National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic 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 IICHENKO

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

БЕЗПЕКА ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ
SECURITY OF STATE INFORMATION RESOURCTS

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА/
EDUCATIONAL PROFESSIONAL PROGRAMME

Перший (бакалаврський) 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 Cybersecurity and information protection
Knowledge branch: 12 Information technologies
Qualification: Bachelor's degree in cybersecurity and information protection

ID 57879

Введено в дію з 2024/25 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:

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

Члени групи/Team members:

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

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

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

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

ПОГОДЖЕНО/AGREED:

Науково-методична комісія університету зі спеціальності 125 Кібербезпека та захист інформації (протокол № 1 від «30» квітня 2024 р.)/ The Scientific and Methodological Commission of the University on speciality 125 Cybersecurity and information protection (minutes of meeting № 1 of 30.04 2024)

Голова НМКУ-125 (для ІСЗЗІ)/Chairman of the SMCU-125 (for ISCIP)

_____ Владислав ГОЛЬ/Vladislav HOL

Методична рада КПІ ім. Ігоря Сікорського (протокол № 7 від 09.05.24р.)/ 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/Anatoly MELNICHENKO

ЛИСТ ПОГОДЖЕННЯ / LETTER OF APPROVAL

Безпека державних інформаційних ресурсів / Security of state information resourse

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА / EDUCATIONAL PROFESSIONAL PROGRAMME

першого (бакалаврського) рівня вищої освіти / the first (bachelor) level of higher education

за спеціальністю/ speciality	**125 Кібербезпека та захист інформації / 125 Cybersecurity and information protection**
галузі знань / knowledge branch	**12 Інформаційні технології / 12 Information technologies**
Кваліфікація / Qualification	**Бакалавр з кібербезпеки та захисту інформації / Bachelor's degree in cybersecurity and information protection**

ПОГОДЖЕНО / APPROVED

Голова Державної служби спеціального зв'язку та захисту України / Head of the State Service for Special Communications and Protection of Ukraine

_____ Юрій МИРОНЕНКО / Yurii MYRONENKO

___.___.20___

ПОГОДЖЕНО / APPROVED

Директор Департаменту військової освіти і науки Міністерства оборони України / Director of the Department of Military Education and Science of the Ministry of Defense of Ukraine

_____ Володимир МІРНЕНКО / Volodymyr MIRNENKO

___.___.20___

ВРАХОВАНО/CONSIDERED:

1. Постанову Кабінету Міністрів України від 15 грудня 1997 року № 1410 "Про трансформацію системи військової освіти" (із змінами, внесеними згідно з Постановою КМ №1490 від 30.12.2022 року. Набрала чинності від 04.01.2023). https://zakon.rada.gov.ua/laws/show/1410-97-%D0%BF#Text

2. Наказ Міністерства Оборони України від 15 лютого 2024 року № 120 "Про затвердження Положення про особливості організації освітнього процесу у вищих військових навчальних закладах Міністерства оборони України, військових навчальних підрозділах закладів вищої освіти, закладах фахової передвищої військової освіти".

3. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 23 січня 2024 року № 38.

4. Проєкт наказу МОН України «Про внесення змін до деяких стандартів вищої освіти», а саме в частині доповнення переліку загальних компетентностей 8 пунктом https://mon.gov.ua/news/mon-proponue-do-gromadskogo-obgovorennya-proekt-nakazu-pro-vsesennya-zmin-do-deyakikh-standartiv-vishchoi-osviti

1. Resolution of the Cabinet of Ministers of Ukraine of 15 December 1997 No. 1410 "On Transformation of the Military Education System"(as amended by Resolution of the Cabinet of Ministers of Ukraine No. 1490 of 30 December 2022). Entered into force on 04.01.2023). https://zakon.rada.gov.ua/laws/show/1410-97-%D0%BF#Text

2. Order of the Ministry of Defence of Ukraine dated 15 February 2024 No. 120 "On Approval of the Regulation on Peculiarities of Organisation of the Educational Process in Higher Military Educational Institutions of the Ministry of Defence of Ukraine, Military Educational Units of Higher Educational Institutions, Institutions of Professional Pre-Higher Military Education".

3. Order of the Administration of the State Service for Special Communications and Information Protection of Ukraine dated 23 January 2024 No. 38.

4. The draft order of the Ministry of Education and Science of Ukraine "On Amendments to Some Standards of Higher Education", namely, in the part of supplementing the list of general competencies with 8th points https://mon.gov.ua/news/mon-proponue-do-gromadskogo-obgovorennya-proekt-nakazu-pro-vsesennya-zmin-do-deyakikh-standartiv-vishchoi-osviti.

Освітньо-професійну програму обговорено після надходження всіх пропозицій, побажань і зауважень від здобувачів вищої освіти, випускників та стейкхолдерів і схвалено на засіданні Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського (протокол № 8/2 від 29 квітня 2024 року).

Еволюція ОП/Evolution of the EP:

***2016 рік** – започатковано ОП Безпека державних інформаційних ресурсів з метою підготовки висококваліфікованих фахівців ступеня вищої освіти бакалавр для професійної діяльності на посадах органів та підрозділів Держспецзв'язку.*

***2019 рік** – оновлення ОП з метою врахування:*

Наказу Міністерства освіти і науки України №1074 від 4 жовтня 2018 року про затвердження Стандарту вищої освіти за спеціальністю 125 "Кібербезпека" галузі знань 12 "Інформаційні технології" для першого (бакалаврського) рівня вищої освіти.

***2023 рік** – оновлення ОП з метою врахування:*

Постанови Кабінету Міністрів України від 16 грудня 2022 року № 1392 "Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти";

Наказу Міністерства Економіки України (Мінекономіки) від 29 грудня 2022 року № 5573 "Про затвердження Зміни № 11 до національного класифікатора ДК 003:2010". https://zakon.rada.gov.ua/rada/show/v5573930-22#n5*;*

Наказ Міністерства Економіки України (Мінекономіки) від 25 жовтня 2021 року № 810-21 "Про затвердження Зміни № 10 до національного класифікатора ДК 003:2010. https://zakon.rada.gov.ua/rada/show/v0810930-21#n45*;*

Постанови Кабінету Міністрів України від 19 травня 2021 року № 497 " Про атестацію здобувачів ступеня фахової передвищої освіти та ступенів вищої освіти на першому (бакалаврському) та другому (магістерському) рівнях у формі єдиного державного кваліфікаційного іспиту". https://zakon.rada.gov.ua/laws/show/497-2021-%D0%BF#Text*;*

Наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 19 серпня 2021 року № 507 "Інструкція про порядок організації проведення практичної та військово-професійної підготовки здобувачів вищої освіти в закладі освіти Державної служби спеціального зв'язку та захисту інформації України".

Були внесені зміни:

***2019 рік** – відповідно введеного Стандарту вищої освіти за спеціальністю 125 "Кібербезпека" галузі знань 12 "Інформаційні технології" для першого (бакалаврського) рівня вищої освіти.*

***2023 рік** – зміна назви спеціальності, за якою здійснюється підготовка здобувачів вищої освіти з 125 "Кібербезпека" на 125 "Кібербезпека та захист інформації".*

– зміни пов'язані з унесенням до розділу 5 "КЛАСИФІКАЦІЯ ПРОФЕСІЙ" національного класифікатора ДК 003:2010 в професійних назвах робіт унесено: фахівець з реагування на інциденти кібербезпеки, фахівець з технічного захисту інформації, фахівець з криптографічного захисту інформації, фахівець сфери захисту інформації;

– атестацію здобувачів ступеня вищої освіти на першому (бакалаврському) рівні проводити у формі єдиного державного кваліфікаційного іспиту;

– зміни пов'язані з порядком організації та проведенням навчальної практики та військового стажування для здобувачів ступеня вищої освіти на першому (бакалаврському) рівні в закладах Державної служби спеціального зв'язку та захисту інформації України.

***2016** - the educational programme Security of State Information Resources was launched to train highly qualified specialists with a bachelor's degree for professional activities in the positions of the State Special Communications Service of Ukraine.*

***2019** - update of the EP to take into account:*

Order of the Ministry of Education and Science of Ukraine No. 1074 of 4 October 2018 on approval of the Standard of Higher Education in the speciality 125 "Cybersecurity" of the field of knowledge 12 "Information Technology" for the first (bachelor's) level of higher education.

***2023** - update of the EP to take into account:*

Resolution of the Cabinet of Ministers of Ukraine dated 16 December 2022 No. 1392 "On Amendments to the List of Fields of Knowledge and Specialities in which Higher Education Applicants are Trained";

Order of the Ministry of Economy of Ukraine (Ministry of Economy) dated 29 December 2022 No. 5573 "On Approval of Amendment No. 11 to the National Classifier DK 003:2010". https://zakon.rada.gov.ua/rada/show/v5573930-22#n5*;*

Order of the Ministry of Economy of Ukraine (Ministry of Economy) dated 25 October 2021 No. 810-21 "On Approval of Amendment No. 10 to the National Classifier DK 003:2010". https://zakon.rada.gov.ua/rada/show/v0810930-21#n45*;*

Resolution of the Cabinet of Ministers of Ukraine dated 19 May 2021 No. 497 "On Certification of Applicants for Degrees of Professional Higher Education and Degrees of Higher Education at the First (Bachelor's) and Second (Master's) Levels in the Form of a Unified State Qualification Exam". https://zakon.rada.gov.ua/laws/show/497-2021-%D0%BF#Text*;*

Order of the Administration of the State Service for Special Communications and Information Protection of Ukraine dated 19 August 2021 No. 507 "Instruction on the Procedure for Organising Practical and Military Professional Training of Higher Education Applicants at an Educational Institution of the State Service for Special Communications and Information Protection of Ukraine".

Changes were made:

2019 -** in accordance with the introduction of the Standard of Higher Education in the specialty 125 "Cybersecurity" of the field of knowledge 12 "Information Technology" for the first (bachelor's) level of higher education**.

***2023 -** change of the name of the speciality in which higher education students are trained from 125 "Cybersecurity" to 125 "Cybersecurity and Information Protection".*

- amendments related to the introduction of the following professional titles in section 5 "CLASSIFICATION OF PROFESSIONS" of the national classifier DC 003:2010: specialist in response to cybersecurity incidents, specialist in technical information protection, specialist in cryptographic information protection, specialist in information protection.

- certification of applicants for higher education degrees at the first (bachelor's) level should be conducted in the form of a single state qualification exam;

- amendments related to the procedure for organising and conducting educational practice and military internships for applicants for higher education at the first (bachelor's) level in the institutions of the State Service for Special Communications and Information Protection of Ukraine.

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ/ EDUCATIONAL PROGRAMME PROFILE

1 – Загальна інформація/General information		
Повна назва ЗВО та навчального підрозділу/ Full name of HE institution and faculty/institute	Національний технічний університет України “Київський політехнічний інститут імені Ігоря Сікорського”, Інститут спеціального зв’язку та захисту інформації	National Technical University of Ukraine "Ihor Sikorsky Kyiv Polytechnic Institute", Institute of Special Communication and Information Protection
Ступінь вищої освіти та назва кваліфікації/ Higher education degree and qualification title	Ступінь ВО – бакалавр Кваліфікація – бакалавр з кібербезпеки та захисту інформації	Higher education degree - bachelor's degree Qualification title - bachelor's degree in cybersecurity and information protection
Офіційна назва ОП/ Educational programme official title	Безпека державних інформаційних ресурсів	Security of state information resources
Тип диплому та обсяг ОП/ Diploma type and EP scope	Диплом бакалавра, освітня складова 240 кредитів ЄКТС, термін навчання 3 роки і 10,5 місяців	Bachelor's degree, educational component 240 ECTS credits, duration of study 3 years and 10.5 months
Інформація про акредитацію / Accreditation information of EP	Сертифікат про акредитацію серія УД № 11017498. Галузь знань: 12 Інформаційні технології, спеціальність: 125 Кібербезпека та захист інформації у Національному технічному університеті України «Київський політехнічний інститут імені Ігоря Сікорського. Строк дії сертифікату до 1 липня 2028 року.	Certificate of accreditation series UD № 11017498. Field of knowledge: 12 Information technology, speciality: 125 Cybersecurity and information protection at the National Technical University of Ukraine ‘Igor Sikorsky Kyiv Polytechnic Institute’. The certificate is valid until 1 July 2028.
Цикл, рівень ВО/ Education cycle, level of HE	Цикл – перший цикл НРК України – 6 рівень	QF-EHEA – first cycle EQF-LLL – 6 level
Передумови/Prerequisites	Наявність повної загальної середньої освіти	Complete general secondary education

Форма здобуття освіти/ Forms of Education	Денна	full-time form
Мова(и) викладання/ Language (s) of instruction	Українська	Ukrainian
Інтернет-адреса розміщення ОП /URL of the educational program	https://osvita.kpi.ua/ (розділ “Освітні програми”)/	https://osvita.kpi.ua/ (section "Educational programs")

2 – Мета освітньої програми/Educational programme purpose

Метою освітньо-професійної програми “Безпека державних інформаційних ресурсів” є підготовка висококваліфікованих фахівців ступеня бакалавра в галузі кібербезпеки та захисту інформації, здатних самостійно розв’язувати складні спеціалізовані задачі у галузі відповідної професійної діяльності на посадах органів та підрозділів Держспецзв’язку, що передбачає здійснення розробки, впровадження й дослідження у різних галузях людської діяльності, національної економіки та виробництва в умовах: – науково-технічного прогресу та сталого розвитку суспільства; – інтернаціоналізації освіти; – урахування трансформації посадових обов’язків випускників шляхом взаємодії з Адміністрацією Держспецзв’язку; – всебічного професійного, соціального, інтелектуального та творчого розвитку особистості в освітньо-професійному середовищі. Мета освітньо-професійної програми відповідає стратегії розвитку КПІ ім. Ігоря Сікорського на 2020-2025 роки щодо формування суспільства майбутнього на засадах концепції сталого розвитку.	The purpose of the educational-professional program "Security of state information resources" is to train highly qualified bachelor's degree specialists in the field of cybersecurity and information protection, capable of independently solving complex specialized tasks in the field of relevant professional activities in the positions of bodies and units of the State Special Communications Service of Ukraine, which involves the development, implementation and research in various fields of human activity, national economy and production in the conditions: - scientific and technological progress and sustainable development of society; - internationalization of education; - taking into account the transformation of graduates' job responsibilities through cooperation with the Administration of the State Special Communications Service; - comprehensive professional, social, intellectual and creative development of the individual in the educational and professional environment. The purpose of the educational-professional program corresponds to the development strategy of Igor Sikorsky Kyiv Polytechnic Institute for 2020-2025 to form the society of the future based on the concept of sustainable development.

3 – Характеристика освітньої програми/ Educational programme characteristics

Предметна область/Subject area

Об’єкти професійної діяльності випускників: – об’єкти інформатизації, включаючи комп’ютерні, автоматизовані, комунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-комунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою об’єктів, що підлягають захисту.	Objects of professional activity of graduates: - objects of informatization, including computer, automated, communication, information, information and analytical, information and communication systems, information resources and technologies; - technologies for ensuring information security; - processes of managing information and/or cybersecurity of objects to be protected.
Цілі навчання підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки.	Learning objectives training of specialists capable of using and implementing information and/or cybersecurity technologies.
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.	Theoretical content of the subject area Knowledge - the legislative, regulatory and legal framework of Ukraine and the requirements of relevant international standards and practices for the implementation of professional activities; - principles of maintenance of information and/or cybersecurity systems and complexes; - theory, models and principles of access control to information resources; - theory of information and/or cybersecurity management systems; - methods and means of identifying, managing and identifying risks; - methods and tools for assessing and ensuring the required level of information security; - methods and means of technical and cryptographic protection of information; - modern information and communication technologies; - modern software and hardware; - information-communication technologies; - automated design systems.
Методи, методики та технології: Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/або кібербезпеки.	Methods, techniques and technologies: Methods, techniques, information and communication technologies and other technologies for ensuring information and/or cybersecurity.
Інструменти та обладнання: – системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.	Tools and equipment: - systems for developing, ensuring, monitoring and controlling information and/or cybersecurity processes; - modern software and hardware of information and communication technologies.

Орієнтація ОП/Aspect	
Освітньо-професійна	Educational – professional
Основний фокус ОП/Main focus	
Базовий фокус освітньої програми – системи та процеси кіберпростору, засоби та заходи захисту державних інформаційних ресурсів, що циркулюють в інформаційно-комунікаційних системах та на об'єктах інформаційної діяльності. Ключові слова: державні інформаційні ресурси, інформаційно-комунікаційна система, інформаційна безпека, кібербезпека, кіберзахист, технічний захист інформації, криптографічний захист інформації.	The main focus of the educational program is on cyberspace systems and processes, means and measures to protect state information resources circulating in information and communication systems and information activity facilities. Keywords: state information resources, information and communication system, information security, cybersecurity, cyber defense, technical protection of information, cryptographic protection of information.
Особливості ОП/Features	
Особливості освітньої програми полягають в наступному: – освітня програма розроблена з урахуванням вимог професійних стандартів військового фахівця Держспецзв'язку, що визначені замовником на підготовку військових фахівців Держспецзв'язку; – до викладання освітніх компонент освітньої програми залучаються фахівців Держспецзв'язку, інших навчальних закладів та провідних компаній відповідного сектору економіки; – навчальна практика проводиться в територіальних підрозділах Держспецзв'язку або в закладі освіти Держспецзв'язку науково-педагогічними працівниками закладу освіти Держспецзв'язку, як практичні заняття, відповідно до навчального плану та складається з: – військове стажування в восьмому семестрі відбувається в територіальних підрозділах Держспецзв'язку у формі індивідуальної самостійної роботи (виконання здобувачами обов'язків на первинних посадах у підрозділах Держспецзв'язку) під керівництвом науково-педагогічних працівників закладу освіти Держспецзв'язку або посадових осіб підрозділів Держспецзв'язку, на базі яких воно проводиться.	The features of the educational program are as follows: - the educational program is developed taking into account the requirements of the professional standards of the military specialist of the State Service for Special Communications and Information Protection, which are determined by the customer for the training of military specialists of the State Service for Special Communications and Information Protection; - the educational components of the educational program are taught by specialists of the State Service for Special Communications and Information Protection of Ukraine, other educational institutions and leading companies of the relevant sector of the economy; - training practice is conducted in the territorial units of the State Service for Special Communications and Information Services or in: - military internship in the eighth semester takes place in the territorial units of the State Service for Special Communications and Information Protection in the form of individual independent work (performance of duties by applicants in primary positions in the units of the State Service for Special Communications and Information Protection) under the guidance of scientific and pedagogical staff of the educational institution of the State Service for

– проведення практичних занять організовано з застосуванням сучасного обладнання Лабораторії технічного захисту інформації Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського; – підготовка здобувачів вищої освіти на першому (бакалаврському) рівні вищої освіти здійснюється у статусі студента – 1 рік, у статусі курсанта – 2 роки і 10,5 місяців.	Special Communications and Information Protection or officials of the units of the State Service for Special Communications and Information Protection, on the basis of which it is conducted. - Practical classes are organized with the use of modern equipment of the Laboratory of Technical Information Protection of the Special department No. 1 of the ISCIP of Igor Sikorsky Kyiv Polytechnic Institute; - training of applicants for higher education at the first (bachelor's) level of higher education is carried out in the status of a student - 1 year, in the status of a cadet - 2 years and 10.5 months.
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 та Зміною №11 випускники можуть працювати на посадах, що відповідають професійній назві роботи: 2139.2 Фахівець з реагування на інциденти кібербезпеки; 2139.2 Фахівець з криптографічного захисту інформації; 2139.2 Фахівець з технічного захисту інформації; 2139.2 Фахівець сфери захисту інформації. Замовником фахівців зі спеціальності 125 Кібербезпека та захист інформації виступає Державна служба спеціального зв'язку та захисту інформації України.	According to the State Classification of Occupations DK 003:2010 with Amendment No. 10 and Amendment No. 11, graduates can work in positions corresponding to the professional title of the job: 2139.2 Cybersecurity incident response specialist; 2139.2 Specialist in cryptographic information security; 2139.2 Specialist in technical information security; 2139.2 Specialist in the field of information security. The customer for specialists in the specialty 125 Cybersecurity and Information Protection is the State Service for Special Communications and Information Protection of Ukraine.
Подальше навчання/Further study	
Мають право продовжити навчання на другому (магістерському) рівні вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти.	They have the right to continue their studies at the second (master's) level of higher education. Acquisition of additional qualifications in the system of postgraduate education.
5 – Викладання та оцінювання/Teaching and assessment	
Викладання та навчання/Teaching and studying	
Проблемно-орієнтоване та студенто-центроване навчання з набуттям	Problem-based and student-centered learning with the acquisition of competencies sufficient to

компетентностей, достатніх для продукування ідей, розв'язання складних спеціалізованих задач у професійній галузі та самостійного отримання глибинних знань, яке включає: лекції, лабораторні, практичні та семінарські заняття, технології змішаного навчання, самостійну роботу з використанням науково-технічних інформаційно-літературних джерел, консультації із викладачами, проходження навчальної практики та військового стажування. Навчання закінчується складанням єдиного державного кваліфікаційного іспиту та захисту кваліфікаційної роботи/проекту.	generate ideas, solve complex specialized problems in the professional field and independently obtain in-depth knowledge, which includes: lectures, laboratory, practical and seminar classes, blended learning technologies, independent work using scientific and technical information and literary sources, consultations with teachers, internships and military internships. The program ends with a unified state qualification exam and the defense of a qualification paper/project.
Оцінювання/Assessment	
Оцінювання навчальних досягнень здобувачів вищої освіти здійснюється за рейтинговою системою оцінювання відповідно до Положення про систему оцінювання результатів навчання в КПІ ім. Ігоря Сікорського (до 100 балів) та за шкалою оцінювання Університету ("відмінно", "дуже добре", "добре", "задовільно", "достатньо" та "незадовільно") Результати навчання студента, що відображають досягнутий ним рівень компетентностей відносно очікуваних, ідентифікуються та вимірюються під час контрольних заходів (усних і письмових заліків та екзаменів, тестування тощо) за допомогою критеріїв, що корелюються з описом освітнього рівня Національної рамки кваліфікацій і характеризують співвідношення вимог до рівня компетентностей і показників оцінки за рейтинговою шкалою.	Evaluation of academic achievements of higher education students is carried out according to the rating system in accordance with the Regulations on the system of evaluation of learning outcomes in Igor Sikorsky Kyiv Polytechnic Institute (up to 100 points) and according to the University's evaluation scale ("excellent", "very good", "good", "satisfactory", "sufficient" and "unsatisfactory") The student's learning outcomes, which reflect the level of competencies achieved by him/her in relation to the expected ones, are identified and measured during control measures (oral and written tests and examinations, testing, etc.) using criteria that correlate with the description of the educational level of the National Qualifications Framework and characterize the correlation between the requirements for the level of competencies and the assessment indicators on the rating scale.
6 – Програмні компетентності/Programme competencies	
Інтегральна компетентність/Integral competence	
Здатність розв'язувати складні спеціалізовані задачі або практичні завдання у галузі кібербезпеки та захисту інформації характеризується комплексністю та невизначеністю умов, що передбачає глибоке переосмислення наявних цілісних знань та/або професійної практики.	The ability to solve complex specialized problems or practical tasks in the field of cybersecurity and information protection and is characterized by complexity and uncertainty of conditions, which requires a deep rethinking of existing holistic knowledge and/or professional practice.

Загальні компетентності (ЗК)/General competencies	
ЗК 1. Здатність застосовувати знання у практичних ситуаціях.	Ability to apply knowledge in practical situations.
ЗК 2. Знання та розуміння предметної області та розуміння професії.	Knowledge and understanding of the subject area and understanding of the profession.
ЗК 3. Здатність професійно спілкуватися державною та іноземною мовою як усно, так і письмово.	Ability to communicate professionally in the state and foreign languages, both orally and in writing.
ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.	Ability to identify, formulate and solve problems in the professional field.
ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.	Ability to search for, process and analyze information.
ЗК 6. 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.	Ability to realize one's rights and responsibilities as a member of society, to realize the values of civil (free democratic) society and the need for its sustainable development, the rule of law, human and civil rights and freedoms in Ukraine.
ЗК 7. 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.	Ability to preserve and increase 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, technology and technology, to use various types and forms of physical activity for active recreation and healthy lifestyle.
ЗК 8. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.	Ability to make decisions and act in accordance with the principle of inadmissibility of corruption and any other manifestations of dishonesty.
Фахові компетентності (ФК)/Professional competencies	
ФК 1. Здатність застосовувати законодавчу та нормативно правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної	Ability to apply the legislative and regulatory framework, as well as national and international requirements, practices and standards in order to carry out professional activities in the field of

діяльності в галузі інформаційної та/або кібербезпеки.	information and/or cybersecurity.
ФК 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.	Ability to use information-communication technologies, modern methods and models of information security and/or cybersecurity.
ФК 3. Здатність до використання програмних та програмно апаратних комплексів, засобів захисту інформації в інформаційно-комунікаційних (автоматизованих) системах.	Ability to use software and hardware complexes, information security tools in information-communication (automated) systems.
ФК 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.	Ability to ensure business continuity in accordance with the established information and/or cybersecurity policy.
ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-комунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.	Ability to ensure the protection of information processed in information-communication (automated) systems in order to implement the established information and/or cybersecurity policy.
ФК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-комунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.	The ability to restore normal operation of information, information and communication (automated) systems after threats, cyberattacks, failures and failures of various classes and origins.
ФК 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів и методів, процедур, практичних прийомів та ін.)	Ability to implement and ensure the functioning of integrated information security systems (complexes of regulatory, organisational and technical means and methods, procedures, practices, etc.)
ФК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.	Ability to implement incident management procedures, conduct investigations, and evaluate them.
ФК 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.	Ability to carry out professional activities on the basis of the implemented system management information and/or cybersecurity.

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 the objects of information activity.
ФК 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-комунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.	Ability to monitoring of functioning processes of information, information-communication (automated) systems in accordance with the established information and/or cybersecurity policy.
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.	Ability to analyze, identify and assess possible threats, vulnerabilities and destabilizing factors to the information space and information resources in accordance with the established information and/or cybersecurity policy.
ФК 13. Здатність засвоювати загальні принципи побудови та функціонування засобів та комплексів криптографічного захисту інформації, принципи, їх схемотехнічної реалізації.	Ability to master the general principles of construction and functioning of means and complexes of cryptographic information security, principles of their circuitry realization.
Фахові компетентності Блок 1. Професійний стандарт. Фахівець з реагування на інциденти кібербезпеки/Professional competences Block 1. Professional standard. Specialist in response cybersecurity incident	
ФКбл 1.1. Здатність зіставляти дані про інциденти, для визначення конкретних вразливостей та надання рекомендацій, які дозволять швидко їх усунути.	The ability to correlate incident data to identify specific vulnerabilities and provide recommendations that will allow them to be addressed quickly.
ФКбл 1.2. Здатність здійснювати збір артефактів вторгнення і використовувати виявленні дані для запобігання потенційним інцидентам кібербезпеки в межах підприємства (установи, організації). Здатність забезпечувати своєчасне виявлення, ідентифікацію та сповіщення про можливі атаки/вторгнення, аномальну діяльність і дії зловживання та відрізняти ці інциденти та події від доброякісних дій.	The ability to collect intrusion artefacts and use the data to prevent potential cybersecurity incidents within the enterprise (institution, organisation). The ability to provide timely detection, identification and notification of possible attacks/intrusions, anomalous activity and misuse and to distinguish these incidents and events from benign activities.
ФКбл 1.3. Здатність супроводжувати тематичні дослідження (процеси оцінки відповідності) засобів криптографічного захисту інформації. Здатність проводити	Ability to support case studies (conformity assessment processes) of cryptographic information security. Ability to conduct special studies of

спеціальні дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності.	information processing tools, technical means and objects of information activity.
Фахові компетентності Блоку 2. Професійний стандарт. Фахівець з криптографічного захисту інформації/Professional competences Block 2. Professional standard Specialist in cryptographic information security	
ФКбл 2.1. Здатність забезпечувати контроль (моніторінг) поточного стану рівня безпеки криптографічного захисту інформації в органі (установі, підприємстві) та оцінку його відповідності вимогам нормативних документів.	Ability to provide control (monitoring) of the current state of the level of security of cryptographic protection of information in the body (institution, enterprise) and assess its compliance with the requirements of regulatory documents.
ФКбл 2.2. Здатність аналізувати потреби та вимоги користувачів (замовників) щодо криптографічного захисту інформації з метою впровадження систем та комплексів захисту інформації.	Ability to analyse the needs and requirements of users (customers) for cryptographic protection of information in order to implement information security systems and complexes.
ФКбл 2.3. Здатність проводити аналіз файлів журналу зрізних джерел та аналізувати сигнали сповіщення про мережу з метою визначення можливих загроз безпеці мережі. Здатність проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності.	Ability to analyse log files from various sources and analyse network alerts to identify possible network security threats. Ability to conduct special studies of information processing tools, technical means and objects of information activity.
Фахові компетентності Блоку 3. Професійний стандарт.Фахівець з технічного захисту інформації/Professional competences Block 3. Professional standard Specialist in technical information security	
ФКбл 3.1. Здатність розробляти, впроваджувати та аналізувати та обґрунтовувати технічні документи, положення, інструкції щодо систем та комплексів захисту інформації.	Ability to develop, implement and analyse and justify technical documents, regulations, instructions for information security systems and complexes.
ФКбл 3.2. Здатність проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності. Здатність виявляти закладні пристрої на об'єктах інформаційної діяльності.	Ability to conduct special studies of information processing tools, technical means and objects of information activity. The ability to detect embedded devices on information objects.
ФКбл 3.3. Здатність проводити аналіз файлів журналу з різних джерел та аналізувати	Ability to analyse log files from various sources and analyse network alerts to identify possible network security threats.

сигнали сповіщення про мережу з метою визначення можливих загроз безпеці мережі. Здатність супроводжувати тематичні дослідження (процеси оцінки відповідності) засобів криптографічного захисту інформації.	Ability to support case studies (conformity assessment processes) of cryptographic information security.
Фахові компетентності Блоку 4. Професійний стандарт. Фахівець сфери захисту інформації/Professional competences Block 4. Professional standard. Specialist in the field of information security	
ФКбл 4.1. Здатність проводити оцінку відповідності (державну експертизу) комплексних систем захисту інформації та засобів технічного захисту інформації.	Ability to conduct a conformity assessment (state examination) of integrated information security systems and technical information security equipment.
ФКбл 4.2. Здатність здійснювати контроль за станом технічного та криптографічного захисту інформації.	Ability to monitor the state of technical and cryptographic protection of information.
ФКбл 4.3. Здатність проводити аналіз файлів журналу з різних джерел та аналізувати сигнали сповіщення про мережу з метою визначення можливих загроз безпеці мережі. Здатність супроводжувати тематичні дослідження (процеси оцінки відповідності) засобів криптографічного захисту інформації. Здатність проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності.	Ability to analyse log files from various sources and analyse network alerts to identify possible network security threats. Ability to support case studies (conformity assessment processes) of cryptographic information security. Ability to conduct special studies of information processing tools, technical means and objects of information activity.
Військово-професійні компетентності (ВПК)/ Military-professional competencies (MPC)	
ВПК 1. Здатність сумлінно і чесно виконувати службовий обов'язок у відповідності з вимогами Статутів Збройних Сил України, іншими нормативно-правовими актами, що регламентують службову діяльність у Держспецзв'язку, та вимагати від підлеглих їх дотримання та виконання.	**MPC 1.** Ability to perform official duties in good faith and honestly in accordance with the requirements of the Statutes of the Armed Forces of Ukraine, other regulatory legal acts governing official activities in the State Special Communications Service of Ukraine, and to demand that subordinates comply with and fulfil them.
ВПК 2. Здатність планувати, організовувати бій та управляти підрозділом (механізованим взводом) в основних видах бою (тактичних дій).	**MPC 2.** The ability to plan, organise combat and manage a unit (mechanised platoon) in the main types of combat (tactical actions).

ВПК 3. Здатність застосовувати на практиці основні положення теорії управління і прийняття рішень, алгоритми прийняття управлінських рішень, принципи та процедури ефективного управління підрозділом (у тому числі за стандартами НАТО); проводити історико-ретроспективний аналіз.	**MPC 3.** Ability to apply in practice the basic provisions of the theory of management and decision-making, algorithms for making managerial decisions, principles and procedures for effective management of the unit (including NATO standards); conduct historical and retrospective analysis.
ВПК 4. Здатність аналізувати і усвідомлювати місію; вести за собою особовий склад до її виконання, демонструючи цінності, властивості характеру і мислення на основі прикладів етносу Воїна та видатного військового лідерства.	**MPC 4.** Ability to analyse and understand the mission; lead personnel to achieve it, demonstrating the values, character traits and mindset of the Warrior ethos and outstanding military leadership.
ВПК 5. Здатність вдосконалювати свої фахові, методичні та фізичні навички; особисто проводити заняття з бойової підготовки з особовим складом (підрозділом); працювати з таємними документами, зберігати зброю і боєприпаси, забезпечувати додержання заходів безпеки на заняттях; підтримувати постійну готовність підрозділу до виконання завдань за призначенням у мирний та воєнний час.	**MPC 5.** The ability to improve professional, methodological and physical skills; personally conduct combat training classes with personnel (unit); work with secret documents, store weapons and ammunition, ensure compliance with security measures during classes; maintain the unit's constant readiness to perform assigned tasks in peacetime and wartime.
ВПК 6. Здатність організовувати РХБ захист в підрозділі; застосовувати засоби індивідуального захисту та долати райони зараження в різних умовах обстановки в ході виконання завдань за призначенням.	**MPC 6.** Ability to organise CBRN protection in the unit; use personal protective equipment and overcome contaminated areas in various conditions in the course of performing assigned tasks.
ВПК 7. Здатність визначати тактичні властивості місцевості при веденні бойових дій в різних умовах; працювати з топографічними картами та фотодокументами; орієнтуватися на місцевості за картою, без карти та за допомогою навігаційних приладів.	**MPC 7.** Ability to determine the tactical properties of the terrain in combat operations in various conditions; work with topographic maps and photographic documents; navigate the terrain with a map, without a map and with the help of navigation devices.
ВПК 8. Здатність виконувати завдання інженерної підтримки в різних видах бою.	**MPC 8.** Ability to perform engineering support tasks in various types of combat.
ВПК 9. Здатність організовувати та підтримувати зв'язок у підрозділі штатними засобами зв'язку.	**MPC 9.** Ability to organise and maintain communication in the unit using standard means of communication.
ВПК 10. Здатність виконувати професійну діяльність в умовах тривалих різнопланових	**MPC 10.** The ability to perform professional activities under conditions of prolonged, diverse

фізичних навантажень і психічних напружень; організувати підготовку військовослужбовців для забезпечення їх фізичної готовності до виконання завдань за призначенням; організувати виконання завдань з тактичної медицини.	physical exertion and mental stress; to organise the training of servicemen to ensure their physical readiness to perform assigned tasks; to organise the performance of tactical medicine tasks.
ВПК 11. Здатність готувати штатну зброю підрозділу до бойового застосування; ефективно використовувати бойові і технічні можливості озброєння (зброї) під час ведення бою (бойових дій), проведенні усіх видів занять із підпорядкованим особовим складом; здатність особисто володіти прийомами та способами ведення влучного вогню зі штатного озброєння (зброї) по цілях, що з'являються та рухаються, вдень та вночі; здатність управляти вогнем підпорядкованих і приданих підрозділів (вогневих засобів) під час виконання бойових завдань.	**MPC 11.** Ability to prepare regular weapons of the unit for combat use; effectively use the combat and technical capabilities of weapons (weapons) during combat (combat operations), conducting all types of training with subordinate personnel; ability to personally master the techniques and methods of accurate fire from regular weapons (weapons) at targets that appear and move, day and night; ability to control the fire of subordinate and attached units (firearms) during combat missions.
ВПК 12. Здатність застосовувати дисциплінарну практику по відношенню до підпорядкованого особового складу; керувати підрозділом з дотриманням норм міжнародного гуманітарного права.	**MPC 12.** Ability to apply disciplinary practices in relation to subordinate personnel; manage the unit in compliance with international humanitarian law.
Військово-спеціальні компетентності (ВСК) *Military-special competencies (MSC)*	
ВСК 1. Здатність володіти знаннями і навичками застосування інформаційно-комунікаційних систем (комплексів сучасних рухомих вузлів зв'язку та засобів урядового польового зв'язку).	**MSC 1.** Ability to possess knowledge and skills in the use of information-communication systems (complexes of modern mobile communication nodes and government field communication equipment).
ВСК 2. Здатність готувати штатне обладнання станцій і вузлів інформаційно-комунікаційних систем до виконання завдань з урядового польового зв'язку; виконувати схему-наказ на організацію урядового зв'язку; організовувати чергування на вузлу урядового польового зв'язку; вести експлуатаційно-технічну документацію; організовувати захист від засобів радіоелектронної боротьби; організовувати охорону і оборону польового вузла урядового зв'язку.	**MSC 2.** Ability to prepare standard equipment of stations and nodes of information and communication systems to perform tasks on government field communications; execute the scheme-order for the organisation of government communications; organise duty at the government field communications node; maintain operational and technical documentation; organise protection against electronic warfare; organise protection and defence of the government field communications node.

ВСК 3. Здатність проводити планування з виконання вузлом урядового зв'язку завдань за призначенням; організовувати виконання першочергових заходів щодо підготовки до виконання завдань як в підготовчий період так і в ході виконання завдань з урядового польового зв'язку; розроблювати і оформлювати оперативні (бойові) документи з урядового зв'язку; ставити завдання особовому складу вузла урядового зв'язку на виконання завдань за призначенням; забезпечувати виконання вузлом урядового зв'язку поставлених завдань відповідно до плану бойового застосування Територіального вузла урядового зв'язку.	**MSC 3.** Ability to plan for the performance of assigned tasks by the government communications node; organize the implementation of priority measures to prepare for the performance of tasks both in the preparatory period and in the course of performing government field communications tasks; develop and execute operational (combat) documents on government communications; set tasks for the personnel of the government communications node to perform assigned tasks; ensure that the government communications node performs its tasks in accordance with the plan of combat use of the Territorial government communications node.
ВСК 4. Здатність до організації, планування та забезпечення режиму секретності в установах та організаціях.	**MSC 4.** Ability to organise, plan and ensure secrecy in institutions and organisations.
7 – Програмні результати навчання (ПРН)/ Programme learning outcomes (PLO)	
ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.	**PLO 1**. Apply knowledge of the state and foreign languages to ensure the effectiveness of professional communication.
ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язання складних спеціалізованих задач та практичних проблем у професійної діяльності, оцінювати їхню ефективність.	**PLO 2**. Organize own professional activities, choose optimal methods and ways to solve complex specialized tasks and practical problems in professional activities, evaluate their effectiveness.
ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.	**PLO 3**. Use the results of independent search, analysis and synthesis of information from various sources to effectively solve specialized problems of professional activity.
ПРН 4. 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.	**PLO 4**. Analyze, argue, make decisions when solving complex specialized tasks and practical problems in professional activities characterized by complexity and incomplete certainty of conditions, and be responsible for decisions made.
ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.	**PLO 5**. Adapt to frequent changes in professional technologies and predict the final result.

ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.	**PLO 6**. Critically comprehend the basic theories, principles, methods and concepts in education and professional activities.
ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки.	**PLO 7**. To act on the basis of the legislative and regulatory framework of Ukraine and the requirements of relevant standards, including international standards in the field of information and/or cybersecurity.
ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки.	**PLO 8**. Prepare proposals for regulations on information and/or cybersecurity.
ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.	**PLO 9**. Implement processes based on national and international standards for detecting, identifying, analyzing and responding to information and/or cybersecurity incidents.
ПРН 10. Виконувати аналіз та декомпозицію інформаційно-комунікаційних систем.	**PLO 10**. Analyze and decompose information-communication systems.
ПРН 11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.	**PLO 11**. Analyze the relationship between information processes on remote computer systems.
ПРН 12. Розробляти моделі загроз та порушника**.**	**PLO 12**. Develop threat and intruder models.
ПРН 13. Аналізувати проекти інформаційно-комунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.	**PLO 13**. Analyze projects of information-communication systems based on standardized technologies and data transfer protocols.
ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-комунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.	**PLO 14**. Solve problems of protecting programs and information processed in information and communication systems by software and hardware and evaluate the effectiveness of the quality of decisions made.
ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.	**PLO 15**. Use modern software and hardware of information and communication technologies.
ПРН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємств) відповідно до вимог нормативно-правових документів.	**PLO 16**. Implement comprehensive information security systems in the automated systems (AS) of the organization (enterprises) in accordance with the requirements of regulatory-legal documents.

ПРН 17. Забезпечувати процеси захисту та функціонування інформаційно-комунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектор та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.	**PLO 17**. Ensure the processes of protection and functioning of information-communication (automated) systems based on practices, skills and knowledge of structural (structural-logical) schemes, network topology, modern architectures and models of protection of electronic information resources with the reflection of interconnections and information flows, processes for internal and remote components.
ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.	**PLO 18**. Use software and hardware systems to protect information resources.
ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-комунікаційних системах.	**PLO 19**. Apply theories and methods of protection to ensure the security of information in information-communication systems.
ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-комунікаційних системах.	**PLO 20**. Ensure the functioning of special software to protect information from destructive software influences and destructive codes in information-communication systems.
ПРН 21. Забезпечувати функціонування спеціального програмного забезпечення щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-комунікаційних системах.	**PLO 21**. Ensure the functioning of special software to protect information from destructive software influences and destructive codes in information-communication systems.
ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної та/або кібербезпеки.	**PLO 22**. Solve problems of managing procedures for identification, authentication, authorization of processes and users in information-communication systems in accordance with the established information and/or cybersecurity policy.
ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-комунікаційних (автоматизованих) системах.	**PLO 23**. Implement measures to counteract unauthorized access to information resources and processes in information and information-communication (automated) systems.
ПРН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-комунікаційних (автоматизованих) системах на основі моделей управління доступом	**PLO 24**. Solve problems of managing access to information resources and processes in information and information-communication (automated) systems based on access control models (mandatory, discretionary, role-based).

(мандатних, дискреційних, рольових).	
ПРН 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-комунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур їх захисту.	**PLO 25**. Ensure the introduction of an accountability system for managing access to electronic information resources and processes in information and information-communication (automated) systems using event logs, their analysis and established security procedures.
ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу та захисту інформаційних та інформаційно-комунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.	**PLO 26**. Implement measures and ensure the implementation of processes to prevent unauthorized access and protect information and information-communication (automated) systems based on the reference model of open systems interaction.
ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-комунікаційних (автоматизованих) системах.	**PLO 27**. Solve problems of data flow protection in information, information-communication (automated) systems.
ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-комунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки.	**PLO 28**. Analyze and evaluate the efficiency and level of security of resources of various classes in information and information-communication (automated) systems during tests in accordance with the established information and/or cybersecurity policy.
ПРН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-комунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.	**PLO 29**. To assess the possibility of potential threats to information processed in information-communication systems and the effectiveness of the use of security systems in the face of threats of various classes.
ПРН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-комунікаційних систем.	**PLO 30**. Assess the possibility of unauthorized access to elements of information-communication systems.
ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-комунікаційних систем.	**PLO 31**. Apply theories and methods of protection to ensure the security of elements of information-communication systems.
ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики	**PLO 32**. Solve the tasks of managing the processes of restoring the normal functioning of information-communication systems using backup procedures in accordance with the established security policy.

безпеки.	
ПРН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.	**PLO 33**. Solve problems of ensuring the continuity of the organization's business processes based on risk theory.
ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.	**PLO 34**. Participate in the development and implementation of the information security and/or cybersecurity 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-комунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.	**PLO 35**. Solve the tasks of providing and maintaining integrated information security systems, as well as counteracting unauthorized access to information resources and processes in information and information-communication (automated) systems in accordance with the established information and/or cybersecurity policy.
ПРН 36. Виявляти небезпечні сигнали технічних засобів.	**PLO 36**. Detect dangerous signals from technical equipment.
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.	**PLO 37**. Measure the parameters of dangerous and interfering signals during 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-комунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.	**PLO 38**. Interpret the results of special measurements using technical means, control the characteristics of information and communication systems in accordance with the requirements of regulatory documents of the technical information security system.
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.	**PLO 39**. Carry out certification (based on records and surveys) of restricted areas (zones), premises, etc. in compliance with the secrecy regime, with the results recorded in the relevant documents.

ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІКС відповідно до вимог нормативних документів системи технічного захисту інформації.	**PLO 40**. Interpret the results of special measurements using technical means, control of ICS characteristics in accordance with the requirements of regulatory documents of the technical information security system.
ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.	**PLO 41**. Ensure the continuity of the process of maintaining event and incident logs based on automated procedures.
ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.	**PLO 42**. Implement processes for detecting, identifying, analyzing and responding to information and/or cybersecurity incidents.
ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.	**PLO 43**. Apply national and international information security and/or cybersecurity regulations 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.	**PLO 44**. Solve the tasks of ensuring the continuity of the organization's business-processes based on the 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.	**PLO 45**. Apply different classes of information security and/or cybersecurity policies based on risk-based access control to information assets.
ПРН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-комунікаційних системах.	**PLO 46**. Analyze and minimize risks of information processing in information-communication systems.
ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-комунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.	**PLO 47**. Solve the problems of protecting information processed in information-communication systems using modern methods and means of cryptographic information protection.
ПРН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти	**PLO 48**. Implement and support intrusion detection systems and use cryptographic security components to ensure the required level of

криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-комунікаційних системах.	information security in information-communication systems.
ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.	**PLO 49**. Ensure proper functioning of the system for monitoring information resources and processes in information-communication systems.
ПРН 50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).	**PLO 50.** Ensure the functioning of software and hardware complexes detection systems of various levels and classes (statistical, signature, statistical-signature).
ПРН 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-комунікаційних системах.	**PLO 51.** Maintain the performance and ensure the configuration of intrusion detection systems in information and communication systems.
ПРН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-комунікаційних системах.	**PLO 52**. Use tools to monitor processes in information-communication systems.
ПРН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.	**PLO 53**. Solve problems of analyzing program code for possible threats.
ПРН 54. Усвідомлювати цінності громадського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.	**PLO 54**. Understand the values of a civil (free democratic) society and the need for its sustainable development, the rule of law, human and civil rights and freedoms in Ukraine.
ПРН 55. Будувати системи протидії технічним розвідкам.	**PLO 55**. Build countermeasure systems technical intelligence.
ПРН 56. Використовувати 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.	**PLO 56**. Use knowledge and understanding of mathematics and physics in professional activities, formalise the tasks of the subject area of cybersecurity and information protection, formulate their mathematical formulation and choose a rational method of solution.
Програмні результати навчання Блоку 1. Професійний стандарт. Фахівець з реагування на інциденти кібербезпеки / Programme learning outcomes Block 1. Professional standard. Specialist in response cybersecurity	

incident	
ПРНбл 1.1. Використовувати інструменти кореляції подій безпеки. Визначати та пріоритезувати заходи реагування на ризики кібербезпеки. Розробляти або брати участь у розробці порядку проведення оцінки інцидентів кібербезпеки. Проводити оцінку дій противника та його методів, виявляти техніки, тактики та процедури нападу.	**PLObl 1.1**. Use security event correlation tools. Identify and prioritise responses to cybersecurity risks. Develop or participate in the development of a procedure for assessing cybersecurity incidents. Assess enemy actions and methods, identify attack techniques, tactics and procedures.
ПРНбл 1.2. Зберігати цілістність доказів відповідно до стандартних оперативних процедур або національних стандартів. Застосовувати методики виявлення вторгнень з боку хоста та мережі за допомогою технологій виявлення вторгнень. Проводити процедури сканування вразливостей в системах безпеки.	**PLObl 1.2**. Maintain the integrity of evidence in accordance with standard operating procedures or national standards. Apply techniques to detect host and network intrusions using intrusion detection technologies. Conduct security vulnerability scanning procedures.
ПРНбл 1. 3. Готувати документи (запити, заявки, вихідні дані тощо) для проведення тематичних досліджень (оцінки відповідності) засобів криптографічного захисту інформації. Використовувати матеріали та звіти за результатами тематичних досліджень (оцінки відповідності) засобів криптографічного захисту інформації для їх раціонального застосування на обєктах інформаційної діяльності. Надавати в необхідних випадках керівництву пропозиції щодо укладання договорів на проведення тематичних досліджень (їх окремих складових) та оцінки відповідності засобів криптографічного захисту інформації. Проводити спеціальні дослідження засобів обробки інформації, технічних засобів (визначати складові та режими роботи засобів обробки інформації та технічних засобів, визначати тестові сигнали, складати схеми спеціальних досліджень, виявляти та вимірювати небезпечні (тестові) електричні, електромагнітні та оптичні сигнали,	**PLObl 1.3**. Prepare documents (requests, applications, initial data, etc.) for conducting case studies (conformity assessment) of cryptographic information protection means. Use materials and reports based on the results of case studies (conformity assessment) of cryptographic information protection means for their rational application at information activity facilities. To submit proposals to the management, if necessary, on concluding contracts for conducting case studies (their individual components) and assessing the conformity of cryptographic information protection means. Conduct special studies of information processing facilities, technical means (determine components and modes of operation of information processing facilities and technical means, determine test signals, draw up schemes for special studies, detect and measure dangerous (test) electrical, electromagnetic and optical signals, determine information security indicators of information processing facilities, technical means and the possibility (impossibility) of creating certain technical channels of information leakage by them or through them).

визначати показники захищеності інформації засобів обробки інформації, технічних засобів та можливість (неможливість) створення ними або через них певних технічних каналів витоку інформації).	
Програмні результати навчання Блоку 2. Професійний стандарт. Фахівець з криптографічного захисту інформації / Programme learning outcomes Block 2. Professional standard Specialist in cryptographic information security	
ПРНбл 2. 1. Розробляти плани, програми, інструкції та настанови щодо контролю рівня безпеки криптографічного захисту інформації в органі (установі, підприємстві). Здійснювати перевірку повноти і відповідності реалізованих заходів із захисту інформації в органі (установі, підприємстві) вимогам нормативних документів з питань криптографічного захисту інформації. Робити висновки та складати акти за результатами контрольних заходів.	**PLObl 2.1**. To develop plans, programmes, instructions and guidelines for controlling the level of security of cryptographic protection of information in the body (institution, enterprise). To verify the completeness and compliance of the implemented information security measures in the body (institution, enterprise) with the requirements of regulatory documents on cryptographic information security. Draw conclusions and draw up acts based on the results of control measures.
ПРНбл 2. 2. Визначати (формулювати) потреби щодо криптографічного захисту інформації на підприємствах, (установах, організаціях). Визначати та аналізувати вимоги щодо криптографічного захисту інформації на підприємствах, (установах, організаціях). Здійснювати попередню оцінку достатності та коректності вимог і потреб користувачів (замовників)для побудови підсистеми криптографічного захисту інформації з необхідним рівнем безпеки. Аналізувати потреби та вимоги користувачів з метою планування і проведення розробки системи.	**PLObl 2.2**. Identify (formulate) the needs for cryptographic protection of information at enterprises, (institutions, organisations). Determine and analyse the requirements for cryptographic protection of information at enterprises, (institutions, organisations). Carry out a preliminary assessment of the sufficiency and correctness of the requirements and needs of users (customers) to build a cryptographic information security subsystem with the required level of security. Analyse the needs and requirements of users in order to plan and conduct system development.
ПРНбл 2. 3. Працювати з файлами журналів та аналізувати їх. Отримувати та аналізувати сигнали сповіщення про мережу від різних джерел в середині організації та визначати можливі причини появи таких сигналів. Проводити спеціальні дослідження	**PLObl 2.3**. Work with and analyse log files. Receive and analyse network alerts from various sources within the organisation and identify possible causes of such alerts. Conduct special studies of information processing facilities, technical means (determine components and modes of operation of information processing

засобів обробки інформації, технічних засобів (визначати складові та режими роботи засобів обробки інформації та технічних засобів, визначати тестові сигнали, складати схеми спеціальних досліджень, виявляти та вимірювати небезпечні (тестові) електричні, електромагнітні та оптичні сигнали, визначати показники захищеності інформації засобів обробки інформації, технічних засобів та можливість (неможливість) створення ними або через них певних технічних каналів витоку інформації).	facilities and technical means, determine test signals, draw up schemes for special studies, detect and measure dangerous (test) electrical, electromagnetic and optical signals, determine information security indicators of information processing facilities, technical means and the possibility (impossibility) of creating certain technical channels of information leakage by them or through them).
Програмні результати навчання Блоку 3. Професійний стандарт. Фахівець з технічного захисту інформації / Programme learning outcomes Block 3. Professional standard Specialist in technical information security	
ПРНбл 3. 1. Формулювати (брати участь у формулюванні) вимог до захисту інформації в інформаційно-комунікаційних системах та на об'єктах інформаційної діяльності. Розробляти (брати участь у розробці) політики безпеки інформації в інформаційно-комунікаційних системах. Розробляти (брати участь у розробці) технічної та експлуатаційної документації щодо створення, державної експертизи, (атестації), введення в експлуатацію, експлуатації систем та комплексів захисту інформації.	**PLObl 3.1**. To formulate (participate in the formulation of) requirements for information security in information and communication systems and at information activity facilities. Develop (participate in the development of) information security policies in information and communication systems. To develop (participate in the development of) technical and operational documentation for the creation, state examination, (certification), commissioning, operation of information security systems and complexes.
ПРНбл 3. 2. Проводити спеціальні дослідження засобів обробки інформації, технічних засобів (визначати складові та режими роботи засобів обробки інформації та технічних засобів, визначати тестові сигнали, складати схеми спеціальних досліджень, виявляти та вимірювати небезпечні (тестові) електричні, електромагнітні та оптичні сигнали, визначати показники захищеності інформації засобів обробки інформації, технічних засобів та можливість (неможливість) створення ними або через них певних технічних каналів витоку інформації). Проводити	**PLObl 3. 2.** Conduct special studies of information processing facilities and technical means (determine the components and operating modes of information processing facilities and technical means, determine test signals, draw up schemes for special studies, detect and measure dangerous (test) electrical, electromagnetic and optical signals, determine the information security indicators of information processing facilities and technical means and the possibility (impossibility) of creating certain technical channels of information leakage by them or through them). Conduct special studies of information activity objects (draw up schemes of special studies, detect and measure dangerous (test) acoustic,

спеціальні дослідження об’єктів інформаційної діяльності (складати схеми спеціальних досліджень, виявляти та вимірювати небезпечні (тестові) акустичні, віброакустичні, акустоелектричні, акустоелектромагнітні, лазерні сигнали, визначати показники захищеності мовної інформації на об’єкті інформаційної діяльності та можливість (неможливість) створення на ОІД певних технічних каналів витоку інформації). Визначати вимоги до показників (характеристик) апаратних засобів технічного захисту інформації, які необхідні для забезпечення захищеності інформації в системі або на об’єкті інформаційної діяльності. Складати протоколи спеціальних досліджень. Складати приписи на експлуатацію засобів обробки інформації та об’єктів інформаційної діяльності.	vibroacoustic, acoustoelectric, acoustoelectro-magnetic, laser signals, determine the security indicators of speech information at the information activity object and the possibility (impossibility) of creating certain technical channels of information leakage at the OIA). Determine the requirements for indicators (characteristics) of hardware means of technical protection of information, which are necessary to ensure the security of information in the system or at the object of information activity; draw up protocols of special studies. Draw up protocols of special studies. Draw up instructions for the operation of information processing facilities and information activities.
ПРНбл 3. 3. Працювати з файлами журналів та аналізувати їх. Отримувати та аналізувати сигнали сповіщення про мережу від різних джерел в середині організації та визначати можливі причини появи таких сигналів. Готувати документи (запити, заявки, вихідні дані тощо) для проведення тематичних досліджень (оцінки відповідності) засобів криптографічного захисту інформації. Використовувати матеріали та звіти за результатами тематичних досліджень (оцінки відповідності) засобів криптографічного захисту інформації для їх раціонального застосування на об ‘єктах інформаційної діяльності. Надавати в необхідних випадках керівництву пропозиції щодо укладання договорів на проведення тематичних досліджень (їх окремих складових) та оцінки відповідності засобів криптографічного захисту інформації.	**ПРНбл 3. 3.** Work with and analyse log files. Receive and analyse network alerts from various sources within the organisation and identify possible causes of such alerts. Prepare documents (requests, applications, initial data, etc.) for conducting case studies (conformity assessment) of cryptographic information protection means. Use materials and reports based on the results of case studies (conformity assessment) of cryptographic information protection means for their rational application at information activity facilities. To submit proposals to the management, if necessary, on concluding contracts for conducting case studies (their individual components) and assessing the conformity of cryptographic information protection means.
Програмні результати навчання Блоку 4. Професійний стандарт.	

Фахівець сфери захисту інформації/Programme learning outcomes Block 4. Professional standard. Specialist in the field of information security.	
ПРНбл 4. 1. Складати програму та методику проведення державної експертизи комплексних систем захисту інформації. Проводити попереднє ознайомлення з об'єктом експертизи та поглиблене обстеження об'єкта експертизи. Проводити експертні випробування та дослідження комплексних систем захисту інформації (оцінювати функціональні послуги безпеки, оцінювати рівні гарантій коректності реалізації функціональних послуг безпеки, перевіряти наявність зареєстрованого акта атестації комплексу ТЗІ, якщо такий комплекс входить до складу комплексної системи захисту інформації, або проводити його атестацію). Оформлювати протоколи експертних випробувань та атестати відповідності комплексних систем захисту інформації. Здійснювати експертизу комплексних систем захисту інформації шляхом декларування, оформлювати декларації відповідності комплексних систем захисту інформації та організовувати їх затвердження та реєстрацію. Здійснювати експертизу засобів технічного захисту інформації, оформлювати протоколи експертних випробувань засобів технічного захисту інформації та експертні висновки на засоби ТЗІ, організовувати затвердження і реєстрацію експертних висновків.	**PLObl 4.1**. Develop a programme and methodology for conducting the state examination of integrated information security systems. Carry out a preliminary examination of the object of examination and an in-depth examination of the object of examination. Conduct expert tests and studies of integrated information security systems (evaluate functional security services, assess the level of guarantees for the correct implementation of functional security services, check the availability of a registered certificate of certification of a complex of TDI, if such a complex is part of an integrated information security system, or conduct its certification). To issue expert test reports and certificates of conformity of integrated information security systems. Carry out examination of integrated information security systems by way of declaration, issue declarations of conformity of integrated information security systems and organise their approval and registration.
ПРНбл 4. 2. Організовувати (приймати участь у організації) контроль за станом технічного та криптографічного захисту інформації. Перевіряти виконання вимог нормативно-правових актів та нормативних документів з технічного та криптографічного захисту інформації на підприємствах/в організаціях. Застосовувати засоби контролю захищеності інформації. Користуватися інструментарієм контролю за станом технічного та криптографічного захисту інформації. Визначати стан технічного та криптографічного захисту інформації на підприємстві/в організації. Оформлювати документи за результатами контролю стану технічного та криптографічного захисту інформації на підприємстві/в організації.	**PLObl 4.2**. To limit (take part in organising) control over the state of technical and cryptographic protection of information. To check compliance with the requirements of regulatory legal acts and normative documents on technical and cryptographic protection of information at enterprises/in organisations. Apply information security controls. Use tools for monitoring the state of technical and cryptographic protection of information. Determine the state of technical and cryptographic protection of information at an enterprise/organisation. Draw up documents based on the results of monitoring the state of technical and cryptographic protection of information at the enterprise/organisation.

ПРНбл 4. 3. Працювати з файлами журналів та аналізувати їх. Отримувати та аналізувати сигнали сповіщення про мережу від різних джерел в середині організації та визначати можливі причини появи таких сигналів. Готувати документи (запити, заявки, вихідні дані тощо) для проведення тематичних досліджень (оцінки відповідності) засобів криптографічного захисту інформації. Використовувати матеріали та звіти за результатами тематичних досліджень (оцінки відповідності) засобів криптографічного захисту інформації для їх раціонального застосування на об ‘єктах інформаційної діяльності. Надавати в необхідних випадках керівництву пропозиції щодо укладання договорів на проведення тематичних досліджень (їх окремих складових) та оцінки відповідності засобів криптографічного захисту інформації. Проводити спеціальні дослідження засобів обробки інформації, технічних засобів (визначати складові та режими роботи засобів обробки інформації та технічних засобів, визначати тестові сигнали, складати схеми спеціальних досліджень, виявляти та вимірювати небезпечні (тестові) електричні, електромагнітні та оптичні сигнали, визначати показники захищеності інформації засобів обробки інформації, технічних засобів та можливість (неможливість) створення ними або через них певних технічних каналів витоку інформації).	**PLObl 4.3**. Work with and analyse log files. Receive and analyse network alerts from various sources within the organisation and identify possible causes of such alerts. Prepare documents (requests, applications, initial data, etc.) for conducting case studies (conformity assessment) of cryptographic information protection means. Use materials and reports based on the results of case studies (conformity assessment) of cryptographic information protection means for their rational application at information activity facilities. To submit proposals to the management, if necessary, on concluding contracts for conducting case studies (their individual components) and assessing the conformity of cryptographic information protection means. Conduct special studies of information processing facilities, technical means (determine components and modes of operation of information processing facilities and technical means, determine test signals, draw up schemes for special studies, detect and measure dangerous (test) electrical, electromagnetic and optical signals, determine information security indicators of information processing facilities, technical means and the possibility (impossibility) of creating certain technical channels of information leakage by them or through them).
Військово-професійна підготовка/ Military-professional training	
ПРНвпп 1. Застосовувати вимоги Статутів Збройних Сил України при організації службової діяльності в підрозділі, внутрішньої і вартової служб, підтриманні військової дисципліни та забезпеченні стройової злагодженості підрозділу.	**PLOмрт 1**. To apply the requirements of the Statutes of the Armed Forces of Ukraine in the organisation of service activities in the unit, internal and guard service, maintaining military discipline and ensuring the unit's coherence.

ПРНвпп 2. Здійснювати підготовку підрозділу (механізованого взводу) до ведення бою (тактичних дій), управляти діями підрозділу в ході ведення бою (тактичних дій).	**PLOмрт 2.** To prepare the unit (mechanised platoon) for combat (tactical operations), to manage the actions of the unit during combat (tactical operations).
ПРНвпп 3. Знати і розуміти принципи та процедури управління підрозділом за стандартами НАТО та вміти їх використовувати для досягнення службових і бойових цілей; приймати обґрунтовані рішення на дії підрозділу в умовах бойової обстановки з використанням принципів і процедур за стандартами НАТО; вміти проводити історико-ретроспективний аналіз дій.	**PLOмрт 3.** Know and understand the principles and procedures of unit management in accordance with NATO standards and be able to use them to achieve service and combat objectives; make informed decisions on the unit's actions in a combat situation using principles and procedures in accordance with NATO standards; be able to conduct historical and retrospective analysis of actions.
ПРНвпп 4. Знати і розуміти особливості професії офіцера, основи військового лідерства, цінності, властивості характеру і види мислення видатних військових лідерів на прикладах їх військово-професійної діяльності і етносу Воїна.	**PLOмрт 4.** To know and understand the peculiarities of the officer's profession, the basics of military leadership, values, character traits and types of thinking of outstanding military leaders on the examples of their military professional activities and the ethnicity of the Warrior.
ПРНвпп 5. Знати методи вдосконалення своїх фахових та методичних навичок, особисто проводити заняття з бойової підготовки з особовим складом (підрозділом); вміти працювати з таємними документами; надійно зберігати зброю і боєприпаси, майно підрозділу, керувати веденням ротного господарства підрозділу; забезпечувати додержання заходів безпеки на заняттях, стрільбах (польотах, походах), навчаннях (тренуваннях), перевірках готовності.	**PLOмрт 5.** Know the methods of improving their professional and methodological skills, personally conduct combat training classes with personnel (unit); be able to work with secret documents; securely store weapons and ammunition, unit property, manage the unit's company economy; ensure compliance with safety measures during classes, firing (flights, campaigns), exercises (training), readiness checks.
ПРНвпп 6. Організовувати РХБ захист в підрозділі (застосовувати засоби індивідуального захисту та долати райони зараження) в різних умовах обстановки в ході виконання завдань за призначенням.	**PLOмрт 6.** Organise CBRN protection in the unit (use personal protective equipment and overcome contaminated areas) in various conditions of the situation in the course of performing assigned tasks.
ПРНвпп 7. Визначати тактичні властивості місцевості при веденні бойових дій в різних умовах; працювати з топографічними картами та	**PLOмрт 7.** Determine the tactical properties of the terrain when conducting combat operations in various conditions; work with topographic maps and photographic documents; navigate unfamiliar

фотодокументами; орієнтуватися на незнайомій місцевості за картою, без карти та за допомогою навігаційних приладів вдень і вночі за будь-якої погоди і пори року.	terrain with or without a map and using navigation devices, day and night, in any weather and season.
ПРНвпп 8. Формувати вказівки з інженерної підтримки взводу в різних видах бою, використовуючи розуміння основних заходів інженерної підтримки; здійснювати практичне обладнання та маскування елементів взводного опорного пункту; організовувати заходи щодо встановлення та подолання одиночних мін та мінних полів штатними засобами.	**PLOмрт 8.** Formulate platoon engineering support instructions for various types of combat, using an understanding of basic engineering support activities; to carry out practical equipment and camouflage of the elements of the platoon stronghold; organise measures to detect and clear single mines and minefields using regular means.
ПРНвпп 9. Використовувати штатні засоби зв'язку, які перебувають на озброєнні підрозділу для організації зв'язку; організовувати заходи із захисту від засобів радіоелектронної боротьби противника під час підготовки та ведення бою.	**PLOмрт 9.** Use regular communications equipment in service with the unit to organise communications; organise measures to protect against enemy electronic warfare during the preparation and conduct of combat.
ПРНвпп 10. Застосовувати знання щодо забезпечення потреб військовослужбовця під час дій в автономних умовах за рахунок природних ресурсів; захисту від впливу фізико-географічних умов за допомогою природних та підручних засобів; вміти організовувати виконання завдань з тактичної медицини.	**PLOмрт 10.** Apply knowledge of how to meet the needs of a serviceman during operations in autonomous conditions at the expense of natural resources; protection from the impact of physical-geographical conditions using natural and improvised means; be able to organise the performance of tactical medicine tasks.
ПРНвпп 11. Застосовувати знання матеріальної частини стрілецької зброї, правил стрільби, експлуатації та обслуговування стрілецької зброї, методики організації та проведення занять для навчання особового складу підрозділу, підготовки озброєння до стрільби у похідному (бойовому) поводженні та при виконанні бойових завдань; застосовувати знання та навички з управління вогнем підрозділу в бою.	**PLOмрт 11.** Apply knowledge of the material part of small arms, rules of fire, operation and maintenance of small arms, methods of organising and conducting classes to train unit personnel, prepare weapons for firing in marching (combat) handling and in the performance of combat missions; apply knowledge and skills of unit fire control in combat.
ПРНвпп 12. Розуміти порядок проходження військової служби,	**PLOмрт 12.** Understand the procedure for military service, bringing servicemen to criminal,

притягнення військовослужбовців до кримінальної, адміністративної та матеріальної відповідальності; соціального та правового захисту військовослужбовців та членів їх сімей; знати порядок проведення службового розслідування в Збройних Силах України; застосовувати знання норм міжнародного гуманітарного права.	administrative and material liability; social and legal protection of military personnel and their families; know the procedure for conducting an internal investigation in the Armed Forces of Ukraine; apply knowledge of international humanitarian law.
ПРНвпп 13. Знати і вміти впевнено застосувати інформаційно-комунікаційні системи (комплексів сучасних рухомих вузлів зв'язку та засобів урядового польового зв'язку).	**PLOмрт 13.** To know and be able to confidently apply information-communication systems (complexes of modern mobile communication nodes and government field communication equipment).
ПРНвпп 14. Вміти готувати штатне обладнання станцій і вузлів інформаційно-комунікаційних систем до виконання завдань з урядового польового зв’язку; виконувати схему-наказ на організацію урядового зв’язку; організовувати чергування на вузлу урядового польового зв’язку; вести експлуатаційно-технічну документацію; організовувати захист від засобів радіоелектронної боротьби; організовувати охорону і оборону польового вузла урядового зв’язку.	**PLOмрт 14.** Be able to prepare the standard equipment of stations and nodes of information and communication systems for performing government field communications tasks; execute the scheme-order for the organisation of governmental communications; organise duty at the governmental field communications node; maintain operational and technical documentation; organise protection against electronic warfare; organise the protection and defence of the government communications field node.
ПРНвпп 15. Вміти проводити планування з виконання вузлом урядового зв’язку завдань за призначенням; організовувати виконання першочергових заходів щодо підготовки до виконання завдань як в підготовчий період так і під час виконання завдань з урядового польового зв’язку; розроблювати і оформлювати оперативні (бойові) документи з урядового зв’язку; ставити завдання особовому складу вузла зв’язку на виконання завдань за призначенням; забезпечувати виконання вузлом урядового зв’язку поставлених завдань відповідно до плану бойового застосування Територіального вузла урядового зв’язку.	**PLOмрт 15.** Be able to plan for the performance of assigned tasks by the government communications centre; organise the implementation of priority measures to prepare for the performance of tasks both in the preparatory period and during the performance of government field communications tasks; develop and execute operational (combat) documents on government communications; set tasks for the personnel of the communications centre to perform assigned tasks; ensure that the government communications node performs its tasks in accordance with the plan of combat use of the Territorial government communications node.

ПРНвпп 16. Організовувати та проводити заходи по забезпеченню режиму секретності в установах, організаціях та в підрозділах Держспецзв'язку.	**PLOмрт 16.** To organise and carry out measures to ensure the secrecy regime in institutions, organisations and units of the State Service for Special Communications and Information Protection of Ukraine.
8 – Ресурсне забезпечення реалізації програми/ Resource provision for programme implementation	
Кадрове забезпечення/Staffing	
Відповідно до кадрових вимог щодо забезпечення провадження освітньої діяльності для бакалаврського рівня вищої освіти, затверджених Постановою Кабінету Міністрів України від 30 грудня 2015 року № 1187 (в чинній редакції). Загальна кількість науково-педагогічних, педагогічних та наукових працівників: 21 Кількість науково-педагогічних, педагогічних та наукових працівників, які працюють за основним місцем роботи (в тому числі за суміщенням) з них кількість: - докторів наук та (або) професорів: 6 - кандидатів наук та (або) доцентів: 15 (12)	In accordance with the staffing requirements for ensuring the implementation of educational activities for the bachelor's level of higher education, approved by the Resolution of the Cabinet of Ministers of Ukraine No. 1187 dated December 30, 2015 (as amended). Total number of research, teaching and scientific staff: 21 Number of research and teaching, pedagogical and scientific employees working at the main place of work (including part-time) of which: - Doctors of Sciences and (or) Professors: 6 - candidates of sciences and (or) associate professors: 15 (12)
Матеріально-технічне забезпечення/Material-technical support	
Відповідно до технологічних вимог щодо матеріально-технічного забезпечення освітньої діяльності для бакалаврського рівня вищої освіти, затверджених Постановою Кабінету Міністрів України від 30 грудня 2015 року № 1187 (в чинній редакції). Для реалізації освітньо-професійної програми підготовки бакалаврів задіяно: навчальна лабораторія з технічного захисту інформації імені Скрипника Л. В., 4 навчальні станції спеціального зв'язку, одна комп'ютерна навчальна лабораторія, обладнання Науково-дослідного центру ІСЗЗІ КПІ ім. Ігоря Сікорського. Навчальні аудиторії забезпечені мультимедійним обладнанням на достатньому рівні.	In accordance with the technological requirements for the material and technical support of educational activities for the bachelor's level of higher education, approved by the Resolution of the Cabinet of Ministers of Ukraine No. 1187 of December 30, 2015 (as amended). The following facilities are involved in the implementation of the Bachelor's degree programme: training laboratory for technical protection of information named after L. V. Skrypnyk, 4 training stations of special communication, one computer training laboratory, equipment of the Research Centre Igor Sikorsky Kyiv Polytechnic Institute, a sufficient level of provision of classrooms with multimedia equipment.
Інформаційне та навчально-методичне забезпечення/ Information and methodical support of the educational process	

Відповідно до вимог щодо інформаційного та навчально-методичного забезпечення освітньої діяльності відповідного рівня вищої освіти, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 в чинній редакції. Користування Науково-технічною бібліотекою ті іншими інформаційними ресурсами КПІ ім. Ігоря Сікорського. Користування бібліотекою Навчального відділу ІСЗЗІ КПІ ім. Ігоря Сікорського. Користування Спеціальною бібліотекою Режимно-секретного відділу.	In accordance with the requirements for information and educational and methodological support of educational activities of the appropriate level of higher education, approved by the Resolution of the Cabinet of Ministers of Ukraine of 30.12.2015 № 1187 in the current version. Use of the Scientific and Technical Library and other information resources of Igor Sikorsky Kyiv Polytechnic Institute. Use of the library of the Educational Department of the Igor Sikorsky Kyiv Polytechnic Institute. Use of the Special library of the Secretive department.
9 – Академічна мобільність/Academic mobility	
Національна кредитна мобільність/National credit mobility	
Національна кредитна мобільність за даною освітньо-професійною програмою не передбачена.	National credit mobility is not provided for this study programme.
Міжнародна кредитна мобільність/International credit mobility	
Можливість укладання угод про академічну мобільність, про тривалі міжнародні проекти, які передбачають включене навчання здобувачів вищої освіти (за рішенням Голови Держспецзв'язку).	Possibility to conclude agreements on academic mobility, on long-term international projects that provide for the inclusion of training for higher education students (by decision of the Head of the State Special Communications Service).
Навчання іноземних здобувачів ВО/ Study of Foreign applicants of HE	
Навчання іноземних здобувачів вищої освіти за даною освітньо-професійною програмою не передбачено.	Training of foreign applicants for higher education in this educational–professional program is not provided.

2. ПЕРЕЛІК ОСВІТНІХ КОМПОНЕНТІВ/EDUCATIONAL COMPONENTS

Код/ Code	Освітні компоненти/Educational Components	Кредити ЄКТС/ ECTS credits	Форма підсумкового контролю/ Final control measure form
Обов'язкові (нормативні) компоненти/Required (standard) components			
Цикл загальної підготовки/General training cycle			
ЗО 1	Українська мова за професійним спрямуванням./Ukrainian language for professional purposes.	2	залік/test
ЗО 2	Історія України./History of Ukraine.	2	залік/test
ЗО 3.1	Практичний курс іноземної мови. Частина 1./Practical course of a foreign language. Part 1.	3	залік/test
ЗО 3.2	Практичний курс іноземної мови. Частина 2./Practical course of a foreign language. Part 2.	3	залік/test
ЗО 4.1	Практичний курс іноземної мови професійного спрямування. Частина 1./Practical course of a foreign language for professional purposes. Part 1.	3	залік/test
ЗО 4.2	Практичний курс іноземної мови професійного спрямування. Частина 2./ Practical course of a foreign language for professional purposes. Part 2.	3	екзамен/ exam
ЗО 5	Безпека життєдіяльності та цивільний захист./ Life safety and civil defense.	2	залік/test
ЗО 6.1	Вища математика. Частина 1. Лінійна алгебра. Аналітична геометрія. Диференціальне числення однієї та кількох змінних./ Higher mathematics. Part 1: Linear algebra. Analytical geometry. Differential calculus of one and several variables.	8	екзамен/ exam
ЗО 6.2	Вища математика. Частина 2. Інтегральне числення функції однієї змінної. Диференціальні рівняння. Числові і функціональні ряди і інтеграл Фур'є./Higher mathematics. Part 2. Integral calculus of a function of one variable. Differential equations. Numerical and functional series and the Fourier integral.	7	екзамен/ exam
ЗО 7.1	Фізика. Частина 1. Електромагнетизм. Коливання та хвилі. Оптика./Physics. Part 1: Electromagnetism.	5	екзамен/ exam

	Oscillations and waves. Optics.		
ЗО 7.2	Фізика. Частина 2. Основи квантової фізики. Фізика твердого тіла. Основи квантової електроніки/ Physics. Part 2. Fundamentals of quantum physics. Solid state physics. Fundamentals of quantum electronics.	5	екзамен/ exam
ЗО 8	Дискретна математика/Discrete mathematics.	6	екзамен/ exam
ЗО 9	Дискретна математика. Курсова робота / Discrete mathematics. Course work.	1	залік/test
ЗО 10.1	Програмування. Частина 1. Алгоритмізація та програмування/ Programming. Part 1: Algorithmization and programming.	4	залік/test
ЗО 10.2	Програмування. Частина 2. Об'єктно-орієнтоване програмування/Programming. Part 2. Object-oriented programming.	6	залік/test
ЗО 11	Правові основи національної безпеки/Legal basis of national security.	3	залік/test
ЗО 12	Філософські проблеми воєнної теорії та практики/Philosophical problems of military theory and practice.	2	залік/test
ЗО 13	Теорія ймовірностей і математична статистика./Theory of probability and mathematical statistics.	4	екзамен/ exam
Цикл професійної підготовки/Professional training cycle			
ПО 1	Архітектура комп'ютерних систем/ Architecture of computer systems	3	залік/test
ПО 2.1	Фізичне виховання. Частина 1. Розвиток координаційних здібностей засобами фізичних вправ та спортивних ігор/ Physical education. Part 1. Development of coordination skills through physical exercises and sports games.	4	залік/test
ПО 2.2	Фізичне виховання. Частина 2. Прискорене пересування та легка атлетика, спортивні ігри/ Physical education. Part 2. Accelerated movement and athletics, sports games.	4	залік/test
ПО 2.3	Фізичне виховання. Частина 3. Гімнастика, прискорене пересування та спортивні ігри/ Physical education. Part	4	залік/test

	3. Gymnastics, accelerated movement and sports games.		
ПО 2.4	Фізичне виховання. Частина 4. Удосконалення силових якостей та витривалості/ Physical education. Part 4. Improve strength and endurance.	4	залік/test
ПО 3	Інформаційно-комунікаційні мережі/Information-communication networks.	4	залік/test
ПО 4	Теоретична криптологія/ Theoretical cryptology	4	залік/test
ПО 5	Криптографія/Cryptography	4	екзамен/ exam
ПО 6	Криптографія. Курсова робота/ Cryptography. Course work	1	залік/test
ПО 7	Технічний захист інформації/ Technical protection of information.	4	залік/test
ПО 8	Кібербезпека/Cybersecurity.	8	екзамен/ exam
ПО 9	Кібербезпека. Курсовий проект/ Cybersecurity. Course work.	2	залік/test
ПО 10	Основи протидії технічним розвідкам/ Fundamentals of counteraction technical intelligence.	3	залік/test
ПО 11	Нормативно-правове забезпечення інформаційної безпеки/Regulatory and legal support of information security	3	залік/test
ПО 12	Основи створення комплексних систем захисту інформації/Fundamentals of creating integrated security systems information.	4	екзамен/ exam
ПО 13	Основи створення комплексних систем захисту інформації. Курсова робота/Fundamentals of creating integrated security systems information. Course work.	1	залік/test
ПО 14	Основи убезпечення інформації від витоку технічними каналами/ Fundamentals of protecting information from leakage through technical channels.	4	екзамен/ exam
ПО 15	Основи убезпечення інформації від витоку технічними каналами. Курсова робота/ Fundamentals of protecting information from leakage through technical channels. Course work.	1	залік/test

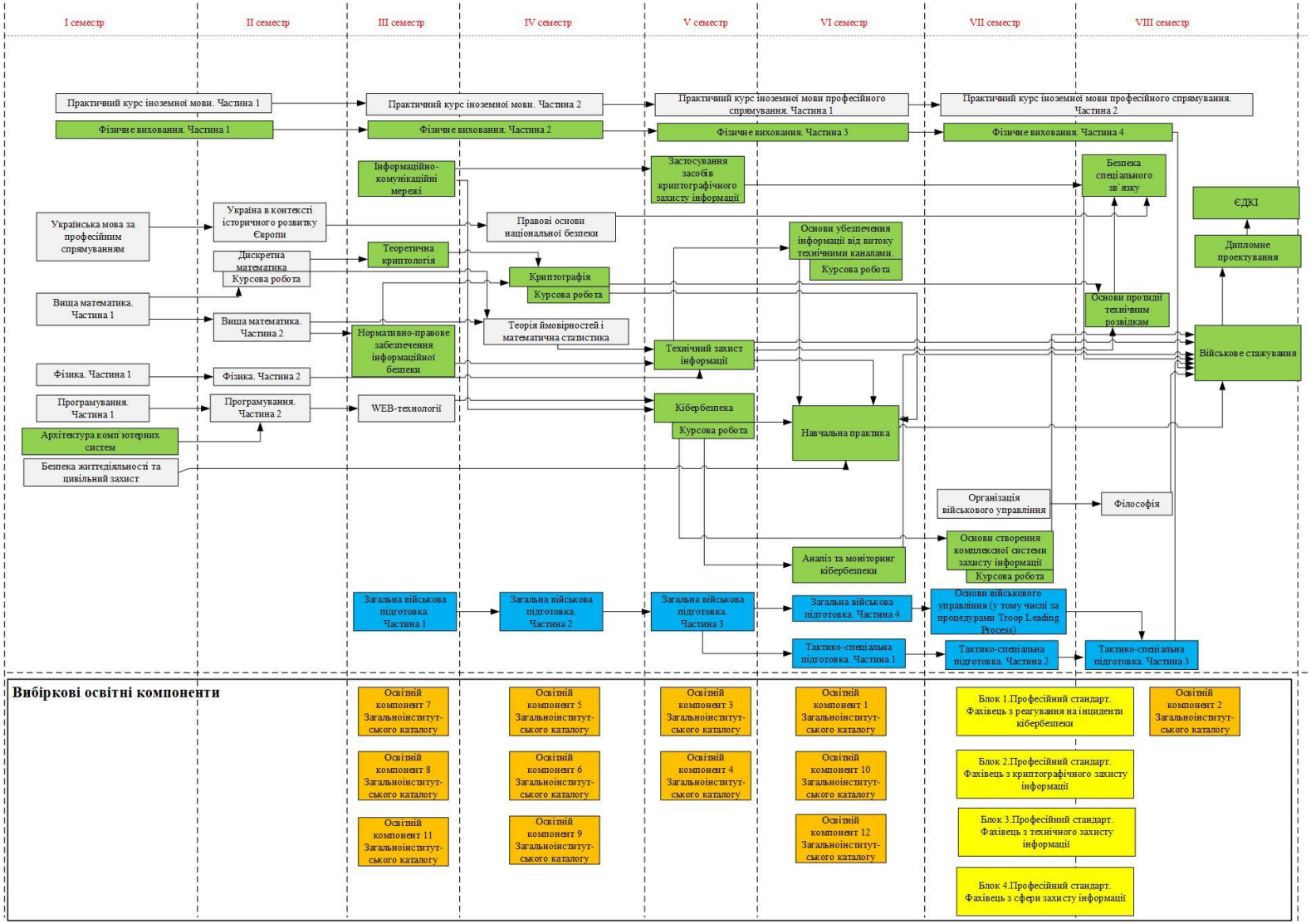
ПО 16	Застосування засобів криптографічного захисту інформації/Application of cryptographic information security tools.	3	залік/test
ПО 17	Безпека спеціального зв'язку/Security of special communications.	3	залік/test
ПО 18	Навчальна практика/ Educational practice.	2	залік/test
ПО 19	Військове стажування/ Military internship	3	залік/test
ПО 20	Дипломне проєктування/ Diploma design	6	захист/ defense
Цикл військово-професійної підготовки/Military-professional training cycle			
Базовий курс тактичного рівня військової освіти (L-1A)/ Basic Course of Tactical Level Military Education (L-1A)			
ВПП 1	Загальна військова підготовка. Частина 1. Основи тактичної підготовки/General military training. Part 1. Fundamentals of tactical training.	3	залік/test
ВПП 2	Загальна військова підготовка. Частина 2. Бойове забезпечення військових підрозділів/General military training. Part 2. Combat support for military units.	5	залік/test
ВПП 3	Загальна військова підготовка. Частина 3. Управління і тактика бойових дій/General military training. Part 3. Management and tactics of combat operations.	5	екзамен/ exam
ВПП 4	Загальна військова підготовка. Частина 4. Основи військового мистецтва/General military training. Part 4. Fundamentals of military art.	4	залік/test
ВПП 5	Основи військового управління (у тому числі за процедурами Troop Leading Process)/ Fundamentals of military management (including Troop Leading Process procedures).	3	залік/test
Фаховий курс тактичного рівня військової освіти (L-1B)/ Professional Course of Tactical Level Military Education (L-1B			
ВПП 6	Тактико-спеціальна підготовка. Частина 1. Основи організації військового зв’язку/Tactical-specialized training. Part 1. Fundamentals of military	4	залік/test

	communications organization.		
ВПП 7	Тактико-спеціальна підготовка. Частина 2. Організація урядового зв'язку/Tactical-specialized Training. Part 2. Organisation of government communications.	4	залік/test
ВПП 8	Тактико-спеціальна підготовка. Частина 3. Управління підрозділами урядового зв'язку/Tactical-specialized Training. Part 3. Managing government communications units.	5	екзамен/ exam
Вибіркові компоненти/Elective components			
Цикл професійної підготовки/Professional training cycle			
Вибіркові освітні компоненти Ф-каталогу**/** Elective educational components of the P-catalog			
ПВ1	Вибіркова дисципліна 1 з Ф-Каталогу/ Elective Subject 1 from P-Catalogue.	4	залік/test
ПВ2	Вибіркова дисципліна 2 з Ф-Каталогу/ Elective Subject 2 from P-Catalogue.	4	залік/test
ПВ3	Вибіркова дисципліна 3 з Ф-Каталогу/ Elective Subject 3 from P-Catalogue.	4	залік/test
ПВ4	Вибіркова дисципліна 4 з Ф-Каталогу/ Elective Subject 4 from P-Catalogue.	4	залік/test
ПВ5	Вибіркова дисципліна 5 з Ф-Каталогу/ Elective Subject 5 from P-Catalogue.	4	залік/test
ПВ6	Вибіркова дисципліна 6 з Ф-Каталогу/ Elective Subject 6 from P-Catalogue.	4	залік/test
ПВ7	Вибіркова дисципліна 7 з Ф-Каталогу/ Elective Subject 7 from P-Catalogue.	4	залік/test
ПВ8	Вибіркова дисципліна 8 з Ф-Каталогу/ Elective Subject 8 from P-Catalogue.	4	залік/test
ПВ9	Вибіркова дисципліна 9 з Ф-Каталогу/ Elective Subject 9 from P-Catalogue.	4	залік/test
ПВ10	Вибіркова дисципліна 10 з Ф-Каталогу/ Elective Subject 10 from P-Catalogue.	4	залік/test

ПВ11	Вибіркова дисципліна 11 з Ф-Каталогу/ Elective Subject 11 from P-Catalogue.	4	залік/test
ПВ12	Вибіркова дисципліна 12 з Ф-Каталогу/ Elective Subject 12 from P-Catalogue.	4	залік/test
Вибіркові освітні компоненти блочного вибору/ Selective educational components of the block programme			
Блок 1. Професійний стандарт. Фахівець з реагування на інциденти кібербезпеки / Block 1. Professional standard. Specialist in response cybersecurity incident			
ПВ13	Аналіз вразливостей інформаційних систем/ Analysis of information system vulnerabilities.	4	залік/test
ПВ14	Безпека інформаційно-комунікаційних систем/ Security of information and communication systems.	4	залік/test
ПВ15	Тематичні дослідження для систем спеціального зв'язку (в частині суміжних напрямків) 1./Case studies for special communication systems (in terms of related areas) 1.	4	залік/test
Блок 2. Професійний стандарт. Фахівець з криптографічного захисту інформації/Block 2. Professional standard Specialist in cryptographic information security			
ПВ13	Моніторінг та оцінювання рівня безпеки криптографічного захисту інформації в державних установах/Monitoring and assessment of the level of security of cryptographic protection of information in state institutions.	4	залік/test
ПВ14	Криптографічні протоколи/Cryptographic protocols.	4	залік/test
ПВ15	Тематичні дослідження для систем спеціального зв'язку (в частині суміжних напрямків) 2./ Case studies for special communication systems (in terms of related areas) 2.	4	залік/test
Блок 3. Професійний стандарт. Фахівець з технічного захисту інформації / Block 3. Professional standard Specialist in technical information security			
ПВ13	Створення та атестація комплексів технічного захисту інформації на об’єктах інформаційної діяльності/ Creation and certification of technical information security complexes at information facilities.	4	залік/test

ПВ14	Основи спеціальних досліджень/Fundamentals of specialised research.	4	залік/test
ПВ15	Тематичні дослідження для систем спеціального зв'язку (в частині суміжних напрямків) 3./ Case studies for special communication systems (in terms of related areas) 3.	4	залік/test
Блок 4. Професійний стандарт. Фахівець сфери захисту інформації / Block 4. Professional standard Specialist in information security			
ПВ13	Створення та оцінювання систем захисту інформації в інформаційних системах/Creating and evaluating information security systems in information systems.	4	залік/test
ПВ14	Організація та здійснення державного контролю в сфері криптографічного та технічного захисту інформації/Organisation and implementation of state control in the field of cryptographic and technical protection of information/	4	залік/test
ПВ15	Тематичні дослідження для систем спеціального зв'язку/Case studies for special communication systems.	4	залік/test
		Загальний обсяг обов'язкових компонентів/ Total scope of the required components:	180
		Загальний обсяг вибіркових компонентів/ 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	147
		Обсяг освітніх компонентів, що забезпечують здобуття компетентностей визначених ***L-1A, L-1B/*** Total scope of the educational components aimed at acquisition of competencies specified in the ***L-1A, L-1B***	33
		ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ/ OTAL SCOPE 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 “Безпека державних інформаційних ресурсів” здійснюється у формі єдиного державного кваліфікаційного іспиту та захисту кваліфікаційної роботи/проекту бакалавра, що забезпечує оцінювання досягнутих програмних результатів навчання, визначених стандартом вищої освіти за спеціальністю 125 “Кібербезпека та захист інформації” для першого (бакалаврського) рівня вищої освіти та освітньо-професійною програмою.

До атестації допускаються здобувачі, які успішно виконали освітньо-професійну програму підготовки. Кваліфікаційна робота/проект передбачає розв’язування складної спеціалізованої задачі у сфері кібербезпеки та захисту інформації і не може містити академічного плагіату та фальсифікації. З цією метою робота перевіряється на наявність плагіату згідно з процедурою, визначеною системою забезпечення якості освітньої діяльності та якості вищої освіти Університетом.

Атестація здійснюється з дотриманням відкритості та публічності. В разі наявності в кваліфікаційній роботі/проекті інформації з обмеженим доступом, то захист проводиться в закритому режимі з неухильним дотриманням і виконанням вимог чинного законодавства щодо збереження службової та державної таємниці.

Attestation of applicants for higher education in the educational and professional program "Security of State Information Resources" is carried out in the form of a single state qualification exam and defense of a bachelor's thesis/project, which provides an assessment of the achieved program learning outcomes defined by the standard of higher education in the specialty 125 "Cybersecurity and Information Protection" for the first (bachelor's) level of higher education and the educational and professional program.

Applicants who have successfully completed the educational and professional training programme are admitted to certification. The qualification work/project provides for the ability of the higher education applicant to solve a complex specialised problem in the field of cybersecurity and information protection and may not contain academic plagiarism and falsification. To this end, the work is checked for plagiarism in accordance with the procedure determined by the University's system of ensuring the quality of educational activities and the quality of higher education.

Attestation is carried out in an open and public manner. If the qualification work/project contains information with restricted access, the defence is conducted in a closed mode with strict observance and fulfilment of the requirements of the current legislation on the preservation of official and state secrets.

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

	ЗО 1	ЗО 2	ЗО 3	ЗО 4	ЗО 5	ЗО 6	ЗО 7	ЗО 8	ЗО 9	ЗО 10	ЗО 11	ЗО 12	ЗО 13	ПО 1	ПО 2	ПО 3	ПО 4	ПО 5	ПО 6	ПО 7	ПО 8	ПО 9	ПО 10	ПО 11	ПО 12	ПО 13	ПО 14	ПО 15	ПО 16	ПО 17	ПО 18	ПО 19	ПО 20
ЗК1	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+			+	+	+	+	+		+	+	+
ЗК2	+	+	+		+	+	+	+	+							+	+	+	+	+	+	+			+	+	+	+	+		+	+	+
ЗК3	+		+	+			+				+	+									+				+	+	+		+		+	+	+
ЗК4		+			+	+		+			+	+	+	+		+	+	+	+	+								+			+	+	+
ЗК5		+				+			+	+	+	+										+			+	+			+			+	+
ЗК6			+		+						+	+																				+	+
ЗК7		+									+	+			+																		+
ЗК8	+																																
ФК1			+	+													+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ФК2	+					+		+	+				+	+		+					+	+			+	+			+		+	+	+
ФК3																					+	+			+	+			+		+	+	+
ФК4																					+	+			+						+	+	+
ФК5																	+	+			+	+		+		+			+			+	+
ФК6							+									+					+	+										+	+
ФК7						+	+																		+	+	+					+	+
ФК8																																+	+

ФК9																							+	+						+		+	+
ФК10						+	+						+					+	+	+			+				+	+	+	+	+	+	+
ФК11																																+	+
ФК12							+						+											+	+	+				+		+	+
ФК13																		+	+		+												+

5.1 МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ З ВІЙСЬКОВО-ПРОФЕСІЙНОЇ ПІДГОТОВКИ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ/COMPLIANCE MATRIX OF PROGRAMME COMPETENCIES MILITARY PROFESSIONAL TRAINING WITH PROGRAMME COMPONENTS

	ВПП 1	ВПП 2	ВПП 3	ВПП 4	ВПП 5	ВПП 6	ВПП 7	ВПП 8
ВПК1		+						
ВПК2	+				+			
ВПК3				+	+			
ВПК4				+				
ВПК5			+					
ВПК6			+					
ВПК7			+					
ВПК8			+					
ВПК9						+		
ВПК10		+						
ВПК11		+						
ВПК12				+				
ВСК1						+		
ВСК2							+	
ВСК3								+
ВСК4								+

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

	ЗО 1	ЗО 2	ЗО 3	ЗО 4	ЗО 5	ЗО 6	ЗО 7	ЗО 8	ЗО 9	ЗО 10	ЗО 11	ЗО 12	ЗО 13	ПО 1	ПО 2	ПО 3	ПО 4	ПО 5	ПО 6	ПО 7	ПО 8	ПО 9	ПО 10	ПО 11	ПО 12	ПО 13	ПО 14	ПО 15	ПО 16	ПО 17	ПО 18	ПО 19	ПО 20
ПРН1	+	+	+	+							+	+									+	+		+	+	+			+	+	+	+	+
ПРН2		+				+		+		+			+	+			+	+	+			+	+	+					+	+		+	+
ПРН3		+				+			+				+	+			+	+	+			+	+	+	+	+				+		+	+
ПРН4		+			+	+		+		+			+	+			+	+	+		+		+	+					+	+	+	+	+
ПРН5		+				+							+								+		+	+						+	+	+	+
ПРН6		+				+		+			+	+	+	+																		+	+
ПРН7				+							+	+						+	+		+	+	+	+	+		+	+	+	+	+	+	+
ПРН8											+																+	+				+	+
ПРН9				+																	+	+								+	+		+
ПРН 10						+								+		+											+		+				+
ПРН 11																															+		+
ПРН 12						+	+													+					+	+					+		+
ПРН 13																															+	+	+

ПРН 14																														+	+
ПРН 15										+				+		+														+	+	+
ПРН 16																			+					+	+					+		+
ПРН 17																						+		+						+	+	+
ПРН 18																				+	+			+	+	+	+			+		+
ПРН 19												+				+	+	+													+	+
ПРН 20																								+						+		+
ПРН 21																				+	+										+	+
ПРН 22																	+			+	+				+						+	+
ПРН 23																	+			+	+	+		+	+					+		+
ПРН 24																				+	+										+	+
ПРН 25																				+	+										+	+
ПРН 26																								+	+					+		+
ПРН																	+							+	+			+			+	+

27																															
ПРН 28													+												+						+	+
ПРН 29																									+						+	+
ПРН 30																															+	+
ПРН 31													+												+	+	+	+			+	+
ПРН 32																+					+	+									+	+
ПРН 33																															+	+
ПРН 34																							+							+	+	+
ПРН 35																		+							+	+					+	+
ПРН 36							+													+							+				+		+
ПРН 37							+													+							+				+		+
ПРН 38							+													+							+	+			+		+
ПРН 39																																+	+
ПРН 40							+													+							+	+			+		+

ПРН 41																														+		+
ПРН 42																		+													+	+
ПРН 43																							+								+	+
ПРН 44																															+	+
ПРН 45																															+	+
ПРН 46																															+	+
ПРН 47																	+	+	+										+	+	+	+
ПРН 48																	+	+	+											+	+	+
ПРН 49																															+	+
ПРН 50																														+		+
ПРН 51																														+		+
ПРН 52																														+		+
ПРН 53										+																				+		+
ПРН			+								+	+			+								+	+					+			+

54																															
ПРН 55																					+			+							+
ПРН 56														+			+	+		+	+								+			

6.1. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ З ВІЙСЬКОВО-ПРОФЕСІЙНОЇ ПІДГОТОВКИ ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ/ COMPLIANCE MATRIX OF PROGRAMME LEARNING OUTCOMES IN MILITARY-PROFESSIONAL TRAINING WITH PROGRAMME COMPONENTS

	ВПП 1	ВПП 2	ВПП 3	ВПП 4	ВПП 5	ВПП 6	ВПП 7	ВПП 8
ПРНВПП 1			+					
ПРНВПП 2	+				+			
ПРНВПП 3				+	+			
ПРНВПП 4				+				
ПРНВПП 5			+					
ПРНВПП 6		+						
ПРНВПП 7		+						
ПРНВПП 8		+						
ПРНВПП 9						+		
ПРНВПП 10			+					
ПРНВПП 11			+					
ПРНВПП 12				+				
ПРНВПП 13						+		
ПРНВПП 14							+	
ПРНВПП 15								+
ПРНВПП 16								+