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 № 5
від / dated 27.06.2025)

Голова Вченої ради / Head of the Academic Council

_____ Михайло Ільченко / Mykhailo ILCHENKO

БЕЗПЕКА ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ
SECURITY OF STATE INFORMATION RESOURCES

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА /
EDUCATIONAL PROFESSIONAL PROGRAMME

Другий (магістерський) рівень вищої освіти Спеціальність: F5 Кібербезпека та захист інформації Галузь знань: F Інформаційні технології Кваліфікація: магістр з кібербезпеки та захисту інформації	The second (master) level of higher education Speciality: F5 Cybersecurity and data protection Knowledge branch: F Information technologies Qualification: master's degree in cybersecurity and data protection

ID 81877

Введено в дію з / Enacted since
2025/2026 навчального року / academic year
наказом ректора / by rector's order
№ НОД/560/25 від / dated 27.06 2025

Київ / Kyiv
2025

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 / Head of the project team:

Самойлов Ігор Володимирович, кандидат технічних наук, доцент, доцент Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського / Ihor SAMOILOV, candidate of technical sciences, associate professor, associate professor of the Special department № 1 ISCIP of the Igor Sikorsky Kyiv Polytechnic Institute.

Члени робочої групи / Project team members:

Голь Владислав Дмитрович, кандидат технічних наук, професор, завідувач Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського / Vladyslav Hol, candidate of technical sciences, professor, head of the Special department № 1 ISCIP of the Igor Sikorsky Kyiv Polytechnic Institute.

Іванченко Сергій Олександрович, доктор технічних наук, професор, професор Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського / Sergiy Ivanchenko, doctor of technical sciences, professor, professor of the Special Department № 1 ISCIP of the Igor Sikorsky Kyiv Polytechnic Institute.

Олексійчук Антон Миколайович, доктор технічних наук, професор, професор Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського / Anton Oleksiichuk, doctor of technical sciences, professor, professor of the Special department № 1 ISCIP of the Igor Sikorsky Kyiv Polytechnic Institute.

Конотопець Микола Миколайович, кандидат технічних наук, доцент, доцент Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського / Mykola Konotopets, candidate of technical sciences, associate professor, associate professor of the Special department № 1 ISCIP of the Igor Sikorsky Kyiv Polytechnic Institute.

Сторчак Антон Сергійович, кандидат технічних наук, доцент, доцент Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського / Anton Storchak, candidate of technical sciences, associate professor, associate professor of the Special department № 1 ISCIP of the Igor Sikorsky Kyiv Polytechnic Institute.

Ніколаєнко Богдан Анатольович, кандидат технічних наук, доцент, головний спеціаліст управлінні ДКІ Адміністрації Держспецзв'язку / Bohdan Nikolayenko, candidate of technical sciences, associate professor, chief specialist DCI of the State Special Communications Service of Ukraine.

Бархаленко Кирило Миколайович, інженер другої категорії лабораторії Спеціальної кафедри № 1 / Kyrylo Barkhalenko, second category engineer of the laboratory of the Special Department № 1.

Ярощук Вадим Дмитрович, курсант магістерського курсу (спеціальність 125 Кібербезпека та захист інформації) ІСЗЗІ КПІ ім. Ігоря Сікорського / Vadym Yaroshchuk, master's student (specialty 125 Cybersecurity and Data Protection) Igor Sikorsky Kyiv Polytechnic Institute.

ПОГОДЖЕНО / AGREED:

Науково-методична комісія університету зі спеціальності F5 Кібербезпека та захист інформації / The Scientific and Methodological Commission of the University on speciality F5 Cybersecurity and data protection (протокол / minutes of meeting № 4 від / dated 05.05 2025)
Голова НМКУ-F5 (для ІСЗЗІ) / Head of the SMCU- F5 (for ISCIP)
_____ Владислав ГОЛЬ / Vladyslav HOL

Методична рада КПІ ім. Ігоря Сікорського / The Methodological Council of Igor Sikorsky Kyiv Polytechnic Institute (протокол / minutes of meeting № 7 від / dated 08.05 2025)
Голова Методичної ради / Head of the Methodological Council
_____ Тетяна ЖЕЛЯСКОВА / Tatiana ZHELIASKOVA

ВРАХОВАНО / CONSIDERED:

Постанову Кабінету Міністрів України від 30 серпня 2024 року № 1021 "Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти".

Наказ Міністерства Економіки України від 13.12.2024 № 27751 "Про затвердження Зміни до № 14 національного класифікатора ДК 003:2010".

Освітньо-професійну програму обговорено після надходження всіх пропозицій, побажань і зауважень від здобувачів вищої освіти, випускників та стейкхолдерів і схвалено на засіданні Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського (протокол № 9/1 від 05.05 2025 року).

The Resolution of the Cabinet of Ministers of Ukraine dated August 30, 2024 No. 1021 "On Amendments to the List of Fields of Knowledge and Specialties for Training of Higher and Professional Higher Education Applicants" was taken into account".

Order of the Ministry of Economy of Ukraine dated 13.12.2024 No. 27751 "On Approval of Amendments to No. 14 of the National Classifier DK 003:2010".

The educational and professional program was discussed after receiving all the proposals, wishes and comments from higher education students, graduates and stakeholders and approved at a meeting of the special department № 1 of the ISCIP of Igor Sikorsky Kyiv Polytechnic Institute (minutes № 9/1 of 05.05 2025).

ЕВОЛЮЦІЯ ОСВІТНЬОЇ ПРОГРАМИ / EVOLUTION OF THE EDUCATIONAL PROGRAMME:

Освітньо-професійна програма "Безпека державних інформаційних ресурсів" другого (магістерського) рівня вищої освіти за спеціальністю F5 Кібербезпека та захист інформації є правонаступницею ОПП "Безпека державних інформаційних ресурсів" другого (магістерського) рівня вищої освіти за спеціальністю 125 Кібербезпека, яка була започаткована у 2016 році з метою підготовки висококваліфікованих фахівців ступеня вищої освіти магістр для професійної діяльності на посадах органів та підрозділів Держспецзв'язку.

2019 рік – оновлення ОПП у зв'язку з переходом на новий термін навчання здобувачів вищої освіти (1 рік 4 місяця).

2021 рік – оновлення ОПП з метою врахування Стандарту вищої освіти за спеціальністю 125 Кібербезпека для другого (магістерського) рівня вищої освіти (Наказ МОН України № 332 від 18.03.2021). Приведено до стандарту назви компетентностей та програмних результатів навчання.

2023 рік – оновлення ОПП з метою врахування: Постанови Кабінету Міністрів України від 16.12.2022 № 1392 "Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти"; Наказів Міністерства Економіки України від 29.12.2022 № 5573 та від 25.10.2021 № 810-21"Про затвердження Зміни до національного класифікатора ДК 003:2010". Оновилась назва спеціальності 125 Кібербезпека та захист інформації, внесено зміни щодо придатності до працевлаштування випускників.

2024 рік – оновлення ОПП з метою врахування пропозиції від ДКІ Адміністрації Держспецзв'язку щодо впровадження змін в освітньо-професійну програму підготовки магістрів за спеціальністю 125 Кібербезпека та захист інформації (вх. №5352/ВС від 27.02.2024).

The Educational and Professional Program "Security of State Information Resources" of the second (master's) level of higher education in the specialty 125 Cybersecurity and Data Protection is the successor to the EPP "Security of State Information Resources" of the second (master's) level of higher education in the specialty 125 Cybersecurity, which was launched in 2016 to train highly qualified specialists of the master's degree for professional activities in the positions of bodies and units of the State Special Communications Service.

2019 - update of the EPP in connection with the transition to a new term of study for higher education students (1 year 4 months).

2021 - update of the EPP to take into account the Standard of Higher Education in the specialty 125 Cybersecurity for the second (master's) level of higher education (Order of the Ministry of Education and Science of Ukraine № 332 of 18.03.2021). The names of competencies and program learning outcomes were brought in line with the standard.

2023 - update of the EPP to take into account: Resolution of the Cabinet of Ministers of Ukraine № 1392 of 16.12.2022 "On Amendments to the List of Fields of Knowledge and Specialties for the Training of Higher Education Applicants"; Orders of the Ministry of Economy of Ukraine № 5573 of 29.12.2022 and № 810-21 of 25.10.2021 "On Approval of Amendments to the National Classifier SC 003: 2010". The name of the specialty 125 Cybersecurity and Information Protection was updated, and changes were made to the employability of graduates.

2024 - update of the EPP to take into account the proposal from the SCCI of the State Special Communications Service of Ukraine to introduce changes to the educational and professional program for masters in the specialty 125 Cybersecurity and Information Protection (inc. №5352 / BC of 27.02.2024).

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 інституту імені Ігоря Сікорського", Інститут спеціального зв'язку та захисту інформації	National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Institute of special communication and information protection
Ступінь вищої освіти та назва освітньої кваліфікації / Higher education degree and education qualification title	Ступінь – магістр, кваліфікація – магістр з кібербезпеки та захисту інформації	Degree - master, qualification - master's degree in cybersecurity and data protection
Професійна кваліфікація (за наявності) / Professional qualification	Не передбачено присвоєння професійної кваліфікації	No provision for the award of professional qualifications
Офіційна назва освітньої програми / Educational programme official title	Безпека державних інформаційних ресурсів	Security of state information resources
Тип диплому та обсяг освітньої програми / Diploma type and educational programme volume	Диплом магістра, 90 кредитів, термін навчання 1 рік 4 місяці	Master's degree, 90 credits, duration of study 1 year 4 months
Інформація про акредитацію / Accreditation information of the educational programme	Сертифікат про акредитацію № 15033, виданий Національним агентством із забезпечення якості вищої освіти 21.06.2025, дійсний до 01.07.2030	Accreditation certificate № 9817, issued by the National Agency for Higher Education Quality Assurance on 24.12.2024, valid until 01.07.2030
Цикл, рівень вищої освіти / Education cycle, level of higher education	НРК України – 7 рівень, QF-EHEA – другий цикл, EQF-LLL – 7 рівень	NQF of Ukraine - level 7, QF-EHEA - second cycle, EQF-LLL - level 7
Передумови / Prerequisites	ступеня бакалавра	Bachelor's degree is required
Форма здобуття освіти / Forms of education	Очна (денна)	Full-time (day)
Мова(и) викладання / Language(s) of instruction	Українська	Ukrainian
Інтернет-адреса розміщення освітньої програми / URL of the educational programme	https://osvita.kpi.ua/F5_OPPM_BDIR	

2 – Мета освітньої програми / Educational programme purpose	
Метою освітньо-професійної програми "Безпека державних інформаційних ресурсів" є підготовка висококваліфікованих фахівців, здатних вирішувати складні задачі і проблеми у галузі інформаційних технологій, кібербезпеки та здійснювати інноваційну професійну діяльність для проєктування, розробки, впровадження, супроводу та аудиту захищених інформаційних систем та засобів захисту.	The purpose of the educational and professional program "Security of State Information Resources" is to train highly qualified specialists who are able to solve complex problems and challenges in the field of information technology, cybersecurity and carry out innovative professional activities for the design, development, implementation, maintenance and audit of secure information systems and security tools. The purpose of the educational and professional

Мета освітньо-професійної програми відповідає стратегії розвитку КПІ ім. Ігоря Сікорського на 2020-2025 роки щодо формування суспільства майбутнього на засадах концепції сталого розвитку та фундаменталізації підготовки фахівців.	program corresponds to the development strategy of Igor Sikorsky Kyiv Polytechnic Institute for 2020-2025 to form the society of the future based on the concept of sustainable development and fundamentalization of training.
3 – Характеристика освітньої програми / Educational programme characteristics	
Предметна область / Subject area	
Об'єкти вивчення: - сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; - інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; - інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; - системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); - програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; - системи управління інформаційною безпекою та/або кібербезпекою; - технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки.	**Objects of study:** - modern processes of research, analysis, creation and maintenance of information systems and technologies, other business operational processes at information activity facilities and critical infrastructures in the field of information security and/or cybersecurity; - information systems (information and communication, information and telecommunication, automated) and technologies; - infrastructure of information activity objects and critical infrastructures; - systems and complexes for the creation, processing, transmission, storage, destruction, protection and display of data (information flows); - information resources of various classes (including state information resources); - software and hardware (means) of cyber defense; - information security and/or cybersecurity management systems; - technologies, methods, models and tools of information security and/or cybersecurity.
Цілі навчання Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки.	**Learning objectives** Training of specialists capable of solving research and/or innovation problems in the field of information and/or cybersecurity.
Теоретичний зміст предметної області Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки.	**Theoretical content of the subject area** Theoretical foundations of science-intensive technologies, physical and mathematical fundamental knowledge, theories of identification and decision-making, system analysis, complex systems, modeling and process optimization, theory of mathematical statistics, cryptographic and technical information security, risk theory and other interdisciplinary theories and practices in the field of information security and/or cybersecurity.
Методи, методики та технології Методи, моделі, методики та технології створення, обробки, передачі, приймання,	**Methods, techniques and technologies** Methods, models, techniques and technologies for creating, processing, transmitting, receiving,

знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. **Інструменти та обладнання** Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.	destroying, displaying, protecting (cybersecurity) information resources in cyberspace, as well as methods and models for developing and using application and specialized software to solve professional problems in the field of information security and/or cybersecurity. Technologies, methods and models of research, analysis, management and support of business/operational processes using a set of regulatory, legal, organizational and technical methods and means of protecting information resources in cyberspace. **Tools and equipment** Tools, devices, network equipment and environment, application and specialized software, automated systems and complexes for designing, modeling, operating, controlling, monitoring, processing, displaying and protecting data (information flows), as well as methods and models of risk theory and information resource management in the study and support of information activities in the field of information security and/or cybersecurity.
Орієнтація освітньої програми / Scope	
Освітньо-професійна	Educational professional
Основний фокус освітньої програми / Main focus	
Базовий фокус освітньої програми – системи та процеси кіберпростору, сучасні методи та засоби захисту інформації. *Ключові слова:* кібербезпека, математичні методи кібербезпеки, системи і технології кібербезпеки, захист об'єктів критичної інфраструктури, розвиток засобів захисту інформації.	*The basic focus of the educational program* is on cyberspace systems and processes, modern methods and means of information protection. *Key words*: cybersecurity, mathematical methods of cybersecurity, cybersecurity systems and technologies, protection of critical infrastructure, development of information security tools.
Особливості освітньої програми / Features	
Підготовка фахівців здійснюється у статусі курсанта. Залучення до викладання навчальних дисциплін фахівців з підрозділів Держспецзв'язку інших навчальних закладів, наукових установ. Практики проводяться відповідно до "Інструкції про порядок організації проведення практичної та військово-професійної підготовки здобувачів вищої освіти в закладі освіти Державної служби спеціального зв'язку та захисту інформації України", затвердженої наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 19 серпня 2021 року № 507 та складаються з: кібернавчань, які проводяться в другому та	Specialists are trained in the status of cadets. Involvement of specialists from the units of the State service for special communications and information services of Ukraine and other educational institutions and scientific institutions in teaching disciplines. Practices are carried out in accordance with the "Instruction on the procedure for organizing practical and military-professional training of higher education students in an educational institution of the State service for special communications and Information protection of Ukraine", approved by the order of the Administration of the State service for special communications and Information protection of

третьому семестрах, на платформі Навчального ситуаційного центру кібербезпеки ІСЗЗІ КПІ ім. Ігоря Сікорського та платформі Тренінгового центру Кіберцентру UA30; експлуатаційної практики, яка проводиться в другому семестрі, на базі Лабораторії технічного захисту інформації ІСЗЗІ КПІ ім. Ігоря Сікорського; військового стажування в третьому семестрі яке проводиться в підрозділах Держспецзв'язку.	Ukraine of August 19, 2021, N 507, and consist of: cyber exercises, which are held in the second and third semesters, on the platform of the Training situational center for cybersecurity of the ISCIP of Igor Sikorsky Kyiv Polytechnic Institute and the platform of the Training Center of the UA30 Cyber Center; operational practice, which is conducted in the second semester, on the basis of the Laboratory of technical information protection ISCIP of Igor Sikorsky Kyiv Polytechnic Institute; military internship in the third semester, which is conducted in the units of the State special communications service.
4 – Придатність випускників до працевлаштування та подальшого навчання / Eligibility of graduates for employment and further study	
Придатність до працевлаштування / Eligibility for employment	
Відповідно до Державного класифікатору професій ДК 003:2010 випускники можуть працювати на посадах, що відповідають класифікаційним угрупованням: 2132.2 Розробник систем захисту інформації 2139.2 Аналітик систем захисту інформації 2139.2 Аналітик з оцінки вразливостей 2139.2 Аналітик загроз безпеки 2490 Аналітик з оцінки ризиків, загроз та стану захищеності об'єктів критичної інфраструктури (за видами діяльності) 23 Професіонал в галузі освіти та навчання Замовником фахівців зі спеціальності F5 Кібербезпека та захист інформації виступає Державна служба спеціального зв'язку та захисту інформації України.	According to the State Classification of Professions DK 003:2010, graduates can work in positions corresponding to the classification groups: 2132.2 Developer of information security systems 2139.2 Analyst of information security system 2139.2 Analyst of vulnerability assessment 2139.2 Analyst of security threat 2490 Analyst for assessing risks, threats and security of critical infrastructure facilities (by type of activity) 23 Professional in the field of education and training The customer for specialists in the specialty F5 Cybersecurity and data protection is the State service for special communications and information protection of Ukraine.
Подальше навчання / Further study	
Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі освіти дорослих.	Continuing education at the third (educational and scientific) level of higher education. Acquisition of additional qualifications in the adult education system.
5 – Викладання та оцінювання / Teaching and assessment	
Викладання та навчання / Teaching and studying	
Програмою передбачено проблемно-орієнтоване навчання з набуттям компетентностей, необхідних для продукування нових ідей, розв'язання комплексних проблем у професійній галузі, яке включає лекції, практичні та семінарські заняття, технологія змішаного навчання, підготовка та захист магістерської дисертації.	The program provides for problem-based learning with the acquisition of competencies necessary to generate new ideas, solve complex problems in the professional field, which includes lectures, practical and seminar classes, blended learning technology, preparation and defense of a master's thesis.
Оцінювання / Assessment	
Всі види навчальної діяльності та контрольні заходи (усні та письмові заліки, екзамени, тестування) оцінюються відповідно до Положення про систему оцінювання результатів навчання в КПІ ім. Ігоря Сікорського за	All types of educational activities and control measures (oral and written tests, exams, testing) are evaluated in accordance with the Regulations on the system of evaluation of learning outcomes in Igor Sikorsky Kyiv Polytechnic Institute on a stobal

стобальною шкалою з подальшим переведенням в оцінки університетської шкали. Навчання завершується написанням і публічним захистом магістерської дисертації.	scale with further conversion to university scale grades. The training ends with the writing and public defense of a master's thesis.
6 – Програмні компетентності / Programme competencies	
Інтегральна компетентність / Integral competence	
Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.	The ability of a person to solve research and/or innovation problems in the field of information security and/or cybersecurity.
Загальні компетентності (ЗК) / General competencies	
ЗК 1 Здатність застосовувати знання у практичних ситуаціях.	Ability to apply knowledge in practical situations.
ЗК 2 Здатність проводити дослідження на відповідному рівні.	Ability to conduct research at the appropriate level.
ЗК 3 Здатність до абстрактного мислення, аналізу та синтезу.	Ability to think abstractly, analyze and synthesize.
ЗК 4 Здатність оцінювати та забезпечувати якість виконуваних робіт.	Ability to evaluate and ensure the quality of work performed.
ЗК 5 Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).	Ability to communicate with representatives of other professional groups of different levels (with experts from other fields of knowledge / types of economic activity).
Фахові компетентності (ФК) / Professional competencies	
ФК 1 Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.	Ability to reasonably apply, integrate, develop and improve modern information technologies, physical and mathematical models, as well as technologies for creating and using application and specialized software to solve professional problems in the field of information security and/or cybersecurity.
ФК 2 Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.	Ability to develop, implement and analyze regulations, provisions, instructions and requirements of technical and organizational direction, as well as integrate, analyze and use the best world practices, standards in professional activities in the field of information security and/or cybersecurity.
ФК 3 Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	Ability to research, develop and maintain methods and means of information security and/or cybersecurity at information and critical infrastructure facilities.
ФК 4 Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.	Ability to analyze, develop and maintain an organization's information security and/or cybersecurity management system, formulate information security strategy and policies, taking into account national and international standards and requirements.
ФК 5 Здатність до дослідження, системного аналізу та забезпечення безперервності	Ability to research, system analysis and ensure the continuity of business/operational processes in

бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	order to identify vulnerabilities of information systems and resources, analyze risks and determine the assessment of their impact in accordance with the established strategy and policy of information security and/or cybersecurity of the organization.
ФК 6 Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	Ability to analyze, control and provide a system of access control to information resources in accordance with the established strategy and policy of information security and/or cybersecurity of the organization.
ФК 7 Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.	Ability to research, develop and implement methods and measures to counteract cyber incidents, carry out management, control and investigation procedures, as well as provide recommendations for the prevention and analysis of cyber incidents in general.
ФК 8 Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	Ability to research, develop, implement and maintain methods and means of cryptographic and technical protection of information at information activities and critical infrastructure, in information systems, as well as the ability to evaluate the effectiveness of their use, in accordance with the established strategy and policy of information security and/or cybersecurity of the organization.
ФК 9 Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.	Ability to analyze, develop and maintain a system of audit and monitoring of the effectiveness of information systems and technologies, business / operational processes in the field of information security and/or cybersecurity of the organization as a whole.
ФК 10 Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.	Ability to conduct research and teaching activities, plan training, monitor and support work with staff, and make effective decisions on information security and/or cybersecurity issues.
ФК 11 Здатність реалізовувати технічні вимоги на основі технік оцінки рівня захищеності інформаційних систем, технологій аналізу мережевого трафіку та принципів протидії кібератакам.	Ability to implement technical requirements based on techniques for assessing the level of security of information systems, technologies for analyzing network traffic and principles of countering cyber attacks.
ФК 12 Здатність проводити дослідження, перевірку, аналіз, оцінювання об'єктів інформаційної діяльності щодо їх відповідності вимогам нормативних документів із технічного захисту інформації.	Ability to conduct research, verification, analysis, evaluation of information objects for their compliance with the requirements of regulatory documents on technical protection of information.
ФК 13 Здатність аналізувати, інтегрувати і використовувати кращі світові практики, міжнародні стандарти при розробці криптографічних систем захисту інформації в спеціальних інформаційно-комунікаційних системах.	Ability to analyze, integrate and use the best world practices, international standards in the development of cryptographic information security systems in special information and communication systems.
ФК 14 Здатність застосовувати комплекс	Ability to apply the complex of physical training of

фізичної підготовки військовослужбовців для розвитку загальних і спеціальних фізичних якостей, формування військово-прикладних навичок та виховання вольових і психічних якостей.	servicemen for the development of general and special physical qualities, the formation of military-applied skills and the education of volitional and mental qualities.
ФК 15 Здатність аналізувати, контролювати та забезпечувати формування та реалізацію державної політики у сфері захисту критичної інфраструктури.	Ability to analyze, control and ensure the formation and implementation of state policy in the field of critical infrastructure protection.
7 – Програмні результати навчання (ПРН) / Programme learning outcomes	
ПРН 1 Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	Communicate fluently in the state and foreign languages, orally and in writing, to present and discuss research and innovation results, business/operational processes and professional issues in the field of information security and/or cybersecurity.
ПРН 2 Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.	Integrate fundamental and specialized knowledge to solve complex information security and/or cybersecurity problems in broad or multidisciplinary contexts.
ПРН 3 Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	Conduct research and/or innovation activities in the field of information security and/or cybersecurity, as well as in the field of technical and cryptographic protection of information in cyberspace.
ПРН 4 Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.	Apply, integrate, develop, implement and improve modern information technologies, physical and mathematical methods and models in the field of information security and/or cybersecurity.
ПРН 5 Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.	To critically comprehend the problems of information security and/or cybersecurity, including at the interdisciplinary and interdisciplinary level, in particular, based on an understanding of the new results of engineering and physical and mathematical sciences, as well as the development of technologies for creating and using specialized software.
ПРН 6 Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	Analyze and evaluate the security of systems, complexes and means of cyber defense, technologies for creating and using specialized software.
ПРН 7 Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	To justify the use, implement and analyze the best international standards and practices in order to solve complex problems of professional activity in the field of information security and/or cybersecurity.
ПРН 8 Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	Research, develop and maintain information security and/or cybersecurity systems and tools at information and critical infrastructure facilities.

ПРН 9 Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	Analyze, develop and maintain the organization's information security and/or cybersecurity management system based on the information security strategy and policy.
ПРН 10 Забезпечувати безперервність бізнес / операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	Ensure the continuity of business/operational processes, as well as identify vulnerabilities of information systems and resources, analyze and assess risks to information security and/or cybersecurity of the organization.
ПРН 11 Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	Analyze, control and ensure the effective functioning of the system of access control to information resources in accordance with the established strategy and policy of information security and/or cybersecurity of the organization.
ПРН 12 Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.	Research, develop and implement methods and measures to counteract cyber incidents, carry out management, control and investigation procedures, as well as provide recommendations for the prevention and analysis of cyber incidents in general.
ПРН 13 Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.	To research, develop, implement and use methods and means of cryptographic and technical protection of information of business/operational processes, as well as to analyze and evaluate the effectiveness of their use in information systems, at information activity facilities and critical infrastructure.
ПРН 14 Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\абокібербезпеки в цілому.	Analyze, develop and maintain a system for auditing and monitoring the effectiveness of information systems and technologies, business/operational processes in the field of information and/or cybersecurity in general.
ПРН 15 Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.	Clearly and unambiguously communicate own conclusions on information security and/or cybersecurity issues, as well as knowledge and explanations that justify them to staff, partners and others.
ПРН 16 Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.	To make informed decisions on organizational and technical issues of information security and/or cybersecurity in complex and unpredictable conditions, including the use of modern methods and tools for optimization, forecasting and decision-making.
ПРН 17 Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.	Have the skills of autonomous and independent learning in the field of information security and/or cybersecurity and related fields of knowledge, analyze their own educational needs and objectively evaluate learning outcomes.
ПРН 18 Планувати навчання, а також	Plan training, as well as support and monitor work

супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.	with staff in the field of information security and/or cybersecurity.
ПРН 19 Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.	Select, analyze and develop suitable standard analytical, computational and experimental methods of cybersecurity, develop, implement and support projects for the protection of information in cyberspace, innovation and intellectual property protection.
ПРН 20 Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.	To set and solve complex engineering, applied and scientific problems of information security and/or cybersecurity, taking into account the requirements of national and international standards and best practices.
ПРН 21 Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.	Use methods of natural, physical and computer modeling to study processes related to information security and/or cybersecurity.
ПРН 22 Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.	Plan and perform experimental and theoretical research, formulate and test hypotheses, select appropriate methods and tools, perform statistical data processing, assess the reliability of research results, and justify conclusions.
ПРН 23 Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.	To justify the choice of software, equipment and tools, engineering technologies and processes, as well as restrictions on them in the field of information security and/or cybersecurity based on current knowledge in related fields, scientific, technical and reference literature and other available information.
ПРН 24 Оцінювати стан інформаційних систем, розподіляти послуги безпеки і обирати механізми безпеки, впроваджувати технологічні рішення інноваційного характеру щодо виявлення та блокування загроз інформаційним ресурсам.	Assess the state of information systems, distribute security services and select security mechanisms, implement innovative technological solutions to identify and block threats to information resources.
ПРН 25 Застосовувати методики щодо оцінювання захищеності об'єктів інформаційної діяльності та державних інформаційних ресурсів від несанкціонованого доступу.	Apply methods for assessing the security of information objects and state information resources from unauthorized access.
ПРН 26 Використовувати результати аналізу кращих світових практик, стандартів із захисту інформації при розробці криптографічних систем захисту інформації в спеціальних інформаційно-комунікаційних системах.	Use the results of the analysis of best international practices, information security standards in the development of cryptographic information security systems in special information and communication systems.
ПРН 27 Застосовувати спеціальні фізичні якості та військово-прикладні навички при виконанні бойових завдань.	To apply special physical qualities and military-applied skills in the performance of combat missions.
ПРН 28 Забезпечувати безпеку та стійкість об'єктів критичної інфраструктури, запобігати	Ensure the security and resilience of critical infrastructure facilities, prevent unauthorized

проявам несанкціонованого втручання в їх функціонування, прогнозування та запобігання кризовим ситуаціям на об'єктах критичної інфраструктури.	interference in their operation, forecast and prevent crisis situations at critical infrastructure facilities.
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 вищої освіти, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 в чинній редакції. Реалізація освітніх компонент забезпечується науково-педагогічними працівниками, які мають науковий ступінь та/або вчене звання та працюють за основним місцем роботи. Залучаються до викладання професійно-орієнтованих дисциплін фахівців-практиків в галузі кібербезпеки та захисту інформації.	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 dated 30.12.2015 № 1187 in the current version. The implementation of educational components is provided by research and teaching staff who have a scientific degree and/or academic title and work at their main place of work. Practitioners in the field of cybersecurity and information protection are involved in teaching professionally oriented disciplines.
Матеріально-технічне забезпечення / Material-technical support	
Відповідно до технологічних вимог щодо матеріально-технічного забезпечення освітньої діяльності відповідного рівня вищої освіти, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 в чинній редакції. Для забезпечення освітньо-професійної програми використовуються матеріально-технічні бази: КПІ ім. Ігоря Сікорського; ІСЗЗІ (навчальний ситуаційний центр з кібербезпеки, група реагування на комп'ютерні інциденти, спеціальна лабораторія з технічного захисту інформації); Державного центру кіберзахисту та Кіберцентру UA30 Держспецзв'язку; полігони Територіальних вузлів урядового зв'язку.	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, № 1187 in the current version. To ensure the educational and professional program, the material and technical bases are used: Igor Sikorsky Kyiv Polytechnic Institute; ISCIP (cybersecurity training situational center, computer incident response team, special laboratory for technical information protection); State Center for Cyber Defense and Cyber Center UA30 of the State Special Communications Service; training grounds of the Territorial Government Communication Nodes.
Інформаційне та навчально-методичне забезпечення / Information and methodological support of the educational process	
Відповідно до вимог щодо інформаційного та навчально-методичного забезпечення освітньої діяльності відповідного рівня вищої освіти, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 в чинній редакції. Користування Науково-технічною бібліотекою КПІ ім. Ігоря Сікорського, загальноінститутської та секретною бібліотеками ІСЗЗІ.	In accordance with the requirements for information and educational and methodological support of educational activities of the relevant level of higher education, approved by the Resolution of the Cabinet of Ministers of Ukraine of 30.12.2015 № 1187 in the current version. Use of the Scientific and Technical Library of Igor Sikorsky Kyiv Polytechnic Institute, the general institutional and secret libraries of the ISCIP.
9 – Академічна мобільність / Academic mobility	
Національна кредитна мобільність / National credit mobility	
Програма не передбачає національної кредитної мобільності.	The program does not provide for national credit mobility.
Міжнародна кредитна мобільність / International credit mobility	
Можливість укладання угод про академічну	Possibility of concluding agreements on academic

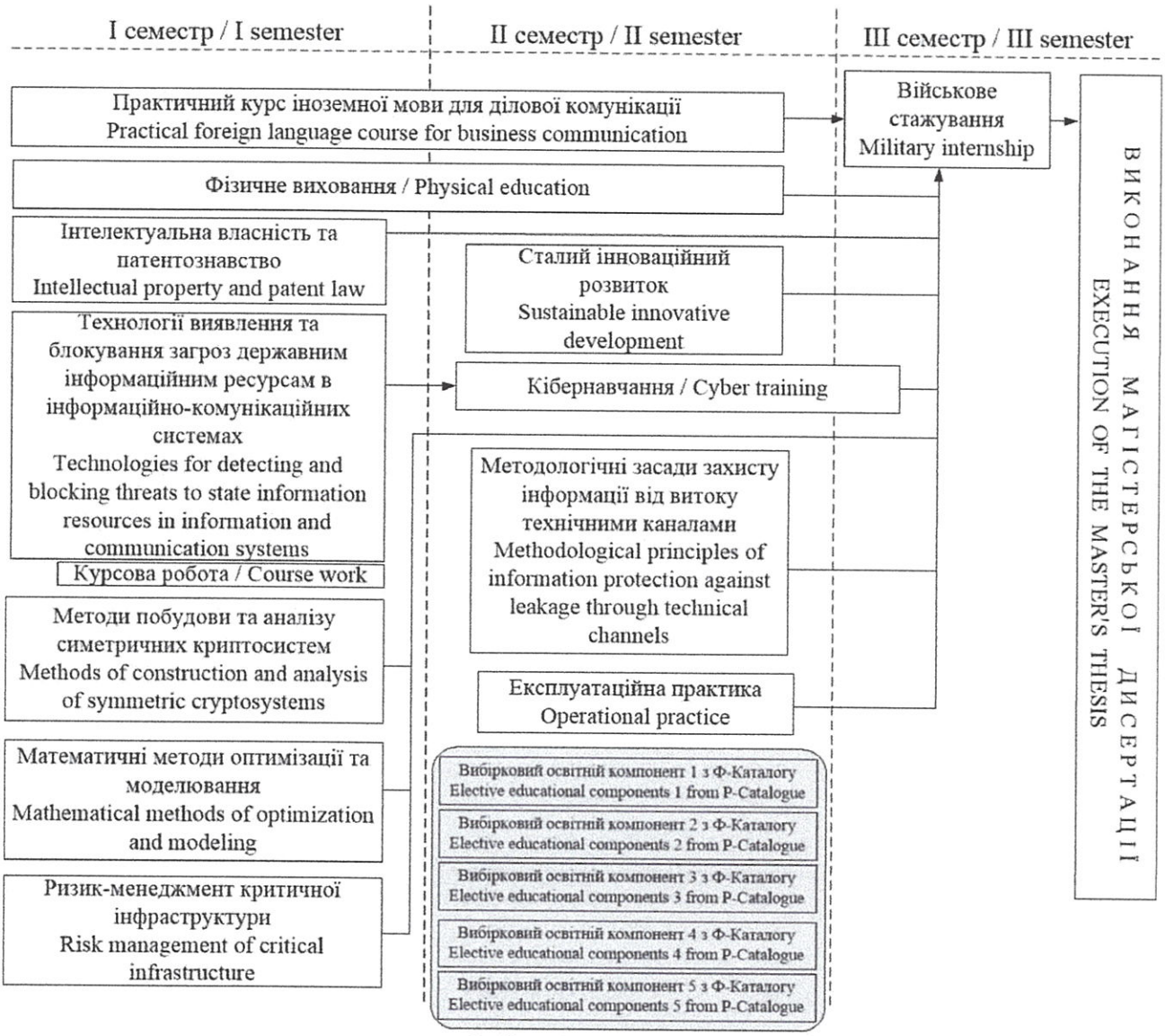
мобільність, про тривалі міжнародні проєкти, які передбачають включене навчання здобувачів вищої освіти (за рішенням Голови Держспецзв'язку).	mobility, long-term international projects that provide for the inclusion of training for higher education applicants (by decision of the Head of the State special communications service).
Навчання іноземних здобувачів вищої освіти / Study of foreign applicants of higher education	
Навчання іноземних здобувачів вищої освіти за даною освітньо-професійною програмою не передбачено.	Training of foreign higher education students under this educational and professional program is not provided.
10 – Процедура присвоєння професійних кваліфікацій / Procedure for awarding professional qualifications	
Не передбачається присвоєння професійних кваліфікацій	No professional qualifications are expected to be awarded

2. ПЕРЕЛІК ОСВІТНІХ КОМПОНЕНТІВ / EDUCATIONAL COMPONENTS

Код / Code	Освітні компоненти / Educational components	Кредити ЄКТС / ECTS credits	Форма підсумкового контролю / Final control form
Нормативні освітні компоненти / Standard educational components			
Цикл загальної підготовки / General training cycle			
ЗО 01	Інтелектуальна власність та патентознавство / Intellectual property and patent law	3	залік Final test
ЗО 02	Сталий інноваційний розвиток / Sustainable innovative development	4	залік Final test
ЗО 03	Практичний курс іноземної мови для ділової комунікації / Practical foreign language course for business communication	3	залік Final test
Цикл професійної підготовки / Professional training cycle			
ПО 1	Фізичне виховання / Physical education	4	залік Final test
ПО 2	Технології виявлення та блокування загроз державним інформаційним ресурсам в інформаційно-комунікаційних системах / Technologies for detecting and blocking threats to state information resources in information and communication systems	4	залік Final test
ПО 3	Технології виявлення та блокування загроз державним інформаційним ресурсам в інформаційно-комунікаційних системах. Курсова робота / Technologies for detecting and blocking threats to state information resources in information and communication systems. Course work	1	залік Final test
ПО 4	Методи побудови та аналізу симетричних криптосистем / Methods of construction and analysis of symmetric cryptosystems	3	залік Final test
ПО 5	Математичні методи оптимізації та моделювання / Mathematical methods of optimization and modeling	6	екзамен Exam
ПО 6	Ризик-менеджмент критичної інфраструктури / Risk management of critical infrastructure	5	екзамен Exam

ПО 7	Методологічні засади захисту інформації від витоку технічними каналами / Methodological principles of information protection against leakage through technical channels	5	залік Final test
ПО 8	Виконання магістерської дисертації / Execution of the master's thesis	14	захист Defense
Практики / Practices			
ПО 9	Кібернавчання / Cyber training	3	залік Final test
ПО 10	Експлуатаційна практика / Operational practice	3	залік Final test
ПО 11	Військове стажування / Military internship	9	залік Final test
Вибіркові освітні компоненти / Elective educational components			
Цикл професійної підготовки / Professional training cycle			
ПВ 1	Вибірковий освітній компонент 1 з Ф-Каталогу / Elective educational components 1 from P-Catalogue	4	залік Final test
ПВ 2	Вибірковий освітній компонент 2 з Ф-Каталогу / Elective educational components 2 from P-Catalogue	5	екзамен Exam
ПВ 3	Вибірковий освітній компонент 3 з Ф-Каталогу / Elective educational components 3 from P-Catalogue	4	залік Final test
ПВ 4	Вибірковий освітній компонент 4 з Ф-Каталогу / Elective educational components 4 from P-Catalogue	5	екзамен Exam
ПВ 5	Вибірковий освітній компонент 5 з Ф-Каталогу / Elective educational components 5 from P-Catalogue	5	екзамен Exam
	Загальний обсяг нормативних освітніх компонентів / Total volume of the standard educational components:		67
	Загальний обсяг вибіркових освітніх компонентів / Total volume of the elective educational components:		23
	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		63
	ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ / TOTAL VOLUME OF THE EDUCATIONAL PROGRAMME		**90**

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



Вибіркові освітні компоненти

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

Атестація здобувачів вищої освіти за освітньо-професійною програмою "Безпека державних інформаційних ресурсів" здійснюється у формі єдиного державного кваліфікаційного іспиту та захисту кваліфікаційної роботи, що забезпечує оцінювання досягнення результатів навчання, визначених стандартом вищої освіти та завершується видачею документа встановленого зразка про присудження йому ступеня магістра з присвоєнням освітньої кваліфікації: магістр з кібербезпеки та захисту інформації, за освітньо-професійною програмою "Безпека державних інформаційних ресурсів".

Кваліфікаційна робота має передбачати розв'язання складної задачі дослідницького та/або інноваційного характеру у сфері кібербезпеки та захисту інформації. Кваліфікаційна робота не повинна містити академічного плагіату, фальсифікації, фабрикації.

Кваліфікаційна робота перевіряється на плагіат, фабрикацію та фальсифікацію і після захисту розміщується в навчальній бібліотеці ІСЗЗІ КПІ ім. Ігоря Сікорського в архіві наукових та освітніх матеріалів для вільного доступу.

Атестація здійснюється відкрито і публічно. Але, якщо кваліфікаційна робота містить інформацію з обмеженим доступом, то захист проводиться в закритому режимі з неухильним дотриманням і виконанням вимог чинного законодавства щодо збереження службової та державної таємниці.

Certification of applicants for higher education in the educational and professional programme "Security of state information resources" is carried out in the form of a single state qualification examination and defence of qualification work, which ensures the assessment of the achievement of learning outcomes defined by the standard of higher education and ends with the issuance of a document of the established form on awarding a master's degree with the award of educational qualification: Master of Cybersecurity and Data Protection, in the educational and professional programme "Security of state information resources".

The qualification work is checked for plagiarism, fabrication and falsification and, after defense, is placed in the academic library of the Igor Sikorsky Kyiv Polytechnic Institute in the archive of scientific and educational materials for free access.

The qualification work is checked for plagiarism and after defense is placed in the educational library of the Igor Sikorsky Kyiv Polytechnic Institute in the archive of scientific and educational materials for free access.

Certification is carried out openly and publicly. However, if the qualification work contains information with limited access, the defense is conducted in a closed mode with strict observance and fulfillment of the requirements of current legislation on the preservation of official and state secrets.

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

	ЗО1	ЗО2	ЗО3	ПО1	ПО2	ПО3	ПО4	ПО5	ПО6	ПО7	ПО8	ПО9	ПО10	ПО11
ЗК1	+	+	+		+	+	+	+		+	+	+	+	+
ЗК2		+	+		+			+		+	+		+	+
ЗК3		+					+	+	+		+	+		+
ЗК4	+	+									+		+	+
ЗК5	+	+	+		+			+			+	+	+	+
ФК1							+	+	+		+	+		+
ФК2	+	+					+			+	+		+	+
ФК3					+	+					+		+	+
ФК4					+				+		+	+		+
ФК5					+	+		+	+		+	+		+
ФК6							+				+	+		+
ФК7					+						+	+		+
ФК8							+	+		+	+		+	+
ФК9					+	+					+	+		+
ФК10	+	+									+			+
ФК11					+	+					+	+		+
ФК12										+	+		+	+
ФК13							+				+	+		+
ФК14				+										+
ФК15					+				+		+	+		+

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

	ЗО1	ЗО2	ЗО3	ПО1	ПО2	ПО3	ПО4	ПО5	ПО6	ПО7	ПО8	ПО9	ПО10	ПО11
ПРН1	+	+	+					+			+	+		+
ПРН2	+	+			+		+	+		+	+	+		+
ПРН3		+					+	+			+		+	+
ПРН4	+						+	+			+	+	+	+
ПРН5	+	+	+					+			+			+
ПРН6					+	+	+		+		+	+	+	+
ПРН7			+					+			+		+	+
ПРН8					+	+					+	+		+
ПРН9					+	+			+		+	+		+
ПРН10					+	+			+		+	+	+	+
ПРН11					+	+					+	+		+
ПРН12					+	+					+	+		+
ПРН13	+						+	+			+		+	+
ПРН14					+	+					+			+
ПРН15	+	+	+					+			+			+
ПРН16								+		+	+	+		+
ПРН17	+	+						+			+	+		+
ПРН18	+	+									+		+	+
ПРН19								+			+		+	+
ПРН20			+				+	+			+			+
ПРН21					+	+		+			+	+	+	+
ПРН22	+	+					+	+		+	+		+	+
ПРН23								+			+			+
ПРН24					+						+	+		+
ПРН25										+	+		+	+
ПРН26							+				+	+		+
ПРН27				+										+
ПРН28					+	+			+		+	+		+