*Neural Networks*	*4,0*	*Test*
ST 25	*Open Source Intelligence (OSINT)*	*4,0*	*Test*
2. Practical training			
PT 1	*Industrial practice*	*6,0*	*Test*
PT 2	*Technological practice*	*6,0*	*Test*
3. Attestation			
	Attestation	*6,0*	
General amount mandatory components		***179***	
4. Optional educational components			
4.1 Specialised training			
Profiled package of educational components 01 "Artificial Intelligence in Security Systems"			
EC 1.1	*Ethical hacking*	*3,0*	*Exam*
EC 1.2	*Date of mining*	*3,0*	*Exam*
EC 1.3	*Mathematical foundations of artificial intelligence*	*3,0*	*Exam*
EC 1.4	*Python for artificial intelligence and machine learning*	*3,0*	*Exam*
EC 1.5	*Genetic algorithms*	*3,0*	*Exam*
EC 1.6	*Python for internet things*	*3,0*	*Exam*
EC 1.7	*Systems engineering*	*3,0*	*Exam*
Profiled package of educational components 02 "Blockchain technology and security of banking systems"			
EC 2.1	*Decentralised systems*	*3,0*	*Exam*
EC 2.2	*Risk management*	*3,0*	*Exam*
EC 2.3	*Blockchain: basics and application examples*	*3,0*	*Exam*
EC 2.4	*Security of banking systems*	*3,0*	*Exam*
EC 2.5	*Protecting critical infrastructure facilities*	*3,0*	*Exam*
EC 2.6	*Organising document management with restricted access*	*3,0*	*Exam*
EC 2.7	*DevOps Security*	*3,0*	*Exam*
Profiled package of educational components в 03 "Innovation Campus"			
EC 3.1	*Basics of cybersecurity*	*3,0*	*Exam*
EC 3.2	*Development of corporate information systems (part 1)*	*3,0*	*Exam*
EC 3.3	*Development of corporate information systems (part 2)*	*3,0*	*Exam*
EC 3.4	*Databases for corporate information systems*	*3,0*	*Exam*
EC 3.5	*Architecture of corporate information systems*	*3,0*	*Exam*

EC 3.6	*Security and audit of wireless and mobile networks*	*3,0*	*Exam*
EC 3.7	*Protecting critical infrastructure facilities*	*3,0*	*Exam*
4.2 Educational components of free choice of professional training of the general institute catalog			
ECPT 1	*EC FC PT 1*	*4,0*	*Test*
ECPT 2	*EC FC PT 2*	*4,0*	*Test*
ECPT 3	*EC FC PT 3*	*4,0*	*Test*
ECPT 4	*EC FC PT 4*	*4,0*	*Test*
ECPT 5	*EC FC PT 5*	*4,0*	*Test*
ECPT 6	*EC FC PT 6*	*4,0*	*Test*
ECPT 7	*EC FC PT 7*	*4,0*	*Test*
4.3 Educational components of free choice of general training			
ECGT 1	*EC FC GT 1*	*4,0*	*Test*
ECGT 2	*EC FC GT 2*	*4,0*	*Test*
ECGT 3	*EC FC GT 3*	*4,0*	*Test*
Total amount for elective components:		***61***	
GENERAL SCOPE OF THE EDUCATIONAL AND PROFESSIONAL PROGRAM:		***240***	

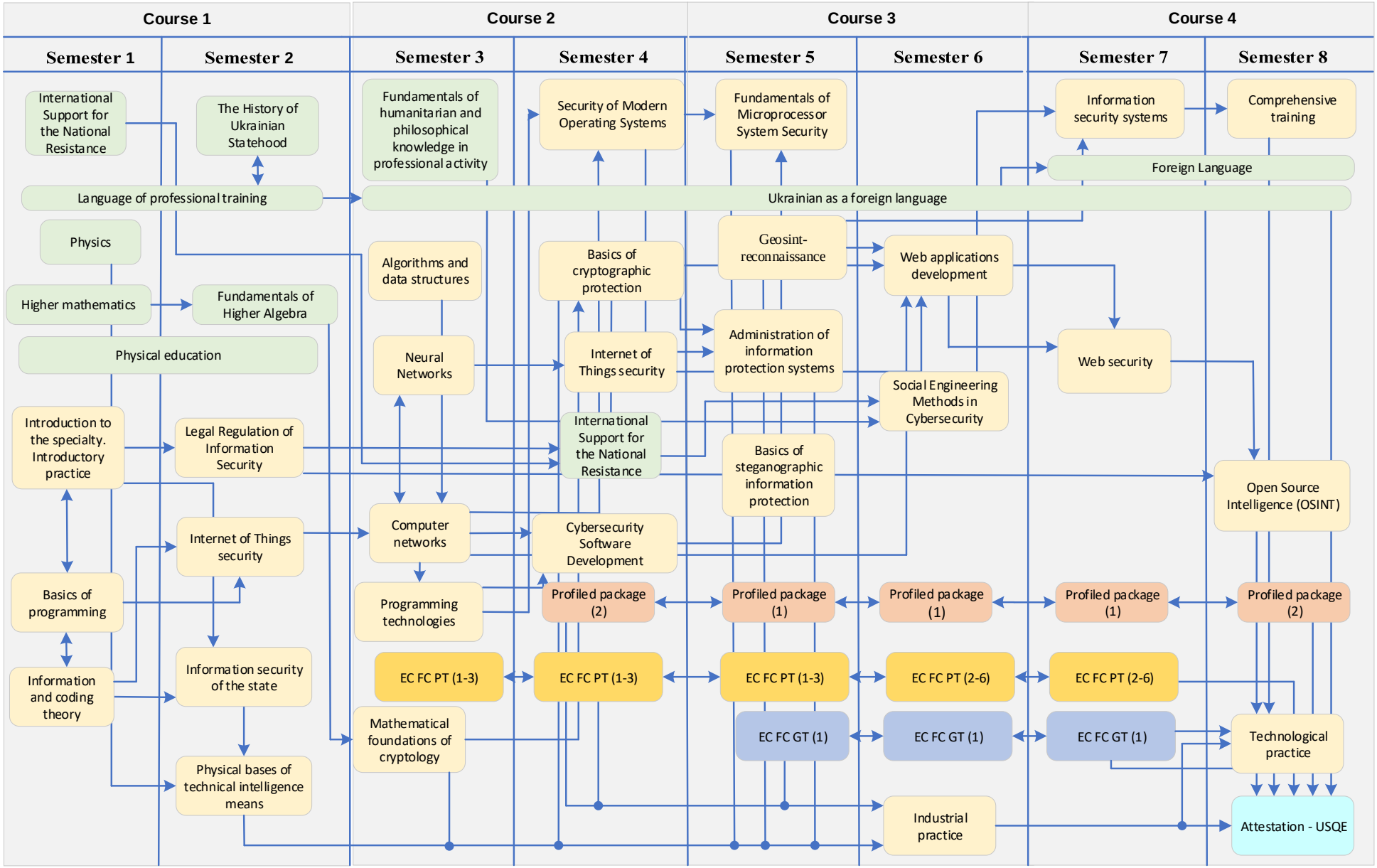
3. DISTRIBUTION CONTENT EDUCATIONAL AND PROFESSIONAL PROGRAMS BY IN GROUPS COMPONENTS AND CYCLES PREPARATION

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	58 / 24,2	-	**58 / 24,2**
2	Special (professional) training	103/ 42,9	-	**103/ 42,9**
3	Practical training	12/5	-	**12/5**
4	Attestation	6/2,5	-	**6/2,5**
5	Optional educational components	-	61 / 25,4	**61 / 25,4**
Total for the entire term teaching		**179 / 74,6**	**61 / 25,4**	**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				
GC 1	Зн2	Ум1		
GC 2	Зн2	Ум1	К1	
GC 3			К1, К3	
GC 4			К1, К3	
GC 5	Зн1, Зн2	Ум1	К2	АВ3
GC 6	Зн1		К1	АВ2, АВ3, АВ4
GC 7			К1	АВ2
GC 8	Зн2		К2	АВ3
SPECIAL (PROFESSIONAL) COMPETENCES				
SK1	Зн2	Ум1	К2	
SK2	Зн1, Зн2	Ум1	К2	
SK3		Ум1		АВ1
SK4		Ум1		АВ1
SK5		Ум1	К2	АВ1, АВ2
SK6		Ум1	К1	АВ1
SK7		Ум1	К1	АВ1
SK8	Зн2	Ум1		
SK9	Зн2	Ум1		
SK10		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	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
LO1	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT9 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22			GT1 GT7 GT8 ST1 ST2 ST5 ST6 ST7 ST8 ST10 ST11 ST13 ST14 ST17 ST18 ST20 ST24 PT1 PT2															

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST23 ST24 ST25 PT1 PT2																		
LO2	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT9 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20				GT3 GT4 ST7 ST8 ST11 ST12 ST14 ST24														

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST21 ST22 ST23 ST24 ST25 PT1 PT2																		
LO3	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT9 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18						GT1 GT2 ST1 ST4 ST7	GT1 ST4 ST7											

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST19 ST20 ST21 ST22 ST23 ST24 ST25 PT1 PT2																		
LO4	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT9 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16	GT1 GT5 GT ST2 ST3 ST4 ST5 ST7 ST8 ST9 ST10 ST11 ST12 ST14 ST15 ST16 ST19 ST21 ST22 ST23 ST24 ST25 PT1 PT2	GT1 GT5 GT6 GT7 GT8 ST1 ST2 ST4 ST5 ST6 ST7 ST10 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22 ST23 ST25 PT1 PT2																	

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST17 ST18 ST19 ST20 ST21 ST22 ST23 ST24 ST25 PT1 PT2																		
LO5	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT9 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14	GT1 GT5 GT ST2 ST3 ST4 ST5 ST7 ST8 ST9 ST10 ST11 ST12 ST14 ST15 ST16 ST19 ST21 ST22 ST23 ST24 ST25 PT1 PT2	GT1 GT5 GT6 GT7 GT8 ST1 ST2 ST4 ST5 ST6 ST7 ST10 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22 ST23 ST25																	

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22 ST23 ST24 ST25 PT1 PT2		PT1 PT2																
LO6	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT9 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12		GT1 GT5 GT6 GT7 GT8 ST1 ST2 ST4 ST5 ST6 ST7 ST10 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22						GT2 GT5 GT6 GT ST1 ST3 ST17 ST20 ST23 ST25									

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22 ST23 ST24 ST25 PT1 PT2		ST23 ST25 PT1 PT2																
LO7	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT9 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10	GT1 GT5 GT ST2 ST3 ST4 ST5 ST7 ST8 ST9 ST10 ST11 ST12 ST14 ST15 ST16 ST19 ST21 ST22 ST23							GT2 GT5 GT6 GT ST1 ST3 ST17 ST20 ST23 ST25										

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22 ST23 ST24 ST25 PT1 PT2	ST24 ST25 PT1 PT2																	
LO8	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT9 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8					GT1 GT5 GT7 GT8 ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST9 ST10 ST11 ST12 ST14 ST15 ST16														

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22 ST23 ST24 ST25 PT1 PT2					ST23 ST25													
LO9	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT9 GT ST1 ST2 ST3 ST4 ST5 ST6						GT1 ST1 ST4 ST7			GT1 ST1 ST4 ST7 ST8 ST10 ST11 ST14 ST20 ST23 ST24									

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22 ST23 ST24 ST25 PT1 PT2																		
LO10	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT9 GT ST1 ST2 ST3 ST4										ST2 ST3 ST5 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST16 ST17 ST18 ST19								

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22 ST23 ST24 ST25 PT1 PT2										ST20 ST21 ST22 ST23 ST24 ST25 PT1								
LO11	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT9 GT ST1 ST2											ST11 ST14 ST20 ST21 ST24							

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22 ST23 ST24 ST25 PT1 PT2																		
LO12	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT9 GT												ST9 ST11 ST12 ST14 ST19 ST20 ST21 ST22 ST23 ST24						

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22 ST23 ST24 ST25 PT1 PT2												ST25						
LO13	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8												ST9 ST11 ST12 ST14 ST19 ST20 ST21 ST22						

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	GT9 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22 ST23 ST24 ST25 PT1 PT2												ST23 ST24 ST25						
LO14	GT1 GT2 GT3 GT4 GT5 GT6													ST8 ST11 ST14 ST15 ST21 ST24					

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	GT7 GT8 GT9 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22 ST23 ST24 ST25 PT1 PT2													ST25					
LO15	GT1 GT2 GT3 GT4													ST8 ST11 ST14 ST15					

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	GT5 GT6 GT7 GT8 GT9 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22 ST23 ST24 ST25 PT1 PT2													ST21 ST24 ST25					
LO16	GT1 GT2														ST11 ST12				

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	GT3 GT4 GT5 GT6 GT7 GT8 GT9 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22 ST23 ST24 ST25 PT1 PT2														ST14 ST20 ST23 ST25 PT2				

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
LO17	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT9 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22 ST23 ST24 ST25															ST7 ST16 ST23 ST25 PT1 PT2			

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	PT1 PT2																		
LO18	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT9 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21 ST22 ST23																ST3 ST9 ST11 ST12 ST14 ST15 ST18 ST21 ST23 ST24 ІПП2		

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST24 ST25 PT1 PT2																		
LO19	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT9 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19 ST20 ST21																ST3 ST9 ST11 ST12 ST14 ST15 ST18 ST21 ST23 ST24 ПП2		

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST22 ST23 ST24 ST25 PT1 PT2																		
LO20	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT9 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17 ST18 ST19																	ST6 ST12 ST14 ST15 ST19 ST20 ST22 ST23 PT2	

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST20 ST21 ST22 ST23 ST24 ST25 PT1 PT2																		
LO21	GT1 GT2 GT3 GT4 GT5 GT6 GT7 GT8 GT9 GT ST1 ST2 ST3 ST4 ST5 ST6 ST7 ST8 ST9 ST10 ST11 ST12 ST13 ST14 ST15 ST16 ST17																		ST8 ST11 ST14 ST16 ST18 ST23 ST24 ST25 PT1

Learning outcomes	Competences																		
	Integral competenc	General competences								Special (professional) competences									
		GC1	GC2	GC3	GC4	GC5	GC6	GC7	GC8	SK1	SK2	SK3	SK4	SK5	SK6	SK7	SK8	SK9	SK10
	ST18 ST19 ST20 ST21 ST22 ST23 ST24 ST25 PT1 PT2																		

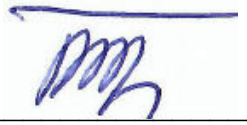
7. THE RESULTS OF DISCUSSING THE EDUCATIONAL PROGRAM

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.	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.
Guarantor of the EPP, Sergii YEVSEIEV, doctor of technical sciences, professor, head 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, Sergii YEVSEIEV, doctor of	In order to bring it into line with modern terminology and standards of higher	Taken into account.	As part of the periodic review of the educational program, taking into

technical sciences, professor, head of the cybersecurity department. Members of the EPP Working Group	education, update the names of individual disciplines of the educational program.		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.
Olena VOLOSHCHUK, Candidate of Technical Sciences, Head of Educational Programs of Distributed Lab LLC.	Positive response. Without remarks.	-	-
Ivan OPIRSKY, 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.	-	-
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  Andrii TKACHOV

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. Considered at the meeting of the department, 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. Considered at the meeting of the department, Protocol No. 12 of 14.03.2025.	The period of time to the next accreditation of OP. Responsible: Head of the Department, teachers of the department.
Using a cyberpoligon to familiarize students with his capabilities	Long -term	Using a cyberpoligon to familiarize students with his capabilities.	The period of time to the next accreditation of OP.

		Considered at the meeting of the department, Protocol No. 12 of 14.03.2025.	Responsible: guarantor OP, Head 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. Considered at the meeting of the department, 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 _____ Andrii TKACHOV