**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 №_____
від / dated _____20___ р.
Голова Вченої ради / Head of the Academic Council
_____ Михайло ІЛЬЧЕНКО / Mykhailo ILCHENKO

# СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ
## SYSTEMS OF TECHNICAL PROTECTION OF INFORMATION

## ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА / PROFESSIONAL EDUCATIONAL PROGRAMME

Перший (бакалаврський) рівень вищої освіти
Спеціальність: F5 Кібербезпека та захист інформації
Галузь знань: F Інформаційні технології
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
Qualification: Bachelor of Cybersecurity and Information Protection

ID: **81880**

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

Новіков Олексій
Миколайович
д.т.н., професор, директор
Навчально-наукового фізико-
технічного інституту /
Oleksii NOVIKOV
Dr. Sc, Full Professor, Director
of Educational and Research
Institute of Physics and
Technology

Члени робочої групи / Project team members:

Ланде Дмитро Володимирович

д.т.н., професор, завідувач кафедри інформаційної безпеки /

Dmytro LANDE

Dr. Sc, Full Professor,

Head of the department of information security

Мачуський Євген Андрійович

д.т.н., професор, професор кафедри інформаційної безпеки /

Eugene MACHUSKY

Dr. Sc, Full Professor,

Professor of the department of information security

Луценко Володимир Миколайович

к.т.н., доцент,

доцент кафедри інформаційної безпеки /

Volodymyr LUTSENKO

PhD, Associate Professor,

Professor of the department of information security

Прогонов Дмитро Олександрович

д.т.н., доцент,

доцент кафедри інформаційної безпеки /

Dmytro PROGONOV

Dr. Sc, Associate Professor, Professor of the department of information security

**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 information protection (протокол / minutes of meeting №___ від / dated _____ 20___)

Голова НМКУ-125 / Head of the SMCU-125

_____ Дмитро ЛАНДЕ / Dmytro LANDE

Методична рада КПІ ім. Ігоря Сікорського / The Methodological Council of Igor Sikorsky Kyiv Polytechnic Institute (протокол / minutes of meeting №___ від / dated _____ 20___)

Голова Методичної ради / Head of the Methodological Council

_____ Тетяна ЖЕЛЯСКОВА / Tetiana ZHELIASKOVA

**ВРАХОВАНО / CONSIDERED:**

Представники роботодавців

Мохонько Олексій Анатолійович к.ф.-м.н., R&D директор з інформаційної безпеки, ТОВ “Самсунг Електронікс Україна Компані”, український центр досліджень та розробок Samsung

Соловйов Євгеній Валерійович Начальник Управління інформаційними технологіями Служби зовнішньої розвідки України

Авдєєв Ігор Володимирович полковник служби цивільного захисту, Начальник Центру оперативного зв’язку, телекомунікаційних систем та інформаційних технологій Державної служби з надзвичайних ситуацій

Виборні представники студентських організацій

Сафонов Богдан

студент 4 курсу бакалаврату
за спеціальністю
F5 Кібербезпека та захист
інформації

Островський Станіслав
студент 2 курсу бакалаврату
за спеціальністю
F5 Кібербезпека та захист
інформації

Employers' representatives

Oleksii MOKHONKO
PhD, Information security R&D
Director, LLC “Samsung R&D
Institute Ukraine”

Eugene SOLOVYOV
Head of Information
Technology Management
Foreign Intelligence Service of
Ukraine

Ihor AVDEYEV
Col. of the Civil Defense
Service, Head of the Center for
Operational Communication,
Telecommunication Systems
and Information Technologies
of the State Emergency Service

Representatives of student organizations

Bohdan SAFONOV

a 4th-year undergraduate
student in the specialty F5
Cybersecurity and Information
Protection

Stanislav OSTROVSKY
2nd year undergraduate
student in the specialty
F5 Cyber security and
information protection

## ЕВОЛЮЦІЯ ОСВІТНЬОЇ ПРОГРАМИ / EVOLUTION OF THE EDUCATIONAL PROGRAMME

Підготовка здобувачів за освітньо-професійною програмою (ОПП) «Системи технічного захисту інформації» першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека та захист інформації проводиться з 2017 року. Розробка ОПП почалася в 2016 році та

враховувала багаторічний досвід підготовки фахівців в галузі технічного захисту інформації (з 2000 року) викладачами кафедр фізико-технічних засобів захисту інформації та інформаційної безпеки.

Протягом 2016-2020 року проводилася послідовна модернізація ОПП для врахування тенденцій розвитку галузі кібернетичної та інформаційної безпеки в Україні та світі, а також відповідності стандартам вищої освіти в галузі 125 Кібербезпека. Зміни ОПП були спрямовані на приведення змісту та наповнення освітніх компонентів ОПП до вимог стандарту вищої освіти, розширення можливостей здобувачів щодо формування індивідуальної траєкторії навчання та залучанню нових роботодавців в якості стейкхолдерів за програмою підготовки (зокрема ТОВ “Самсунг Електронікс Україна Компані”, Державної служби з надзвичайних ситуацій та Служби зовнішньої розвідки України).

Суттєве оновлення ОПП відбулося у 2022 році у зв'язку з набуттям Фізико-технічного інституту статусу Навчально-наукового інституту. Внесено зміни у склад проектної групи та склад стейкхолдерів. Також враховано зміни щодо придатності до працевлаштування згідно Зміни №10 до Державного класифікатору професій ДК 003:2010. Враховано Постанову від 19 травня 2021 р. № 497 щодо внесення єдиного державного комплексного іспиту зі спеціальності до атестації здобувачів вищої освіти та Постанову Кабінету Міністрів України від 24 березня 2021 р. № 365 «Про внесення змін до постанови Кабінету Міністрів України від 30 грудня 2015 р. № 1187 Про затвердження Ліцензійних умов провадження освітньої діяльності».

Наступне оновлення освітньої програми відбулося у 2023 році у зв’язку зі зміною назви спеціальності. Внесено корективи у відповідності з вимогами Постанови Кабінету Міністрів України від 16.12.2022 № 1392 “Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти” Внесено зміни у склад стейкхолдерів.

В 2024 році внесено зміни до переліку освітніх компонентів, що відносяться до циклів загальної та професійної підготовки. Зокрема, збільшено кількість кредитів для освітніх компонентів, вивчення котрих закінчується заліком або іспитом. Також вилучено освітні компоненти «Інформаційні технології», «Алгебра та геометрія 2», «Основи моделювання систем обробки акустичних сигналів», «Технічний захист інформації» та «Проектування систем технічного захисту інформації» для посилення підготовки за фундаментальними курсами з курсу загальної та професійної підготовки. Враховано зміни до стандарту вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для першого (бакалаврського) рівня вищої освіти, затвердженого наказом Міністерства освіти і науки України від 04.10.2018 №1074.

Актуальна редакція програми підготовлена в 2025 році. Внесено зміни до переліку загальних дисциплін, зокрема введено курс «Теоретична підготовка базової загальновійськової підготовки». Також введено додаткові курси до циклу професійної підготовки, а саме «Теорія функцій комплексної змінної», «Електроакустичні пристрої» та «Антени і поширення електромагнітних хвиль», з метою посилення фахової підготовки за напрямком технічного захисту інформації. Вилучено курси «Системна інженерія», «Проектування систем технічного захисту інформації» та «Теоретичні основи захисту інформації» для посилення фахової підготовки в частині роботи з комплексами технічного захисту. При оновленні ОПП враховано зміни до стандарту вищої освіти зі спеціальності 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти, затвердженого наказом Міністерства освіти і науки України від 29.10.2024 №1547.

Також враховано оновлення в організації освітнього процесу згідно наказу ректора КПІ ім. Ігоря Сікорського №НОД/362/25 від 25 квітня 2025 року «Про організації та планування навчального процесу на 2025-2026 роки».

Training of applicants for the educational professional program (EPP) "Technical information protection systems" of the first (bachelor) level of higher education in the specialty 125 Cyber security and information protection has been held since 2017. The development of the EPP began in 2016 and took into account many years of experience in training specialists in the field of technical information protection (since 2000) by teachers of the departments of physical and technical means of information protection and information security.

During 2016-2020, the EPP was continuously modernized to take into account the development trends of the field of cyber and information security in Ukraine and the world, as well as compliance with the standards of higher education in the field of 125 Cyber Security. The changes in the EPP were aimed at bringing the content and content of the educational components of the EPP to the requirements of the higher education standard, expanding the EPP opportunities of applicants to form an individual learning trajectory, and attracting new employers as stakeholders in the training program (in particular, Samsung Electronics Ukraine Company LLC, the State Emergency Service situations and the Foreign Intelligence Service of Ukraine).

A significant update of the EPP took place in 2022 in connection with the Institute of Physics and Technologies acquiring the status of an Educational and Scientific Institute. In addition, changes in the composition of the project group and the composition of stakeholders took places. Also taken into account are the changes regarding suitability for employment according to Amendment No. 10 to the State Classifier of Professions DK 003:2010. Taking into account Resolution No. 497 of May 19, 2021 regarding the introduction of a unified state comprehensive exam in a specialty for certification of higher education applicants and Resolution of the Cabinet of Ministers of Ukraine No. 365 of March 24, 2021 "On Amendments to the Resolution of the Cabinet of Ministers of Ukraine of December 30, 2015 No. 1187 On the approval of the Licensing conditions for the conduct of educational activities.

The next update of the educational program took place in 2023 due to a change in the name of the specialty. Corrections were made in accordance with the requirements of the Resolution of the Cabinet of Ministers of Ukraine dated 16.12.2022 No. 1392 "On making changes to the list of fields of knowledge and specialties for which higher education applicants are trained" Changes were made to the composition of stakeholders.

In 2024, changes were made to the list of educational components related to the cycles of general and professional training. In particular, the number of credits for educational components, the study of which ends with a test or exam, was increased. The educational components "Information Technologies", "Algebra and Geometry 2", "Fundamentals of Modeling Acoustic Signal Processing Systems", "Technical Information Protection" and "Design of Technical Information Protection Systems" were also removed to strengthen training in fundamental courses from the course of general and professional training. Changes were taken into account to the standard of higher education in the specialty 125 "Cybersecurity" of the field of knowledge 12 "Information Technologies" for the first (bachelor's) level of higher education, approved by the order of the Ministry of Education and Science of Ukraine dated 04.10.2018 No. 1074.

The current version of the program was prepared in 2025. Changes have been made to the list of general courses, in particular, the “Theoretical Training of Basic Combined-Arms Training” has been introduced. Additional courses have also been introduced to the professional training cycle, namely “Theory of Complex Variable Functions”, “Electroacoustic Devices” and “Antennas and Propagation of Electromagnetic Waves”, in order to strengthen professional training in the field of technical information protection. The courses “System Engineering”, “Design of Technical Information Protection Systems” and “Theoretical Fundamentals of Information Protection” have been removed to strengthen professional training in working with technical protection complexes. When updating the OPP, changes to the higher education standard in specialty 125 “Cybersecurity” for the first (bachelor’s) level of higher education, approved by the order of the Ministry of Education and Science of Ukraine dated 10/29/2024 No. 1547, were taken into account.

Updates in the organization of the educational process were also taken into account in accordance with the order of the rector of Igor Sikorsky Kyiv Polytechnic Institute No. NOD/362/25 dated April 25,

2025 "On the organization and planning of the educational process for 2025-2026."

## 1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ / EDUCATIONAL PROGRAMME PROFILE

| 1 – Загальна інформація / General information | | |
|---|---|---|
| Повна назва закладу вищої освіти та навчального підрозділу / Full name of higher education institution and faculty / educational and scientific institute | Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Навчально-науковий фізико-технічний інститут | National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Educational and Research Institute of Physics and Technology |
| Ступінь вищої освіти та назва освітньої кваліфікації / Higher education degree and education qualification title | Ступінь бакалавра<br>бакалавр з кібербезпеки та захисту інформації | Bachelor Degree<br>Bachelor of Cybersecurity and Information Protection |
| Офіційна назва освітньої програми / Educational programme official title | Системи технічного захисту інформації | Systems of Technical Protection of Information |
| 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<br>QF-EHEA – перший цикл<br>EQF-LLL – 6 рівень | NQF of Ukraine - 6 level<br>QF-EHEA – 1 cycle<br>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_STZI | |

| 2 – Мета освітньої програми / Educational programme purpose | |
|---|---|
| Метою освітньої програми є підготовка фахівців, здатних вирішувати складні задачі в галузі кібернетичної безпеки особистості, спільноти, суспільства та держави, всебічного професійного, інтелектуального, соціального та творчого розвитку особистості на найвищих рівнях досконалості в освітньо-науковому середовищі.<br>Мета освітньої програми відповідає стратегії розвитку КПІ ім. Ігоря Сікорського на 2025-2030 рік щодо формування суспільства майбутнього на засадах концепції сталого розвитку<br>З цією метою освітня програма передбачає:<br>1. Фундаментальну підготовку фахівців в галузі математики, фізики, філософії природи та суспільства;<br>2. Гармонізовану спеціалізовану підготовку фахівців в галузі інформаційно-комунікаційних систем різної фізичної природи: від класичної термодинаміки і електродинаміки до квантової гравідинаміки і хромодинаміки;<br>3. Спеціалізовану гармонізовану підготовку фахівців в галузі континуальної, дискретної та квантової обробки інформації математичними та фізичними методами та засобами;<br>4. Гармонізовану міждисциплінарну організаційно-економічну та нормативно-правову підготовку фахівців, здатних створювати нові стартапи та успішно конкурувати на високотехнологічних ринках праці;<br>Міждисциплінарну педагогічно-психологічну підготовку фахівців для подальшого саморозвитку і праці в різних галузях освіти, науки та інженерії. | The purpose of the educational program is to train specialists capable of solving complex problems in the field of cyber security of the individual, community, society and the state, comprehensive professional, intellectual, social and creative development of the individual at the highest levels of excellence in the educational and scientific environment.<br>The purpose of the educational program corresponds to the development strategy of Igor Sikorsky Kyiv Polytechnic Institute for 2025-2030 regarding the formation of the society of the future based on the concept of sustainable development.<br>For this purpose, the educational program provides:<br>1. Fundamental training of specialists in the field of mathematics, physics, philosophy of nature and society;<br>2. Harmonized specialized training of specialists in the field of information and communication systems of various physical nature: from classical thermodynamics and electrodynamics to quantum gravidynamics and chromodynamics;<br>3. Specialized harmonized training of specialists in the field of continuous, discrete and quantum information processing by mathematical and physical methods and means;<br>4. Harmonized interdisciplinary organizational, economic and regulatory training of specialists capable of creating new startups and successfully competing in high-tech labor markets;<br>Interdisciplinary pedagogical and psychological training of specialists for further self-development and work in various fields of education, science and engineering |

| 3 – Характеристика освітньої програми / Educational programme characteristics | |
|---|---|
| **Предметна область / Subject area** | |
| Об’єкти професійної діяльності випускників:<br>• технології кібербезпеки та захисту інформації;<br>• процеси управління кібербезпекою та захистом інформації; об’єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології.<br>Цілі навчання: підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв’язувати складні задачі у галузі кібербезпеки та захисту інформації.<br>Теоретичний зміст предметної області:<br>Принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільтсва, держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.<br>Методи, методики та технології:<br>методи, методики та технології розв’язання теоретичних і практичних задач кібербезпеки та захисту інформації<br>Інструменти та обладнання:<br>засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків). | Objects of professional activity of graduates:<br>• cybersecurity and information protection technologies;<br>• cybersecurity and information protection management processes; objects of information activity, including information and information and communication systems, information resources and technologies.<br>The purpose of training is to train specialists capable of using and implementing cybersecurity and information protection technologies and solving complex problems in the field of cybersecurity and information protection.<br>Theoretical content of the subject area:<br>Principles, concepts, theories of protecting the vital interests of man, society, and the state when using cyberspace, which ensure the sustainable development of the information society and the digital communicative environment, as well as the timely detection, prevention, and neutralization of real and potential threats to the national security of Ukraine in cyberspace<br>Methods, techniques and technologies:<br>methods, techniques and technologies for solving theoretical and practical problems of cybersecurity and information protection<br>Tools and equipment:<br>tools, devices, network equipment, application and specialized software, information systems and complexes for designing, modeling, controlling, monitoring, storing, processing, displaying and protecting data (information flows). |
| **Орієнтація освітньої програми / Scope** | |
| Освітньо-професійна | Educational professional |
| **Основний фокус освітньої програми / Main focus** | |

| | |
|---|---|
| Основні фокуси програми:<br>1. Посилена підготовка в галузі дискретної математики та квантової інформатики;<br>2. Посилена підготовка в галузі механіки, електроніки, радіотехніки, акустики, оптоелектроніки;<br>3. Посилена підготовка в галузі дискретної обробки інформації логіко-математичними методами та фізико-технічними засобами;<br>4. Фундаментальна підготовка щодо проектування, розробки, впровадження та супроводу комплексних систем захисту інформації, що циркулює на об’єктах інформаційної діяльності державної та приватної форми власності;<br>5. Посилена підготовка в галузі міждисциплінарного системного аналізу з метою створення комплексних систем захисту інформаційних потоків у комунікаційних мережах;<br>6. Широке залучення здобувачів вищої освіти до участі у провідних міжнародних конференціях в галузі кібернетичної безпеки;<br>7. Проведення щорічних конференцій та олімпіад з нових напрямків кібернетичної безпеки з метою навчання здобувачів вищої освіти розробці індивідуальних стартапів на етапі підготовки кваліфікаційної роботи.<br>Ключові слова: кібернетична безпека, технічні засоби захисту інформації, технічний аудит, проектування та створення комплексів технічного захисту інформації | The main focuses of the program:<br>1. Enhanced training in the field of discrete mathematics and quantum informatics;<br>2. Enhanced training in mechanics, electronics, radio engineering, acoustics, optoelectronics;<br>3. Enhanced training in the field of discrete processing of information using logical-mathematical methods and physical-technical means;<br>4. Fundamental training on the design, development, implementation and support of complex systems for the protection of information that circulates on the objects of information activity of state and private ownership;<br>5. Enhanced training in the field of interdisciplinary system analysis with the aim of creating complex systems for the protection of information flows in communication networks;<br>6. Wide involvement of higher education students in participation in leading international conferences in the field of cyber security;<br>7. Holding of annual conferences and olympiads on new areas of cyber security for the purpose of training higher education students to develop individual startups at the stage of preparation for qualification work.<br>Keywords: cyber security, technical means of information protection, technical audit, design and creation of technical information protection complexes |
| **Особливості освітньої програми / Features** | |
| 1. Перехід від стандартних методів класичної математики та класичної фізики до квантово-механічних та квантово-обчислювальних напрямків розвитку сучасної математичної фізики;<br>2. Посилена підготовка в галузі природничих наук (математики, фізики), а також технічних наук (програмування, обробки сигналів різної фізичної природи, розробка та оптимізація пристроїв захисту інформації);<br>3. Фундаментальна підготовка щодо проектування, розробки, впровадження та супроводу комплексних систем захисту інформації, що циркулює на об’єктах інформаційної діяльності державної та приватної форми власності;<br>4. Проходження практик на провідних підприємствах галузі захисту інформації. | 1. Transition from standard methods of classical mathematics and classical physics to quantum-mechanical and quantum-computational directions of development of modern mathematical physics;<br>2. Enhanced training in the field of natural sciences (mathematics, physics), as well as technical sciences (programming, signal processing of various physical nature, development and optimization of information protection devices);<br>3. Fundamental training regarding the design, development, implementation and support of complex information protection systems circulating on the objects of information activity of state and private ownership;<br>4. Internship at leading enterprises in the field of information protection. |

| 4 – Придатність випускників до працевлаштування та подальшого навчання / Eligibility of graduates for employment and further study | |
|---|---|
| **Придатність до працевлаштування / Eligibility for employment** | |
| На посади у структурних підрзділах установ / підприємств / організацій, які передбачають наявність вищої освіти зі спеціальності 125 Кібербезпека та захист інформації<br>Відповідно до Державного класифікатору професій ДК 003:2010 зі Зміною №10 випускники можуть працювати на посадах, що відповідають класифікаційним угрупованням:<br>2139.2 фахівець з технічного захисту інформації<br>3121 Фахівець з інформаційних технологій.<br>3139 Фахівець із організації захисту інформації з обмеженим доступом;<br>Фахівець із організації інформаційної безпеки<br>Можуть працювати фахівцями із захисту інформації в складі інформаційних департаментів підприємств та банків, співробітниками служб захисту інформації; аудиторами інформаційної та кібернетичної безпеки, адміністраторами інформаційної та кібернетичної безпеки, проектувальниками систем захисту інформації в кіберпросторі; розробниками програмних та програмно-апаратних засобів захисту інформації в кіберпросторі, аналітиками кібербезпеки в установах державної та інших форм власності, спеціалістами з забезпечення кібербезпеки в кіберфізичних системах, зокрема, об’єктах критичної інфраструктури. | For positions in structural divisions of institutions / enterprises / organizations that require higher education in specialty 125 Cybersecurity and Information Protection<br>According to the State Classifier of Professions DK 003:2010 with Amendment No. 10, graduates can work in positions corresponding to the classification groups:<br>2139.2 specialist in technical information protection<br>3121 Specialist in information technologies.<br>3139 Specialist in the organization of information protection with limited access;<br>Specialist in the organization of information security<br>They can work as information protection specialists in the information departments of enterprises and banks, employees of information protection services; auditors of information and cybernetic security, administrators of information and cybernetic security, designers of information protection systems in cyberspace; developers of software and software and hardware means of information protection in cyberspace, cyber security analysts in institutions of state and other forms of ownership, specialists in ensuring cyber security in cyber physical systems, in particular, objects of critical infrastructure. |
| **Подальше навчання / Further study** | |
| Продовження освіти за другим (магістерським) рівнем вищої освіти.<br>Здобуття або вдосконалення освіти та професійної підготовки в системі освіти дорослих. | Continuation of education at the second (master's) level of higher education.<br>Obtaining or improving education and professional training in the adult education system. |
| **5 – Викладання та оцінювання / Teaching and assessment** | |
| **Викладання та навчання/Teaching and studying** | |
| Програмою передбачено студентоцентроване навчання. Викладання проводиться у таких формах: лекції, практичні та семінарські заняття, комп’ютерні практикуми і лабораторні роботи; курсові проекти і роботи; технологія змішаного навчання, практики; виконання дипломного проекту і дипломної роботи | The program provides for student-centered learning. Teaching is carried out in the following forms: lectures, practical and seminar classes, computer workshops and laboratory works; course projects and works; mixed learning technology, practices; completion of the diploma project and 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); екзамени, заліки, індивідуальні завдання тощо. | Assessment of students' knowledge is carried out in accordance with the Regulation on the system of assessment of learning outcomes of Ihor Sikorsky Kyiv Polytechnic Institute for all types of classroom and extra-auditory work (incoming, current, calendar, final control); exams, assessments, individual tasks, etc. |

| 6 – Програмні компетентності / Programme competencies | | |
|---|---|---|
| **Інтегральна компетентність / Integral competence** | | |
| Здатність розв’язувати складні спеціалізовані задачі і практичні проблеми у галузі кібербезпеки та захисту інформації | | The ability to solve complex specialized tasks and practical problems in the field of cybersecurity and information protection |
| **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 виконання свого конституційного обов’язку щодо захисту Вітчизни, національно-патріотичної налаштованості, відданості українському народові | Ability to fulfill the constitutional duty to protect the Motherland, uphold national-patriotic attitude, devotion to the Ukrainian people |
| **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 в галузі інформаційної та/або кібербезпеки | 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 in the field of information and/or cyber security |
| *ФК 02* | Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки | Ability to use information and communication technologies, modern methods and models of information security and/or cyber security |
| *ФК 03* | Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки | Ability to ensure business continuity in accordance with established information and/or cyber security policies |

| | | |
|---|---|---|
| *ФК 04* | Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки | The ability to ensure the protection of information processed in information and telecommunication (automated) systems for the purpose of implementing the established information and/or cyber security policy |
| *ФК 05* | Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження | The ability to restore the normal functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber attacks, failures and failures of various classes and origins |
| *ФК 06* | Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) | The ability to implement and ensure the functioning of complex information protection systems (complexes of legal, organizational and technical means and methods, procedures, practical techniques, etc.) |
| *ФК 07* | Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою | The ability to carry out professional activities based on an implemented information and/or cyber security 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 досліджувати ефективність роботи давачів сигналів різної фізичної природи, проводити їх оптимізацію для заданих умов роботи | The ability to investigate the effectiveness of signal transmitters of different physical nature, to carry out their optimization for given operating conditions |
| *ФК 12* | Здатність виявляти та локалізувати джерела небезпечних сигналів в умовах обмеженості апріорних даних щодо їх характеристик та фізичної природи | The ability to identify and localize sources of dangerous signals in conditions of limited a priori data regarding their characteristics and physical nature |
| *ФК 13* | Здатність проводити спеціальні дослідження об’єктів інформаційної діяльності згідно нормативних актів в галузі технічного захисту інформації | The ability to conduct special research of objects of information activity in accordance with normative acts in the field of technical information protection |

| 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, 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, 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* | Вирішувати задачі розробки, впровадження та супроводу систем моніторингу джерел небезпечних сигналів різної фізичної природи | To solve the problems of development, implementation and support of monitoring systems of sources of dangerous signals of various physical nature |
| *ПРН 23* | Здійснювати аналіз та обробку сигналів різної фізичної природи з використанням новітніх методів статистичного, спектрального та структурного аналізу | Analyze and process signals of various physical nature using the latest methods of statistical, spectral and structural analysis |
| *ПРН 24* | Застосовувати нормативні документи в галузі технічного захисту інформації при вирішенні задач розробки, впровадження та супроводу комплексних систем захисту інформації | Apply regulatory documents in the field of technical information protection when solving problems of development, implementation and support of complex information protection systems |
| *ПРН 25* | Знати та вміти використовувати основні засоби захисту та оборони держави, співвітчизників, матеріальних цінностей та територіальної цілісності держави, зокрема, у разі військових дій та надзвичайних ситуацій | Know how to use and be able to apply basic means of protection and defence of the state, fellow citizens, material assets, and the territorial integrity of the state, particularly in the event of military actions and emergency situations |

| 8 – Ресурсне забезпечення реалізації програми / Resource provision for programme implementation | |
|---|---|
| **Кадрове забезпечення / Staffing** | |
| Відповідно до кадрових вимог щодо забезпечення провадження освітньої діяльності для відповідного рівня ВО, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 (в чинній редакції). | In accordance with the personnel requirements for ensuring the implementation of educational activities for the corresponding level of HE, approved by the Resolution of the Cabinet of Ministers of Ukraine dated 12.30.2015 No. 1187 (in the actual version). |
| **Матеріально-технічне забезпечення / Material-technical support** | |
| Відповідно до технологічних вимог щодо матеріально-технічного забезпечення освітньої діяльності відповідного рівня ВО, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 (в чинній редакції).<br>Використання обладнання для проведення лекцій у форматі презентацій, мережевих технологій, зокрема на платформі дистанційного навчання Sikorsky. | In accordance with the technological requirements for the material and technical support of educational activities of the corresponding level of HE, approved by the Resolution of the Cabinet of Ministers of Ukraine dated 12.30.2015 No. 1187 (in the actual version).<br>Use of equipment for conducting lectures in the format of presentations, network technologies, in particular on the Sikorsky distance learning platform. |
| **Інформаційне та навчально-методичне забезпечення / Information and 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).<br>Користування Науково-технічною бібліотекою КПІ ім. Ігоря Сікорського. | In accordance with the technological requirements for educational, methodological and informational support of educational activities of the corresponding level of HE, approved by Resolution of the Cabinet of Ministers of Ukraine dated 12.30.2015 No. 1187 (as amended).<br>Use of the Scientific and Technical Library of Ihor Sikorsky Kyiv Polytechnic Institute. |
| **9 – Академічна мобільність / Academic mobility** | |
| **Національна кредитна мобільність / National credit mobility** | |
| Участь студентів в програмах академічної мобільності, можливість укладення угод одержання студентами подвійних дипломів | Participation of students in academic mobility programs, the possibility of concluding agreements for students to receive double diplomas |
| **Міжнародна кредитна мобільність / International credit mobility** | |
| Можливість укладення угод про міжнародну академічну мобільність, про подвійне дипломування, про тривалі міжнародні проекти | The possibility of concluding agreements on international academic mobility, on double graduation, on long-term international projects |
| **Навчання іноземних здобувачів вищої освіти / Study of foreign applicants of higher education** | |
| Навчання іноземних здобувачів ВО, які опановують ОП за програмами міжнародної академічної мобільності, навчання може проводитись англійською або українською мовою, за умови володіння здобувачем мовою навчання на рівні не нижче В2. | The training of foreign higher education students who master the OP under international academic mobility programs can be conducted in English or Ukrainian, provided the student has a language proficiency of no lower than B2. |
| **10 – Процедура присвоєння професійних кваліфікацій / Procedure for awarding professional qualifications** | |
| | |

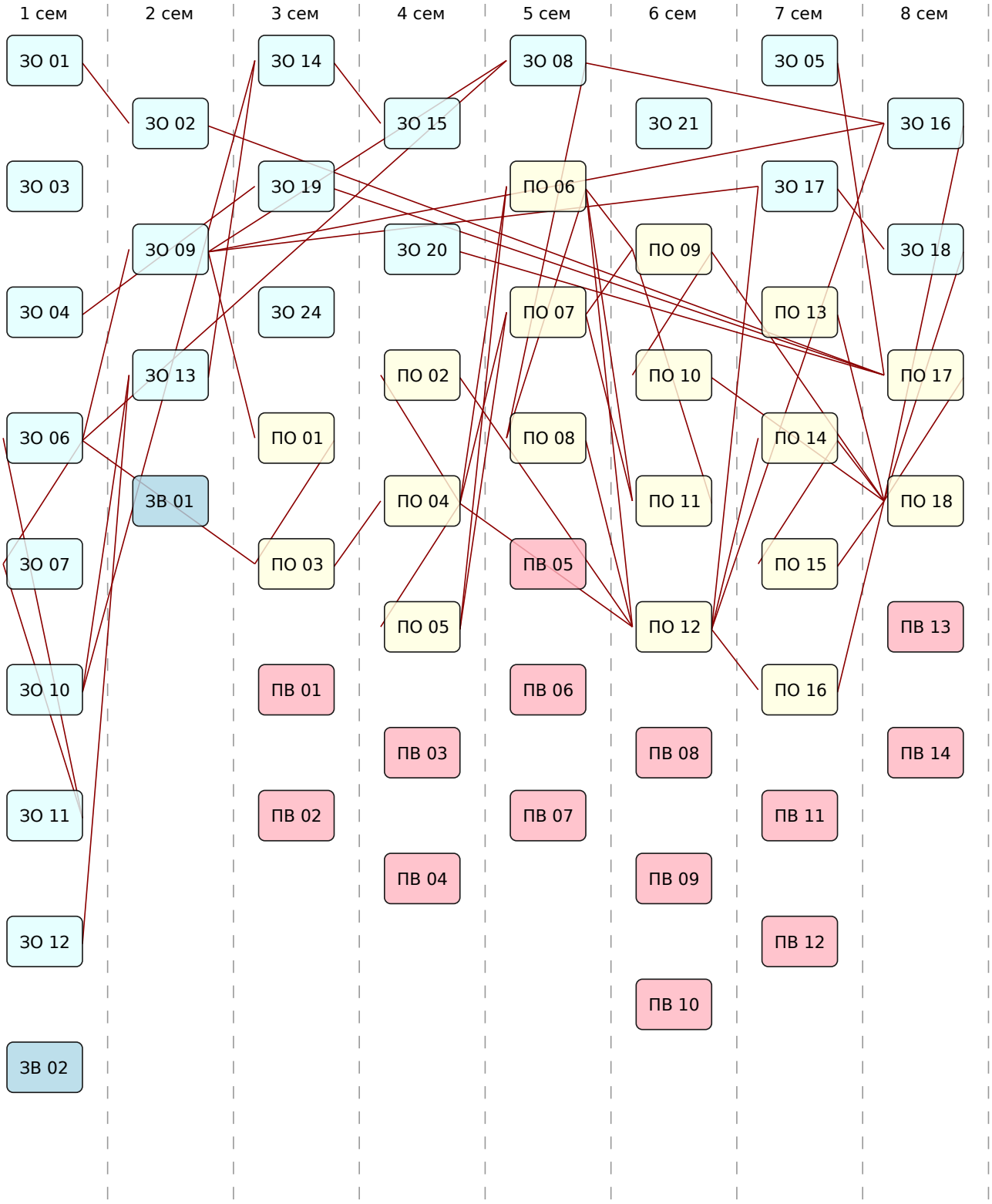
## 2. ПЕРЕЛІК КОМПОНЕНТІВ ОСВІТНЬОЇ ПРОГРАМИ / COMPONENTS of EDUCATIONAL PROGRAMME

| Код/Code | Освітні компоненти програми/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* | Історія науки і техніки / History of Science and Technology | 2.0 | Залік / Final test |
| *ЗО 03* | Основи здорового способу життя / Fundamentals of Healthy Lifestyle | 3.0 | Залік / Final test |
| *ЗО 04* | Англійська мова / English | 5.0 | Залік / Final test |
| *ЗО 05* | Основи економіки / Fundamentals of Economics | 2.0 | Залік / Final test |
| *ЗО 06* | Математичний аналіз / Mathematical Analysis | | |
| *ЗО 06.1* | Математичний аналіз. Частина 1 / Mathematical Analysis. Part 1 | 5.0 | Екзамен / Exam |
| *ЗО 06.2* | Математичний аналіз. Частина 2 / Mathematical Analysis. Part 2 | 5.0 | Екзамен / Exam |
| *ЗО 07* | Фізика / Physics | | |
| *ЗО 07.1* | Фізика. Частина 1 / Physics. Part 1 | 5.0 | Залік / Final test |
| *ЗО 07.2* | Фізика. Частина 2 / Physics. Part 2 | 6.0 | Екзамен / Exam |
| *ЗО 08* | Теорія ймовірності та математична статистика / Probability Theory and Mathematical Statistics | 3.0 | Залік / Final test |
| *ЗО 09* | Дискретна математика / Discrete Mathematics | 5.0 | Екзамен / Exam |
| *ЗО 10* | Програмування / Programming | | |
| *ЗО 10.1* | Програмування. Частина 1 / Programming. Part 1 | 5.0 | Екзамен / Exam |
| *ЗО 10.2* | Програмування. Частина 2 / Programming. Part 2 | 4.0 | Залік / Final test |
| *ЗО 11* | Алгебра та геометрія / Algebra and Geometry | 5.0 | Екзамен / Exam |
| *ЗО 12* | Вступ до кібернетичної безпеки / Introduction to cyber security | 4.0 | Залік / Final test |
| *ЗО 13* | Основи комп’ютерних мереж / Basics of computer networks | 4.0 | Залік / Final test |
| *ЗО 14* | Архітектура комп’ютерних систем / Architecture of computer systems | 5.0 | Екзамен / Exam |
| *ЗО 15* | Операційні системи / Operating Systems | 5.0 | Екзамен / Exam |
| *ЗО 16* | Криптографія та стеганографія / Cryptography and steganography | 5.0 | Залік / Final test |
| *ЗО 17* | Комплексні системи захисту інформації: проектування, впровадження, супровід / Complex information protection systems: design, implementation, support | 4.0 | Залік / Final test |
| *ЗО 18* | Управління інформаційною безпекою / Information security management | 5.0 | Екзамен / Exam |
| *ЗО 19* | Англійська мова професійного спрямування / English for Professional Purposes | 5.0 | Залік / Final test |
| *ЗО 20* | Філософські основи наукового пізнання / Philosophical Foundations of Scientific Knowledge | 2.0 | Залік / Final test |
| *ЗО 21* | Правові основи інформаційної безпеки / Legal Foundations of Information Security | 2.0 | Залік / Final test |
| *ЗО 24* | Базова загальновійськова підготовка / Basic General Military Training | | |
| *ЗО 24.1* | Практична підготовка базової загальновійськової підготовки / Practical Course of Basic General Military Training | 7.0 | Залік / Final test |

| Код/Code | Освітні компоненти програми/Components | Кредитів ЄКТС/ECTS credits | Форма підсумкового контролю / Final control form |
|---|---|---|---|
| *ЗО 24.2* | Теоретична підготовка базової загальновійськової підготовки / Цивільний захист, оборона та патріотичне виховання / Theoretical Course of Basic General Military Training / Civil Protection, Defence and Patriotic Education | 3.0 | Залік / Final test |
| Обов’язкові компоненти циклу професійної підготовки /Professional training cycle | | | |
| *ПО 01* | Теорія функцій комплексної змінної /<br>Theory of Functions of a Complex Variable | 4.0 | Залік / Final test |
| *ПО 02* | Електроакустичні пристрої /<br>Electroacoustic devices | 4.0 | Залік / Final test |
| *ПО 03* | Основи теорії кіл /<br>Fundamentals of Circuits Theory | 6.0 | Екзамен / Exam |
| *ПО 04* | Теорія сигналів /<br>Theory of signals | 5.0 | Екзамен / Exam |
| *ПО 05* | Теорія сигналів. Курсова робота /<br>Theory of signals. Coursework | 1.0 | Залік / Final test |
| *ПО 06* | Аналогова схемотехніка /<br>Analog circuitry | 5.0 | Екзамен / Exam |
| *ПО 07* | Цифрова схемотехніка /<br>Digital circuitry | 5.0 | Екзамен / Exam |
| *ПО 08* | Метрологія та вимірювання /<br>Metrology and measurement | 5.0 | Екзамен / Exam |
| *ПО 09* | Системи передавання та приймання інформації /<br>Information transmission and reception systems | 5.0 | Екзамен / Exam |
| *ПО 10* | Системи передавання та приймання інформації. Курсова робота /<br>Information transmission and reception systems. Coursework | 1.0 | Залік / Final test |
| *ПО 11* | Антени і поширення електромагнітних хвиль /<br>Antennas and the propagation of electromagnetic waves | 5.0 | Екзамен / Exam |
| *ПО 12* | Методи та засоби технічного захисту інформації /<br>Methods and means of technical information protection | 5.0 | Екзамен / Exam |
| *ПО 13* | Телекомунікаційні системи і мережі /<br>Telecommunication systems and networks | 5.0 | Екзамен / Exam |
| *ПО 14* | Технічні засоби охорони об’єктів /<br>Technical means of protection of objects | 6.0 | Екзамен / Exam |
| *ПО 15* | Технічні засоби охорони об’єктів. Курсова робота /<br>Technical means of protection of objects. Coursework | 1.0 | Залік / Final test |
| *ПО 16* | Основи стандартизації в галузі інформаційної безпеки /<br>Basics of standardization in the field of information security | 4.0 | Залік / Final test |
| *ПО 17* | Переддипломна практика /<br>Pre-diploma Practice | 6.0 | Залік / Final test |
| *ПО 18* | Дипломне проектування /<br>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 /<br>Educational Component 1 from GU-Catalogue | 2.0 | Залік / Final test |
| *ЗВ 02* | Освітній компонент 2 ЗУ-Каталогу /<br>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 /<br>Educational Component 1 from P-Catalogue | 4.0 | Залік / Final test |
| *ПВ 02* | Освітній компонент 2 Ф-каталогу /<br>Educational Component 2 from P-Catalogue | 4.0 | Залік / Final test |
| *ПВ 03* | Освітній компонент 3 Ф-каталогу /<br>Educational Component 3 from P-Catalogue | 4.0 | Залік / Final test |
| *ПВ 04* | Освітній компонент 4 Ф-каталогу /<br>Educational Component 4 from P-Catalogue | 4.0 | Залік / Final test |
| *ПВ 05* | Освітній компонент 5 Ф-каталогу /<br>Educational Component 5 from P-Catalogue | 4.0 | Залік / Final test |
| *ПВ 06* | Освітній компонент 6 Ф-каталогу /<br>Educational Component 6 from P-Catalogue | 4.0 | Залік / Final test |

| Код/Code | Освітні компоненти програми/Components | Кредитів ЄКТС/ECTS credits | Форма підсумкового контролю / Final control form |
|---|---|---|---|
| *ПВ 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: | | 180 | |
| ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ / TOTAL VOLUME OF THE EDUCATIONAL PROGRAMME | | 240 | |

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



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

Атестація  здобувачів вищої освіти за освітньо-професійною програмою «Системи технічного захисту інформації» здійснюється у формі виконання єдиного державного кваліфікаційного іспиту та публічного захисту кваліфікаційного проекту/роботи. Атестація завершується видачею документу встановленого зразка про присвоєння кваліфікації бакалавра з кібербезпеки та захисту інформації.

На атестацію виноситься сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання. До атестації допускаються студенти, які виконали всі вимоги програми підготовки.

Кваліфікаційна робота перевіряється на плагіат та після захисту розміщується в репозиторії науково-технічної бібліотеки університету для вільного доступу.

Certification of higher education applicants under the educational and professional program "Systems of technical protection of information" is carried out in the form of a unified state qualification exam and public defense of a qualification project/work. The attestation ends with the issuance of a document of the established model on the awarding of the bachelor's qualification in cyber security and information protection.

The totality of knowledge, abilities, skills, and other competencies acquired by a person during the training process is submitted to the certification. Students who have fulfilled all the requirements of the training program are admitted to attestation.

The qualification work is checked for plagiarism and after protection is placed in the repository of the scientific and technical library of the university for free access.

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

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