



ЗАТВЕРДЖЕНО / APPROVED

Вченою радою КПІ ім. Ігоря Сікорського /
by the Academic Council
of Igor Sikorsky Kyiv Polytechnic Institute
(протокол / minutes of meeting № _____

від / dated _____ 20__ р.

Голова Вченої ради / Head of the Academic Council
_____ Михайло ІЛЬЧЕНКО / Mykhailo ILCHENKO

МАТЕМАТИЧНІ МЕТОДИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ MATHEMATICAL METHODS OF CRYPTOGRAPHIC SECURITY

ОСВІТНЬО-НАУКОВА ПРОГРАМА / EDUCATIONAL SCIENTIFIC PROGRAMME

Другий (магістерський) рівень вищої освіти
Спеціальність: F1 Прикладна математика
Галузь знань: F Інформаційні технології
Кваліфікація: Магістр з прикладної математики

Second (master) level of higher education
Speciality : F1 Applied mathematics
Knowledge branch: F Information Technologies
Qualification: Master of Applied Mathematics

ID: **83418**

Введено в дію з / Enacted since
2025/2026 навчального року / academic year
наказом ректора / by rector's order
№ _____ від / dated _____ 2025

Київ / Kyiv
2025

ПРЕАМБУЛА / PREAMBLE**РОЗРОБЛЕНО / DESIGNED****Керівник робочої групи / Head of the project team:**

Яковлев Сергей Владимирович, кандидат технических наук, зав. кафедрой математических методов защиты информации / Serhii YAKOVLIEV, PhD, Head of the Department of Mathematical Methods of Information Security

Члени робочої групи / Project team members:

Завадська Людмила Олексіївна, кандидат фізико-математичних наук, с.н.с., доцент кафедри математичних методів захисту інформації / Ludmila ZAVADSKA, PhD, Senior Scientist, Associate Professor of the Department of Mathematical Methods of Information Security

Фесенко Андрій В'ячеславович, кандидат фізико-математичних наук, старший викладач кафедри математичних методів захисту інформації / Andrii FESENKO, PhD, Senior Lecturer of the Department of Mathematical Methods of Information Security

Кудін Антон Михайлович, д.т.н., проф., чл.-кор. НАНУ, головний експерт управління безпеки інформації Департаменту безпеки НБУ / Anton KUDIN, Doctor of Science, Professor, Corresponding Member of NAS of Ukraine, Lead expert of Department of Information Security Management, National Bank of Ukraine

Якимчук Олексій Петрович, аспірант 3 курсу / Olexii YAKYMCHUK, post-graduate student

ПОГОДЖЕНО / AGREED:

Науково-методична комісія університету зі спеціальності F1 Прикладна математика/ The Scientific and Methodological Commission of the University on speciality F1 Applied Mathematics

(протокол / minutes of meeting №__ від / dated _____ 20__)

Голова НМКУ - F1 / Head of the SMCU - F1

_____ Олег ЧЕРТОВ / Oleg CHERTOV

Методична рада КПІ ім. Ігоря Сікорського / The Methodological Council of Igor Sikorsky Kyiv Polytechnic Institute

(протокол / minutes of meeting №__ від / dated _____ 20__)

Голова Методичної ради / Head of the Methodological Council

_____ Тетяна ЖЕЛЯСКОВА / Tetiana ZHELIASKOVA

ВРАХОВАНО / CONSIDERED:

Положення про освітні програми КПІ ім. Ігоря Сікорського <https://osvita.kpi.ua/node/137>.

Наказ КПІ ім. Ігоря Сікорського №НОД/362/25 від 25.04.2025 «Про планування та організацію освітнього процесу 2025/2026 н.р.».

Фахову експертизу стейкхолдерів:

Фісуненко Андрій Леонідович, віце-президент з розробок і досліджень ТОВ Самсунг Електронікс Україна Компані, Центр розробок і досліджень

Грубіян Євген Олександрович, провідний дослідник Distributed Lab

Паршин Олександр Юрійович, аспірант 1 курсу

Бондар Петро Олександрович, магістр 1 курсу

Кістаєв Матвій Андрійович, магістр 1 курсу

Regulation on the Educational Programs at Igor Sikorsky Kyiv Polytechnic Institute <https://osvita.kpi.ua/node/137>.

Order of Igor Sikorsky Kyiv Polytechnic Institute No. NOD/362/25 dated 25.04.2025 "On the Planning and the Organization of the Educational Process for the 2025-2026 Academic Year."

Expertise of Stakeholders:

Andriy FISUNENKO, Vice President of Development and Research, Samsung R&D Institute Ukraine, Development and Research Center

Yevhen HRUBIIAN, Lead Researcher, Distributed Lab

Olexandr PARSHYN, post-graduate student

Petro BONDAR, graduate student

Matvii KISTAIEV, graduate student

ЕВОЛЮЦІЯ ОСВІТНЬОЇ ПРОГРАМИ / EVOLUTION OF THE EDUCATIONAL PROGRAMME

Освітньо-наукову програму «Математичні методи криптографічного захисту інформації» було створено 2019 року на основі попередньої програми «Прикладна криптологія». Програма продовжує багаторічні традиції кафедри ММЗІ з підготовки фахівців у галузі прикладної математики, комп'ютерних наук та криптології, з акцентом як на глибинній теоретичній підготовці, так і на практичних навичках, необхідних для створення та аналізу систем криптографічного захисту інформації.

Під час модернізації 2021 року на пропозиції стейкхолдерів (роботодавців та студентів) був переглянутий перелік освітніх компонент, зокрема, було збільшено об'єм та зміст дисципліни «Методи криптоаналізу», центральної для ОНП, та сформовано ряд вибіркових дисциплін для посилення фахової компетентності у галузі криптології.

Під час модернізації 2022 року було уточнено перелік загальних та фахових компетентностей, а також програмних результатів навчання; зроблено деталізацію освітніх компонент, які формують загальні за фахові компетентності, та їх частин по семестрах, уточнено форми підсумкового контролю. Також у програмі були ураховані зміни до національного Класифікатора професій ДК 003:2010, зокрема, уточнено розділ «Придатність до працевлаштування».

Модернізація 2024 року передбачає збільшення об'єму дисциплін «Основи наукових досліджень», «Сучасні алгебраїчні криптосистеми» та оновлення змісту дисципліни «Квантові обчислення та квантова криптографія». Дисципліна «Організаційні аспекти криптографії» на пропозицію стейкхолдерів перероблена та перенесена з нормативних у вибіркові.

Згідно постанови Кабінету Міністрів України від 30 серпня 2024 р. № 1021 ОНП переведена в

галузь знань F Інформаційні технології, спеціальність F1 Прикладна математика.

Модернізація 2025 року передбачає збільшення об'єму науково-дослідної практики для посилення практичних навичок здобувачів вищої освіти. На пропозицію стейкхолдерів буде переглянуто та оновлено зміст дисципліни "Методи криптоаналізу", з посиленням фокусу на навітні підходи та методи, зокрема, за напрямком аналізу постквантово стійких алгоритмів. Разом із компанією Distributed Labs ведеться робота по впровадженню сертифікатної програми по прикладних застосуваннях доведень із нульовими розголошеннями у розподілених системах.

The educational and scientific program "Mathematical methods of cryptographic protection of information" was created in 2019 on the basis of the previous program, "Applied Cryptology". The program continues the long-standing traditions of the Department of Mathematical Methods of Information Security of training specialists in the field of applied mathematics, computer science and cryptology, with an emphasis on both in-depth theoretical training and practical skills necessary for the creation and analysis of cryptographic security systems.

During the modernization of 2021, at the proposal of stakeholders (employers and students), the list of educational components was revised. In particular, the volume and content of the discipline "Methods of Cryptanalysis", central to this program, was increased, and a number of selective disciplines were formed to strengthen professional competence in the field of cryptology.

During the 2022 modernization, the list of general and professional competencies, as well as program learning outcomes, was clarified. Educational components that form general professional competencies and their parts by semester have been detailed; the forms of the final control have been specified. Also, the program took into account changes to the National Classifier of Professions DK 003:2010, in particular, the section "Suitability for employment" was clarified.

The modernization of 2024 involves an enhancement of the disciplines "Fundamentals of Scientific Research" and "Modern Algebraic Cryptosystems", as well as updating the content of the discipline "Quantum Computing and Quantum Cryptography". The discipline "Organizational Aspects of Cryptography" was reworked and transferred from normative to selective at the proposal of stakeholders.

According to Resolution No. 1021 of the Cabinet of Ministers of Ukraine dated 30 August 2024, the program has been transferred to the field of knowledge F Information Technology and the speciality F1 Applied Mathematics.

The 2025 modernization involves increasing the amount of research practice to strengthen the skills of higher education students. At the suggestion of stakeholders, the content of the 'Methods of Cryptanalysis' course is being reviewed and updated to focus more on new approaches and methods, particularly in the area of post-quantum resistant algorithm analysis. In collaboration with Distributed Labs, a certificate programme on the practical application of zero-knowledge proofs in distributed systems is being developed.

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ / EDUCATIONAL PROGRAMME PROFILE

1 - Загальна інформація / General information		
Повна назва закладу вищої освіти та навчального підрозділу / Full name of higher education institution and faculty / educational and scientific 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 освітньої кваліфікації / Higher education degree and education qualification title	Ступінь магістра Магістр з прикладної математики	Master Degree Master of Applied Mathematics
Офіційна назва освітньої програми / Educational programme official title	Математичні методи криптографічного захисту інформації	Mathematical Methods of Cryptographic Security
Тип диплому та обсяг освітньої програми / Diploma type and educational programme volume	Диплом магістра, 120 кредитів ЄКТС, термін навчання 1 рік 9 місяців	Master diploma, 120 credits ECTS, training period 1 year 9 months
Інформація про акредитацію / Accreditation information of the educational programme	Акредитовано НАЗЯВО, сертифікат дійсний до 2028-07-01	Accredited by NAQA, certificate No valid to 2028-07-01
Цикл, рівень вищої освіти / Education cycle, level of higher education	НПК 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);	full-time;
Мова(и) викладання / Language(s) of instruction	Українська	Ukrainian
Інтернет-адреса розміщення освітньої програми / URL of the educational programme	https://osvita.kpi.ua/F1_ONP_M_MMKZI	

2 - Мета освітньої програми / Educational programme purpose

Мета освітньої програми полягає у підготовці професіоналів у галузі математики, статистики, інформаційних технологій, інформаційної безпеки та криптології, здатних формулювати, аналізувати та розв'язувати складні спеціалізовані задачі, а також теоретичні та практичні проблеми прикладної математики у професійній діяльності або у процесі навчання; здійснювати і забезпечувати міжкультурну фахову взаємодію представників науково-технічної спільноти, спрямовану на інтеграцію університетської освіти в європейський освітньо-науковий простір шляхом інтернаціоналізації освітнього процесу в умовах сталого інноваційного науково-технічного розвитку суспільства та формування високої адаптивності здобувачів вищої освіти в умовах трансформації ринку праці через взаємодію з роботодавцями та іншими стейкхолдерами.

Мета освітньої програми відповідає стратегії розвитку КПІ імені Ігоря Сікорського 2025-2030 років щодо досягнення цілей сталого розвитку суспільства, високотехнологічної трансформації держави та зміцнення її обороноздатності, формування якісного людського капіталу для відновлення та стійкого розвитку України

The goal of the educational program is to prepare professionals in the fields of mathematics, statistics, information technology, information security, and cryptology formulating, analyzing and solving complex specialized tasks, as well as theoretical and practical problems of applied mathematics in professional activities or in the process of study; to facilitate and ensure intercultural professional interaction among members of the scientific and technical community, directed towards integrating university education into the European educational and scientific space by internationalizing the educational process which is done within the context of sustainable, innovative, scientific and technical development of society and fostering high adaptability of higher education seekers amid the transformation of the job market through interaction with employers and other stakeholders.

The goal of the educational program aligns with the Igor Sikorsky Kyiv Polytechnic Institute's 2025-2030 development strategy to achieve the aims of sustainable development of society, the high-tech transformation of the state, strengthening of its defence capabilities, and the formation of high-quality human capital for the restoration and sustainable development of Ukraine.

3 - Характеристика освітньої програми / Educational programme characteristics	
Предметна область / Subject area	
Об'єкт діяльності: математичні методи, моделі, алгоритми та програмне забезпечення, що призначені для дослідження, аналізу, проектування процесів та систем в різноманітних конкретних предметних областях. Цілі навчання: підготовка спеціалістів, здатних: – використовувати та впроваджувати математичні методи та технології в галузі прикладної математики; – формулювати, розв'язувати й узагальнювати теоретичні та практичні задачі з використанням фундаментальних та спеціальних прикладних методів математичних та комп'ютерних наук; – розв'язувати задачі математичного моделювання процесів і явищ в умовах невизначеності та неповноти інформації щодо функціонування системи об'єктів; – будувати, досліджувати та застосовувати математичні моделі, що ґрунтуються на даних та на знаннях, створювати та експлуатувати програмне забезпечення. Теоретичний зміст предметної області: математичні методи, що застосовуються в науці, інженерії, бізнесі та промисловості, а також алгоритми і програмні засоби їх реалізації. Методи, методики та технології: прикладні математичні методи та алгоритми; методики вирішення інженерних, наукових, соціально-економічних задач за допомогою спеціалізованих програмних засобів; інформаційні технології проведення комп'ютерного моделювання та обчислювального експерименту, інтелектуального аналізу даних. Інструменти та обладнання: спеціалізовані програмні, апаратні та програмно-апаратні засоби та комплекси для моделювання об'єктів та систем, проведення обчислювальних експериментів тощо; комп'ютеризовані системи у професійній та навчальній діяльності.	Object: mathematical methods, models, algorithms, and software created for research, analysis, and design of processes and systems in various specific subject areas. Educational goals: preparing specialists capable of: – utilizing and implementing mathematical methods and technologies in the field of applied mathematics; – formulating, solving, and generalizing theoretical and practical problems using fundamental and specialized applied methods of mathematical and computer sciences; – solving problems of mathematical modeling of processes under conditions of uncertainty and incomplete information regarding the functioning of the system of objects; – constructing, investigating, and applying mathematical models based on data and knowledge, creating and operating software. Theoretical content of the subject area: mathematical methods applied in science, engineering, business as well as algorithms and software tools for their implementation. Methods, methodologies, and technologies: applied mathematical methods and algorithms; methodologies for solving engineering, scientific, socio-economic problems using specialized software tools; information technologies for conducting computer modeling and computational experiments, intelligent data analysis. Tools and equipment: specialized software and hardware tools for modeling objects and systems, conducting computational experiments, etc.; computerized systems in professional and educational activities.
Орієнтація освітньої програми / Scope	
Освітньо-наукова	Educational and scientific
Основний фокус освітньої програми / Main focus	
Базовий фокус ОП – математичні моделі, методи, алгоритми для задач комп'ютерних наук та криптографічного захисту інформації Ключові слова: математичні методи, алгоритми, криптологія, криптографія, шифрування, цифровий підпис, геш-функція, криптографічний захист інформації	Fundamental focus of the educational program – mathematical models, methods, algorithms for computer science problems and cryptographic information security Keywords: mathematical methods, algorithms, cryptology, cryptography, encryption, digital signature, hash function, cryptographic information security

Особливості освітньої програми / Features	
Різнобічна підготовка фахівців у галузі криптографічного захисту інформації, яка поєднує теоретичну та практичну складову, з акцентом на останніх досягненнях сучасної криптології, новітніх моделях та методах криптографічного захисту інформації та відповідного математичного підґрунтя. Проходження переддипломної практики та виконання спільних проектів на замовлення державних, науково-дослідних установ та провідних ІТ-компаній України за фахом. Дуальна освіта.	Comprehensive training of specialists in the field of cryptographic information security, which combines theoretical and practical components, with an emphasis on the latest achievements of modern cryptology, the latest models and methods of cryptographic information security and the corresponding mathematical basis. Pre-graduation internships and joint projects commissioned by state, research institutions and leading IT companies in Ukraine in the specialty. 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 національного Класифікатору професій ДК 003:2010, випускники можуть працювати на посадах, що відповідають таким класифікаційним угрупованням: 2121.1 Науковий співробітник (прикладна математика); 2121.2 Математик (прикладна математика); 2132.2 Розробник обчислювальних систем; 2139.1 Науковий співробітник (інші галузі обчислень – комп'ютеризація); 2139.2 Професіонали в інших галузях обчислень (комп'ютеризація): Фахівець з криптографічного захисту інформації 2310.2 Інші викладачі закладів вищої освіти Випускники ОП можуть працювати спеціалістами з криптографічного захисту інформації та/або ІТ-технологій, аналітиками даних, розробниками програмних засобів, прикладними програмістами, консультантами із застосування методів математики і статистики для розв'язання прикладних задач широкого спектру, науковими співробітниками.	According to the national Classifier of Professions ДК 003:2010, graduates can work in positions corresponding to the following classification groups: 2121.1 Research Officer (applied mathematics); 2121.2 Mathematician (applied mathematics); 2132.2 Computer Systems Developer; 2139.1 Research Officer (other areas of computing – computerization); 2139.2 Professionals in other areas of computing (computerization): Specialist in cryptographic information security 2310.2 Other teachers of higher education institutions Graduates of the educational program can work as specialists in cryptographic information security and/or IT technologies, data analysts, software developers, application programmers, consultants in the application of mathematics and statistics methods to solve a wide range of applied problems, and researchers.
Подальше навчання / Further study	
Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти; набуття додаткових кваліфікацій у системі післядипломної освіти.	Continuation of education at the third (educational and scientific) level of higher education; acquisition of additional qualifications in the postgraduate education system.

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 (індивідуальні та у малих групах); курсові роботи; технологія змішаного навчання за окремими освітніми компонентами; науково-дослідна практика; виконання дипломної роботи (магістерської дисертації).	The program provides for student-centered learning. Teaching is conducted in the following forms: lectures, practical and seminar classes, computer practicums (individual and small groups); coursework; blended learning technology for separate educational components; research practice; and master's thesis.
Оцінювання / Assessment	
Оцінювання знань студентів здійснюється у відповідності до Положення про систему оцінювання результатів навчання КПІ ім. Ігоря Сікорського за усіма видами аудиторної та позааудиторної роботи (вхідний, поточний, календарний, підсумковий контроль): усні та письмові экзамени, тестування, колоквіуми тощо. Рівень знань по кожній дисципліні оцінюється згідно критеріїв, визначених у Рейтинговій системі оцінювання даної дисципліни.	The assessment of students' knowledge is carried out in accordance with the Regulations on the system of assessment of learning outcomes of the Igor Sikorsky Kyiv Polytechnic Institute for all types of classroom and extracurricular work (incoming, current, calendar, final control): oral and written exams, testing, colloquium, etc. The level of knowledge in each discipline is assessed according to the criteria defined in the Grading System of this discipline.

6 - Програмні компетентності / Programme competencies		
Інтегральна компетентність / Integral competence		
Здатність розв'язувати складні задачі та проблеми у галузі математики та статистики або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.		Ability to solve complex tasks and problems in the field of mathematics and statistics or in the process of learning that involves conducting research and/or implementing innovations and is characterized by uncertainty of conditions and requirements.
Загальні компетентності (ЗК) / General competencies		
ЗК 01	Здатність до самонавчання, пошуку, оброблення та інтелектуального аналізу інформації з різних джерел, вміння виявляти, ставити та вирішувати проблеми.	Ability to self-study, search, process and mine data from various sources; to identify, pose and solve problems.
ЗК 02	Здатність генерувати нові ідеї та нестандартні підходи до їх реалізації, адаптуватись та діяти в нових ситуаціях, виявляти ініціативу, інноваційність та підприємливість.	Ability to generate new ideas and non-standard approaches to their implementation, to adapt and act in new situations, to show initiative, innovation and entrepreneurship.
ЗК 03	Навички та вміння міжособистісної комунікації, здатність представляти і доносити знання й ідеї та працювати в команді	Interpersonal communication skills, the ability to present and convey knowledge and ideas, to work in a team.
ЗК 04	Здатність вести професійну, у тому числі науково-дослідну, діяльність у міжнародному середовищі	Ability to conduct professional, including research, activities in the international environment
ЗК 05	Здатність готувати та здійснювати публічні виступи з презентацією отриманих результатів, готувати науково-технічні публікації (звіти, статті тощо) за результатами виконаних досліджень, в тому числі іноземною мовою	Ability to prepare and make public presentations of the results obtained, prepare scientific and technical publications (reports, articles, etc.) based on the results of research, including in a foreign language
ЗК 06	Здатність орієнтуватися у проблематиці сталого розвитку, системі загальнолюдських цінностей, розуміти значення гуманістичних цінностей для збереження й розвитку сучасної цивілізації.	Ability to navigate the issues of sustainable development, the system of universal human values, understand the importance of humanistic values for the preservation and development of modern civilization.
ЗК 07	Здатність діяти у відповідності до норм інтелектуальної власності	Ability to act in accordance with intellectual property rules
Фахові компетентності (ФК) / Professional competencies		
ФК 01	Здатність формалізувати та розв'язувати складні задачі й проблеми, які потребують оновлення й інтеграції знань, часто в умовах неповної, неточної чи недостатньої інформації та суперечливих вимог.	Ability to formalize and solve complex tasks and problems that require updating and integrating knowledge, often in the face of incomplete, inaccurate, or insufficient information and conflicting requirements
ФК 02	Здатність проводити наукові дослідження з розроблення нових та адаптацією існуючих математичних та комп'ютерних моделей для дослідження різноманітних процесів, явищ і систем, проводити відповідні чисельні експерименти з аналізом одержаних результатів.	Ability to conduct research on the development of new and adaptation of existing mathematical and computer models for the study of various processes, phenomena and systems, to conduct appropriate numerical experiments with the analysis of the results
ФК 03	Здатність формалізувати, будувати та використовувати у практичній діяльності моделі та методи інтелектуального аналізу даних.	Ability to formalize, build and use models and methods of data mining in practice

ФК 04	Здатність використовувати сучасні психолого-педагогічні теорії й методи у професійній діяльності, здійснювати педагогічну діяльність у вищій освіті.	Ability to use modern psychological and pedagogical theories and methods in professional activities, to carry out pedagogical activities in higher education.
ФК 05	Здатність провадити теоретичний та практичний аналіз сучасних криптографічних систем	Ability to conduct theoretical and practical analysis of modern cryptographic systems
ФК 06	Здатність розроблювати новітні механізми криптографічного захисту	Ability to develop the newest cryptographic protection mechanisms
ФК 07	Здатність проектувати, розроблювати та реалізовувати системи криптографічного захисту з урахуванням сучасних досягнень науки та існуючої правової та нормативної бази	Ability to design, develop and implement cryptographic protection systems taking into account modern scientific achievements and the existing legal and regulatory framework
ФК 08	Здатність використовувати та впроваджувати існуючі механізми, протоколи та системи криптографічного захисту інформації	Ability to use and implement existing mechanisms, protocols and systems for cryptographic protection of information

7 - Програмні результати навчання (ПРН) / Programme learning outcomes		
ПРН 01	Використовувати та адаптувати математичні теорії та моделі для забезпечення теоретичного підґрунтя розв'язання наукових та практичних задач	Use and adapt mathematical theories and models to provide a theoretical basis for solving scientific and practical problems
ПРН 02	Застосовувати існуючий математичний апарат, розробляти нові моделі, методи та алгоритми при вирішенні актуальних практичних задач широкого спектру	Apply the existing mathematical apparatus, develop new models, methods and algorithms while solving actual practical problems of a wide range
ПРН 03	Керуватись нормами інтелектуальної власності у професійній діяльності, проводити патентний пошук, оформлювати заявку на патент.	To be guided by intellectual property norms in professional activities, to conduct patent searches, and to file patent applications.
ПРН 04	Організовувати професійну діяльність згідно з принципами сталого розвитку суспільства, загальнолюдськими та гуманістичними цінностями для збереження та розвитку сучасної цивілізації.	To organize professional activities in accordance with the principles of sustainable development of society, universal and humanistic values for the preservation and development of modern civilization.
ПРН 05	Ситуативно й професійно спілкуватись та аналізувати науково-технічну інформацію однією з іноземних мов, організовувати багатосторонню (у тому числі міжкультурну) комунікацію та управляти нею.	Communicate and analyze scientific and technical information in a foreign language in a situational and professional manner, organize and manage multilateral (including intercultural) communication.
ПРН 06	Виявляти ініціативу та підприємливість, організовувати власну професійну діяльність, розробляти інноваційні підприємницькі проекти та створювати компанії для їх реалізації	Show initiative and entrepreneurship, organize own professional activities, develop innovative entrepreneurial projects and create companies for their implementation
ПРН 07	Здійснювати та аналізувати педагогічну діяльність, застосовувати сучасні методи науково-педагогічного дослідження та педагогічні технології	Implement and analyze pedagogical activities, apply modern methods of scientific and pedagogical research, apply pedagogical technologies
ПРН 08	Застосовувати методи здобуття знань із даних, методи оцінки та інтерпретації знайдених закономірностей	Apply methods of gaining knowledge from data, methods of evaluating and interpreting patterns found
ПРН 09	Здійснювати математичне і комп'ютерне моделювання складних систем та процесів, обчислювальні експерименти з використанням сучасних методів інтелектуального аналізу даних та комп'ютерних технологій	Carry out mathematical and computer modeling of complex systems and processes, computational experiments using modern methods of data mining and computer technologies
ПРН 10	Здійснювати пошук, систематизацію та аналіз науково-технічної інформації, вітчизняного та іноземного досвіду з питань професійної діяльності; логічно, послідовно й точно формулювати свої думки та подавати інформацію у професійному спілкуванні; розробляти наукові документи та презентації, доповідати та публікувати результати досліджень	Search, systematize and analyze scientific and technical information, domestic and foreign experience in professional activities; logically, consistently and accurately formulate their thoughts and present information in professional communication; develop scientific documents and presentations, report and publish research results
ПРН 11	Проводити аналіз криптографічних алгоритмів, протоколів та систем	Analyze cryptographic algorithms, protocols and systems
ПРН 12	Орієнтуватись у останніх досягненнях криптології	Navigate in the latest advances of the cryptology
ПРН 13	Розроблювати нові криптографічні алгоритми, механізми та системи захисту	Develop new cryptographic algorithms, mechanisms and security systems

ПРН 14	Керуватись законами, стандартами, технічними специфікаціями та нормативними документами у галузі	Be guided by industry laws, standards, specifications and regulations
ПРН 15	Розроблювати та аналізувати алгоритми у класичній та квантовій моделях обчислень	Develop and analyze algorithms in classical and quantum computing models
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 у чинній редакції		In accordance with the staffing requirements for ensuring the implementation of educational activities for the relevant level of higher education, approved by the Resolution of the Cabinet of Ministers of Ukraine of December 30, 2015, No. 1187 in the current version
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 у чинній редакції Використання обладнання для проведення лекцій у форматі презентацій, мережових технологій, зокрема на платформі дистанційного навчання Sikorsky, демонстраційного галузевого обладнання в ході виконання лабораторних практик та комп'ютерних практикумів		In accordance with the technological requirements for the material and technical support of educational activities of the relevant level of higher education, approved by the Resolution of the Cabinet of Ministers of Ukraine of December 30, 2015, No. 1187 in the current version Use of equipment for lectures in the format of presentations, network technologies, in particular on the Sikorsky distance learning platform, demonstration of industry equipment during laboratory works and computer practices
Інформаційне та навчально-методичне забезпечення / Information and methodological 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. Ресурси Науково-технічної бібліотеки КПІ ім. Ігоря Сікорського, бібліотеки Навчально-наукового фізико-технічного інституту		In accordance with the technological requirements for educational, methodological and information support of educational activities of the relevant level of higher education, approved by the Resolution of the Cabinet of Ministers of Ukraine of December 30, 2015, No. 1187 in the current version. Resources of the Scientific and Technical Library of Igor Sikorsky Kyiv Polytechnic Institute, the library of the Institute of Physics and Technology
9 - Академічна мобільність / Academic mobility		
Національна кредитна мобільність / National credit mobility		
Участь студентів у програмах академічної мобільності, можливість укладення угод про академічну мобільність		Participation of students in academic mobility programs, the possibility of concluding agreements on academic mobility
Міжнародна кредитна мобільність / International credit mobility		
Можливість укладення угод про міжнародну академічну мобільність, про тривалі міжнародні проекти		Possibility to conclude agreements on international academic mobility and long-term international projects
Навчання іноземних здобувачів вищої освіти / Study of foreign applicants of higher education		
Навчання іноземних здобувачів ВО, які опановують ОП за програмами міжнародної академічної мобільності, може проводитись англійською або українською мовою, за умови володіння здобувачем мовою навчання на рівні не нижче B2.		The training of foreign higher education applicants who are studying under international academic mobility programs may be conducted in English or Ukrainian, provided that the applicant has a language proficiency of at least B2.

10 - Процедура присвоєння професійних кваліфікацій / Procedure for awarding professional qualifications

Не передбачено присвоєння професійної кваліфікації

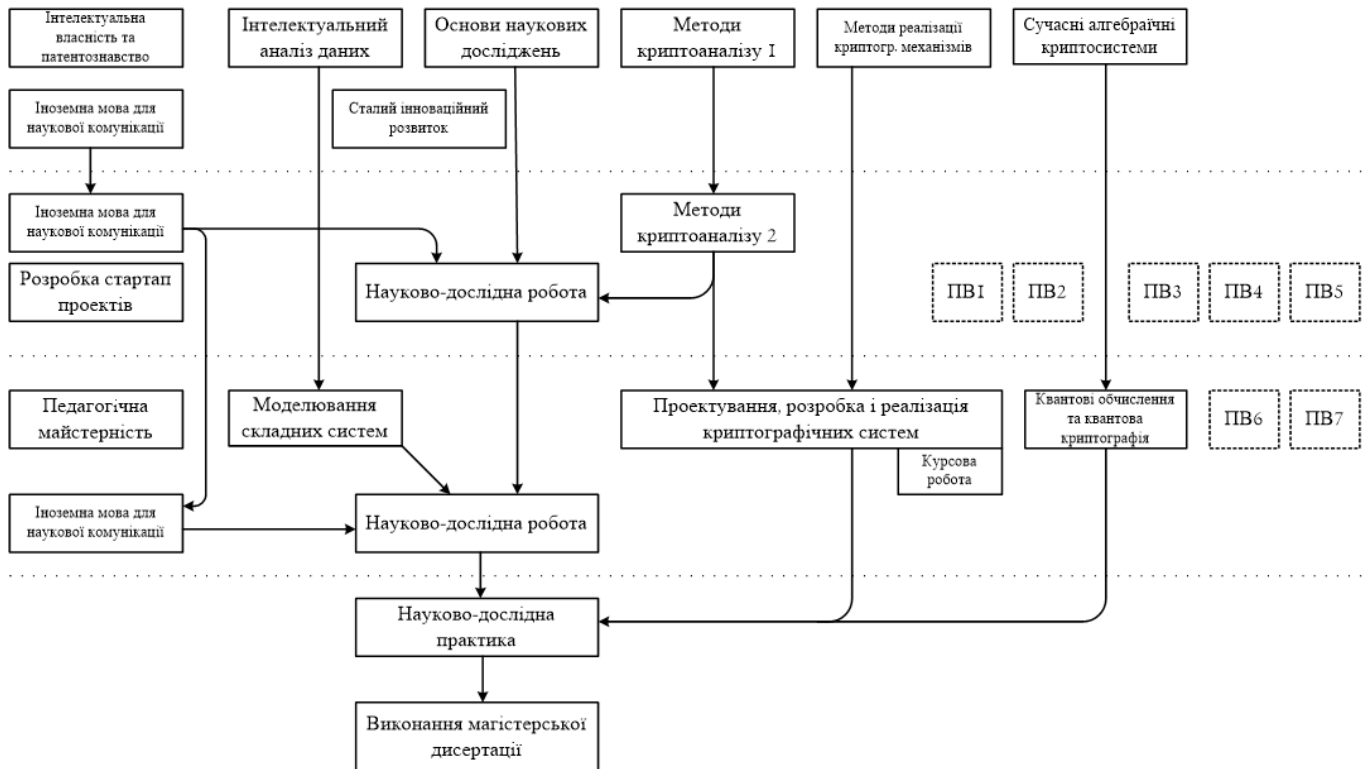
The awarding of a professional qualification is not provided

2. ПЕРЕЛІК КОМПОНЕНТІВ ОСВІТНЬОЇ ПРОГРАМИ / COMPONENTS of EDUCATIONAL PROGRAMME

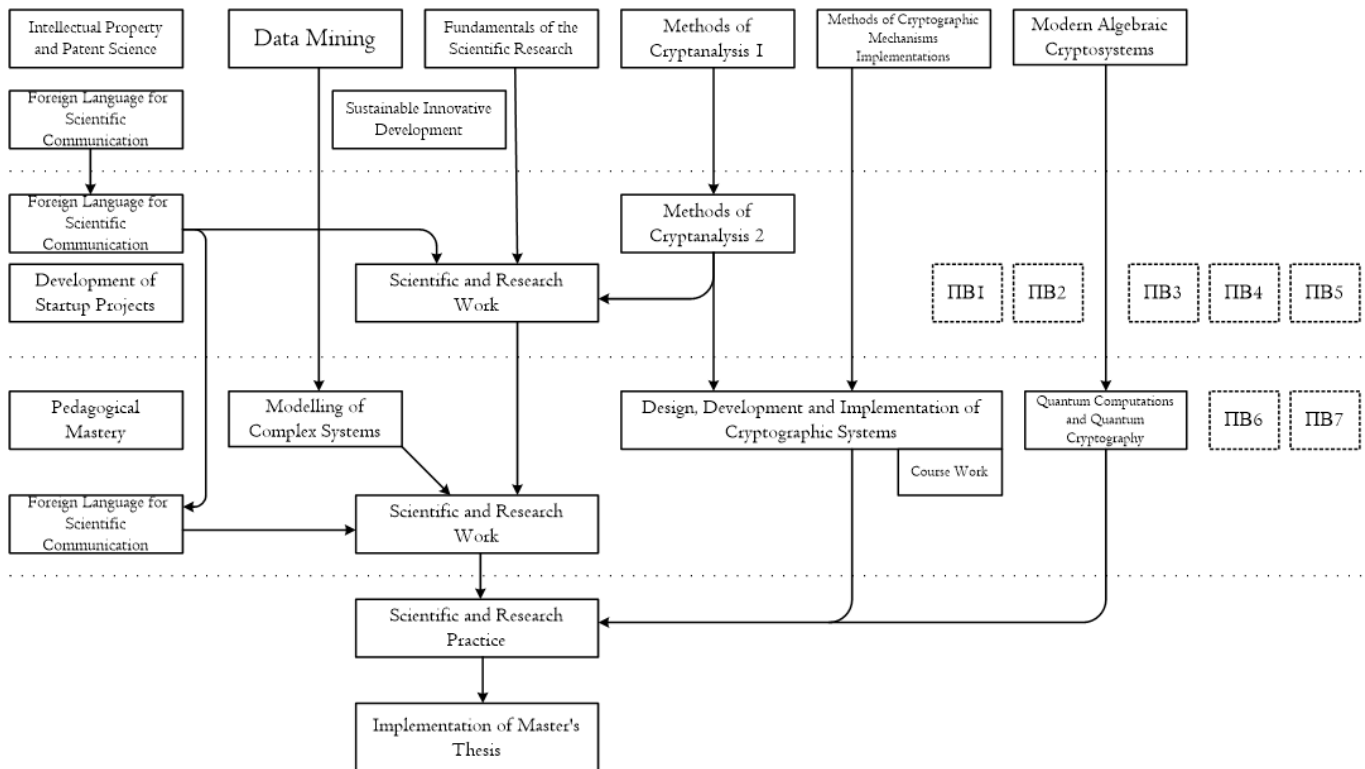
Код/Code	Освітні компоненти програми/Components	Кредитів ECTS/ECTS credits	Форма підсумкового контролю / Final control form
НОРМАТИВНІ освітні компоненти/Required (standard) components			
Обов'язкові компоненти циклу загальної підготовки/General training cycle			
ЗО 01	Інтелектуальна власність та патентознавство / 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 наукової комунікації / Practical Foreign Language Course for Scientific Communication		
ЗО 03.1	Практичний курс іноземної мови для наукової комунікації. Частина 1 / Practical Foreign Language Course for Scientific Communication. Part 1	3.0	Залік / Final test
ЗО 03.2	Практичний курс іноземної мови для наукової комунікації. Частина 2 / Practical Foreign Language Course for Scientific Communication. Part 2	2.0	Залік / Final test
ЗО 04	Розробка стартап проектів / Development of Startup Projects	3.0	Залік / Final test
ЗО 05	Педагогічна майстерність / Pedagogical Mastery	2.0	Залік / Final test
ЗО 06	Інтелектуальний аналіз даних / Data Mining	5.0	Екзамен / Exam
ЗО 07	Моделювання складних систем / Modelling of Complex Systems	5.0	Екзамен / Exam
Обов'язкові компоненти циклу професійної підготовки /Professional training cycle			
ПО 01	Методи криптоаналізу / Methods of Cryptanalysis		
ПО 01.1	Методи криптоаналізу. Частина 1 / Methods of Cryptanalysis. Part 1	5.0	Екзамен / Exam
ПО 01.2	Методи криптоаналізу. Частина 2 / Methods of Cryptanalysis. Part 2	4.0	Залік / Final test
ПО 02	Методи реалізації криптографічних механізмів / Methods of Cryptographic Mechanisms Implementations	5.0	Екзамен / Exam
ПО 04	Сучасні алгебраїчні криптосистеми / Modern Algebraic Cryptosystems	4.0	Залік / Final test
ПО 05	Квантові обчислення та квантова криптографія / Quantum Computations and Quantum Cryptography	4.0	Залік / Final test
ПО 06	Проектування, розробка і реалізація криптографічних систем / Design, Development and Implementation of Cryptographic Systems	5.0	Екзамен / Exam
ПО 07	Проектування, розробка і реалізація криптографічних систем. Курсова робота / Design, Development and Implementation of Cryptographic Systems. Course Work	1.0	Залік / Final test
Дослідницький (науковий) компонент/Research component			
ПО 08	Наукова робота за темою магістерської дисертації / Scientific Work on the Master's Thesis Topic		
ПО 08.1	Наукова робота за темою магістерської дисертації. Частина 1. Основи наукових досліджень / Scientific Work on the Topic of Master's Dissertation. Part 1. Fundamentals of Scientific Research	3.0	Залік / Final test
ПО 08.2	Наукова робота за темою магістерської дисертації. Частина 2. Науково-дослідна робота за темою магістерської дисертації / Scientific Work on the Topic of Master's Dissertation. Part 2. Research Work on the Topic of Master's Dissertation	4.0	Залік / Final test
ПО 09	Науково-дослідна практика / Research practice	14.0	Залік / Final test
ПО 10	Виконання магістерської дисертації / Completion of a Master's Thesis	16.0	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	4.0	Залік / Final test

Код/Code	Освітні компоненти програми/Components	Кредитів ЄКТС/ECTS credits	Форма підсумкового контролю / Final control form
ПВ 03	Освітній компонент 3 Ф-каталогу / Educational Component 3 from P-Catalogue	4.0	Залік / Final test
ПВ 04	Освітній компонент 4 Ф-каталогу / Educational Component 4 from P-Catalogue	5.0	Екзамен / Exam
ПВ 05	Освітній компонент 5 Ф-каталогу / Educational Component 5 from P-Catalogue	5.0	Екзамен / Exam
ПВ 06	Освітній компонент 6 Ф-каталогу / Educational Component 6 from P-Catalogue	4.0	Залік / Final test
ПВ 07	Освітній компонент 7 Ф-каталогу / Educational Component 7 from P-Catalogue	4.0	Залік / Final test
Загальний обсяг обов'язкових компонентів / Total volume of the required components:		90	
Загальний обсяг вибіркових компонентів / Total volume of the elective components:		30	
Обсяг освітніх компонентів, що забезпечують здобуття компетентностей визначених стандартом вищої освіти / Total volume of the educational components aimed at acquisition of competencies specified in the Higher Education Standard:		0	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ / TOTAL VOLUME OF THE EDUCATIONAL PROGRAMME		120	

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



Додаткову інформацію про структуру навчального плану та можливі індивідуальні освітні траєкторії можна знайти тут: <https://mmis.ipt.kpi.ua/education/educational-plans/>



Additional information about the structure of the curriculum and possible individual educational trajectories can be found here: <https://mmis.ipt.kpi.ua/education/educational-plans/>

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

Атестація здобувачів вищої освіти за освітньою програмою «Математичні методи криптографічного захисту інформації» проводиться у формі захисту магістерської дисертації та завершується видачею документа встановленого зразка про присудження йому ступеня магістра з присвоєнням кваліфікації «Магістр з прикладної математики».

Атестація здійснюється відкрито і публічно. Кваліфікаційні роботи (магістерські дисертації) перевіряються на ознаки порушення академічної доброчесності та після захисту публікуються в репозиторії Науково-технічної бібліотеки Університету для вільного доступу.

Students of the "Mathematical methods of cryptographic protection of information" educational program undergo certification in the form of defending their master's thesis, culminating in the issuance of a document of the established form conferring the master's degree with the qualification of "Master of Applied Mathematics".

The certification process is conducted openly and publicly. Qualification works (master's theses) are checked for signs of academic integrity violations and, after defense, are published in the repository of the university's Scientific and Technical Library for open access.

**5. 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	ЗО 06	ЗО 07	ПО 01	ПО 02	ПО 04	ПО 05	ПО 06	ПО 07	ПО 08	ПО 09	ПО 10
ЗК 01					X	X	X	X		X	X		X	X	X	X
ЗК 02				X					X			X	X			
ЗК 03				X												
ЗК 04			X													
ЗК 05			X											X	X	X
ЗК 06		X														
ЗК 07	X															
ФК 01						X	X	X		X	X			X	X	X
ФК 02							X		X				X			X
ФК 03						X										
ФК 04					X											
ФК 05								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			

6. 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	ЗО 06	ЗО 07	ПО 01	ПО 02	ПО 04	ПО 05	ПО 06	ПО 07	ПО 08	ПО 09	ПО 10
ПРН 01						X	X	X		X	X			X	X	X
ПРН 02						X	X	X	X	X	X	X		X	X	X
ПРН 03	X															
ПРН 04		X														
ПРН 05			X													
ПРН 06				X												
ПРН 07					X											
ПРН 08						X		X								
ПРН 09						X	X		X			X				
ПРН 10			X											X	X	X
ПРН 11								X	X	X	X	X	X			
ПРН 12								X	X	X	X	X	X			
ПРН 13									X			X	X		X	X
ПРН 14												X	X		X	X
ПРН 15								X			X					