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

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

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

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

СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ
SYSTEMS OF TECHNICAL PROTECTION OF INFORMATION

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА / PROFESSIONAL EDUCATIONAL PROGRAMME

ЄДЕБО ID: ***57887***

Перший (бакалавський) рівень вищої освіти
Спеціальність: 125 Кібербезпека та захист інформації
Галузь знань: 12 - Інформаційні технології
Кваліфікація: бакалавр з кібербезпеки та захисту інформації

The first (bachelor) level of higher education
Speciality: 125 Cyber Security and Information protection
Knowledge branch: 12 - Information Technology
Qualification: Bachelor of Cybersecurity and Information Protection

Введено в дію з 2024/2025 н.р.
наказом ректора №_____ від 10.06 2024 р.
НОД/434/24

Enacted since 2024/2025 academic year
by rector's order No._____ of 10.06 2024
НОД/434/24

Київ/Kyiv
2024

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

ПРЕАМБУЛА/PREAMBLE

РОЗРОБЛЕНО/ELABORATED:

Керівник групи/Team leader:

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 групи/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 к.т.н., доцент, доцент кафедри інформаційної безпеки	Dmytro PROGONOV PhD, Associate Professor, Professor of the department of information security

ПОГОДЖЕНО/AGREED:

Науково-методична комісія університету зі спеціальності 125 Кібербезпека та захист інформації (протокол № 3 від «07» 05. 2024 р.)/ The Scientific and Methodological Commission of the University on speciality 125 Cybersecurity and information protection (minutes of meeting № 3 of 07.05 2024)

Голова НМКУ-125/Chairman of the SMCU-125

_____Дмитро ЛАНДЕ/ Dmytro LANDE

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

Голова Методичної ради/Chairman of the Methodological Council

_____Анатолій МЕЛЬНИЧЕНКО / Anatolii MELNYCHENKO

ВРАХОВАНО/CONSIDERED:

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
технологійДержавної служби
з надзвичайних ситуацій

Representatives of student organizations

Зібаров Дмитро
в.о. голови Профбюро НН ФТІ,
студент 4 курсу бакалаврату
за спеціальністю 125
Кібербезпека та захист
інформації

Жуковський Станіслав
студент 4 курсу бакалаврату
за спеціальністю 125
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

Dmytro ZIBAROV
ActingHead of the Professional
Bureau of the NN IPT,
a 4th-year undergraduate
student in the specialty 125
Cybersecurity and Information
Protection

Stanislav ZHYKOVSKY
4th year undergraduate
student in the specialty 125
Cyber security and information
protection

Еволюція ОП/Evolution of the EP

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 проектноїгрупи 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 ПостановуКабінету Міністрів України від 24 березня 2021 р. № 365 «Про внесення змін до постанови Кабінету Міністрів України від 30 грудня 2015 р. № 1187 Про затвердженняЛіцензійних 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 якимиздійснюється підготовка здобувачів вищої освіти” Внесено зміни у склад стейкхолдерів.

Актуальна редакція ОПП підготовлена у 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.

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 EPPortunities 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.

The current version of the EPP was prepared in 2024. Changes have been made to the list of educational components related to cycles of general and professional training. In particular, the number of credits for educational components, the study of which ends with a credit or an exam, has been increased. Educational components "Information technologies", "Algebra and geometry 2", "Fundamentals of modeling acoustic signal processing systems", "Technical protection of

information" 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 to the standard of higher education in the specialty 125 "Cybersecurity" of the field of knowledge 12 "Information technologies" for the first (bachelor) level of higher education, approved by the order of the Ministry of Education and Science of Ukraine dated 04.10.2018 No. 1074, are taken into account.

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ/ EDUCATIONAL PROGRAMME PROFILE

1 – Загальна інформація/General information		
Повна назва ЗВО та навчального підрозділу/Full name of Higher education institution and faculty/institute	Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Навчально-науковий фізико-технічний інститут	National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Educational and Research Institute of Physics and Technology
Ступінь вищої освіти та назва кваліфікації/Higher education degree and qualification title	Ступінь бакалавра бакалавр з кібербезпеки та захисту інформації	Bachelor Degree Bachelor of Cybersecurity and Information Protection
Офіційна назва ОП/Educational programme official title	Системи технічного захисту інформації	Systems of Technical Protection of Information
Тип диплому та обсяг ОП/Diploma type and EP scope	Диплом бакалавра, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців	Bachelor diploma, 240 credits ECTS, training period 3 years 10 months
Наявність акредитації/Prior accreditation	Акредитовано за спеціальністю, сертифікат УД 11017498 від 2023-06-07 дійсний до 2028-07-01	Accredited by MOES, cetificate No УД 11017498 from 2023-06-07 valid to 2028-07-01
Цикл, рівень ВО/Education cycle, level of HE	НРК України – 6 рівень QF-EHEA – перший цикл EQF-LLL – 6 рівень	NQF of Ukraine - 6 level QF-EHEA – 1 cycle EQF-LLL – 6 level
Передумови/Prerequisites	Наявність повної загальної середньої освіти	Complete general secondary education
Форми здобуття освіти/ Forms of Education	Очна (денна);	full-time;
Мова(и) викладання/Language (s) of instruction	Українська	Ukrainian
Інтернет-адреса розміщення ОП /URL of the educational program	https://osvita.kpi.ua/125_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. З цією метою освітня програма передбачає: 1. Фундаментальну підготовку фахівців в галузі математики, фізики, філософії природи та суспільства; 2. Гармонізовану спеціалізовану підготовку фахівців в галузі інформаційно-комунікаційних систем різної фізичної природи: від класичної термодинаміки і електродинаміки до квантової гравідинаміки і хромодинаміки; 3. Спеціалізовану гармонізовану підготовку фахівців в галузі континуальної, дискретної та квантової обробки інформації математичними та фізичними методами та засобами; 4. Гармонізовану міждисциплінарну організаційно-економічну та нормативно-правову підготовку фахівців, здатних створювати нові стартапи та успішно конкурувати на високотехнологічних ринках праці; 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. For this purpose, the educational program provides: 1. Fundamental training of specialists in the field of mathematics, physics, philosophy of nature and society; 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; 3. Specialized harmonized training of specialists in the field of continuous, discrete and quantum information processing by mathematical and physical methods and means; 4. Harmonized interdisciplinary organizational, economic and regulatory training of specialists capable of creating new startups and successfully competing in high-tech labor markets; 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: • об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології; • технології забезпечення безпеки інформації; • процеси управління інформаційною та/або кібербезпекою об’єктів, що підлягають захисту. Цілі навчання підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. Теоретичний зміст предметної області Знання • законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; • принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; • теорії, моделей та принципів управління доступом до інформаційних ресурсів; • теорії систем управління інформаційною та/або кібербезпекою; • методів та засобів виявлення, управління та ідентифікації ризиків; • методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; • методів та засобів технічного та криптографічного захисту інформації; • сучасних інформаційно-комунікаційних технологій; • сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; • автоматизованих систем проектування Методи, методики та технології: • Методи, методики та інформаційно-комунікаційні технології ті інші технології забезпечення інформаційної та/або кібербезпеки. Інструменти та обладнання: • системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/або кібербезпеки; • сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.	Objects of professional activity of graduates: • objects of informatization, including computer, automated, telecommunication, information, information-analytical, information-telecommunication systems, information resources and technologies; • information security technologies; • information and/or cyber security management processes of objects subject to protection. The purpose of training is to train specialists who are able to use and implement information and/or cyber security technologies. Theoretical content of the subject area Knowledge • the legislative, regulatory and legal framework of Ukraine and the requirements of relevant international standards and practices regarding the implementation of professional activities; • principles of supporting information and/or cyber security systems and complexes; • theories, models and principles of managing access to information resources; • theories of information and/or cyber security management systems; • methods and means of detection, management and identification of risks; • methods and means of assessment and ensuring the required level of information security; • methods and means of technical and cryptographic protection of information; • modern information and communication technologies; • modern hardware and software of information and communication technologies; • automated design systems Methods, techniques and technologies: • Methods, techniques and information and communication technologies and other technologies for ensuring information and/or cyber security. Tools and equipment: • systems of development, provision, monitoring and control of information and/or cyber security processes; • modern hardware and software of information and communication technologies.
Орієнтація ОП/Aspect	
Освітньо-професійна	Educational professional
Основний фокус ОП/Main focus	

Основні фокуси програми: 1. Посилена підготовка в галузі дискретної математики та квантової інформатики; 2. Посилена підготовка в галузі механіки, електроніки, радіотехніки, акустики, оптоелектроніки; 3. Посилена підготовка в галузі дискретної обробки інформації логіко-математичними методами та фізико-технічними засобами; 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; 5. Посилена підготовка в галузі міждисциплінарного системного аналізу з метою створення комплексних систем захисту інформаційних потоків у комунікаційних мережах; 6. Силабуси та методичне забезпечення підготовки здобувачів вищої освіти щорічно переглядаються з метою врахування нових науково-технологічних здобутків у галузі кібернетичної безпеки; 7. Широке залучення здобувачів вищої освіти до участі у провідних міжнародних конференціях в галузі кібернетичної безпеки; 8. Проведення щорічних конференцій та олімпіад з нових напрямків кібернетичної безпеки з метою навчання здобувачів вищої освіти розробці індивідуальних стартапів на етапі підготовки кваліфікаційної роботи. Ключові слова: кібернетична безпека, технічні засоби захисту інформації, технічний аудит, проектування та створення комплексів технічного захисту інформації	The main focuses of the program: 1. Enhanced training in the field of discrete mathematics and quantum informatics; 2. Enhanced training in mechanics, electronics, radio engineering, acoustics, optoelectronics; 3. Enhanced training in the field of discrete processing of information using logical-mathematical methods and physical-technical means; 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; 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; 6. Syllabuses and methodological support for the training of higher education applicants are revised annually in order to take into account new scientific and technological achievements in the field of cyber security; 7. Wide involvement of higher education students in participation in leading international conferences in the field of cyber security; 8. 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. Keywords: cyber security, technical means of information protection, technical audit, design and creation of technical information protection complexes
Особливості ОП/Features	
1. Перехід від стандартних методів класичної математики та класичної фізики до квантово-механічних та квантово-обчислювальних напрямків розвитку сучасної математичної фізики; 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); 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; 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; 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); 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; 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	
Відповідно до Державного класифікатору професій ДК 003:2010 зі Зміною №10 випускники можуть працювати на посадах, що відповідають класифікаційним угрупованням: 2139.2 фахівець з технічного захисту інформації 3121 Фахівець з інформаційних технологій. 3139 Фахівець із організації захисту інформації з обмеженим доступом; Фахівець із організації інформаційної безпеки 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.	According to the State Classifier of Professions DK 003:2010 with Amendment No. 10, graduates can work in positions corresponding to the classification groups: 2139.2 specialist in technical information protection 3121 Specialist in information technologies. 3139 Specialist in the organization of information protection with limited access; Specialist in the organization of information security 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	Continuation of education at the second (master's) level of higher education
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 та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризуються комплексністю та неповною визначеністю умов		The ability to solve complex specialized tasks and practical problems in the field of ensuring information security and/or cyber security, which are characterized by complexity and incomplete determination of conditions
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 професійно спілкуватися державною та іноземною мовами як усно, так і письмово.	Ability to communicate professionally in national and foreign languages both orally and in writing
ЗК 04	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.	Ability to identify, pose and solve problems in a professional manner
ЗК 05	Здатність до пошуку, оброблення та аналізу інформації.	Ability to search, process and analyze information
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 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 08	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
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 до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.	Ability to use software and software-hardware complexes of information protection means in information and telecommunication (automated) systems

ФК 04	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 05	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 06	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 07	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 08	Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.	Ability to carry out incident management procedures, conduct investigations, provide them with an assessment
ФК 09	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 10	Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.	Ability to apply methods and means of cryptographic and technical protection of information at objects of information activity
ФК 11	Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	The ability to monitor the functioning of information, information and telecommunication (automated) systems in accordance with the established policy of information and/or cyber security
ФК 12	Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.	The ability to analyze, detect and evaluate possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established policy of information and/or cyber security
ФК 13	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 14	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 15	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	Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.	Apply knowledge of state and foreign languages in order to ensure the effectiveness of professional communication
ПРН 02	Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.	Organize one's own professional activity, choose optimal methods and ways of solving complex specialized tasks and practical problems in professional activity, evaluate their effectiveness
ПРН 03	Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.	Use the results of independent search, analysis and synthesis of information from various sources for the effective solution of specialized tasks for professional activity
ПРН 04	Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем 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 problems in professional activity, which are characterized by complexity and incomplete determination of conditions, be responsible for the decisions made
ПРН 05	Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.	Adapt in the conditions of frequent changes in the technologies of professional activity, predict the final result
ПРН 06	Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.	Critically understand the main theories, principles, methods and concepts in education and professional activity
ПРН 07	Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.	Act on the basis of the legislative and regulatory framework of Ukraine and the requirements of relevant standards, including international ones in the field of information and/or cyber security
ПРН 08	Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.	Prepare proposals for regulatory acts on ensuring information and/or cyber security
ПРН 09	Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.	Implement processes based on national and international standards for detection, identification, analysis and response to information and/or cyber security incidents
ПРН 10	Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.	Perform analysis and decomposition of information and telecommunications systems
ПРН 11	Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах.	Perform analysis of connections between information processes on remote computer systems
ПРН 12	Розробляти моделі загроз та порушника.	Develop threat and intruder models
ПРН 13	Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.	Analyze projects of information and telecommunication systems based on standardized technologies and data transmission protocols
ПРН 14	Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.	Solve the task of protecting programs and information processed in information and telecommunication systems by means of hardware and software and evaluate the effectiveness of the quality of the decisions made

ПРН 15	Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.	Use modern software and hardware of information and communication technologies
ПРН 16	Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.	Implement complex information protection systems in the automated systems (AS) of the organization (enterprise) in accordance with the requirements of regulatory and legal documents
ПРН 17	Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.	To ensure the processes of protection and functioning of information and telecommunication (automated) systems based on practices, skills and knowledge regarding structural (structural-logical) schemes, network topology, modern architectures of information resources with a reflection of relationships and information flows , processes for internal and remote components.
ПРН 18	Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.	Use software and software-hardware protection complexes information resources
ПРН 19	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах	Apply protection theories and methods to ensure information security in information and telecommunication systems
ПРН 20	Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.	To ensure the functioning of special software for the protection of information from destructive software influences, destructive codes in information and telecommunication systems
ПРН 21	Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних системах.	Solve tasks of provision and support (including: review, testing, accountability) of the access control system in accordance with the established security policy in information and information and telecommunication systems
ПРН 22	Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.	To solve the problems of management of procedures of identification, authentication, authorization of processes and users in information and telecommunication systems in accordance with the established policy of information and/or cyber security
ПРН 23	Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.	Implement measures to prevent unauthorized access to information resources and processes in information and information and telecommunication (automated) systems
ПРН 24	Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).	Solve the problems of managing access to information resources and processes in information and information and telecommunications (automated) systems based on access control models (mandatory, discretionary, role-playing)

ПРН 25	Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.	Ensure the introduction of accountability of the access management system to electronic information resources and processes in information and information and telecommunication (automated) systems using logs registration of events, their analysis and established protection procedures
ПРН 26	Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.	Implement measures and ensure the implementation of processes of prevention of unauthorized access and protection of information, information and telecommunication (automated) systems based on the reference model interaction of open systems
ПРН 27	Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.	Solve the problems of data flow protection in information, information and telecommunication (automated) systems
ПРН 28	Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.	Analyze and evaluate the effectiveness and level of security of resources of different classes in information and information and telecommunication (automated) systems during tests in accordance with the established policy of information and/or cyber security
ПРН 29	Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційних та інформаційно-телекомунікаційних системах, ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів	To evaluate the possibility of realizing potential threats to information processed in information and information and telecommunication systems, the effectiveness of the use of protective equipment complexes in the conditions of the realization of threats of various classes
ПРН 30	Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.	Assess the possibility of unauthorized access to elements of information and telecommunication systems
ПРН 31	Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.	Apply security theories and methods to ensure element security information and telecommunication systems
ПРН 32	Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.	Solve the tasks of managing the processes of restoring the normal functioning of information and telecommunication systems using backup procedures in accordance with the established security policy
ПРН 33	Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.	To solve the problems of ensuring the continuity of business processes of the organization on the basis of risk theory
ПРН 34	Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.	Participate in the development and implementation of an information security and/or cyber security strategy in accordance with the goals and objectives of the organization

ПРН 35	Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.	Solve the tasks of providing and supporting complex information protection systems, as well as countering unauthorized access to information resources and processes in information and information-telecommunication (automated) systems in accordance with the established policy of information and/or cyber security
ПРН 36	Виявляти небезпечні сигнали технічних засобів.	Detect dangerous signals of technical means
ПРН 37	Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації	Measure the parameters of dangerous and interfering signals during the instrumental control of information protection processes and determine the effectiveness of information protection against leakage through technical channels in accordance with the requirements of regulatory documents of the technical information protection system
ПРН 38	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації	Interpret the results of special measurements using technical means, control of the characteristics of information and telecommunication systems in accordance with the requirements of regulatory documents systems of technical protection of information
ПРН 39	Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах	Carry out attestation (based on accounting and survey) of regime territories (zones), premises, etc. under the conditions of compliance with the secrecy regime, recording the results in the relevant documents
ПРН 40	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації	Interpret the results of special measurements using technical means, control of ITS characteristics in accordance with the requirements of regulatory documents of the technical information protection system
ПРН 41	Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур	Ensure the continuity of the event and incident logging process based on automated procedures
ПРН 42	Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки	Implement the processes of detection, identification, analysis and response to information and/or cyber security incidents
ПРН 43	Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів	Apply national and international regulatory acts in the field of information security and/or cyber security to investigate incidents
ПРН 44	Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами	To solve the problems of ensuring the continuity of the organization's business processes on the basis of risk theory and the established information security management system, in accordance with domestic and international requirements and standards
ПРН 45	Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів	Apply different classes of information security and/or cyber security policies based on risk-based access control to information assets

ПРН 46	Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах	Analyze and minimize the risks of information processing in information and telecommunication systems
ПРН 47	Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації	Solve the problems of protecting information processed in information and telecommunication systems using modern methods and means of cryptographic protection of information
ПРН 48	Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах	Implement and support intrusion detection systems and use cryptographic protection components to ensure the required level of information security in information and telecommunication systems
ПРН 49	Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах	Ensure the proper functioning of the monitoring system of information resources and processes in information and telecommunication systems
ПРН 50	Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення втрогнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних)	Ensure the functioning of software and software-hardware complexes for detecting intrusions of various levels and classes (statistical, signature, statistical-signature)
ПРН 51	Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах	Maintain operational efficiency and ensure configuration of intrusion detection systems in information and telecommunication systems
ПРН 52	Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах	Use tools for monitoring processes in information and telecommunication systems
ПРН 53	Вирішувати задачі аналізу програмного коду на наявність можливих загроз	Solve problems of software code analysis for the presence of possible threats
ПРН 54	Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні	To be aware of the values of 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
ПРН 55	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 56	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 57	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

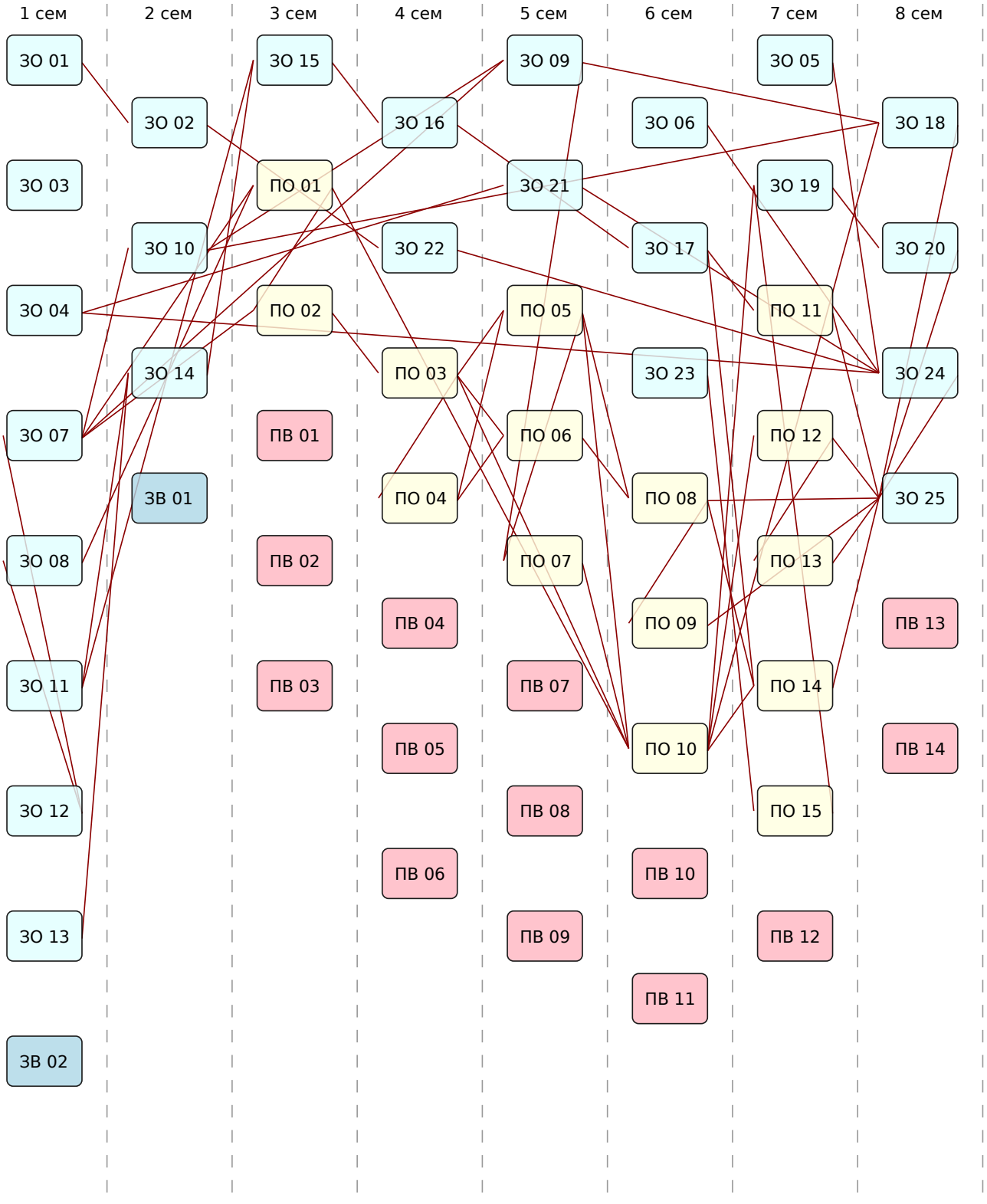
8 – Ресурсне забезпечення реалізації програми/ Resource provision for programme implementation	
Кадрове забезпечення/Staffing	
Відповідно до кадрових вимог щодо забезпечення провадження освітньої діяльності для відповідного рівня ВО, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р.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

2. ПЕРЕЛІК КОМПОНЕНТІВ ОСВІТНЬОЇ ПРОГРАМИ/COMPONENTS of EDUCATIONAL PROGRAMME

Код/Code	Освітні компоненти програми/Components	Кредитів ЄКТС/ECTS credits	Форма підсумкового контролю/Final control measure form
НОРМАТИВНІ освітні компоненти/Required (standard) components			
Обов’язкові компоненти циклу загальної підготовки/General training cycle			
ЗО 01	Українська мова за професійним спрямуванням / Ukrainian Language 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 a Healthy Lifestyle	3.0	Залік / Final test
ЗО 04	Практичний курс іноземної мови / Practical Foreign Language Course		
ЗО 04.1	Практичний курс іноземної мови. Частина 1 / Practical Foreign Language Course. Part 1	3.0	Залік / Final test
ЗО 04.2	Практичний курс іноземної мови. Частина 2 / Practical Foreign Language Course. Part 2	3.0	Залік / Final test
ЗО 05	Основи економіки / Foundations of Economics	2.0	Залік / Final test
ЗО 06	БЖД та цивільний захист / Safety of Life and Civil Defence	2.0	Залік / Final test
ЗО 07	Математичний аналіз / Mathematical Analysis		
ЗО 07.1	Математичний аналіз. Частина 1 / Mathematical Analysis. Part 1	6.0	Екзамен / Exam
ЗО 07.2	Математичний аналіз. Частина 2 / Mathematical Analysis. Part 2	6.0	Екзамен / Exam
ЗО 08	Фізика / Physics		
ЗО 08.1	Фізика. Частина 1 / Physics. Part 1	5.0	Залік / Final test
ЗО 08.2	Фізика. Частина 2 / Physics. Part 2	6.0	Екзамен / Exam
ЗО 09	Теорія ймовірності та математична статистика / Probability Theory and Mathematical Statistics	3.0	Залік / Final test
ЗО 10	Дискретна математика / Discrete Mathematics	5.0	Екзамен / Exam
ЗО 11	Програмування / Programming		
ЗО 11.1	Програмування. Частина 1 / Programming. Part 1	5.0	Екзамен / Exam
ЗО 11.2	Програмування. Частина 2 / Programming. Part 2	4.0	Залік / Final test
ЗО 12	Алгебра та геометрія / Algebra and Geometry	5.0	Екзамен / Exam
ЗО 13	Вступ до кібернетичної безпеки / Introduction to cyber security	4.0	Залік / Final test
ЗО 14	Основи комп’ютерних мереж / Basics of computer networks	4.0	Залік / Final test
ЗО 15	Архітектура комп’ютерних систем / Architecture of computer systems	4.0	Екзамен / Exam
ЗО 16	Операційні системи / Operating Systems	5.0	Екзамен / Exam
ЗО 17	Системна інженерія / Systems Engineering	5.0	Екзамен / Exam
ЗО 18	Криптографія та стеганографія / Cryptography and steganography	4.0	Залік / Final test
ЗО 19	Комплексні системи захисту інформації: проектування, впровадження, супровід / Complex information protection systems: design, implementation, support	4.0	Залік / Final test
ЗО 20	Управління інформаційною безпекою / Information security management	5.0	Екзамен / Exam
ЗО 21	Практичний курс іноземної мови професійного спрямування / Practical Foreign Language Course for Professional Purposes		
ЗО 21.1	Практичний курс іноземної мови професійного спрямування. Частина 1 / Practical Foreign Language Course for Professional Purposes. Part 1	3.0	Залік / Final test
ЗО 21.2	Практичний курс іноземної мови професійного спрямування. Частина 2 / Practical Foreign Language Course for Professional Purposes. Part 2	3.0	Екзамен / Exam
ЗО 22	Філософські основи наукового пізнання / Philosophical Foundations of Scientific Knowledge	2.0	Залік / Final test
ЗО 23	Інформаційна безпека / Information Security	2.0	Залік / Final test
ЗО 24	Переддипломна практика / Pre-diploma Practice	6.0	Залік / Final test
ЗО 25	Дипломне проектування / Bachelor Thesis	6.0	Захист / Defence
Обов’язкові компоненти циклу професійної підготовки /Professional training cycle			
ПО 01	Фізичний лабораторний практикум / Physical laboratory practice	4.0	Залік / Final test
ПО 02	Основи теорії кіл / Fundamentals of Circuits Theory	6.0	Екзамен / Exam

Код/Code	Освітні компоненти програми/Components	Кредитів ЄКТС/ECTS credits	Форма підсумкового контролю/Final control measure form
ПО 03	Теорія сигналів / Theory of signals	7.0	Екзамен / Exam
ПО 04	Теорія сигналів. Курсова робота / Theory of signals. Coursework	1.0	Залік / Final test
ПО 05	Аналогова схемотехніка / Analog circuitry	4.0	Залік / Final test
ПО 06	Цифрова схемотехніка / Digital circuitry	5.0	Екзамен / Exam
ПО 07	Метрологія та вимірювання / Metrology and measurement	5.0	Екзамен / Exam
ПО 08	Системи передавання та приймання інформації / Information transmission and reception systems	6.0	Екзамен / Exam
ПО 09	Системи передавання та приймання інформації. Курсова робота / Information transmission and reception systems. Coursework	1.0	Залік / Final test
ПО 10	Методи та засоби технічного захисту інформації / Methods and means of technical information protection	4.0	Залік / Final test
ПО 11	Телекомунікаційні системи і мережі / Telecommunication systems and networks	4.0	Екзамен / Exam
ПО 12	Технічні засоби охорони об’єктів / Technical means of protection of objects	5.0	Екзамен / Exam
ПО 13	Технічні засоби охорони об’єктів. Курсова робота / Technical means of protection of objects. Coursework	1.0	Залік / Final test
ПО 14	Проектування систем технічного захисту інформації / Design of technical information protection systems	4.0	Залік / Final test
ПО 15	Теоретичні основи захисту інформації / Theoretical foundations of information protection	4.0	Залік / Final test
ВИБІРКОВІ освітні компоненти/Elective components			
Вибіркові компоненти циклу загальної підготовки/General training cycle			
ЗВ 01	Освітній компонент 1 ЗУ-Каталогу / Educational component 1 GU-Catalogue	2.0	Залік / Final test
ЗВ 02	Освітній компонент 2 ЗУ-Каталогу / Educational component 2 GU-Catalogue	2.0	Залік / Final test
Вибіркові компоненти циклу професійної підготовки/Professional training cycle			
ПВ 01	Освітній компонент 1 Ф-Каталогу / Educational Component 1 from P-Catalogue	4.0	Залік / Final test
ПВ 02	Освітній компонент 2 Ф-каталогу / Educational Component 2 from P-Catalogue	4.0	Залік / Final test
ПВ 03	Освітній компонент 3 Ф-каталогу / Educational Component 3 from P-Catalogue	4.0	Залік / Final test
ПВ 04	Освітній компонент 4 Ф-каталогу / Elective Educational Component 4 from P-Catalogue	4.0	Залік / Final test
ПВ 05	Освітній компонент 5 Ф-каталогу / Elective Educational Component 5 from P-Catalogue	4.0	Залік / Final test
ПВ 06	Освітній компонент 6 Ф-каталогу / Elective Educational Component 6 from P-Catalogue	4.0	Залік / Final test
ПВ 07	Освітній компонент 7 Ф-каталогу / Elective Educational Component 7 from P-Catalogue	4.0	Залік / Final test
ПВ 08	Освітній компонент 8 Ф-каталогу / Elective Educational Component 8 from P-Catalogue	4.0	Залік / Final test
ПВ 09	Освітній компонент 9 Ф-каталогу / Elective Educational Component 9 from P-Catalogue	4.0	Залік / Final test
ПВ 10	Освітній компонент 10 Ф-каталогу / Elective Educational Component 10 from P-Catalogue	4.0	Залік / Final test
ПВ 11	Освітній компонент 11 Ф-каталогу / Elective Educational Component 11 from P-Catalogue	4.0	Залік / Final test
ПВ 12	Освітній компонент 12 Ф-каталогу / Elective Educational Component 12 from P-Catalogue	4.0	Залік / Final test
ПВ 13	Освітній компонент 13 Ф-каталогу / Elective Educational Component 13 from P-Catalogue	4.0	Залік / Final test
ПВ 14	Освітній компонент 14 Ф-каталогу / Elective Educational Component 14 from P-Catalogue	4.0	Залік / Final test
Загальний обсяг нормативних компонентів ОП/Total scope of the required components:		180	
Загальний обсяг вибіркових компонентів ОП/Total scope of the elective components:		60	
Обсяг освітніх компонентів, що забезпечують здобуття компетентностей визначених СВО/Total scope of the educational components aimed at acquisition of competencies specified in the Higher Education Standard:		180	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ/TOTAL SCOPE OF THE EDUCATIONAL PROGRAMME		240	

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



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

Атестація здобувачів вищої освіти за 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.

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

	ЗО 01	ЗО 02	ЗО 03	ЗО 04	ЗО 05	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 22	ЗО 23	ЗО 24	ЗО 25	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
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	
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
ЗК 03	X			X				X												X			X	X	X														
ЗК 04		X					X		X	X		X		X	X		X	X	X				X	X	X					X	X	X	X	X	X	X			X
ЗК 05	X	X		X	X		X				X		X			X							X	X	X											X		X	
ЗК 06						X					X		X								X	X	X	X	X														
ЗК 07		X	X		X	X							X								X		X	X	X														
ЗК 08	X																																						
ФК 01					X						X		X					X	X				X	X	X														
ФК 02	X			X			X		X	X	X	X		X	X	X	X						X	X	X							X					X	X
ФК 03														X	X		X		X				X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X
ФК 04																							X	X	X														X
ФК 05																			X				X	X	X								X	X		X			X
ФК 06								X															X	X	X					X	X					X			
ФК 07							X	X											X				X	X	X												X	X	X	
ФК 08																							X	X	X										X				
ФК 09											X												X	X	X										X				X	
ФК 10							X	X	X	X		X						X					X	X	X										X		X	X		
ФК 11											X			X		X							X	X	X											X				
ФК 12					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	X	X	X	X	X	X	X	X	X					
ФК 14													X	X				X	X				X	X	X	X	X	X	X			X	X	X					X
ФК 15														X		X							X	X	X	X	X	X	X	X	X	X	X	X					

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

	ЗО 01	ЗО 02	ЗО 03	ЗО 04	ЗО 05	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 22	ЗО 23	ЗО 24	ЗО 25	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
ПРН 01		X							X	X										X			X	X	X													
ПРН 02		X			X		X		X	X	X	X	X		X		X	X	X				X	X	X		X	X		X	X		X		X		X	
ПРН 03		X					X		X	X	X	X	X	X	X	X		X			X		X	X	X		X	X		X	X		X	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	X
ПРН 05		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														
ПРН 09														X	X			X				X	X	X										X				X	
ПРН 10							X		X	X	X	X		X	X	X	X	X	X				X	X	X								X	X	X			X	X
ПРН 11										X		X					X		X				X	X	X										X			X	
ПРН 12							X	X	X					X			X		X				X	X	X													X	X
ПРН 13														X					X				X	X	X											X		X	
ПРН 14														X				X	X				X	X	X										X	X		X	
ПРН 15											X			X		X							X	X	X								X	X	X	X		X	
ПРН 16																			X				X	X	X									X		X	X	X	
ПРН 17									X														X	X	X										X			X	
ПРН 18														X									X	X	X									X				X	
ПРН 19																		X	X				X	X	X									X	X			X	X
ПРН 20																							X	X											X				
ПРН 21																			X				X	X	X													X	X
ПРН 22														X				X					X	X															
ПРН 23																		X					X	X	X									X		X	X	X	
ПРН 24											X			X					X				X	X														X	X
ПРН 25																							X	X														X	X
ПРН 26														X									X	X	X									X				X	
ПРН 27														X				X					X	X	X													X	
ПРН 28									X	X		X							X				X	X	X										X			X	
ПРН 29						X													X				X	X	X									X	X			X	
ПРН 30									X										X				X	X	X									X	X	X	X	X	X
ПРН 31									X										X				X	X	X									X	X	X	X	X	
ПРН 32									X														X	X											X				
ПРН 33						X			X										X				X	X	X									X				X	
ПРН 34																	X		X				X	X										X		X	X	X	X

	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 22	ЗО 23	ЗО 24	ЗО 25	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
ПРН 35																		X	X				X	X	X									X					
ПРН 36								X															X	X		X				X	X	X	X	X	X				
ПРН 37								X															X	X		X	X	X	X	X	X	X	X	X	X				
ПРН 38								X	X														X	X		X	X	X	X	X	X	X			X		X	X	
ПРН 39																							X	X						X	X		X	X	X		X	X	
ПРН 40								X	X														X	X		X	X	X	X	X	X	X			X		X	X	
ПРН 41														X									X	X															
ПРН 42														X				X					X	X										X		X	X		
ПРН 43																							X	X	X														
ПРН 44					X														X				X	X	X													X	
ПРН 45																							X	X	X														X
ПРН 46																			X				X	X	X														
ПРН 47	X			X										X				X					X	X	X														
ПРН 48														X				X					X	X															
ПРН 49																							X	X										X				X	
ПРН 50														X									X	X										X				X	
ПРН 51														X									X	X										X		X	X	X	
ПРН 52																							X	X	X													X	
ПРН 53																		X					X	X	X														
ПРН 54			X		X	X																	X	X															
ПРН 55									X	X	X				X	X							X	X		X	X	X	X	X	X	X	X	X					
ПРН 56																							X	X		X	X	X	X			X	X	X	X				
ПРН 57									X														X	X		X	X	X	X	X	X	X	X	X	X				