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

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

ЗАТВЕРДЖЕНО / APPROVED
Вченою радою КПІ ім. Ігоря Сікорського /
by the Academic Council
of Igor Sikorsky Kyiv Polytechnic Institute
(протокол / minutes of meeting № 6
від / dated 08.06.2026 р.
Голова Вченої ради / Head of the Academic Council
_____ Михайло ІЛЬЧЕНКО / Mykhailo ILCHENKO

КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ КІБЕРБЕЗПЕКИ

APPLIED CRYPTOGRAPHY IN CYBERSECURITY SYSTEMS

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА / PROFESSIONAL EDUCATIONAL PROGRAMME

Перший (бакалаврський) рівень вищої освіти
Спеціальність: F5 Кібербезпека та захист інформації
Галузь знань: F Інформаційні технології
Освітня кваліфікація: Бакалавр з кібербезпеки та захисту інформації

The first (bachelor) level of higher education
Speciality : F5 Cyber security and data protection
Knowledge branch: F Information Technologies
Educational qualification: Bachelor of Cybersecurity and Information Protection

ID: **89316**

Введено в дію з / Enacted since
2026/2027 навчального року / academic year
наказом ректора / by rector's order
№ НОД/593/26 від / dated 09.07. 2026

Київ / Kyiv
2026

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 / DESIGNED

Керівник робочої групи

ЯКОВЛЄВ Сергій Володимирович, кандидат технічних наук, зав. кафедрою математичних методів захисту інформації, гарант освітньої програми

Члени робочої групи:

ФЕСЕНКО Андрій В'ячеславович, кандидат фізико-математичних наук, старший викладач кафедри математичних методів захисту інформації

ЗАВАДСЬКА Людмила Олексіївна, кандидат фізико-математичних наук, старший науковий співробітник, доцент кафедри математичних методів захисту інформації

СТЬОПОЧКІНА Ірина Валеріївна, кандидат технічних наук, доцент, доцент кафедри інформаційної безпеки

ЯКИМЧУК Олексій Петрович, аспірант 4 курсу

ПОГОДЖЕНО / AGREED:

Науково-методична комісія КПІ ім. Ігоря Сікорського зі спеціальності F5 Кібербезпека та захист інформації / Scientific and Methodological Commission of Igor Sikorsky Kyiv Polytechnic Institute in the specialty F5 Cybersecurity and Information Protection

(*протокол / minutes of meeting No. 4 від / dated June 3, 2026*)

Голова НМКУ – F5 / Head of the NMKU – F5

_____ Дмитро ЛАНДЕ/Dmytro LANDE

Методичною радою КПІ ім. Ігоря Сікорського / The Methodological Council of Igor Sikorsky Kyiv Polytechnic Institute *(протокол / minutes of meeting №* 8 *від / dated «*04*»* 06 *2026)*

Голова Методичної ради / Head of the Methodological Council

_____ Тетяна ЖЕЛЯСКОВА / Tetiana ZHELIASKOVA

ВРАХОВАНО / CONSIDERED:

- Стандарт вищої освіти для першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека та захист інформації
- Положення про освітні програми КПІ ім. Ігоря Сікорського https://osvita.kpi.ua/node/137.
- Наказ КПІ ім. Ігоря Сікорського №НОД/215/26 від 18.03.2026 «Про планування та організацію освітнього процесу 2026/2027 н.р.».
- фахову експертизу стейкхолдерів:
    - Кудін Антон Михайлович, головний експерт управління безпеки інформації Департаменту безпеки НБУ, д.т.н., проф., чл.-кор. НАНУ
    - Ковальчук Андрій Олегович, керівник напрямку відкритих інновацій Samsung R&D Institute Ukraine (SPUKR), відповідальний за співпрацю з університетами
    - Грубіян Євген Олександрович, провідний дослідник Distributed Labs
    - Агамалян Мирон Каренович, студент 3 курсу навчання першого (бакалаврського) рівня
    - Бондар Петро Олександрович, студент 2 курсу навчання другого (магістерського) рівня
    - Паршин Олександр Юрійович, аспірант 2 курсу навчання третього рівня (доктор філософії)

Освітню програму обговорено після надходження всіх побажань та пропозицій від стейкхолдерів та схвалено на розширеному засіданні кафедри математичних методів захисту інформації

    - Грубіян Євген Олександрович, провідний дослідник Distributed Labs
    - Агамалян Мирон Каренович, студент 3 курсу навчання першого (бакалаврського) рівня
    - Бондар Петро Олександрович, студент 2 курсу навчання другого (магістерського) рівня
    - Паршин Олександр Юрійович, аспірант 2 курсу навчання третього рівня (доктор філософії)

Освітню програму обговорено після надходження всіх побажань та пропозицій від стейкхолдерів та схвалено на розширеному засіданні кафедри математичних методів захисту інформації

- Higher education standard for the first (bachelor's) level of higher education in the specialty 125 Cybersecurity and information protection
- Regulations on educational programs of Igor Sikorsky Kyiv Polytechnic Institute https://osvita.kpi.ua/node/137.
- Order of Igor Sikorsky Kyiv Polytechnic Institute No. NOD/215/26 dated 03/18/2026 "On planning and organization of the educational process 2026/2027 academic year".
- Professional expertise of stakeholders:
    - Anton KUDIN, Chief Expert of the Information Security Department of the NBU Security Department, Doctor of Technical Sciences, Professor, Corresponding Member NASU
    - Andriy KOVALCHUK, Head of Open Innovations at Samsung R&D Institute Ukraine (SPUKR), Responsible for Cooperation with Universities
    - Yevhen HRUBIIAN, Lead Researcher at Distributed Labs
    - Myron AHAMALIAN, 3rd year student of the first (bachelor's) level
    - Petro BONDAR, 2nd year student of the second (master's) level
    - Olexandr PARSHYN, 2nd year graduate student of the third level (Doctor of Philosophy)

The educational program was discussed after receiving all the wishes and proposals from stakeholders and approved at an extended meeting of the Department of Mathematical Methods of Information Security

ЕВОЛЮЦІЯ ОСВІТНЬОЇ ПРОГРАМИ / EVOLUTION OF THE EDUCATIONAL PROGRAMME

Освітньо-професійна програма «Криптографічний захист інформації в системах кібербезпеки» впроваджується в дію з 2026-2027 навчального року з метою підготовки висококваліфікованих та конкурентоспроможних фахівців, інтегрованих у європейський та світовий науково-освітній простір. Освітня програма є нащадком освітніх програм «Прикладна криптологія» (2016-2018) та «Математичні методи криптографічного захисту інформації» (2019-2025), які відносились до спеціальності «Прикладна математика», і 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.

Запровадження освітньої програми здійснюється для задоволення потреб держави, суспільства, фізичних і юридичних осіб у висококваліфікованих фахівцях для виконання замовлення ринку праці, забезпечення професійної успішності випускників, зростання ролі Університету у наданні освітніх послуг на міжнародному та державному рівні. Згідно з Законом України “Про основні засади забезпечення кібербезпеки України” (№2163-VIII, зі змінами, внесеними Законом України №№ 4336-IX від 27.03.2025), криптографічний захист інформації є невід’ємною частиною кіберзахисту. Згідно з Методичними рекомендаціями щодо відповідності освітніх програм спеціальностям (Наказ МОН №1734 від 31.12.2025), освітні програми, основний зміст яких стосується криптографічного захисту інформації, відносяться до спеціальності F5 Кібербезпека та захист інформації. Однак фахівці з криптографічних методів захисту інформації, які здатні не тільки реалізовувати, але й створювати та аналізувати криптографічні механізми, повинні мати ґрунтовну обізнаність у моделях і методах аналізу та синтезу криптографічних алгоритмів, примітивів та протоколів. Відповідні навички відносяться до фундаментальних засад дискретної математики та комп’ютерних наук.

Освітня програма «Криптографічний захист інформації в системах кібербезпеки» робить сильний акцент на математичному апараті комп’ютерних наук, який корисний не тільки фахівцям з кібербезпеки, але й програмістам-розробникам, інженерам-дослідникам, аналітикам безпеки. У порівнянні з попередниками, у програмі закладається більша практична орієнтованість у галузі кібербезпеки, суттєво посилена складова з алгоритмики, а також додана складова з опанування технологій Web3, в першу чергу, блокчейнів та смарт-контрактів.

The educational and professional program, "Applied Cryptography in Cybersecurity Systems," launches in the 2026–2027 academic year. The program aims to train highly qualified and competitive specialists who will be integrated into the European and global scientific and educational communities. The educational program is a successor to the programs "Applied Cryptology" (2016–2018) and "Mathematical Methods of Cryptographic Security" (2019–2025). These programs were part of the "Applied Mathematics" major and continued the Department of Mathematical Methods of Information Security long-standing tradition of training specialists in applied mathematics, computer science, and cryptology. The program emphasizes in-depth theoretical training and the practical skills necessary for creating and analyzing cryptographic security and information protection systems.

The educational program is being implemented to meet the state's, society's, and individuals' and legal entities' need for highly qualified specialists. It is also intended to address the demands of the labor market, ensure the professional success of graduates, and enhance the university's role in providing educational services at the international and national levels. According to the Law of Ukraine “On the Basic Principles of Ensuring Cybersecurity in Ukraine” (No. 2163-VIII, as amended by Law of Ukraine No. 4336-IX of March 27, 2025), cryptographic security is an integral part of cybersecurity. According to the Methodological Recommendations on the Alignment of Educational Programs with Specializations (Order of the Ministry of Education and Science No. 1734 of December 31, 2025), educational programs whose primary content relates to cryptographic security fall under Specialty F5 Cybersecurity and Information Protection. However, specialists in cryptographic methods of information security must have a thorough understanding of the models and methods used to analyze and synthesize cryptographic algorithms, primitives, and protocols. These specialists must be capable not only of implementing, but also of designing and analyzing cryptographic mechanisms. These skills are based on the fundamental principles of discrete mathematics and computer science.

The "Applied Cryptography in Cybersecurity Systems" educational program emphasizes the mathematical foundations of computer science, which are useful for cybersecurity specialists, software developers, research engineers, and security analysts. Compared to its predecessors, the program emphasizes practical cybersecurity applications more, significantly strengthens the algorithms component, and adds a component focused on mastering Web3 technologies, particularly blockchains and smart contracts.

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 Scientific Institute for Physics and Technology
Ступінь вищої освіти та назва освітньої кваліфікації / Higher education degree and education qualification title	Ступінь бакалавра Бакалавр з кібербезпеки та захисту інформації	Bachelor Degree Bachelor of Cybersecurity and Information Protection
Офіційна назва освітньої програми / Educational programme official title	Криптографічний захист інформації в системах кібербезпеки	Applied Cryptography in Cybersecurity Systems
Тип диплому та обсяг освітньої програми / Diploma type and educational programme volume	Диплом бакалавра, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців	Bachelor diploma, 240 credits ECTS, training period 3 years 10 months
Інформація про акредитацію / Accreditation information of the educational programme	Не акредитовано	Not accredited
Цикл, рівень вищої освіти / Education cycle, level of higher education	НРК України – 6 рівень QF-EHEA – перший цикл EQF-LLL – 6 рівень	NQF of Ukraine - 6 level QF-EHEA – 1 cycle EQF-LLL – 6 level
Передумови / Prerequisites	Наявність повної загальної середньої освіти	Complete general secondary education
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/F5_OPPB_KZISKB	

2 – Мета освітньої програми / Educational programme purpose	
Мета освітньої програми полягає у підготовці фахівців у галузі інформаційних технологій, кібербезпеки та криптології, здатних розв’язувати складні спеціалізовані задачі та практичні проблеми криптографічного захисту інформації 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 educational program aims to train IT, cybersecurity, and cryptology specialists who can solve complex, specific tasks and practical problems related to cryptographic security in professional activities and educational processes. The program also aims to implement and ensure intercultural, professional interaction among representatives of the scientific and technical community to integrate university education into the European educational and scientific space. The program seeks to achieve this integration by internationalizing the educational process in the context of sustainable, innovative scientific and technological development of society. The program also aims to foster the adaptability of higher education graduates in the context of labor market transformation through interaction with employers and other stakeholders. The educational program's objectives align with the Igor Sikorsky Kyiv Polytechnic Institute’s 2025–2030 development strategy. This strategy aims to achieve sustainable social development, a high-tech transformation of the state, strengthened defense capabilities, and the development of high-quality human capital to recover and sustainably develop Ukraine.

3 – Характеристика освітньої програми / Educational programme characteristics	
Предметна область / Subject area	
Об’єкти вивчення та діяльності: технології кібербезпеки та захисту інформації, математичні методи, моделі, алгоритми та програмне забезпечення, що призначені для дослідження, аналізу, проектування процесів управління кібербезпекою та захистом інформації та інформаційних систем і ресурсів. *Цілі навчання:* підготовка фахівців, здатних • використовувати та впроваджувати технології кібербезпеки та захисту інформації, математичні методи та технології в галузі прикладної математики; • формулювати, розв’язувати й узагальнювати складні теоретичні та практичні задачі в галузі кібербезпеки та захисту інформації з використанням фундаментальних та спеціальних прикладних методів математичних та комп’ютерних наук; • будувати, досліджувати та застосовувати математичні моделі, що ґрунтуються на даних та на знаннях, створювати та експлуатувати програмне забезпечення для задач криптографічного захисту інформації. *Теоретичний зміст предметної області:* принципи, концепції, теорії та математичні методи захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору; алгоритми і програмні засоби їх реалізації; своєчасне виявлення, запобігання і нейтралізація загроз національній безпеці України у кіберпросторі. *Методи, методики та технології*: прикладні математичні методи, алгоритми, методики та технології вирішення теоретичних і прикладних задач кібербезпеки та захисту інформації, зокрема, за допомогою комп’ютерного моделювання та спеціалізованих програмних засобів *Інструменти та обладнання*: спеціалізовані програмні, апаратні та програмно-апаратні засоби, пристрої, комп’ютерні та соціальні мережі, інформаційні системи та комплекси для проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).	*Objects of study and professional activity:* cybersecurity and information protection technologies; mathematical methods, models, algorithms, and software intended for the research, analysis, and design of cybersecurity and information protection management processes, as well as information systems and resources. *Learning objectives:* to prepare specialists capable of • using and implementing cybersecurity and information protection technologies, as well as mathematical methods and technologies in the field of applied mathematics; • formulating, solving, and generalizing complex theoretical and practical problems in cybersecurity and information protection through the application of fundamental and specialized methods of mathematical and computer sciences; • developing, studying, and applying data-driven and knowledge-based mathematical models, and creating and operating software solutions for cryptographic security problems. *Theoretical content of the subject area:* principles, concepts, theories, and mathematical methods for protecting the vital interests of individuals, society, and the state in the use of cyberspace; algorithms and software tools for their implementation; and the timely detection, prevention, and neutralization of threats to the national security of Ukraine in cyberspace. *Methods, methodologies, and technologies:* applied mathematical methods, algorithms, methodologies, and technologies for solving theoretical and applied problems in cybersecurity and information protection, including through computer modeling and specialized software tools. *Tools and equipment:* specialized software, hardware, and integrated hardware-software solutions; devices; computer and social networks; information systems and complexes used for the design, modeling, control, monitoring, storage, processing, visualization, and protection of data (information flows).
Орієнтація освітньої програми / Scope	
Освітньо-професійна	Professional educational
Основний фокус освітньої програми / Main focus	

Базовий фокус ОП – математичні моделі, методи, алгоритми для задач комп'ютерних наук, кібербезпеки та криптографічного захисту інформації *Ключові слова:* кібербезпека, захист інформації, алгоритми, криптологія, криптографія, шифрування, цифровий підпис, геш-функція, блокчейн	The core focus of the educational program is on mathematical models, methods, and algorithms for solving problems in computer science, cybersecurity, and cryptographic security. Keywords: cybersecurity, information security, algorithms, cryptology, cryptography, encryption, digital signature, hash function, blockchain
Особливості освітньої програми / Features	
Багатопрофільна підготовка фахівців. Поглиблена фундаментальна підготовка з дискретної математики, прикладної алгебри, теорії алгоритмів та теорії імовірностей, орієнтована на розв'язування прикладних задач у галузях комп'ютерних наук, кібербезпеки, захисту інформації та криптології. Поєднання теоретичної підготовки та практичних навичок (зокрема, з програмування) у циклі професійної підготовки. Проходження переддипломної практики та виконання спільних проектів на замовлення державних, науково-дослідних установ та провідних IT-компаній України за фахом. Орієнтація на дуальну освіту.	Multidisciplinary specialist training. The program provides advanced fundamental education in discrete mathematics, applied algebra, algorithm theory, and probability theory, with a focus on solving applied problems in computer science, cybersecurity, information security, and cryptology. It combines rigorous theoretical training with practical skills development, including programming, within the professional component of the curriculum. Students complete a pre-graduation internship and participate in collaborative projects commissioned by government agencies, research institutions, and leading Ukrainian IT companies. The program is oriented toward the 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: • 3139 Фахівець із організації захисту інформації з обмеженим доступом; Фахівець із організації інформаційної безпеки • 3121 Фахівець з інформаційних технологій. • 2139.2 Аналітик систем захисту інформації та оцінки вразливостей • 2139.2 Аналітик загроз безпеки • 2132.2 Розробник систем захисту інформації Компетентності, одержані завдяки циклу професійної підготовки освітньої програми, дозволяють працювати на посадах, що відповідають класифіційним угрупованням • 2149 Професіонали із організації інформаційної безпеки • 2139.2 Професіонали в інших галузях обчислень (комп'ютеризація): Фахівець з криптографічного захисту інформації за наявності другого рівня вищої освіти відповідного спрямування (у галузі математики та статистики або інформаційних технологій). Випускники ОП можуть працювати спеціалістами з криптографічного захисту інформації та/або IT-технологій, розробниками програмних засобів, прикладними програмістами, аналітиками безпеки, аналітиками даних, адміністраторами програмних систем та баз даних.	In accordance with the National Classification of Occupations of Ukraine (DK 003:2010), graduates may be employed in positions corresponding to the following occupational groups: • 3139 Information Security Organization Specialist; Restricted-Access Information Protection Organization Specialist. • 3121 Information Technology Specialist. • 2139.2 Information Security and Vulnerability Assessment Analyst. • 2139.2 Security Threat Analyst. • 2132.2 Information Protection Systems Developer. The competencies acquired through the professional training component of the educational program also qualify graduates for positions corresponding to the following occupational groups: • 2149 Information Security Professionals. • 2139.2 Professionals in Other Computing Fields: Cryptographic Information Protection Specialist. *Subject to holding a second-cycle (master's) degree in a relevant field, particularly in mathematics and statistics or information technologies.* Graduates of the educational program may work as cryptographic information protection specialists and/or IT specialists, software developers, application programmers, security analysts, data analysts, software systems administrators, and database administrators.
Подальше навчання / Further study	
Продовження освіти за другим (освітньо-науковим, освітньо-професійним) рівнем вищої освіти; набуття додаткових кваліфікацій у системі післядипломної освіти.	Continuation of studies at the second (master's) level of higher education, under either educational-scientific or educational-professional programs; acquisition of additional qualifications through postgraduate education and professional development programs.

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 та лабораторні роботи (індивідуальні та у малих групах), курсові роботи; технології змішаного та перевернутого навчання за окремими освітніми компонентами; дослідницькі практики; виконання дипломної роботи (бакалаврської дипломної роботи)	The program is based on a student-centered learning approach. Teaching and learning activities include lectures, practical and seminar classes, computer-based practical sessions and laboratory work (both individual and small-group), and course projects. Selected educational components incorporate blended and flipped learning methodologies. The program also includes research-oriented training, internship-based learning experiences, and the preparation and defense of a Bachelor'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 екзамени, тестування, колоквіуми тощо. Рівень знань по кожній дисципліні оцінюється згідно критеріїв, визначених у Рейтинговій системі оцінювання даної дисципліни.	Student achievement is assessed in accordance with the Regulations on the Learning Outcomes Assessment System of Igor Sikorsky Kyiv Polytechnic Institute. Assessment covers all types of in-class and independent student work and includes diagnostic, ongoing, interim, and final evaluation. Various assessment methods are employed, including oral and written examinations, tests, colloquia, and other forms of evaluation. Student performance in each course is assessed according to the criteria specified in the course-specific Assessment Rating System.

6 – Програмні компетентності / Programme competencies		
Інтегральна компетентність / Integral competence		
Здатність розв’язувати спеціалізовані задачі і практичні проблеми у галузі кібербезпеки та криптографічного захисту інформації, що передбачає застосування математичних методів, розробку нових рішень та застосування існуючих		Ability to solve complex specialized tasks and practical problems in the field of cybersecurity and cryptographic security, which involves the application of mathematical methods, the development of new solutions, and the use of existing ones.
Загальні компетентності (ЗК) / General competencies		
ЗК 01	Здатність застосовувати знання у практичних ситуаціях	Ability to apply knowledge in practical situations
ЗК 02	Знання та розуміння предметної області та розуміння професії	Knowledge and understanding of the subject area and understanding of the profession
ЗК 03	Здатність спілкуватися державною мовою як усно, так і письмово	Ability to communicate in the state language both orally and in writing
ЗК 04	Здатність спілкуватися іноземною мовою	Ability to communicate in a foreign language
ЗК 05	Здатність вчитися і оволодівати сучасними знаннями	Ability to learn and master modern knowledge
ЗК 06	Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні	The ability to realize one's rights and responsibilities as a member of society, to be aware of the values of a civil (free democratic) society and the need for its sustainable development, the rule of law, the rights and freedoms of a person and a citizen in Ukraine
ЗК 07	Здатність ухвалювати рішення та діяти, дотримуючи принципу неприпустимості корупції та будь-яких проявів недоброчесності	The ability to make decisions and act in accordance with the principle of inadmissibility of corruption and any manifestations of dishonesty
ЗК 08	Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя	The ability to preserve and multiply moral, cultural, scientific values and achievements of society based on an understanding of the history and patterns of development of the subject area, its place in the general system of knowledge about nature and society and in the development of society, techniques and technologies, to use various types and forms of motor activity for active recreation and leading a healthy lifestyle
ЗК 09	Здатність до національного спротиву, формування громадянської стійкості та національно-патріотичної свідомості	Ability for national resistance, the formation of civic resilience and national-patriotic consciousness
ЗК 10	Здатність до абстрактного мислення, аналізу та синтезу; здатність генерувати нові ідеї, бути критичним і самокритичним.	Ability to think abstractly, analyze and synthesize, generate new ideas, and be critical and self-critical.
ЗК 11	Навички у використанні інформаційних і комунікаційних технологій.	Ability to use information and communication technologies effectively.
Фахові компетентності (ФК) / Professional competencies		
ФК 01	Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності	The ability to apply the legislative and regulatory framework, as well as state and international requirements, practices and standards in order to carry out professional activities
ФК 02	Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації	Ability to use information technologies, modern methods and models of cybersecurity and information protection systems

ФК 03	Здатність забезпечувати неперервність бізнесу згідно встановленої політики кібербезпеки та захисту інформації	Ability to ensure business continuity in accordance with established cybersecurity and information protection policies
ФК 04	Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої политики кібербезпеки й захисту інформації	Ability to ensure information protection in information and information and communication systems in accordance with established cybersecurity and information protection policies
ФК 05	Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження	The ability to restore the functioning of information and information and communication systems after the implementation of threats, cyberattacks, failures and failures of various classes and origins
ФК 06	Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекс нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо)	Ability to implement and ensure the functioning of complex information protection systems (a complex of regulatory, organizational and technical means and methods, procedures, practical techniques, etc.)
ФК 07	Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою	Ability to carry out professional activities based on an implemented information and cybersecurity management system
ФК 08	Здатність застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності	Ability to apply methods and means of cryptographic information protection at information activity facilities
ФК 09	Здатність застосовувати методи та засоби технічного захисту інформації на об’єктах інформаційної діяльності	Ability to apply methods and means of technical information protection at information activity facilities
ФК 10	Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки	Ability to monitor information processes, analyze, identify, and assess possible vulnerabilities and threats to the information space and information resources in accordance with the established information security policy
ФК 11	Здатність виконувати завдання, сформульовані у математичній формі, використовуючи та адаптуючи математичні теорії, моделі та методи	Ability to perform tasks formulated in mathematical terms by applying and adapting mathematical theories, models, and methods.
ФК 12	Здатність обирати та застосовувати математичні методи для розв’язання прикладних задач (зокрема, тих, які виникають при розробці, реалізації та аналізі криптографічних систем), проводити математичне і комп’ютерне моделювання, аналіз та обробку даних, обчислювальні експерименти, розв’язувати формалізовані задачі за допомогою спеціалізованих програмних засобів	Ability to select and apply mathematical methods to solve applied problems (including those arising in the development, implementation, and analysis of cryptographic systems), perform mathematical and computer modeling, data analysis and processing, conduct computational experiments, and solve formalized problems using specialized software tools.
ФК 13	Здатність до ефективної професійної письмової й усної комунікації українською мовою та однією з офіційних мов ЄС, складання наукових звітів із виконаних робіт та досліджень	Ability to communicate effectively in professional written and oral forms in Ukrainian and one of the official languages of the European Union, to prepare scientific reports on research and development activities.

7 – Програмні результати навчання (ПРН) / Programme learning outcomes		
ПРН 01	Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов’язків	Communicate freely in the state language orally and in writing when performing professional duties
ПРН 02	Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації	Communicate in a foreign language to ensure effective professional communication
ПРН 03	Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності	Apply the principle of inadmissibility of corruption and any other manifestations of dishonesty in professional activities
ПРН 04	Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв’язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність	Organize one's own professional activities, choose and use optimal methods and ways of solving complex specialized tasks and practical problems in professional activities, and evaluate their effectiveness.
ПРН 05	Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення	Analyze, argue, make decisions when solving complex specialized tasks and practical tasks in professional activities, which are characterized by complexity and incomplete certainty of conditions, be responsible for the decisions made
ПРН 06	Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат	Adapt to new conditions and technologies of professional activity, predict the final result
ПРН 07	Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, теорії чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчальній та професійній діяльності	Apply and adapt the theories of information and coding, mathematical statistics, number theory, cryptography and steganography, signal processing and transmission, etc., principles, methods, concepts of cybersecurity and information protection in educational and professional activities
ПРН 08	Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення	Apply knowledge and understanding of mathematics and physics in professional activities, formalize problems in the field of cybersecurity and information protection, formulate their mathematical formulation and choose a rational solution method
ПРН 09	Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації	Know and apply the legislation of Ukraine and international requirements, practices and standards in order to carry out professional activities in the field of cybersecurity and information protection
ПРН 10	Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності	Use modern information technologies, methods and models of cybersecurity and information protection systems to carry out professional activities
ПРН 11	Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації	Plan preparation and ensure continuity of business processes in organizations in accordance with the established cybersecurity policy, taking into account information protection requirements
ПРН 12	Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки	Apply methods and means of information protection in information and information and communication systems in accordance with the established information security policy

ПРН 13	Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому	Implement, configure, maintain and support the functioning of software and hardware-software complexes and cybersecurity and information protection systems as necessary procedures for the functioning of information and information and communication systems and/or the infrastructure of the organization as a whole
ПРН 14	Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації	Solve the tasks of managing the processes of restoring the normal functioning of information and information and communication systems using backup procedures in accordance with the established security policy and ensure the functioning of special software for information protection and recovery
ПРН 15	Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи	Collect, process, store, and analyze critical data to prove the implementation of cyber threats, conduct analysis and investigation of a cyber incident in order to promptly restore the functioning of the information system
ПРН 16	Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах	Solve the problems of implementing and maintaining complex information protection systems in information systems
ПРН 17	Забезпечувати функціонування систем управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків	Ensure the functioning of the organization's cybersecurity and information protection management systems, including personnel and management of the consequences of information security threats in crisis situations, based on the implementation of quantitative and qualitative risk assessment procedures
ПРН 18	Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності	Analyze and apply methods and means of cryptographic information protection at information activity facilities
ПРН 19	Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів	Solve problems related to the organization and control of the state of cryptographic information protection, in particular in accordance with the requirements of regulatory documents
ПРН 20	Визначати загрози створення технічних каналів витоку інформації на об’єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації	Identify threats of creating technical channels for information leakage at information activity facilities; implement means and measures for technical protection of information from leakage through technical channels, carry out maintenance and control of the condition of information protection hardware and technical information protection complexes

ПРН 21	Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах	Implement, support, and analyze the effectiveness of systems for detecting unauthorized access, actions with information in the information system, vulnerabilities, and possible threats to the information space and information resources, and use protection complexes to ensure the required level of information security in information systems
ПРН 22	Володіти знаннями та практичними навичками щодо організації дій у надзвичайних і кризових ситуаціях, демонструвати здатність до відповідальної поведінки й прийняття рішень в умовах загроз	Possess knowledge and practical skills in organizing actions in emergency and crisis situations, demonstrate the ability to behave responsibly and make decisions in conditions of threats.
ПРН 23	Володіти основними положеннями та методами математичного аналізу, лінійної та прикладної алгебри, теорії ймовірностей	Demonstrate knowledge of the fundamental concepts and methods of mathematical analysis, linear algebra, applied algebra, and probability theory.
ПРН 24	Володіти основними методами розробки дискретних математичних моделей об’єктів та процесів, аналітичного дослідження властивостей цих моделей	Apply fundamental methods for developing discrete mathematical models of objects and processes and analytically investigate their properties.
ПРН 25	Володіти основними принципами та методами побудови симетричних та асиметричних криптографічних систем у різних моделях обчислення, а також методами їх аналізу	Apply the fundamental principles and methods for constructing symmetric and asymmetric cryptographic systems in various computational models and use appropriate methods for their analysis.
ПРН 26	Знати та вміти використовувати блокчейн-технології та інструменти Web3	Use blockchain technologies and Web3 tools to solve practical tasks in the professional field.

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 delivery of educational activities at the relevant level of higher education, approved by the Resolution of the Cabinet of Ministers of Ukraine dated 30 December 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 у чинній редакції Використання обладнання для проведення лекцій у форматі презентацій, мережевих 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 at the relevant level of higher education, approved by the Resolution of the Cabinet of Ministers of Ukraine dated 30 December 2015 No. 1187, as amended. The use of equipment for delivering lectures in the form of presentations, network technologies (including the Sikorsky distance learning platform), and specialized demonstration equipment during laboratory classes and computer-based practical sessions.
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 and methodological and information support of educational activities at the relevant level of higher education, approved by the Resolution of the Cabinet of Ministers of Ukraine dated 30 December 2015 No. 1187, as amended. Resources of the Scientific and Technical Library of Igor Sikorsky Kyiv Polytechnic Institute and the library of 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 and the possibility of concluding academic mobility agreements.
Міжнародна кредитна мобільність / International credit mobility	
Можливість укладення угод про міжнародну академічну мобільність, про тривалі міжнародні проекти	The possibility of concluding international academic mobility agreements and agreements for 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 В2.	Education of foreign higher education students enrolled in the educational program within the framework of international academic mobility programs. Instruction may be delivered in English or Ukrainian, provided that the student has a language proficiency level 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 програм/Components	Кредитів ЄКТС/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	Українська мова за професійним спрямуванням / Ukrainian for Professional Purposes	2.0	Залік / Final test
ЗО 02	Історико-філософські засади суспільного розвитку / Historical and Philosophical Foundations of Social Development	3.0	Залік / Final test
ЗО 03	Основи здорового способу життя / Fundamentals of Healthy Lifestyle	2.0	Залік / Final test
ЗО 04	Англійська мова / English Language	5.0	Залік / Final test
ЗО 05	Англійська мова професійного спрямування / English for Professional Purposes	5.0	Залік / Final test
ЗО 06	Основи економіки / Fundamentals of Economics	2.0	Залік / Final test
ЗО 07	Основи національного спротиву / Fundamentals of National Resistance	5.0	Залік / Final test
ЗО 08	Вступ до кібернетичної безпеки / Introduction to cyber security	2.0	Залік / Final test
ЗО 09	Правові основи інформаційної безпеки / Legal Foundations of Information Security	2.0	Залік / Final test
ЗО 10	Математичний аналіз / Mathematical Analysis		
ЗО 10.1	Математичний аналіз. Частина 1 / Mathematical Analysis. Part 1	5.0	Екзамен / Exam
ЗО 10.2	Математичний аналіз. Частина 2 / Mathematical Analysis. Part 2	4.0	Залік / Final test
ЗО 11	Алгебра та геометрія / Algebra and Geometry	5.0	Екзамен / Exam
ЗО 12	Дискретна математика / Discrete Mathematics		
ЗО 12.1	Дискретна математика. Частина 1 / Discrete Mathematics. Part 1	3.0	Залік / Final test
ЗО 12.2	Дискретна математика. Частина 2 / Discrete Mathematics. Part 2	5.0	Екзамен / Exam
ЗО 13	Фізика / Physics		
ЗО 13.1	Фізика. Частина 1 / Physics. Part 1	3.0	Залік / Final test
ЗО 13.2	Фізика. Частина 2 / Physics. Part 2	5.0	Екзамен / Exam
ЗО 14	Програмування / Programming		
ЗО 14.1	Програмування. Частина 1 / Programming. Part 1	3.0	Залік / Final test
ЗО 14.2	Програмування. Частина 2 / Programming. Part 2	4.0	Залік / Final test
ЗО 15	Основи комп’ютерних мереж / Basics of computer networks	4.0	Залік / Final test
Обов’язкові компоненти циклу професійної підготовки /Professional training cycle			
ПО 01	Математична логіка та теорія алгоритмів / Mathematical Logic and Algorithm Theory	5.0	Екзамен / Exam
ПО 02	Теорія ймовірностей / Probability Theory	5.0	Екзамен / Exam
ПО 03	Математична статистика / Mathematical Statistics	5.0	Екзамен / Exam
ПО 04	Архітектура комп’ютерних систем / Architecture of computer systems	5.0	Екзамен / Exam
ПО 05	Бази даних та інформаційні системи / Databases and Information Systems	4.0	Залік / Final test
ПО 06	Операційні системи / Operating Systems	4.0	Залік / Final test

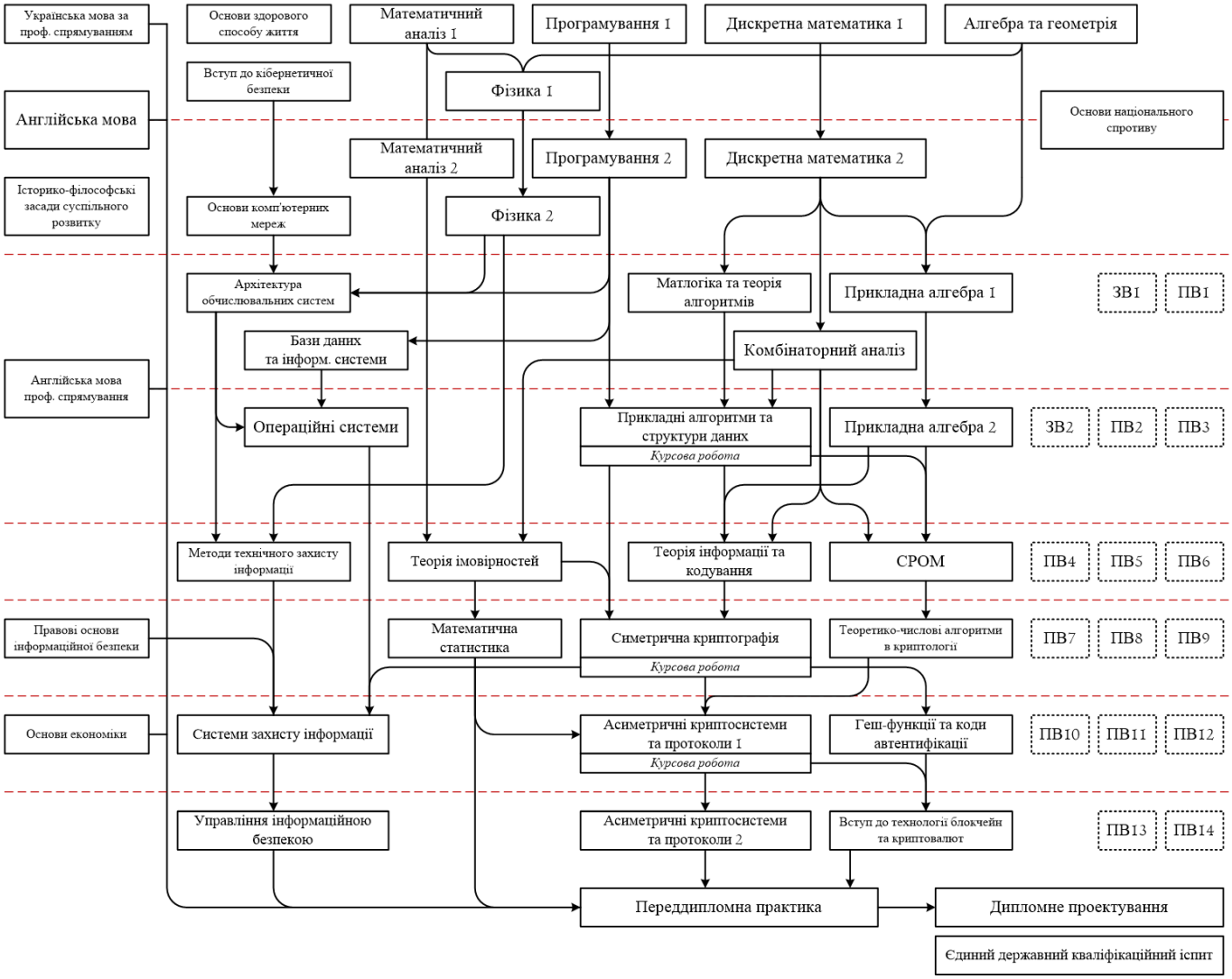
Код/Code	Освітні компоненти програм/Components	Кредитів ЄКТС/ECTS credits	Форма підсумкового контролю / Final control form
ПО 07	Методи та засоби технічного захисту інформації / Methods and means of technical information protection	4.0	Залік / Final test
ПО 08	Системи захисту інформації: проєктування, впровадження, супровід / Information Protection Systems: Design, Implementation, and Maintenance	4.0	Залік / Final test
ПО 09	Управління інформаційною безпекою / Information security management	4.0	Залік / Final test
ПО 10	Прикладна алгебра / Applied Algebra		
ПО 10.1	Прикладна алгебра. Частина 1 / Applied Algebra. Part 1	4.0	Залік / Final test
ПО 10.2	Прикладна алгебра. Частина 2 / Applied Algebra. Part 2	5.0	Екзамен / Exam
ПО 11	Комбінаторний аналіз / Combinatorial Analysis	5.0	Екзамен / Exam
ПО 12	Прикладні алгоритми та структури даних / Applied Algorithms and Data Structures	6.0	Екзамен / Exam
ПО 13	Прикладні алгоритми та структури даних. Курсова робота / Applied Algorithms and Data Structures. Course Work	1.0	Залік / Final test
ПО 14	Спеціальні розділи обчислювальної математики / Selected Topics in Computational Mathematics	5.0	Екзамен / Exam
ПО 15	Теорія інформації та кодування / Information and Coding Theory	4.0	Залік / Final test
ПО 16	Симетрична криптографія / Symmetric Cryptography	6.0	Екзамен / Exam
ПО 17	Симетрична криптографія. Курсова робота / Symmetric Cryptography. Course Work	1.0	Залік / Final test
ПО 18	Теоретико-числові алгоритми в криптології / Number Theory Algorithms in Cryptology	4.0	Залік / Final test
ПО 19	Асиметричні криптосистеми та протоколи / Asymmetric Cryptosystems and Protocols		
ПО 19.1	Асиметричні криптосистеми та протоколи. Частина 1 / Asymmetric Cryptosystems and Protocols. Part 1	5.0	Екзамен / Exam
ПО 19.2	Асиметричні криптосистеми та протоколи. Частина 2 / Asymmetric Cryptosystems and Protocols. Part 2	3.0	Залік / Final test
ПО 20	Асиметричні криптосистеми та протоколи. Курсова робота / Asymmetric Cryptosystems and Protocols. Course Work	1.0	Залік / Final test
ПО 21	Геш-функції та коди автентифікації / Hash Functions and Message Authentication Codes	5.0	Екзамен / Exam
ПО 22	Вступ до технології блокчейн та криптовалют / Introduction to Blockchain Technology and Cryptocurrencies	4.0	Залік / Final test
ПО 23	Переддипломна практика / Pre-diploma Practice	6.0	Залік / Final test
ПО 24	Дипломне проектування / Bachelor Thesis	6.0	Захист / Defence
ВИБІРКОВІ освітні компоненти/Elective components			
Вибіркові компоненти циклу загальної підготовки/General training cycle			
ЗВ 01	Освітній компонент 1 ЗУ-Каталогу / Educational Component 1 from GU-Catalogue	2.0	Залік / Final test
ЗВ 02	Освітній компонент 2 ЗУ-Каталогу / Educational Component 2 from GU-Catalogue	2.0	Залік / Final test
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
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	4.0	Залік / Final test
ПВ 05	Освітній компонент 5 Ф-каталогу / Educational Component 5 from P-Catalogue	4.0	Залік / Final test

Код/Code	Освітні компоненти програм/Components	Кредитів ЄКТС/ECTS credits	Форма підсумкового контролю / Final control form
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
ПВ 08	Освітній компонент 8 Ф-каталогу / Educational Component 8 from P-Catalogue	4.0	Залік / Final test
ПВ 09	Освітній компонент 9 Ф-каталогу / Educational Component 9 from P-Catalogue	4.0	Залік / Final test
ПВ 10	Освітній компонент 10 Ф-каталогу / Educational Component 10 from P-Catalogue	4.0	Залік / Final test
ПВ 11	Освітній компонент 11 Ф-каталогу / Educational Component 11 from P-Catalogue	4.0	Залік / Final test
ПВ 12	Освітній компонент 12 Ф-каталогу / Educational Component 12 from P-Catalogue	4.0	Залік / Final test
ПВ 13	Освітній компонент 13 Ф-каталогу / Educational Component 13 from P-Catalogue	4.0	Залік / Final test
ПВ 14	Освітній компонент 14 Ф-каталогу / Educational Component 14 from P-Catalogue	4.0	Залік / Final test
Загальний обсяг обов’язкових компонентів / Total volume of the required components:		180	
Загальний обсяг вибіркових компонентів / Total volume of the elective components:		60	
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:		136	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ / TOTAL VOLUME OF THE EDUCATIONAL PROGRAMME		240	

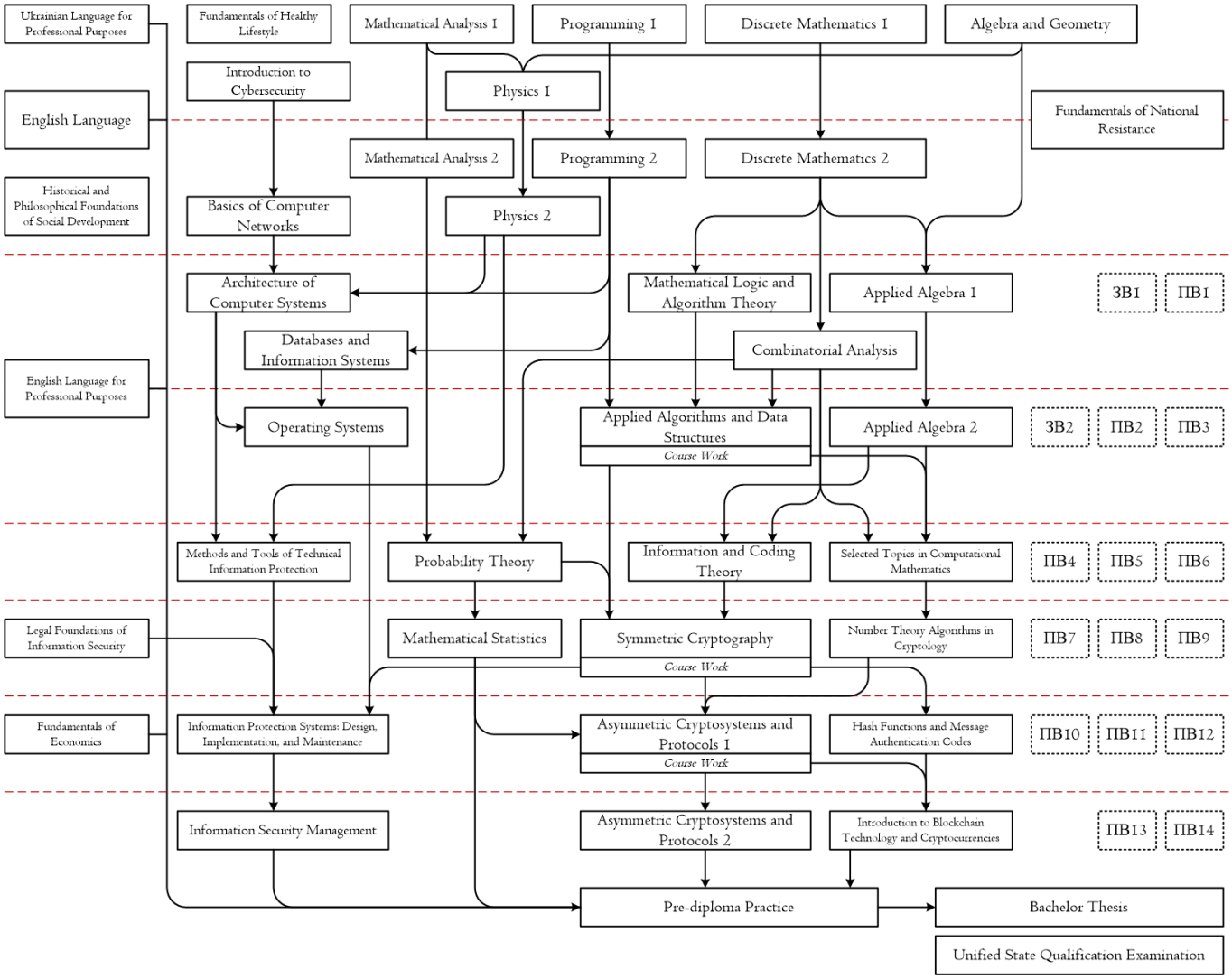
Примітки / Notes:

Для здобувачів освіти, які навчаються за заочною або дистанційною формами здобуття освіти, замість навчальної дисципліни «Основи національного спротиву» вивчається навчальна дисципліна «Цивільний захист, оборона та патріотичне виховання» обсягом 5 кредитів ЄКТС / Students enrolled in part-time or distance learning programmes take the course «Civil Protection, Defence and Patriotic Education» worth 5 ECTS credits instead of the course «Fundamentals of National Resistance»

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 «Криптографічний захист інформації в системах кібербезпеки» проводиться у формі складання Єдиного державного кваліфікаційного іспиту та захисту кваліфікаційної бакалаврської роботи. Атестація завершується видачею документа встановленого зразка про присудження здобувачу ступеня бакалавра з присвоєнням кваліфікації «Бакалавр з кібербезпеки та захисту інформації».

Атестація здійснюється відкрито і публічно. Кваліфікаційні бакалаврські роботи перевіряються на ознаки порушення академічної доброчесності та після захисту публікуються в репозиторії Науково-технічної бібліотеки Університету для вільного доступу (за виключенням робіт, які містять інформацію з обмеженим доступом).

Attestation of higher education students under the Educational Program “Applied Cryptography in Cybersecurity Systems” is carried out in the form of a Unified State Qualification Examination and the defense of a Bachelor's qualification thesis. The attestation is completed by the issuance of a standard diploma awarding the Bachelor’s degree with the qualification “Bachelor of Cybersecurity and Information Protection.”

The attestation process is conducted in an open and public manner. Bachelor's qualification theses are checked for compliance with academic integrity requirements and, after defense, are published in the repository of the Scientific and Technical Library of the University for open access (except for theses containing restricted information).

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	ЗО 08	ЗО 09	ЗО 10	ЗО 11	ЗО 12	ЗО 13	ЗО 14	ЗО 15	ПО 01	ПО 02	ПО 03	ПО 04	ПО 05	ПО 06	ПО 07	ПО 08	ПО 09	ПО 10	ПО 11	ПО 12	ПО 13	ПО 14	ПО 15	ПО 16	ПО 17	ПО 18	ПО 19	ПО 20	ПО 21	ПО 22	ПО 23	ПО 24
ЗК 01		X		X	X	X		X		X	X	X	X	X	X			X	X	X	X	X	X	X		X	X	X		X	X	X	X	X	X	X	X
ЗК 02				X	X			X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X		X	X		X	X	X	X
ЗК 03	X																																				X	X
ЗК 04				X	X																																X	X
ЗК 05	X			X	X					X	X	X	X	X	X	X	X	X	X	X	X	X			X	X	X		X	X	X	X	X	X	X	X	X	X
ЗК 06		X				X			X																													
ЗК 07	X								X																		X				X			X			X	
ЗК 08	X	X	X			X																																
ЗК 09							X																															
ЗК 10		X								X	X	X	X			X	X	X						X	X	X										X	X
ЗК 11														X	X				X	X	X					X		X	X	X	X	X	X	X	X	X	X
ФК 01	X			X	X				X														X	X			X				X			X			X	X
ФК 02								X	X			X		X	X				X	X	X	X	X	X		X	X		X	X	X		X	X		X	X	X
ФК 03						X		X	X					X	X						X		X	X													X	X
ФК 04								X	X					X							X	X	X	X					X	X	X	X	X	X	X			X	X
ФК 05								X							X				X	X	X																X	X
ФК 06														X					X	X	X	X	X				X										X	X
ФК 07								X						X		X	X	X			X		X	X			X		X	X	X	X	X	X	X	X	X	X
ФК 08																	X	X							X						X	X		X	X	X	X	X	X
ФК 09													X									X	X															X	X
ФК 10															X						X		X	X														X	X
ФК 11						X				X	X	X	X	X		X	X	X							X	X	X	X	X	X	X	X	X	X	X	X	X	X
ФК 12										X	X	X	X	X		X	X	X							X	X	X		X	X	X	X	X	X	X	X	X	X
ФК 13	X			X	X																						X				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	ЗО 08	ЗО 09	ЗО 10	ЗО 11	ЗО 12	ЗО 13	ЗО 14	ЗО 15	ПО 01	ПО 02	ПО 03	ПО 04	ПО 05	ПО 06	ПО 07	ПО 08	ПО 09	ПО 10	ПО 11	ПО 12	ПО 13	ПО 14	ПО 15	ПО 16	ПО 17	ПО 18	ПО 19	ПО 20	ПО 21	ПО 22	ПО 23	ПО 24
ПРН 01	X	X																																			X	X
ПРН 02				X	X																																X	X
ПРН 03	X																										X				X			X			X	X
ПРН 04		X	X			X		X																		X	X										X	X
ПРН 05		X								X	X	X		X		X	X	X							X		X	X	X	X	X	X	X	X	X	X	X	X
ПРН 06		X				X																															X	X
ПРН 07								X				X		X		X	X	X							X	X	X		X		X			X			X	X
ПРН 08										X	X	X	X			X	X	X				X			X	X	X		X	X	X		X	X			X	X
ПРН 09									X												X		X	X													X	X
ПРН 10								X	X			X		X	X	X				X	X	X	X	X			X		X	X	X		X	X			X	X
ПРН 11						X		X	X					X	X					X	X		X	X													X	X
ПРН 12								X	X					X	X					X	X	X	X	X													X	X
ПРН 13															X				X	X	X	X															X	X
ПРН 14															X				X	X	X		X														X	X
ПРН 15															X				X	X	X																X	X
ПРН 16																				X		X	X														X	X
ПРН 17																								X													X	X
ПРН 18																														X			X		X		X	X
ПРН 19																							X							X	X		X	X	X	X	X	X
ПРН 20																						X	X														X	X
ПРН 21																							X														X	X
ПРН 22							X																															
ПРН 23										X	X	X					X	X							X	X						X						
ПРН 24											X	X	X			X	X	X							X	X	X			X			X					
ПРН 25																															X	X		X	X			X	X
ПРН 26																																				X	X	X	X