National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

APPROVED
by the Academic Council
of Igor Sikorsky Kyiv Polytechnic Institute
(minutes of meeting №5 of 13.05 2024)
Chairman of the Academic Council
Mykhailo ILCHENKO

ЗАТВЕРДЖЕНО
Вченою радою
КПІ ім. Ігоря Сікорського
(протокол №5 від 13.05 2024 р.)
Голова Вченої ради
Михайло ІЛЬЧЕНКО

СИСТЕМИ, ТЕХНОЛОГІЇ ТА МАТЕМАТИЧНІ МЕТОДИ КІБЕРБЕЗПЕКИ
SYSTEMS, TECHNOLOGIES AND MATHEMATICAL METHODS OF CYBER SECURITY

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА / PROFESSIONAL EDUCATIONAL PROGRAMME

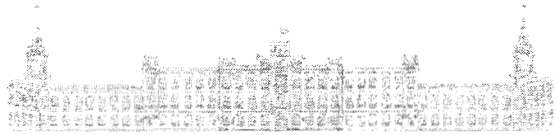
ЄДЕБО ID: ***57895***

Другий (магістерський) рівень вищої освіти
Спеціальність: 125 Кібербезпека та захист інформації
Галузь знань: 12 - Інформаційні технології
Кваліфікація: магістр з кібербезпеки та захисту інформації

Second (master) level of higher education
Speciality: 125 Cyber Security and Information protection
Knowledge branch: 12 - Information Technology
Qualification: Master's degree of Cybersecurity and Information Protection

Введено в дію з 2024/2025 н.р.
наказом ректора №НОД/1434/24 від 10.06 2024 р.

Enacted since 2024/2025 academic year
by rector's order No.НОД/1434/24 of 10.06 2024



Київ/Kyiv
2024

У разі наявності в описі освітньої програми будь-яких розбіжностей, перевагу має текст українською мовою /
In case of any differences in interpretation of the information in the educational programme, the Ukrainian text shall prevail

ПРЕАМБУЛА/PREAMBLE

РОЗРОБЛЕНО/ELABORATED:

Керівник групи/Team leader:

Ланде Дмитро Володимирович д.т.н., професор, завідувач кафедри інформаційної безпеки	Dmytro LANDE Dr. Sc, Full Professor, Head of the department of information security

Члени групи/Team members:

Стьопочкіна Ірина Валеріївна к.т.н., доцент кафедри інформаційної безпеки	Iryna STYOPOCHKINA PhD, Professor of the department of information security
Смирнов Сергій Анатолійович к.ф.-м.н., с.н.с., доцент кафедри інформаційної безпеки	Sergii SMYRNOV PhD, Senior Researcher, Professor of the department of information security
Мачуський Євген Андрійович д.т.н., професор, професор кафедри інформаційної безпеки	Eugene MACHUSKY Dr. Sc, Full Professor, Professor of the department of information security
Прогонов Дмитро Олександрович к.т.н., доцент, доцент кафедри інформаційної безпеки	Dmytro PROGONOV PhD, Associate Professor, Professor of the department of information security

ПОГОДЖЕНО/AGREED:

Науково-методична комісія університету зі спеціальності 125 Кібербезпека та захист інформації (протокол № 3 від 07.05.2024 р.)/ The Scientific and Methodological Commission of the University on speciality 125 Cybersecurity and information protection (minutes of meeting № 3 of 07.05.2024)

Голова НМКУ-125/Chairman of the SMCU-125

_____ Дмитро ЛАНДЕ / Dmytro LANDE

Методична рада КПІ ім. Ігоря Сікорського (протокол № 7 від 09.05.2024 р.)/
The Methodological Council of Igor Sikorsky Kyiv Polytechnic Institute (minutes of meeting № 7 of 09.05.2024)

Голова Методичної ради/Chairman of the Methodological Council

_____ Анатолій МЕЛЬНИЧЕНКО / Anatolii MELNYCHENKO

ВРАХОВАНО/CONSIDERED:

Наказ №НОД/263/24 від 08.04.2024 р. «Про організацію та планування освітнього процесу на 2024-2025 навчальний рік».

Положення про розроблення, затвердження, моніторинг та перегляд освітніх програм в КПІ ім. Ігоря Сікорського.

Положення про реалізацію права на вільний вибір навчальних дисциплін здобувачами вищої освіти КПІ ім. Ігоря Сікорського.

Класифікатор професій ДК 003:2010 (зміни внесено Наказом Мінекономіки №1410 від 16 січня 2024 р.).

Побажання і пропозицій стейкхолдерів:

Ковальчук Андрій Олегович,
Керівник напрямку відкритих інновацій Samsung R&D Institute Ukraine (SPUKR), відповідальний за співпрацю з університетами

Поята Сергій Русланович,
Операційний директор міжнародної компанії з кібербезпеки ISSP

Кудін Антон Михайлович
Головний експерт управління безпеки інформації департаменту безпеки Національного банку України, лауреат Державної премії України в галузі науки і техніки, доктор технічних наук, старший науковий співробітник

Representatives of student organizations

Шрейдер Марія,
член НМКУ 125, студентка 1 курсу магістратури за спеціальністю 125 Кібербезпека та захист інформації

Гуменюк Олег, студент 1 курсу магістратури за спеціальністю 125 Кібербезпека та захист інформації

Проскурня Анна,
студентка 3 курсу бакалаврату за спеціальністю 125 Кібербезпека та захист інформації, Голова студради НН ФТІ

Order No. NOD/263/24 dated April 8, 2024 "On the organization and planning of the educational process for the 2024-2025 academic year."

Regulations on the development, approval, monitoring and revision of educational programs at KPI named after Igor Sikorsky.

Regulations on the exercise of the right to free choice of academic disciplines by higher education applicants of KPI named after Igor Sikorsky.

Classifier of professions DK 003:2010 (amended by Order of the Ministry of Economy No. 1410 of January 16, 2024).

Stakeholders' wishes and suggestions:

Andrii KOVALCHUK
Head of open innovation at
Samsung R&D Institute Ukraine
(SPUKR), responsible for
cooperation with universities

Serhii POYATA
Operations director of the
international cyber security
company ISSP

Anton KUDIN
Chief expert of the Information
security department of the
Security department of the
National Bank of Ukraine,
laureate of the State Prize of
Ukraine in the field of science
and technology, doctor of
technical sciences, senior
researcher

Representatives of student organizations

Mariia SCHREIDER,
member of the Educational and
methodical comission of 125
specialty,
a 1st-year undergraduate
student in the specialty 125
Cybersecurity and Information
Protection

Oleg GUMENIUK, a 1st-year
undergraduate student in the
specialty 125 Cybersecurity
and Information Protection

Anna PROSKURNIA,

3rd year bachelor's student in the specialty 125 Cyber security and information protection, Head of Student Council of ES IPT

Еволюція ОП/Evolution of the EP

Освітня підготовка за ОПП «Системи, технології та математичні методи кібербезпеки» за магістерським рівнем була розпочата з 2017 р., в основу програми було покладено багаторічний досвід підготовки здобувачів за спеціалізацією «Безпека інформаційних та комунікаційних систем», яка здійснювалась на кафедрі інформаційної безпеки.

В 2020 р. програму було грунтовно перероблено із врахуванням пропозицій стейкхолдерів, які внесли пропозиції щодо збільшення різноманітності професійно-орієнтованих дисциплін (студенти) при збереженні насиченої фундаментальної складової (роботодавці). В ОП було внесено також наступні зміни: частину дисциплін перенести до блоків вибіркових, модернізувавши їх наповнення згідно профілю 125 Кібербезпека, запропонувати список вибіркових дисциплін до Факультетського/кафедрального каталогів.

В 2021 р. було внесено корективи щодо обсягів ОК, відведених на дослідницький (науковий) компонент. А також, освітню програму оновлено у зв’язку з виходом стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти від 18.03.2021 № 332, та внесені наступні зміни: доповнено перелік загальних/фахових компетентностей та програмних результатів навчання, змінено кількість кредитів щодо практики. Оновлена освітня програма відповідає вимогам стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти від 18.03.2021 № 332.

В 2022 р. освітню програму оновлено у зв’язку з набуттям Фізико-технічним інститутом статусу Навчально-науковий Фізико-технічний інститут. Внесено зміни у склад проєктної групи та склад стейкхолдерів. Внесено корективи щодо придатності до працевлаштування згідно Зміни №10 до Державного класифікатору професій ДК 003:2010.

В 2023 р. освітню програму було оновлено у зв’язку зі зміною назви спеціальності. Внесено корективи у відповідності з вимогами Постанови Кабінету Міністрів України від 16.12.2022 № 1392 “Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти”.

Educational training for the Master's degree program "Systems, Technologies and Mathematical Methods of Cyber Security" began in 2017, the program was based on many years of experience in training of applicants specializing in "Security of Information and Communication Systems", which was carried out at the Department of Information Security.

In 2020, the program was thoroughly revised, taking into account the proposals of stakeholders, who made proposals to increase the variety of professionally oriented disciplines (students), and to maintain in the same time a well-developed fundamental component (employers). Also, the following changes were made: part of the disciplines were transferred to elective blocks, their content was modified according to profile 125 Cybersecurity, a set of elective disciplines to the Faculty/departmental catalogs was proposed.

In 2021, adjustments were made to the amounts of time allocated to the research (scientific) component. Also, the educational program was updated in connection with the release of the standard of higher education in specialty 125 "Cybersecurity" for the second (master's) level of higher education dated 03.18.2021 No. 332, and the following changes were made: the list of general/professional competencies and program results were enlarged, the number of credits for

practice has been changed. The updated educational program meets the requirements of the standard of higher education in the specialty 125 "Cybersecurity" for the second (master's) level of higher education dated March 18, 2021 No. 332.

In 2022, the educational program was updated in connection with the Physical and Technical Institute acquiring the status of Educational and Scientific Physical and Technical Institute. Changes were made to the composition of the project group and the composition of stakeholders. Corrections were made regarding suitability for employment in accordance with Amendment No. 10 to the State Classifier of Professions DK 003:2010.

In 2023, the educational program was updated in connection with the change of the name of the specialty. Corrections were made in accordance with the requirements of the Resolution of the Cabinet of Ministers of Ukraine dated 16.12.2022 No. 1392 "On Amendments to the List of Fields of Knowledge and Specialties for which Higher Education Candidates are Trained".

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ/ EDUCATIONAL PROGRAMME PROFILE

1 – Загальна інформація/General information		
Повна назва ЗВО та навчального підрозділу/Full name of Higher education institution and faculty/institute	Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Навчально-науковий фізико-технічний інститут	National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Educational and Research Institute of Physics and Technology
Ступінь вищої освіти та назва кваліфікації/Higher education degree and qualification title	Ступінь магістра магістр з кібербезпеки та захисту інформації	Master Degree Master's degree of Cybersecurity and Information Protection
Офіційна назва ОП/Educational programme official title	Системи, технології та математичні методи кібербезпеки	Systems, Technologies and Mathematical Methods of Cyber Security
Тип диплому та обсяг ОП/Diploma type and EP scope	Диплом магістра, 90 кредитів ЄКТС, термін навчання 1 рік 4 місяці	Master diploma, 90 credits ECTS, training period 1 year 4 month
Наявність акредитації/Prior accreditation	Акредитовано НАЗЯВО, сертифікат 6525 від 2023-12-14 дійсний до 2029-07-01	Accredited by NAQA, cetificate No 6525 from 2023-12-14 valid to 2029-07-01
Цикл, рівень ВО/Education cycle, level of HE	НРК України – 7 рівень QF-EHEA – другий цикл EQF-LLL – 7 рівень	NQF of Ukraine - 7 level QF-EHEA – 2 cycle EQF-LLL – 7 level
Передумови/Prerequisites	Наявність ступеня бакалавра	Bachelor Degree
Форми здобуття освіти/ Forms of Education	Очна (денна); Заоч.;	full-time; part-time;
Мова(и) викладання/Language (s) of instruction	Українська	Ukrainian
Інтернет-адреса розміщення ОП /URL of the educational program	https://osvita.kpi.ua/125_OPPM_STMMKB	

2 – Мета освітньої програми/Educational programme purpose	
Підготовка професіоналів, здатних використовувати і впроваджувати новітні системи, технології та математичні методи кібербезпеки, проводити науково-дослідну та інноваційну діяльність в ґалузі захисту інформації і кібернетичної безпеки	Training of professionals capable of using and implementing the modern systems, technologies and mathematical methods of cyber security, conducting research and innovation activities in the field of information protection and cyber security.

3 – Характеристика освітньої програми/ Educational programme characteristics	
Предметна область/Subject area	
Об’єкти вивчення: • сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об’єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; • інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; • інфраструктура об’єктів інформаційної діяльності та критичних інфраструктур; • системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); • інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); • програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; • системи управління інформаційною безпекою та/або кібербезпекою; • технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. **Цілі навчання**: Підготовка фахівців, здатних розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області** Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки. **Методи, методики та технології** Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. **Інструменти та обладнання** Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об’єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.	**Objects of study**: • modern processes of research, analysis, creation and ensuring the functioning of information systems and technologies, other business operational processes at the objects of information activity and critical infrastructures in the field of information security and/or cyber security; • information systems (information and communication, information and telecommunication, automated) and technologies; • infrastructure of information activity objects and critical infrastructures; • systems and complexes of creation, processing, transmission, storage, destruction, protection and display of data (information flows); • information resources of various classes (including state information resources); • software and hardware (means) of cyber protection; • information security and/or cyber security management systems; • technologies, methods, models and means of information security and/or cyber security. **Learning goals**: Training of specialists capable of solving tasks of a research and/or innovative nature in the field of information and/or cyber security. **Theoretical content of the subject area** Theoretical foundations of science-intensive technologies, physical and mathematical fundamental knowledge, theories of identification and decision-making, system analysis, complex systems, modeling and optimization of processes, theory of mathematical statistics, cryptographic and technical protection of information, theory of risks and other interdisciplinary theories and practices in the field of information security and/or cyber security. **Methods, techniques and technologies** Methods, models, techniques and technologies of creation, processing, transmission, reception, destruction, display, protection (cyber protection) of information resources in cyberspace, as well as methods and models of development and use of applied and specialized software for solving professional tasks in the field of information security and /or cyber security. Technologies, methods and models of research, analysis, management and provision of business/operational processes using a set of regulatory and legal and organizational and technical methods and means of protecting information resources in cyberspace. **Tools and equipment** Means, devices, network equipment and environment, applied and specialized software, automated systems and complexes of design, modeling, operation, control, monitoring, processing, display and protection of data (information flows), as well as methods and models of risk theory and information management resources for research and support of objects of information activity in the field of information security and/or cyber security.
Орієнтація ОП/Aspect	
Освітньо-професійна	Educational professional
Основний фокус ОП/Main focus	
Системи, технології та математичні методи кібербезпеки, які базуються на останніх досягненнях науки та техніки. *Ключові слова*: кібернетична безпека, системи і технології кібербезпеки, математичні методи кібербезпеки, аналіз кіберінцидентів, аналіз вразливостей, захист об’єктів критичної інфраструктури	Systems, technologies and mathematical methods of cyber security, which are based on the latest achievements of science and technology. *Keywords*: cyber security, cyber security systems and technologies, mathematical methods of cyber security, cyber incident analysis, vulnerability analysis, protection of critical infrastructure objects
Особливості ОП/Features	
1. Грунтовна фундаментальна підготовка у поєднанні із сучасною професійною підготовкою, яка дозволяє проводити науково-дослідну та інноваційну діяльність і працювати з наукоємними технологіями кібербезпеки; 2. Проходження переддипломної практики на базі підприємств-партнерів та участь студентів у виконанні спільних науково-дослідних проектів на замовлення установ та провідних ІТ-компаній України за фахом; 3. Дуальна освіта.	1. Deep fundamental training in combination with modern professional training, which allows conducting research and innovation activities and working with science-intensive cyber security technologies; 2. Completion of pre-diploma practice on the basis of partner enterprises and participation of students in the implementation of joint research projects commissioned by institutions and leading IT companies of Ukraine by specialty; 3. Dual education

4 – Придатність випускників до працевлаштування та подальшого навчання/ Eligibility of graduates for employment and further study	
Придатність до працевлаштування/Eligibility for employment	
Відповідно до Державного класифікатору професій ДК 003:2010 зі Зміною №10 випускники можуть працювати на посадах, що відповідають класифікаційним угрупованням: 2139.2 Аналітик систем захисту інформації та оцінки вразливостей 2139.2 Аналітик загроз безпеки 2132.2 Розробник систем захисту інформації. 2149 Професіонали із організації інформаційної безпеки. 23 Професіонали в галузі освіти і навчання	According to the State Classifier of Professions DK 003:2010 with Amendment No. 10, graduates can work in positions corresponding to the classification groups: 2139.2 Analyst of information protection systems and vulnerability assessment 2139.2 Security threat analyst 2132.2 Developer of information protection systems. 2149 Professionals from the organization of information security. 23 Professionals in the field of education and training
Подальше навчання/Further study	
Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти. Неформальне навчання.	Continuation of education at the third (educational and scientific) level of higher education. Informal learning.
5 – Викладання та оцінювання/Teaching and assessment	
Викладання та навчання/Teaching and studying	
Програмою передбачено студентоцентроване навчання. Викладання проводиться у таких формах: лекції, практичні та семінарські заняття, комп’ютерні практикуми і лабораторні роботи; курсові роботи; технологія змішаного навчання, практики; виконання дипломного проекту і дипломної роботи (магістерської дисертації)	The program provides for student-centered learning. Teaching is carried out in the following forms: lectures, practical and seminar classes, computer workshops and laboratory works; term papers; mixed learning technology, practices; completion of the diploma project and thesis (master's thesis)
Оцінювання/Assessment	
Оцінювання знань студентів здійснюється у відповідності до Положення про рейтингову систему оцінювання результатів навчання студентів КПІ ім. Ігоря Сікорського за усіма видами аудиторної та позааудиторної роботи (вхідний, поточний, календарний, підсумковий контроль); усних та письмових екзаменів, заліків.	Assessment of students' knowledge is carried out in accordance with the Regulation on the rating system for evaluating the results of students' learning at KPI named after Igor Sikorsky for all types of classroom and extra-auditory work (incoming, current, calendar, final control); oral and written exams, credits.

6 – Програмні компетентності/Programme competencies		
Інтегральна компетентність/Integral competence		
Здатність особи розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки		The ability of a person to solve tasks of a research and/or innovative nature in the field of information security and/or cyber security
Загальні компетентності (ЗК)/General competencies		
ЗК 01	Здатність застосовувати знання у практичних ситуаціях	Ability to apply knowledge in practical situations
ЗК 02	Здатність проведення досліджень на відповідному рівні	Ability to conduct research at the appropriate level
ЗК 03	Здатність до абстрактного мислення, аналізу та синтезу	Ability to abstract thinking, analysis and synthesis
ЗК 04	Здатність оцінювати та забезпечувати якість виконуваних робіт	The ability to evaluate and ensure the quality of the work performed
ЗК 05	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності)	Ability to communicate with representatives of other professional groups of different levels (with experts from other fields of knowledge / types of economic activity)
Фахові компетентності (ФК)/Professional competencies		
ФК 01	Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, науково-технічні розробки, фізичні та математичні фундаментальні знання і моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у галузі інформаційної безпеки та/або кібербезпеки	The ability to reasonably apply, integrate, develop and improve modern information technologies, scientific and technical developments, physical and mathematical fundamental knowledge and models, as well as technologies for creating and using applied and specialized software for solving professional tasks in the field of information security and/or cyber security
ФК 02	Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки	The ability to develop, implement and analyze regulatory documents, provisions, instructions and requirements of technical and organizational direction, as well as integrate, analyze and use the best global practices, standards in order to carry out professional activities in the field of information security and/or cyber security
ФК 03	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури	Ability to research, develop and support methods and means of information security and/or cyber security at objects of information activity and critical infrastructure
ФК 04	Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог	The ability to analyze, develop and support the organization's information security and/or cyber security management system, to form information security strategies and policies, taking into account domestic and international standards and requirements

ФК 05	Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення уразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації	The ability to research, system analysis and ensure the continuity of business/operational processes in order to determine the vulnerabilities of information systems and resources, analyze risks and determine the assessment of their impact in accordance with the established strategy and policy of information security and/or cyber security of the organization
ФК 06	Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації	The ability to analyze, control and provide a management system for access to information resources in accordance with the established strategy and policy of information security and/or cyber security of the organization
ФК 07	Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому	The ability to research, develop and implement methods and measures to counter cyber incidents, to implement management, control and investigation procedures, as well as to provide recommendations on the prevention and analysis of cyber incidents in general
ФК 08	Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи й засоби захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/ або кібербезпеки організації	The ability to research, develop, implement and support methods and means of information protection at objects of information activity and critical infrastructure, in information systems, the ability to evaluate the effectiveness of their use, according to the established strategy and policy of information security and/or cyber security of the organization
ФК 09	Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому	The ability to analyze, develop and support the system of auditing and monitoring the effectiveness of the functioning of information systems and technologies, business\operational processes in the field of information security and/or cyber security of the organization as a whole
ФК 10	Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки	The ability to conduct scientific and pedagogical activities, plan training, monitor and support work with personnel, as well as make effective decisions on information security and/or cyber security
ФК 11	Здатність враховувати сучасні міждисциплінарні науково-практичні контексти при прийнятті рішень стосовно новітніх систем, технологій кібербезпеки, та при використанні та розробці методів кібербезпеки, зокрема, використовуючи апарат аналізу даних та враховуючи вимоги високонавантажених систем	The ability to take into account modern interdisciplinary scientific and practical contexts when making decisions about the latest systems, cyber security technologies, and when using and developing cyber security methods, in particular, using data analysis apparatus and taking into account the requirements of highly loaded systems

7 – Програмні результати навчання (ПРН)/ Programme learning outcomes		
ПРН 01	Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес/операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки	Communicate freely in national and foreign languages, orally and in writing to present and discuss the results of research and innovation, ensuring business/operational processes and issues of professional activity in the field of information security and/or cyber security
ПРН 02	Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах	Integrate fundamental and specialized knowledge to solve complex information security and/or cyber security challenges in broad or multidisciplinary contexts
ПРН 03	Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі	Conduct research and/or innovative activities in the field of information security and/or cyber security, as well as in the field of technical and cryptographic protection of information in cyberspace
ПРН 04	Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки	Apply, integrate, develop, implement and improve modern information technologies, physical and mathematical methods and models in the field of information security and/or cyber security
ПРН 05	Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення	Critically consider the problems of information security and/or cyber security, including at the interdisciplinary and interdisciplinary level, in particular on the basis of understanding the new results of engineering and physical and mathematical sciences, as well as the development of technologies for the creation and use of specialized software
ПРН 06	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення	Analyze and evaluate the security of systems, complexes and means of cyber protection, technologies for creating and using specialized software
ПРН 07	Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки	To justify the use, implement and analyze the best global standards, practices in order to solve complex problems of professional activity in the field of information security and/or cyber security
ПРН 08	Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури	Research, develop and support systems and means of information security and/or cyber security at objects of information activity and critical infrastructure
ПРН 09	Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки	Analyze, develop and support the organization's information security and/or cyber security management system based on information security strategy and policy
ПРН 10	Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації	Ensure the continuity of business/operational processes, as well as identify vulnerabilities of information systems and resources, analyze and assess risks for information security and/or cyber security of the organization

ПРН 11	Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації	Analyze, control and ensure the effective functioning of the access management system to information resources in accordance with the established strategy and policy of information security and/or cyber security of the organization
ПРН 12	Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому	Research, develop and implement methods and measures to counter cyber incidents, implement management, control and investigation procedures, as well as provide recommendations on the prevention and analysis of cyber incidents in general
ПРН 13	Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури	Research, develop, implement and use methods and means of cryptographic and technical information protection of business/operational processes, as well as analyze and provide an assessment of the effectiveness of their use in information systems, objects of information activity and critical infrastructure
ПРН 14	Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому	Analyze, develop and support the system of auditing and monitoring the effectiveness of the functioning of information systems and technologies, business/operational processes in the field of information and/or cyber security as a whole
ПРН 15	Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб	Clearly and unambiguously communicate own conclusions on information security and/or cyber security issues, as well as knowledge and explanations that justify them to staff, partners and other persons
ПРН 16	Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень	Make informed decisions on organizational and technical issues of information security and/or cyber security in complex and unpredictable conditions, including using modern methods and means of optimization, forecasting and decision-making
ПРН 17	Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об’єктивно оцінювати результати навчання	Have the skills of autonomous and independent learning in the field of information security and/or cyber security and related fields of knowledge, analyze your own educational needs and objectively evaluate the results of your studies
ПРН 18	Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки	Plan training, as well as accompany and supervise work with personnel in the area of information security and/or cyber security
ПРН 19	Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності	Choose, analyze and develop suitable typical analytical, calculation and experimental methods of cyber protection, develop, implement and support projects on the protection of information in cyberspace, innovative activities and protection of intellectual property

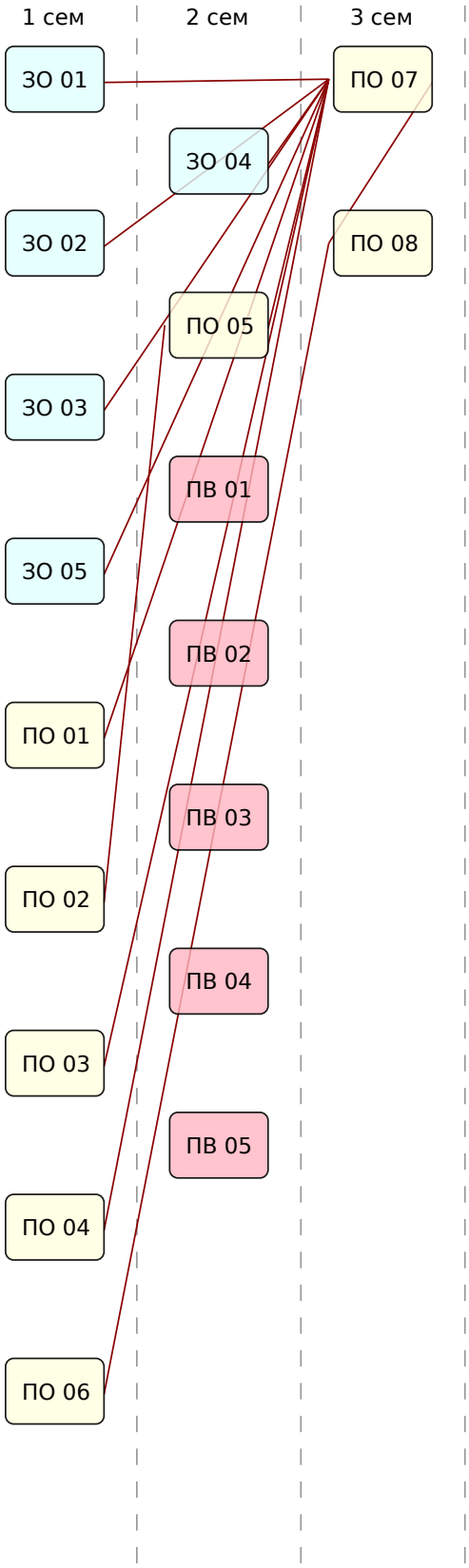
ПРН 20	Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик	Set and solve complex engineering, applied and scientific problems of information security and/or cyber security, taking into account the requirements of domestic and international standards and best practices
ПРН 21	Використовувати методи натурного, фізичного і комп’ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки	Use the methods of natural, physical and computer modeling to study processes related to information security and/or cyber security
ПРН 22	Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки	Plan and carry out experimental and theoretical research, put forward and test hypotheses, choose suitable methods and tools for this, carry out statistical data processing, assess the reliability of research results, argue conclusions
ПРН 23	Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації	To justify the choice of software, equipment and tools, engineering technologies and processes, as well as restrictions on them in the field of information security and/or cyber security on the basis of modern knowledge in related fields, scientific, technical and reference literature and other available information
ПРН 24	Мати навички розроблення, впровадження та супроводження систем кібербезпеки, розробки та використання технологій та математичних методів кібербезпеки з урахуванням сучасних вимог та принципів побудови високонавантажених систем та підходів аналізу даних	Have the skills to develop, implement and support cyber security systems, develop and use cyber security technologies and mathematical methods, taking into account modern requirements and principles of building highly loaded systems and data analysis approaches

8 – Ресурсне забезпечення реалізації програми/ Resource provision for programme implementation	
Кадрове забезпечення/Staffing	
Відповідно до кадрових вимог щодо забезпечення провадження освітньої діяльності для відповідного рівня ВО, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 (в чинній редакції)	In accordance with the personnel requirements for ensuring the implementation of educational activities for the corresponding level of HE, approved by the Resolution of the Cabinet of Ministers of Ukraine dated 12.30.2015 No. 1187 (as amended)
Матеріально-технічне забезпечення/ Material-technical support	
Відповідно до технологічних вимог щодо матеріально-технічного забезпечення освітньої діяльності відповідного рівня ВО, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 (в чинній редакції). 3 комп'ютерних класи, полігон з Кібербезпеки. Використання обладнання для проведення лекцій у форматі презентацій, мережевих технологій, зокрема на платформі дистанційного навчання Sikorsky.	In accordance with the technological requirements for the material and technical support of educational activities of the corresponding level of HE, approved by the Resolution of the Cabinet of Ministers of Ukraine dated 12.30.2015 No. 1187 (in the actual version). 3 computer classrooms, Cyber Security range. Use of equipment for conducting lectures in the format of presentations, network technologies, in particular on the Sikorsky distance learning platform.
Інформаційне та навчально-методичне забезпечення/ Information and methodical support of the educational process	
Відповідно до технологічних вимог щодо навчально-методичного та інформаційного забезпечення освітньої діяльності відповідного рівня ВО, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 (в чинній редакції). Користування Науково-технічною бібліотекою КПІ ім. Ігоря Сікорського.	In accordance with the technological requirements for educational, methodological and informational support of educational activities of the corresponding level of HE, approved by Resolution of the Cabinet of Ministers of Ukraine dated 12.30.2015 No. 1187 (as amended). Use of the Scientific and Technical Library of Ihor Sikorsky Kyiv Polytechnic Institute.
9 – Академічна мобільність/Academic mobility	
Національна кредитна мобільність/National credit mobility	
Участь студентів в програмах академічної мобільності, можливість укладення угод одержання студентами подвійних дипломів	Participation of students in academic mobility programs, the possibility of concluding agreements for students to receive double diplomas
Міжнародна кредитна мобільність/International credit mobility	
Можливість укладення угод про міжнародну академічну мобільність, про подвійне дипломування, про тривалі міжнародні проекти	The possibility of concluding agreements on international academic mobility, on double graduation, on long-term international projects
Навчання іноземних здобувачів ВО/Study of Foreign applicants of HE	
Навчання іноземних здобувачів ВО, які опановують ОП за програмами міжнародної академічної мобільності, навчання може проводитись англійською або українською мовою, за умови володіння здобувачем мовою навчання на рівні не нижче В2.	The training of foreign higher education students who master the OP under international academic mobility programs can be conducted in English or Ukrainian, provided the student has a language proficiency of no lower than B2.

2. ПЕРЕЛІК КОМПОНЕНТІВ ОСВІТНЬОЇ ПРОГРАМИ/COMPONENTS of EDUCATIONAL PROGRAMME

Код/Code	Освітні компоненти програми/Components	Кредитів ЄКТС/ECTS credits	Форма підсумкового контролю/Final control measure form
НОРМАТИВНІ освітні компоненти/Required (standard) components			
Обов’язкові компоненти циклу загальної підготовки/General training cycle			
ЗО 01	Інтелектуальна власність та патентознавство / Intellectual Property and Patent Science	3.0	Залік / Final test
ЗО 02	Сталий інноваційний розвиток / Sustainable Innovative Development	2.0	Залік / Final test
ЗО 03	Практичний курс іноземної мови для ділової комунікації / Practical Foreign Language Course for Business Communication	3.0	Залік / Final test
ЗО 04	Розробка стартап проектів / Development of Startup Projects	3.0	Залік / Final test
ЗО 05	Математичне моделювання систем і процесів / Mathematical modeling of systems and processes	4.0	Залік / Final test
Обов’язкові компоненти циклу професійної підготовки /Professional training cycle			
ПО 01	Проектування високонавантажених систем / Highly loaded systems design	4.0	Залік / Final test
ПО 02	Інтелектуальний аналіз даних / Data Mining	5.0	Екзамен / Exam
ПО 03	Кіберзахист об'єктів критичної інфраструктури / Cyber defense of critical infrastructure facilities	4.0	Залік / Final test
ПО 04	Аналіз кіберінцидентів методами машинного навчання / Cyber incident analysis using machine learning methods	5.0	Екзамен / Exam
ПО 05	Аналіз бінарних вразливостей / Binary vulnerabilities analysis	4.0	Залік / Final test
ПО 06	Основи наукових досліджень / Fundamentals of Scientific Research	2.0	Залік / Final test
ПО 07	Практика / Practice	15.0	Залік / Final test
ПО 08	Виконання магістерської дисертації / Execution of Master's Thesis	13.0	Захист / Defence
ВИБІРКОВІ освітні компоненти/Elective components			
Вибіркові компоненти циклу професійної підготовки/Professional training cycle			
ПВ 01	Освітній компонент 1 Ф-Каталогу / Educational Component 1 from P-Catalogue	4.0	Залік / Final test
ПВ 02	Освітній компонент 2 Ф-каталогу / Educational Component 2 from P-Catalogue	5.0	Екзамен / Exam
ПВ 03	Освітній компонент 3 Ф-каталогу / Educational Component 3 from P-Catalogue	5.0	Екзамен / Exam
ПВ 04	Освітній компонент 4 Ф-каталогу / Elective Educational Component 4 from P-Catalogue	4.0	Залік / Final test
ПВ 05	Освітній компонент 5 Ф-каталогу / Elective Educational Component 5 from P-Catalogue	5.0	Екзамен / Exam
Загальний обсяг нормативних компонентів ОП/Total scope of the required components:		67	
Загальний обсяг вибіркових компонентів ОП/Total scope of the elective components:		23	
Обсяг освітніх компонентів, що забезпечують здобуття компетентностей визначених СВО/Total scope of the educational components aimed at acquisition of competencies specified in the Higher Education Standard:		67	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ/TOTAL SCOPE OF THE EDUCATIONAL PROGRAMME		90	

3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬОЇ ПРОГРАМИ/STRUCTURAL-AND-LOGICAL SCHEME OF THE EDUCATIONAL PROGRAMME



5. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ/ THE FORM OF ATTESTATION FOR DEGREE PURSUERS

Атестація здобувачів вищої освіти за освітньою програмою спеціальності 125 Кібербезпека та захист інформації проводиться у формі захисту кваліфікаційної магістерської роботи та завершується видачею документа встановленого зразка про присудження йому ступеня магістра з кібербезпеки та захисту інформації за освітньою програмою “Системи, технології та математичні методи кібербезпеки”.

Кваліфікаційна робота має розв’язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації.

Атестація здійснюється відкрито і публічно.

Магістерські дисертації перевіряються на ознаки порушення академічної доброчесності та після захисту публікуються в репозиторії НТБ Університету для вільного доступу. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

Attestation of students of higher education according to the educational program of the specialty 125 Cybersecurity and information protection is carried out in the form of defense of a qualifying master's thesis and ends with the issuance of a document of the established model awarding him with a master's degree in cyber security and information protection according to the educational program "Systems, Technologies and Mathematical Methods of Cyber Security".

The qualification work should solve a complex problem of information security and/or cyber security and involve research and/or innovation. The qualification work must not contain academic plagiarism, fabrication, or falsification.

Attestation is carried out openly and publicly.

Master's theses are checked for signs of violation of academic integrity and after defense are published in the NTB repository of the University for free access. The publication of qualifying works with limited access is carried out in accordance with the requirements of the law.

6. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ/COMPLIANCE MATRIX OF PROGRAMME COMPETENCIES WITH PROGRAMME COMPONENTS

	ЗО 01	ЗО 02	ЗО 03	ЗО 04	ЗО 05	ПО 01	ПО 02	ПО 03	ПО 04	ПО 05	ПО 06	ПО 07	ПО 08
ЗК 01	X			X							X	X	X
ЗК 02					X				X		X	X	X
ЗК 03					X		X				X	X	X
ЗК 04									X		X	X	X
ЗК 05		X	X		X						X	X	
ФК 01					X	X	X	X		X	X	X	X
ФК 02	X											X	X
ФК 03								X			X	X	X
ФК 04									X		X	X	X
ФК 05				X	X			X	X	X	X	X	X
ФК 06						X		X		X	X	X	X
ФК 07									X		X	X	X
ФК 08								X			X	X	X
ФК 09				X					X		X	X	X
ФК 10				X								X	
ФК 11						X	X				X	X	X

7. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ/ COMPLIANCE MATRIX OF PROGRAMME LEARNING OUTCOMES WITH PROGRAMME COMPONENTS

	ЗО 01	ЗО 02	ЗО 03	ЗО 04	ЗО 05	ПО 01	ПО 02	ПО 03	ПО 04	ПО 05	ПО 06	ПО 07	ПО 08
ПРН 01			X								X	X	X
ПРН 02					X						X	X	X
ПРН 03		X		X							X	X	X
ПРН 04					X							X	X
ПРН 05					X	X					X	X	X
ПРН 06						X					X	X	X
ПРН 07	X	X						X			X	X	X
ПРН 08								X			X	X	X
ПРН 09								X			X	X	X
ПРН 10										X	X	X	X
ПРН 11						X					X	X	X
ПРН 12							X		X		X	X	X
ПРН 13								X			X	X	X
ПРН 14									X		X	X	X
ПРН 15				X								X	X
ПРН 16					X						X	X	X
ПРН 17											X	X	X
ПРН 18				X								X	
ПРН 19	X										X	X	X
ПРН 20	X										X	X	X
ПРН 21					X						X	X	X
ПРН 22					X						X	X	X
ПРН 23	X										X	X	X
ПРН 24						X	X				X	X	X