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

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

ЗАТВЕРДЖЕНО / APPROVED

Вченою радою КПІ ім. Ігоря Сікорського / by the Academic Council of Igor Sikorsky Kyiv Polytechnic Institute
(протокол / minutes of meeting №___
від / dated _____ 20___)

Голова Вченої ради / Head of the Academic Council

_____ *Михайло ІЛЬЧЕНКО / Mykhailo ILCHENKO*

БЕЗПЕКА ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ
SECURITY OF STATE INFORMATION RESOURCES

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА /
EDUCATIONAL PROFESSIONAL PROGRAMME

Перший (бакалаврський) рівень вищої освіти Спеціальність: F5 Кібербезпека та захист інформації Галузь знань: F Інформаційні технології Кваліфікація: Бакалавр з кібербезпеки та захисту інформації	The first (bachelor) level of higher education Speciality: F5 Cyberse curity and data protection Knowledge branch: F Information technologies Qualification: Bachelor's degree in cyber security and data protection

ID 81876

Введено в дію з / Enacted since
20___/20___ навчального року / academic year
наказом ректора / by rector's order
№_____ від / dated _____20___

Київ / Kyiv
2026

В 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

ЛИСТ ПОГОДЖЕННЯ / LETTER OF APPROVAL

Безпека державних інформаційних ресурсів / Security of state information resources

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА / EDUCATIONAL PROFESSIONAL PROGRAMME

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

за спеціальністю/ speciality	**F5 Кібербезпека та захист інформації / F5 Cybersecurity and data protection**
галузі знань / knowledge branch	**F Інформаційні технології / F Information technologies**
Кваліфікація / Qualification	**Бакалавр з кібербезпеки та захисту інформації/ Bachelor's degree in cybersecurity and data protection**

ПОГОДЖЕНО / APPROVED

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

_____ Олександр ПОТІЙ / Oleksandr POTII

___.___.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___

ПРЕАМБУЛА / PREAMBLE

РОЗРОБЛЕНО / DESIGNED:

Керівник робочої групи / Head of the project team:
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 робочої групи / Project team members:
Голь Владислав Дмитрович, кандидат технічних наук, професор, завідувач Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського / Vladyslav HOL, candidate of technical sciences, professor, head of the Special department № 1 ISCIP of the Igor Sikorsky Kyiv Polytechnic Institute.
Іванченко Сергій Олександрович, доктор технічних наук, професор, професор Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського / 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, професор, професор Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського /Anton Oleksiichuk, doctor of technical sciences, professor, professor of the Special department № 1 ISCIP of the Igor Sikorsky Kyiv Polytechnic Institute.
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, доцент Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського /Anton Storchak, candidate of technical sciences, associate professor, associate professor of the Special department № 1 ISCIP of the Igor Sikorsky Kyiv Polytechnic Institute.
Іванов Андрій Васильович, кандидат технічних наук, у розпорядженні Голови Державної служби спеціального зв'язку та захисту інформації України / Andriy Ivanov, candidate of technical sciences, at the disposal of the Head of the State Service for Special Communications and Information Protection of Ukraine.
Мишеніна Альона Ігорівна, курсантка магістерського курсу (спеціальність: F5 Кібербезпека та захист інформації) ІСЗЗІ КПІ ім. Ігоря Сікорського / Myshenina Alyona Ihorivna, master's degree cadet (speciality: F5 Cybersecurity and data protection) ISCIP of the Igor Sikorsky Kyiv Polytechnic Institute.
Лук'янчук Євген Олександрович, курсант бакалаврського курсу (спеціальність: F5 Кібербезпека та захист інформації) ІСЗЗІ КПІ ім. Ігоря Сікорського / Myshenina Alyona Ihorivna, bachelor's degree student (speciality: F5 Cybersecurity and data protection) ISCIP of the Igor Sikorsky Kyiv Polytechnic Institute.

ПОГОДЖЕНО / AGREED:

Науково-методична комісія університету зі спеціальності F5 Кібербезпека та захист інформації (для ІСЗЗІ) / The Scientific and Methodological Commission of the University on specialty F5 Cyber security and data protection (for ISCIP) (протокол / minutes of meeting №__ від / dated _____ 20___)
Голова НМКУ- F5 (для ІСЗЗІ) / Head of the SMCU- F5 (for ISCIP)
_____ Владислав Голь / Vladyslav HOL

Методична рада КПІ ім. Ігоря Сікорського / The Methodological Council of Igor Sikorsky Kyiv Polytechnic Institute (протокол / minutes of meeting №___ від / dated _____ 20___)
Голова Методичної ради / Head of the Methodological Council
_____ Тетяна ЖЕЛЯСКОВА/ Tatiana ZHELIASKOVA

ВРАХОВАНО / CONSIDERED:

1. Закон України від 27.03.2025 № 4336-IX.,"Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури". https://cip.gov.ua/ua/news/perelik-normativno-pravovikh-aktiv-na-vikonannya-zakonu-4336-ix.
2. Розпорядження Кабінету Міністрів України від 3 грудня 2025р. № 1383-р. Київ. "Про затвердження операційного плану заходів з реалізації у 2025-2028 роках Стратегії розвитку вищої освіти в Україні на 2022-2032 роки та внесення змін до Стратегії розвитку вищої освіти в Україні на 2022-2032 роки." https://zakon.rada.gov.ua/laws/show/1383-2025-%D1%80#Text .
3. Наказ Мінекономіки від 13.12.2024 № 27751 "Про затвердження Зміни № 14 до національного класифікатора ДК 003:2010". https://me.gov.ua/view/074d6e7f-41e2-4bfc-8e77-31d110cacc90.
4. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 29.12.2025 №865 "Про затвердження професійних стандартів у сфері захисту критичної інфраструктури".
5. Постанови Кабінету Міністрів України від 31 грудня 2025 року № 1799 "Про затвердження Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури". https://cip.gov.ua/ua/news/uryad-zatverdiv-novii-poryadok-ocinyuvannya-stanu-kiberzakhistu
6. Розпорядження Міністерства освіти і науки України Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» (КПІ ім. Ігоря Сікорського) від 21.11.2025 № РП/400/25. "Про щорічний моніторинг та оновлення освітніх програм КПІ ім. Ігоря Сікорського".

1. Law of Ukraine dated 27 March 2025 No. 4336-IX, "On Amendments to Certain Laws of Ukraine Regarding Information Protection and Cyber Protection of State Information Resources and Critical Information Infrastructure Facilities.".https://cip.gov.ua/ua/news/perelik-normativno-pravovikh-aktiv-na-vikonannya-zakonu-4336-ix.
2. Decree of the Cabinet of Ministers of Ukraine dated 3 December 2025 No. 1383-r. Kyiv. "On approval of the operational plan of measures for the implementation in 2025-2028 of the Strategy for the Development of Higher Education in Ukraine for 2022-2032 and amendments to the Strategy for the Development of Higher Education in Ukraine for 2022-2032." https://zakon.rada.gov.ua/laws/show/1383-2025-%D1%80#Text .
3. Order of the Ministry of Economy dated 13 December 2024 No. 27751 "On Approval of Amendment No. 14 to the National Classifier DK 003:2010". https://me.gov.ua/view/074d6e7f-41e2-4bfc-8e77-31d110cacc90.
4. Order of the Administration of the State Service for Special Communications and Information Protection of Ukraine dated 29 December 2025 No. 865 "On Approval of Professional Standards in the Field of Critical Infrastructure Protection".
5. Resolution of the Cabinet of Ministers of Ukraine No. 1799 dated 31 December 2025 "On Approval of the Procedure for Assessing the State of Cyber Protection of Information, Electronic Communication and Information and Communication Systems, Critical Infrastructure Facilities, and Critical Information Infrastructure Facilities." https://cip.gov.ua/ua/news/uryad-zatverdiv-novii-poryadok-ocinyuvannya-stanu-kiberzakhistu.
6. Order of the Ministry of Education and Science of Ukraine National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" (Igor Sikorsky KPI) dated 21 November 2025 No. RP/400/25. "On the annual monitoring and updating of educational programmes at Igor Sikorsky KPI".

ЕВОЛЮЦІЯ ОСВІТНЬОЇ ПРОГРАМИ / EVOLUTION OF THE EDUCATIONAL PROGRAMME:

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».
2024 рік – оновлення ОП з метою врахування:
Постанови 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
Наказу 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». https://zakon.rada.gov.ua/laws/show/z0453-24#Text
Наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 23 січня 2024 року № 38.
Проекту 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
Розпорядження КАБІНЕТУ МІНІСТРІВ УКРАЇНИ від 18 жовтня 2024 р. № 1021-р Київ. «Про затвердження плану заходів з реалізації Концепції реформування Державної служби спеціального зв'язку та захисту інформації України на 2024-2025 роки». https://zakon.rada.gov.ua/laws/show/1021-2024-%D1%80#Text.
Наказу Міністерства освіти і науки України №1547 від 29 жовтня 2024 року про внесення змін до Стандарту вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для першого (бакалаврського) рівня вищої освіти. https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2024/30-10-2024/125-kiberbezpeka-bakalavr-1547-vid-29-10-2024.pdf
2025 рік – оновлення ОП з метою врахування:
Наказу Міністерства освіти і науки України від 19.11.2024 № 1625. «Про особливості запровадження змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка

здобувачів вищої та фахової передвищої освіти, затверджених постановою Кабінету Міністрів України від 30 серпня 2024 року № 1021. https://zakon.rada.gov.ua/laws/show/z1833-24#Text.
2026 рік – оновлення ОП з метою врахування:
1. Закон України від 27.03.2025 № 4336-IX.,"Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури". https://cip.gov.ua/ua/news/perelik-normativno-pravovikh-aktiv-na-vikonannya-zakonu-4336-ix.
2. Розпорядження Кабінету Міністрів України від 3 грудня 2025р. № 1383-р. Київ. "Про затвердження операційного плану заходів з реалізації у 2025-2028 роках Стратегії розвитку вищої освіти в Україні на 2022-2032 роки та внесення змін до Стратегії розвитку вищої освіти в Україні на 2022-2032 роки." https://zakon.rada.gov.ua/laws/show/1383-2025-%D1%80#Text
3. Наказ Мінекономіки від 13.12.2024 № 27751 "Про затвердження Зміни № 14 до національного класифікатора ДК 003:2010". https://me.gov.ua/view/074d6e7f-41e2-4bfc-8e77-31d110cacc90.
4. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 29.12.2025 №865 "Про затвердження професійних стандартів у сфері захисту критичної інфраструктури".
5. Постанови Кабінету Міністрів України від 31 грудня 2025 року № 1799 "Про затвердження Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури". https://cip.gov.ua/ua/news/uryad-zatverdiv-novii-poryadok-ocinyuvannya-stanu-kiberzakhistu.

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.
2024 рік – відповідно до Постанови 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).
– зміни пов'язані з реалізацією Концепції трансформації системи військової освіти та введенням на тактичному рівні військової освіти у вищих військових навчальних закладах, військових навчальних підрозділах закладів вищої освіти курсів професійної військової освіти базового (L-1A) та фахового (L-1B);
– відповідно до Наказу 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»;
– зміни пов'язані з впровадженням військово-професійних компетентностей та військово-спеціальних компетентностей, специфічних компетентностей, які визначаються професійним стандартом військового фахівця Збройних Сил України за військово-обліковою спеціальністю (спорідненими військово-обліковими спеціальностями) та необхідні для виконання службових (бойових) функцій на посаді за призначенням в умовах мирного часу та в особливий період і не

повинні повторювати (дублювати) компетентності, визначені у відповідних стандартах вищої, фахової передвищої освіти за спеціальностями;
– відповідно до Наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 23 січня 2024 року № 38, зміни пов'язані з введенням в дію професійних стандартів: Фахівець з реагування на інциденти кібербезпеки; Фахівець з криптографічного захисту інформації; Фахівець з технічного захисту інформації; Фахівець сфери захисту інформації;
– відповідно до доповнення в Стандарт вищої освіти зі спеціальності 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для першого (бакалаврського) рівня вищої освіти, затвердженого наказом Міністерства освіти і науки України від 04.10.2018 № 1074, позиції «Загальні компетентності» розділу «IV. Перелік компетентностей випускника» пунктом 8. Чинна редакція від 29.10.2024;
– зміни пов'язані з доповненням до загальних компетентностей випускника пункту «КЗ 8. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності»;
– відповідно до Розпорядження Кабінету Міністрів України від 18 жовтня 2024 р. № 1021-р Київ. "Про затвердження плану заходів з реалізації Концепції реформування Державної служби спеціального зв'язку та захисту інформації України на 2024-2025 роки".
– зміни пов'язані з впровадженням вимог професійних стандартів та приведення в відповідність з вимогам визначеними в відомостях з баз даних ESCO (ECSF);
– відповідно до Наказ Міністерства освіти і науки України №1547 від 29 жовтня 2024 року про внесення змін до Стандарту вищої освіти за спеціальністю 125 "Кібербезпека" галузі знань 12 "Інформаційні технології" для першого (бакалаврського) рівня вищої освіти;
– зміни пов'язані з впровадженням оновлених програмних компетентностей та результатів навчання.
2025 рік – відповідно до Наказом Міністерства освіти і науки України від 19.11.2024 № 1625. "Про особливості запровадження змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти, затверджених постановою Кабінету Міністрів України від 30 серпня 2024 року № 1021".
– зміни пов'язані з введенням в дію нових кодів і найменувань спеціальностей.
2026 рік – відповідно до Закону України від 27.03.2025 № 4336-IX."Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури".
– зміни пов'язані з впровадженням комплексного підхіду до управління ризиками, реагування на кіберзагрози та розбудови професійної кіберспільноти. Для повної реалізації норм Закону передбачено прийняття низки підзаконних актів – постанов Кабінету Міністрів та наказів Адміністрації Держспецзв'язку, які деталізують та впроваджують його положення на практиці.
– відповідно до Розпорядження Кабінету Міністрів України від 3 грудня 2025р. № 1383-р. Київ. "Про затвердження операційного плану заходів з реалізації у 2025-2028 роках Стратегії розвитку вищої освіти в Україні на 2022-2032 роки та внесення змін до Стратегії розвитку вищої освіти в Україні на 2022-2032 роки."
– зміни пов'язані з запровадженням оновленням змісту ОК ПВ3: "Основи проектування цифрових засобів" з введенням занять з нової галузі сучасних технологій – Інтернет речей або IoT, що відповідає завданню сприяння використанню інноваційних технологій і новітніх засобів навчання в освітньому процесі;
– зміни пов'язані з запровадженням оновленням змісту ОК В15: "Документальне забезпечення захисту і стійкості критичної інфраструктури", що відповідає завданню розвитку загальних компетентностей, правової культури, рухової активності, спорту та студентських змагань;
– зміни пов'язані з оновленням формулювання мети освітньо-професійної програми, що відповідає завданнями: підтримки міжнародної академічної мобільності студентів, а також направлення на навчання до іноземних університетів; гармонізації структури вищої освіти відповідно до зобов'язань країн-членів Європейського простору вищої освіти; розвитку національної системи кваліфікацій; трансформації освіти в секторі безпеки та оборони відповідно до доктринальних підходів і принципів НАТО.

– відповідно до Наказ Мінекономіки від 13.12.2024 № 27751 "Про затвердження Зміни № 14 до національного класифікатора ДК 003:2010".
– зміни пов'язані з унесенням до розділу 5 «КЛАСИФІКАЦІЯ ПРОФЕСІЙ» національного класифікатора ДК 003:2010 в професійних назвах робіт унесено: фахівець із захисту та стійкості критичної інфраструктури;
– відповідно до Наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 29.12.2025 №865 "Про затвердження професійних стандартів у сфері захисту критичної інфраструктури".
– зміни пов'язані з введенням в дію професійного стандарту: "Фахівець із захисту та стійкості критичної інфраструктури" з урахуванням та приведення в відповідність з вимогами визначеними в відомостях з баз даних ISCO/ ESCO (ECSF), що підсилює позиції ОПП у співпраці з роботодавцями та міжнародними проєктами;
– відповідно до Постанови Кабінету Міністрів України від 31 грудня 2025 року № 1799 "Про затвердження Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури".
– зміни пов'язані з запровадженням оновлення змісту ОК В15: "Документальне забезпечення захисту і стійкості критичної інфраструктури".

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».
2024 – update of the EP to take into account:
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
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». https://zakon.rada.gov.ua/laws/show/z0453-24#Text

Order of the Administration of the State Service for Special Communications and Information Protection of Ukraine dated 23 January 2024 No. 38.
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.
Order of the Ministry of Education and Science of Ukraine No. 1547 of 29 October 2024 on amendments to 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. https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2024/30-10-2024/125-kiberbezpeka-bakalavr-1547-vid-29-10-2024.pdf
2025 – update of the EP to take into account:
Order of the Ministry of Education and Science of Ukraine dated 19.11.2024 No. 1625. 'On the peculiarities of introducing changes to the list of fields of knowledge and specialities in which applicants for higher and professional higher education are trained, approved by the Resolution of the Cabinet of Ministers of Ukraine of 30 August 2024 No. 1021. https://zakon.rada.gov.ua/laws/show/z1833-24#Text.
2026 – update of the EP to take into account:
Law of Ukraine dated 27 March 2025 No. 4336-IX, "On Amendments to Certain Laws of Ukraine Regarding Information Protection and Cyber Protection of State Information Resources and Critical Information Infrastructure Facilities.".https://cip.gov.ua/ua/news/perelik-normativno-pravovikh-aktiv-na-vikonannya-zakonu-4336-ix.
Decree of the Cabinet of Ministers of Ukraine dated 3 December 2025 No. 1383-r. Kyiv. "On approval of the operational plan of measures for the implementation in 2025-2028 of the Strategy for the Development of Higher Education in Ukraine for 2022-2032 and amendments to the Strategy for the Development of Higher Education in Ukraine for 2022-2032." https://zakon.rada.gov.ua/laws/show/1383-2025-%D1%80#Text .
Order of the Ministry of Economy dated 13 December 2024 No. 27751 "On Approval of Amendment No. 14 to the National Classifier DK 003:2010". https://me.gov.ua/view/074d6e7f-41e2-4bfc-8e77-31d110cacc90.
Order of the Administration of the State Service for Special Communications and Information Protection of Ukraine dated 29 December 2025 No. 865 "On Approval of Professional Standards in the Field of Critical Infrastructure Protection".
Resolution of the Cabinet of Ministers of Ukraine No. 1799 dated 31 December 2025 "On Approval of the Procedure for Assessing the State of Cyber Protection of Information, Electronic Communication and Information and Communication Systems, Critical Infrastructure Facilities, and Critical Information Infrastructure Facilities." https://cip.gov.ua/ua/news/uryad-zatverdiv-novii-poryadok-ocinyuvannya-stanu-kiberzakhistu.

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.

2024 – in accordance with the Resolution of the Cabinet of Ministers of Ukraine of 15 December 1997 No. 1410 'On the Transformation of the Military Education System' (as amended by the Resolution of the Cabinet of Ministers of Ukraine No. 1490 of 30 December 2022). Entered into force on 04.01.2023).
– changes are related to the implementation of the Concept of Transformation of the Military Education System and the introduction of basic (L-1A) and professional (L-1B) military education courses at the tactical level of military education in higher military educational institutions and military educational units of higher education institutions;
– in accordance with the Order of the Ministry of Defence of Ukraine dated 15 February 2024 No. 120 'On Approval of the Regulation on the Peculiarities of Organising the Educational Process in Higher Military Educational Institutions of the Ministry of Defence of Ukraine, Military Educational Units of Higher Education Institutions, and Institutions of Professional Higher Military Education';
– changes are related to the introduction of military professional competences and military special competences, specific competences defined by the professional standard of a military specialist of the Armed Forces of Ukraine in a military speciality (related military specialities) and necessary to perform official (combat) functions in the position of assignment in peacetime and in a special period and should not repeat (duplicate) the competences defined in the relevant standards of higher, professional education.
– in accordance with the Order of the Administration of the State Service for Special Communications and Information Protection of Ukraine dated 23 January 2024 No. 38, changes related to the introduction of professional standards: Cybersecurity Incident Response Specialist; Cryptographic Information Protection Specialist; Technical Information Protection Specialist; Information Security Specialist;
– in accordance with the addition to 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, approved by the order of the Ministry of Education and Science of Ukraine dated 04.10.2018 № 1074, the position 'General competencies' of the section 'IV. List of graduate competences section 8. Current version as of 29.10.2024;
– the changes are related to the addition of the item 'CG 8. Ability to make decisions and act in accordance with the principle of inadmissibility of corruption and any other manifestations of dishonesty;
– in accordance with the Order of the Cabinet of Ministers of Ukraine of 18 October 2024 No. 1021-r Kyiv. 'On Approval of the Action Plan for the Implementation of the Concept of Reforming the State Service for Special Communications and Information Protection of Ukraine for 2024-2025';
– the changes related to the implementation of professional standards and alignment with the requirements set out in the ESCO database (ECSF);
– in accordance with the Order of the Ministry of Education and Science of Ukraine No. 1547 dated 29 October 2024 on Amendments to 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;
– the changes are related to the introduction of updated programme competences and learning outcomes.
2025 – in accordance with the Order of the Ministry of Education and Science of Ukraine dated 19.11.2024 No. 1625. 'On the peculiarities of introducing amendments to the list of fields of knowledge and specialities in which applicants for higher and professional higher education are trained, approved by the Resolution of the Cabinet of Ministers of Ukraine No. 1021 dated 30 August 2024.
–the changes are related to the introduction of new codes and names of specialities.
2026 – in accordance with the Law of Ukraine dated 27 March 2025 No. 4336-IX, "On Amendments to Certain Laws of Ukraine Regarding Information Protection and Cyber Protection of State Information Resources and Critical Information Infrastructure Facilities".
– changes related to the implementation of a comprehensive approach to risk management, response to cyber threats, and development of a professional cyber community. In order to fully implement the provisions of the Law, a number of subordinate acts are to be adopted, including resolutions of the Cabinet of Ministers and orders of the State Special Communications Service Administration, which will detail and implement its provisions in practice.
– in accordance with the Decree of the Cabinet of Ministers of Ukraine dated 3 December 2025 No. 1383-r. Kyiv. "On approval of the operational plan of measures for the implementation in 2025-2028 of the Strategy for the Development of Higher Education in Ukraine for 2022-2032 and amendments to the Strategy for the Development of Higher Education in Ukraine for 2022-2032."

– changes related to the introduction of updates to the content of OK PV3: 'Fundamentals of Digital Design' with the introduction of classes in a new field of modern technologies – the Internet of Things or IoT, which corresponds to the task of promoting the use of innovative technologies and the latest teaching tools in the educational process;
– changes related to the introduction of updates to the content of OK B15: 'Documentary support for the protection and sustainability of critical infrastructure', which corresponds to the task of developing general competencies, legal culture, physical activity, sports and student competitions;
– changes related to updating the wording of the educational and professional programme objectives, which correspond to the tasks of supporting international academic mobility of students, as well as sending them to study at foreign universities; harmonising the structure of higher education in accordance with the commitments of the member countries of the European Higher Education Area; developing a national qualifications system; transforming education in the security and defence sector in line with NATO's doctrinal approaches and principles.
– in accordance with the Order of the Ministry of Economy dated 13 December 2024 No. 27751 "On Approval of Amendment No. 14 to the National Classifier DK 003:2010".
– changes related to the addition to Section 5 'CLASSIFICATION OF PROFESSIONS' of the national classifier DK 003:2010 in the professional titles of jobs: specialist in critical infrastructure protection and resilience;
– in accordance with the Order of the Administration of the State Service for Special Communications and Information Protection of Ukraine dated 29 December 2025 No. 865 "On Approval of Professional Standards in the Field of Critical Infrastructure Protection".
– changes related to the introduction of the professional standard: 'Critical Infrastructure Protection and Resilience Specialist', taking into account and bringing it into line with the requirements specified in the ISCO/ESCO (ECSF) databases, which strengthens the position of the OPP in cooperation with employers and international projects;
– in accordance with the Resolution of the Cabinet of Ministers of Ukraine No. 1799 dated 31 December 2025 "On Approval of the Procedure for Assessing the State of Cyber Protection of Information, Electronic Communication and Information and Communication Systems, Critical Infrastructure Facilities, and Critical Information Infrastructure Facilities."
– changes related to the introduction of updates to the content of OK B15: 'Documentary support for the protection and resilience of critical infrastructure'.

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ / EDUCATIONAL PROGRAMME PROFILE

1 – Загальна інформація / General information		
Повна назва закладу вищої освіти та навчального підрозділу / Full name of higher education institution and faculty / educational and scientific institute	Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Інститут спеціального зв'язку та захисту інформації	National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Institute of special communication and information protection
Ступінь вищої освіти та назва освітньої кваліфікації / Higher education degree and education qualification title	Ступінь ВО – бакалавр Кваліфікація – бакалавр з кібербезпеки та захисту інформації	Higher ED – bachelor's degree Qualification title - bachelor's degree in cyber security and data protection
Професійна кваліфікація (за наявності) / Professional qualification	Можливо присвоєння професійної кваліфікації шляхом проходження тестування в визначених Державною службою спеціального зв'язку та захисту інформації України Кваліфікаційному центрі інформаційних технологій і кібербезпеки після отримання освітньої кваліфікації бакалавр з кібербезпеки та захисту інформації	It is possible to obtain a professional qualification by passing a test at the Qualification Centre of Information Technology and Cyber Security established by the State Service for Special Communications and Information Protection of Ukraine after obtaining a bachelor's degree in cybersecurity and information security
Офіційна назва освітньої програми / Educational programme official title	Безпека державних інформаційних ресурсів	Security of state information resources
Тип диплому та обсяг освітньої програми / Diploma type and educational programme volume	Диплом 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 the educational programme	Сертифікат про акредитацію серія УД № 11019768, дата видачі 30.04.2025. Галузь знань: F Інформаційні технології, спеціальність: F5 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 № 11019768, date of issue 30.04.2025. Field of knowledge: F Information technology, speciality: F5 Cyber security and data protection at the National Technical University of Ukraine 'Igor Sikorsky Kyiv Polytechnic Institute'. The certificate is valid until 1 July 2028.
Цикл, рівень вищої освіти / Education cycle, level of higher education	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 освітньої програми / URL of the educational programme		

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; – гармонізації структури вищої освіти відповідно до зобов'язань країн-членів Європейського простору вищої освіти; – формування пріоритетів підготовки фахівців з вищою освітою, зокрема ІТ-спеціальностей, на основі моніторингу ринку праці; – гармонізації освітніх та професійних стандартів, залучення бізнесу та професійних спільнот до їх розроблення; – розвитку національної системи кваліфікацій; – трансформації освіти в секторі безпеки та оборони відповідно до доктринальних підходів і принципів НАТО. – 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 2025-2030 роки щодо формування суспільства майбутнього на засадах концепції сталого розвитку.	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; – harmonising the structure of higher education in accordance with the commitments of the member countries of the European Higher Education Area; – setting priorities for training specialists with higher education, particularly in IT specialities, based on labour market monitoring; – harmonising educational and professional standards, involving business and professional communities in their development; – developing a national qualifications system; – transforming education in the security and defence sector in line with NATO doctrinal approaches and principles. – taking into account the transformation of graduates' job responsibilities through interaction with the State Special Communications Administration; – 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 2025-2030 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 вивчення: – технології кібербезпеки та захисту інформації; – процеси управління кібербезпекою та захистом інформації;	Objects of study: - cybersecurity and information protection technologies; - cybersecurity and information protection management processes; objects of information activity, including information and information and communication

– об'єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології.	systems, information resources and technologies.
Цілі навчання: підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації, та розв'язувати складні задачі у галузі кібербезпеки та захисту інформації.	Learning objectives: training of specialists capable of using and implementing cybersecurity and information protection technologies and solving complex problems in the field of cybersecurity and information protection.
Теоретичний зміст предметної області: Створення та впровадження моделей, методів, технологій, процесів та способів розроблення, виробництва, що стосуються: управління стратегією, політиками, державними інформаційними ресурсами та плануванням системи менеджменту інформаційної безпеки та кібербезпеки інформаційних систем і технологій; концептуалізації і забезпечення захищених інформаційні технологій, інформаційно-комунікаційних систем і мереж та інформаційної інфраструктури; виявлення та ідентифікації кіберзагроз різних класів, проведення моніторингу інформаційних процесів, підтримання інфраструктури кіберпростору, аналізу та пом'якшення результатів кіберінцидентів (зменшення ризиків), включаючи забезпечення процесів управління та реагування на кіберінциденти в кіберпросторі; супроводу, підтримки, адміністрування та технічного обслуговування, як необхідних процедур для функціонування системи ефективного захисту інформаційних ресурсів і технологій, а також інформаційних систем та інфраструктури організації в цілому; методів та засобів технічного та криптографічного захисту інформації на об'єктах інформаційної діяльності та критичної інформаційної інфраструктури.	Theoretical content of the subject area: Creation and implementation of models, methods, technologies, processes and methods of development, production related to: management of strategy, policies, public information resources and planning of the information security management system and cybersecurity of information systems and technologies; conceptualisation and provision of secure information technologies, information and communication systems and networks and information infrastructure; detecting and identifying cyber threats of various classes, monitoring information processes, maintaining the infrastructure of cyberspace, analysing and mitigating the results of cyber incidents (risk reduction), including ensuring the processes of managing and responding to cyber incidents in cyberspace; support, maintenance, administration and technical service as necessary procedures for the functioning of the system of effective protection of information resources and technologies, as well as information systems and infrastructure of the organisation as a whole; methods and means of technical and cryptographic protection of information at the objects of information activities and critical information infrastructure.
Методи, методики та технології: методи, методики та технології розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації.	Methods, techniques and technologies: methods, techniques and technologies for solving theoretical and practical problems of cyber security and data protection.
Інструменти та обладнання: засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).	Tools and equipment: tools, devices, network equipment, application and specialised software, information systems and complexes for designing, modelling, controlling, monitoring, storing, processing, displaying and protecting data (information flows).

Орієнтація освітньої програми / Scope	
Освітньо-професійна	Educational – professional
Основний фокус освітньої програми / 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 defence, technical protection of information, cryptographic protection of information.
Особливості освітньої програми / Features	
Особливості освітньої програми полягають в наступному: – освітня програма розроблена з урахуванням вимог доктринальних підходів та принципів НАТО; – до викладання освітніх компонент освітньої програми залучаються фахівці Держспецзв'язку, інших навчальних закладів та провідних компаній відповідного сектору економіки; – навчальна практика проводиться в шостому семестрі в закладі освіти Держспецзв'язку науково-педагогічними працівниками закладу освіти Держспецзв'язку, як практичні заняття, відповідно до навчального плану; – 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 та посадових осіб підрозділів Держспецзв'язку, на базі яких воно проводиться. – 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.	The features of the educational program are as follows: – the educational programme has been developed taking into account the requirements of NATO doctrinal approaches and principles; – 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; – the training practice is conducted in the sixth semester at the educational institution of the State Service for Special Communications and Information Technology by the scientific and pedagogical staff of the educational institution of the State Service for Special Communications and Information Technology as practical classes, in accordance with the curriculum; - 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 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 України ДК 003:2010 зі Зміною №10 та Зміною №11 випускники можуть працювати на посадах, що відповідають професії (професійній назві роботи): 2139. Професіонал в інших галузях обчислень (комп'ютерізації). З врахуванням наявних професійних стандартів, що відповідають професійним кваліфікаціям: 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 з протидії технічним розвідкам.	According to the State Classification of Occupations of Ukraine DK 003:2010 with Amendment No. 10 and Amendment No. 11, graduates may work in positions corresponding to their profession (professional job title): 2139. Professional in other areas of computing (computerisation). And taking into account the existing professional standards corresponding to professional qualifications: 2139.2 Cybersecurity incident response specialist; 2139.2 Specialist in cryptographic information security; 2139.2 Specialist in technical information security; 2139.2 Technical counterintelligence specialist.
Замовником фахівців зі спеціальності F5 Кібербезпека та захист інформації виступає Державна служба спеціального зв'язку та захисту інформації України. Також можливе працевлаштування на посади у структурних підрозділах установ/підприємств/ організацій, які передбачають наявність вищої освіти зі спеціальності F5 Кібербезпека та захист інформації.	The customer for specialists in the specialty F5 Cyber security and Data Protection is the State Service for Special Communications and Information Protection of Ukraine. It is also possible to get a job in the structural units of institutions/enterprises/organisations that require a higher education in the speciality F5 Cyber security and Data Protection.
Подальше навчання / Further study	
Мають право на здобуття освіти на другому (магістерському) рівні вищої освіти. Здобуття або вдосконалення освіти та професійної підготовки в системі освіти дорослих.	Have the right to receive education at the second (master's) level of higher education. Obtaining or improving education and vocational training in the adult education system.
5 – Викладання та оцінювання / Teaching and assessment	
Викладання та навчання / Teaching and studying	
Проблемно-орієнтоване та студенто-центроване навчання з набуттям 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,	Problem-based and student-centred learning with the acquisition of competencies sufficient to 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

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.	teachers, internships and military internships. The program ends with a unified state qualification exam and the defence 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 і практичні завдання у галузі кібербезпеки та захисту інформації.	Ability to solve complex specialised problems and practical tasks in the field of cybersecurity and information protection.
Загальні компетентності (ЗК) / General competencies	
ЗК 01 Здатність застосовувати знання у практичних ситуаціях.	Ability to apply knowledge in practical situations.
ЗК 02 Знання та розуміння предметної області і розуміння професійної діяльності.	Knowledge and understanding of the subject area and understanding of professional activities.
ЗК 03 Здатність спілкуватися державною мовою як усно, так і письмово.	Ability to communicate in the state language both orally and in writing.
ЗК 04 Здатність спілкуватися іноземною мовою.	Ability to communicate in a foreign language.
ЗК 05 Здатність вчитися і оволодівати сучасними знаннями.	Ability to learn and master modern knowledge.
ЗК 06 Здатність реалізувати свої права і	Ability to realize one's rights and responsibilities as a member of

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.	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 07 Здатність ухвалювати рішення й 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.
ЗК 08 Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.	Ability to preserve and enhance 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.
Фахові компетентності (ФК) / Professional competencies	
ФК 01 Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти у професійній діяльності.	Ability to apply the legal and regulatory framework, as well as national and international requirements, practices and standards in professional activities**.**
ФК 02 Здатність використовувати інформаційні технологій, сучасні методи і моделей кібербезпеки та систем захисту інформації.	Ability to use information technology, modern methods and models of cybersecurity and information security systems.
ФК 03 Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.	Ability to ensure the continuity of business processes in accordance with the established cybersecurity and information protection policy.
ФК 04 Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.	Ability to ensure the protection of information in information and information and communication systems in accordance with the established cybersecurity and information protection policy.
ФК 05 Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.	Ability to restore the functioning of information and information and communication systems after threats, cyber attacks, failures and disruptions of various classes and origins.
ФК 06 Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)	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 07 Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.	Ability to carry out professional activities on the basis of the implemented information and cybersecurity management system.
ФК 08 Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах	Ability to apply methods and means of cryptographic protection of information at the objects of information

інформаційної діяльності.	activity.
ФК 09 Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.	Ability to apply methods and means of technical protection of information at information activity facilities.
ФК 10 Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.	Ability to monitor information processes, analyse, identify, assess possible vulnerabilities and threats to the information space and information resources in accordance with the established information security policy.
ФК 11 Здатність розробляти та впроваджувати комплексні плани та системи протидії технічним розвідкам.	Ability to develop and implement comprehensive plans and systems to counter technical intelligence.
ФК 12 Здатність застосовувати систему принципів, законів і категорій діалектики у пізнавальній і практичній діяльності фахівців в сфері організації Держспецзв'язку.	Ability to apply the system of principles, laws and categories of dialectics in the cognitive and practical activities of specialists in the field of organization of the State Service of Special Communications and Information Protection of Ukraine.
ФК 13 Здатність оперувати правовими засадами, визначеними як національним так і міжнародним законодавством, відносно національної безпеки України.	Ability to operate within the legal framework defined by both national and international legislation in relation to the national security of Ukraine.
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.	Ability to correlate incident data to identify specific vulnerabilities and provide recommendations that will allow them to be addressed quickly.
ФКбл 1.2. 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. Здатність визначати засоби технічної розвідки та їх носії, які здійснюють або можуть здійснювати збір інформації з обмежентм доступом про об'єкти протидії, на підставі результатів аналізу моделей технічних розвідок.	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. Ability to identify technical reconnaissance means and their carriers that collect or may collect restricted information about countermeasure objects, based on the results of technical reconnaissance model analysis.
ФКбл 1.3. 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.	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.

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 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. Здатність визначати засоби технічної розвідки та їх носії, які здійснюють або можуть здійснювати збір інформації з обмежентм доступом про об'єкти протидії, на підставі результатів аналізу моделей технічних розвідок.	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. Ability to identify technical reconnaissance means and their carriers that collect or may collect restricted information about countermeasure objects, based on the results of technical reconnaissance model analysis.
ФКбл 2.3. 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.
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 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 3.2. 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 визначати засоби технічної розвідки та їх носії, які здійснюють або можуть здійснювати збір інформації з обмежентм доступом про об'єкти протидії, на підставі результатів аналізу моделей технічних розвідок.	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 identify technical reconnaissance means and their carriers that collect or may collect restricted information about countermeasure objects, based on the results of technical reconnaissance model analysis.
ФКбл 3.3. 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.

Фахові компетентності Блоку 4. Професійний стандарт. Фахівець з протидії технічним розвідкам /Professional competences Block 4. Professional standard. Specialist in counter technical intelligence	
ФКбл 4.1. Здатність визначати засоби технічної розвідки та їх носії, які здійснюють або можуть здійснювати збір інформації з обмежентм доступом про об'єкти протидії, на підставі результатів аналізу моделей технічних розвідок.	Ability to identify technical reconnaissance means and their carriers that collect or may collect restricted information about countermeasure objects, based on the results of technical reconnaissance model analysis.
ФКбл 4.2. 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.
ФКбл 4.3. Здатність визначати методи та способи протидії засобам технічної розвідки та проводити розрахунки граничних показників і ресурсів.	Ability to determine methods and means of countering technical reconnaissance and to calculate limit indicators and resources.
Військово-професійні компетентності (ВПК)/Military-professional competencies	
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.	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).	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.	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.	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,	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

зберігати зброю і боєприпаси, забезпечувати додержання заходів безпеки на заняттях; підтримувати постійну готовність підрозділу до виконання завдань за призначенням у мирний та воєнний час.	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.	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.	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.	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.	Ability to organise and maintain communication in the unit using standard means of communication.
ВПК 10. Здатність виконувати професійну діяльність в умовах тривалих різнопланових фізичних навантажень і психічних напружень; організувати підготовку військовослужбовців для забезпечення їх фізичної готовності до виконання завдань за призначенням; організувати виконання завдань з тактичної медицини.	Ability to perform professional activities under conditions of prolonged, diverse 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.	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.	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	
ВСК 1. Здатність володіти знаннями і навичками застосування інформаційно-	Ability to possess knowledge and skills in the use of information-communication systems (complexes of modern mobile

комунікаційних систем (комплексів сучасних рухомих вузлів зв'язку та засобів урядового польового зв'язку).	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.	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.	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.	Ability to organise, plan and ensure secrecy in institutions and organisations.
7 – Програмні результати навчання (ПРН) / Programme learning outcomes	
ПРН 01 Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.	Communicate fluently in the state language orally and in writing in the performance of professional duties.
ПРН 02 Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.	Communicate in a foreign language to ensure the effectiveness of professional communication.
ПРН 03 Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.	Apply the principle of inadmissibility of corruption and any other manifestations of dishonesty in professional activities.
ПРН 04 Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.	Organise own professional activities, choose and use optimal methods and ways to solve complex specialised tasks and practical problems in professional activities, evaluate their effectiveness.
ПРН 05 Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.	Analyse, argue, make decisions in solving complex specialised problems and practical tasks in professional activities characterised by complexity and incomplete certainty of conditions, and be responsible for decisions made.
ПРН 06 Адаптуватися до нових умов і технологій	Adapt to new conditions and technologies of professional activity,

професійної діяльності, прогнозувати кінцевий результат.	predict the final result.
ПРН 07 Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.	Apply and adapt theories of information and coding, mathematical statistics, numbers, cryptography and steganography, signal processing and transmission, etc., principles, methods and concepts of cybersecurity and information protection in education and professional activities.
ПРН 08 Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.	Apply knowledge and understanding of mathematics and physics in professional activities, formalise the tasks of the subject area of cybersecurity and information protection, formulate their mathematical formulation and choose a rational method of solution.
ПРН 09 Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.	Know and apply the legislation of Ukraine and international requirements, practices and standards in order to carry out professional activities in the field of cybersecurity and information protection.
ПРН 10 Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.	Use modern information technologies, methods and models of cybersecurity and information security systems to carry out professional activities.
ПРН 11 Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації.	Plan the preparation and ensure the continuity of business processes in organisations in accordance with the established cybersecurity policy, taking into account information security requirements.
ПРН 12 Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.	Apply methods and means of information protection in information and information and communication systems in accordance with the established information security policy.
ПРН 13 Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.	Implement, configure, maintain and support the functioning of software and hardware systems and cybersecurity and information protection systems as necessary procedures for the functioning of information and information and communication systems and/or the organisation's infrastructure as a whole.
ПРН 14 Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.	Manage the processes of restoring the normal functioning of information and information and communication systems using backup procedures in accordance with the established security policy and ensure the operation of special software for information protection and recovery.
ПРН 15 Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування	Collect, process, store, analyse critical data to prove the implementation of cyber threats, to analyse and investigate a cyber incident in order to promptly restore the functioning of the information system.

інформаційної системи.	
ПРН 16 Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.	Solve the problems of implementing and maintaining integrated information security systems in information systems.
ПРН 17 Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.	Ensure the functioning of the organisation's cybersecurity and information protection management system, including personnel and management of the consequences of information security threats in crisis situations, based on the implementation of quantitative and qualitative risk assessment procedures.
ПРН 18 Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.	Analyse and apply methods and means of cryptographic protection of information at information activity facilities.
ПРН 19 Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.	Solve tasks related to organising and monitoring the state of cryptographic protection of information, in particular in accordance with the requirements of regulatory documents.
ПРН 20 Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.	Identify threats of creating technical channels of information leakage at information objects; implement means and measures of technical protection of information from leakage through technical channels, maintain and monitor the condition of information protection hardware and technical information protection complexes.
ПРН 21 Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.	Implement, maintain, analyse the effectiveness of systems for detecting unauthorised access, actions with information in the information system, vulnerabilities, possible threats to the information space and information resources, and use security systems to ensure the required level of information security in information systems.
ПРН 22 Знати структуру та зміст планувальної документації (організаційні, технічні, режимні та операційні заходи), теоретичні основи, існуючих та новітніх методів і способів протидії засобам технічної розвідки (радіоелектронна боротьба, маскування, дезінформація, організаційні та інженерно-технічні заходи). Створювати чіткі інструкції для персоналу щодо використання встановлених систем ПДТР. Уміти налаштувати параметри технічних систем під конкретну завадову обстановку об'єкта.	
ПРН 23 Використовувати у практичній діяльності в сфері організації Держспецзв'язку систему принципів, законів і категорій діалектики.	To use the system of principles, laws and categories of dialectics in practical activities in the field of organization of the State Service of Special Communications and Information Protection of Ukraine.

ПРН 24 Застосовувати в професійній діяльності правову базу національної безпеки України.	Apply the legal framework of national security of Ukraine in professional activities.
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.	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. 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.	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.
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).	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).
Розуміти концепцію та структуру моделі технічних розвідок, включно з типовими сценаріями, об'єктами та суб'єктами розвідувальної діяльності. Уміння на основі аналізу даних (включаючи результати спеціальних перевірок, радіомоніторингу, візуального спостереження) ідентифікувати конкретні типи засобів технічної розвідки та їх можливих носіїв, які загрожують об’єктам протидії.	Understand the concept and structure of technical reconnaissance models, including typical scenarios, objects and subjects of reconnaissance activities. Be able to identify specific types of technical reconnaissance means and their possible carriers that threaten countermeasures objects based on data analysis (including the results of special checks, radio monitoring, visual observation).
ПРНбл 1.3. 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.	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.

Проводити процедури сканування вразливостей в системах безпеки.	
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.	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. 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 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). Розуміти концепцію та структуру моделі технічних розвідок, включно з типовими сценаріями, об'єктами та суб'єктами розвідувальної діяльності. Уміння на основі аналізу даних (включаючи результати спеціальних перевірок, радіомоніторингу, візуального спостереження) ідентифікувати конкретні типи засобів технічної розвідки та їх можливих носіїв, які загрожують об’єктам протидії.	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 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). Understand the concept and structure of technical reconnaissance models, including typical scenarios, objects and subjects of reconnaissance activities. Be able to identify specific types of technical reconnaissance means and their possible carriers that threaten countermeasures objects based on data analysis (including the results of special checks, radio monitoring, visual observation).
ПРНбл 2.3. 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	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.

рівнем безпеки. Аналізувати потреби та вимоги користувачів з метою планування і проведення розробки системи.	
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. 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 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.	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, 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 3.2. 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.	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. Provide proposals to the management, as appropriate, on concluding contracts for conducting case studies (their individual components) and assessing the compliance of cryptographic information security.

Розуміти концепцію та структуру моделі технічних розвідок, включно з типовими сценаріями, об'єктами та суб'єктами розвідувальної діяльності. Уміння на основі аналізу даних (включаючи результати спеціальних перевірок, радіомоніторингу, візуального спостереження) ідентифікувати конкретні типи засобів технічної розвідки та їх можливих носіїв, які загрожують об’єктам протидії.	Understand the concept and structure of technical reconnaissance models, including typical scenarios, objects and subjects of reconnaissance activities. Be able to identify specific types of technical reconnaissance means and their possible carriers that threaten countermeasures objects based on data analysis (including the results of special checks, radio monitoring, visual observation).
ПРНбл 3.3. 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.	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.
Програмні результати навчання Блоку 4. Професійний стандарт. Фахівець з протидії технічним розвідкам/Programme learning outcomes for Block 4. Professional standard. Specialist in countering technical intelligence	
ПРНбл 4.1. Розуміти концепцію та структуру моделі технічних розвідок, включно з типовими сценаріями, об'єктами та суб'єктами розвідувальної діяльності. Уміння на основі аналізу даних (включаючи результати спеціальних перевірок, радіомоніторингу, візуального спостереження) ідентифікувати конкретні типи засобів технічної розвідки та їх можливих носіїв, які загрожують об’єктам протидії.	Understand the concept and structure of technical reconnaissance models, including typical scenarios, objects and subjects of reconnaissance activities. Be able to identify specific types of technical reconnaissance means and their possible carriers that threaten countermeasures objects based on data analysis (including the results of special checks, radio monitoring, visual observation).
ПРНбл 4.2. 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	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. Submit proposals to the management, if necessary, on concluding contracts for conducting case studies (their individual components) and assessing the conformity of cryptographic

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).	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).
ПРНбл 4.3. Знати теоретичні основ, існуючих та новітніх методів і способів протидії засобам технічної розвідки (радіоелектронна боротьба, маскування, дезінформація, організаційні та інженерно-технічні заходи). Обирати найбільш адекватні та ефективні методи і способи протидії для нейтралізації конкретних видів засобів технічної розвідки з урахуванням ОПД та умов застосування. Оперативно збирати, верифікувати та аналізувати вихідні дані, необхідних для проведення точних розрахунків.	Know the theoretical foundations, existing and latest methods and means of countering technical reconnaissance (electronic warfare, camouflage, disinformation, organisational and engineering measures). Select the most appropriate and effective methods and means of countering specific types of technical reconnaissance, taking into account the OPD and conditions of use. Promptly collect, verify and analyse the source data necessary for accurate calculations.
Програмні результати навчання військово-професійна та військово-спеціальні підготовка / Programme learning outcomes military-professional training and military- special 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.	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).	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.	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	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

прикладах їх військово-професійної діяльності і етносу Воїна.	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.	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.	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 фотодокументами; орієнтуватися на незнайомій місцевості за картою, без карти та за допомогою навігаційних приладів вдень і вночі за будь-якої погоди і пори року.	Determine the tactical properties of the terrain when conducting combat operations in various conditions; work with topographic maps and photographic documents; navigate unfamiliar 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.	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.	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.	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)	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.

поводженні та при виконанні бойових завдань; застосовувати знання та навички з управління вогнем підрозділу в бою.	
ПРНВПП 12. Розуміти порядок проходження військової служби, 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.	Understand the procedure for military service, bringing servicemen to criminal, 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.
ПРНВСП 13. Знати і вміти впевнено застосувати інформаційно-комунікаційні системи (комплексів сучасних рухомих вузлів зв'язку та засобів урядового польового зв'язку).	Know and be able to confidently apply information-communication systems (complexes of modern mobile communication nodes and government field communication equipment).
ПРНВСП 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.	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.
ПРНВСП 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.	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.
ПРНВСП 16. Організовувати та проводити заходи по забезпеченню режиму секретності в установах, організаціях та в підрозділах Держспецзв’язку.	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: 23 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: 18 (14)	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: 23 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: 18 (14)
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., одна навчальна лабораторія технологій захисту мереж, 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, one training laboratory for network security technologies, 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 methodological support of the educational process	
Відповідно до вимог щодо інформаційного та навчально-методичного забезпечення освітньої діяльності відповідного рівня вищої освіти, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 в чинній редакції. Користування Науково-технічною бібліотекою 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 вищої освіти / Study of foreign applicants of higher education	
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.
10 – Процедура присвоєння професійних кваліфікацій / Procedure for awarding professional qualifications	
Суб'єктом, уповноваженим законодавством на присвоєння/підтвердження та визнання професійних кваліфікацій є Кваліфікаційний центр інформаційних технологій та кібербезпеки при Держ.НДІ технологій кібербезпеки та захисту інформації Держспецзв'язку на основі підготовки здобувачів вищої освіти за спеціальністю F5 Кібербезпека та захист інформації на першому (бакалаврському) рівні вищої освіти та отримані освітньої кваліфікація – бакалавр з кібербезпеки та захисту інформації.	The entity authorised by law to award/confirm and recognise professional qualifications is the Qualification centre for information technology and cybersecurity at the State Research Institute of cybersecurity and information protection of the State special communications service of Ukraine on the basis of training of higher education students in the speciality F5 Cybersecurity and information protection at the first (bachelor's) level of higher education and obtaining the educational qualification - bachelor of cyber security and data protection.

2. ПЕРЕЛІК ОСВІТНІХ КОМПОНЕНТІВ / EDUCATIONAL COMPONENTS

Код / Code	Освітні компоненти / Educational components	Кредити ЄКТС / ECTS credits	Форма підсумкового контролю / Final control form
Обов'язкові (нормативні) освітні компоненти / Required (standard) educational components			
Цикл загальної підготовки / General training cycle			
ЗО 01	Українська мова за професійним спрямуванням./Ukrainian language for professional purposes.	2	залік/test
ЗО 02	Україна в контексті історичного розвитку Європи./ Ukraine in the context of historical development of Europe.	2	залік/test
ЗО 03.1	Англійська мова. Частина 1./ English language. Part 1.	3	залік/test
ЗО 03.2	Англійська мова. Частина 2./ English language. Part 2.	3	залік/test
ЗО 04.1	Англійська мова професійного спрямування. Частина 1./ English language for professional purposes. Part 1.	3	залік/test
ЗО 04.2	Англійська мова професійного спрямування. Частина 2./ English language for professional purposes. Part 2.	3	залік/test
ЗО 5	WEB – технології. / WEB – technologies.	4	екзамен/exam
ЗО 06	Математичний аналіз./ Mathematical analysis.		
ЗО 06.1	Математичний аналіз. Частина 1. Диференціальне числення однієї та кількох змінних./ Mathematical analysis. Part 1: Differential calculus of one and several variables.	5	екзамен/ exam
ЗО 06.2	Математичний аналіз. Частина 2. Інтегральне числення функції однієї змінної. Диференціальні рівняння. Числові і функціональні ряди і інтеграл Фур'є./ Mathematical analysis. Part 2. Integral calculus of a function of one variable. Differential equations. Numerical and functional series and the Fourier integral.	5	екзамен/ exam
ЗО 07	Фізика./Physics.		
ЗО 07.1	Фізика. Частина 1. Електромагнетизм. Коливання та хвилі. Оптика./Physics. Part 1: Electromagnetism. Oscillations and waves. Optics.	5	залік/test
ЗО 07.2	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.	6	екзамен/ exam
ЗО 08	Дискретна математика/Discrete mathematics.	5	екзамен/exam
ЗО 09	Дискретна математика. Курсова робота / Discrete mathematics. Course work.	1	залік/test
ЗО 10	Програмування/ Programming.		
ЗО 10.1	Програмування. Частина 1. Алгоритмізація та програмування/ Programming. Part 1. Algorithmization and programming.	5	екзамен/ exam
ЗО 10.2	Програмування. Частина 2. Об'єктно-орієнтоване програмування/Programming. Part 2. Object-oriented programming.	4	залік/test

ЗО 11	Правові основи національної безпеки України/Legal basis of national security of Ukraine.	3	залік/test
ЗО 12	Філософія/Philosophy.	2	залік/test
ЗО 13	Теорія ймовірностей і математична статистика./Theory of probability and mathematical statistics.	4	екзамен/ exam
ЗО 14	Лінійна алгебра та аналітична геометрія / Linear algebra and analytical geometry.	5	екзамен/ exam
Цикл професійної підготовки / Professional training cycle			
ПО 01.1	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 01.2	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 01.3	Фізичне виховання. Частина 3. Гімнастика, прискорене пересування та спортивні ігри/ Physical education. Part 3. Gymnastics, accelerated movement and sports games.	4	залік/test
ПО 01.4	Фізичне виховання. Частина 4. Удосконалення силових якостей та витривалості/ Physical education. Part 4. Improve strength and endurance.	4	залік/test
ПО 02	Інформаційно-комунікаційні мережі/Information-communication networks.	4	залік/test
ПО 03	Теоретична криптологія/ Theoretical cryptology.	4	залік/test
ПО 04	Криптографія/Cryptography.	4	екзамен/exam
ПО 05	Криптографія. Курсова робота/ Cryptography. Course work	1	залік/test
ПО 06	Технічний захист інформації/ Technical protection of information.	4	залік/test
ПО 07	Кібербезпека/Cybersecurity.	6	екзамен/exam
ПО 08	Кібербезпека. Курсовий проект/ Cybersecurity. Course project.	2	залік/test
ПО 09	Основи організації та здійснення комплексних заходів з протидії технічним розвідкам на обєктах протидії/ Fundamentals of organising and implementing comprehensive measures to counter technical reconnaissance at countermeasures facilities.	3	залік/test
ПО 10	Регулювання в сфері інформаційної безпеки. / Regulation in the field of information security	4	залік/test
ПО 11	Основи створення систем безпеки інформації./ Basics of creating information security systems.	4	екзамен/ exam
ПО 12	Основи створення систем безпеки інформації. Курсова робота/ Basics of creating information security systems. Course work.	1	залік/test
ПО 13	Основи убезпечення інформації від витоку технічними каналами/ Fundamentals of protecting information from leakage through technical channels.	4	екзамен/ exam
ПО 14	Основи убезпечення інформації від витоку технічними каналами. Курсова робота/ Fundamentals of protecting	1	залік/test

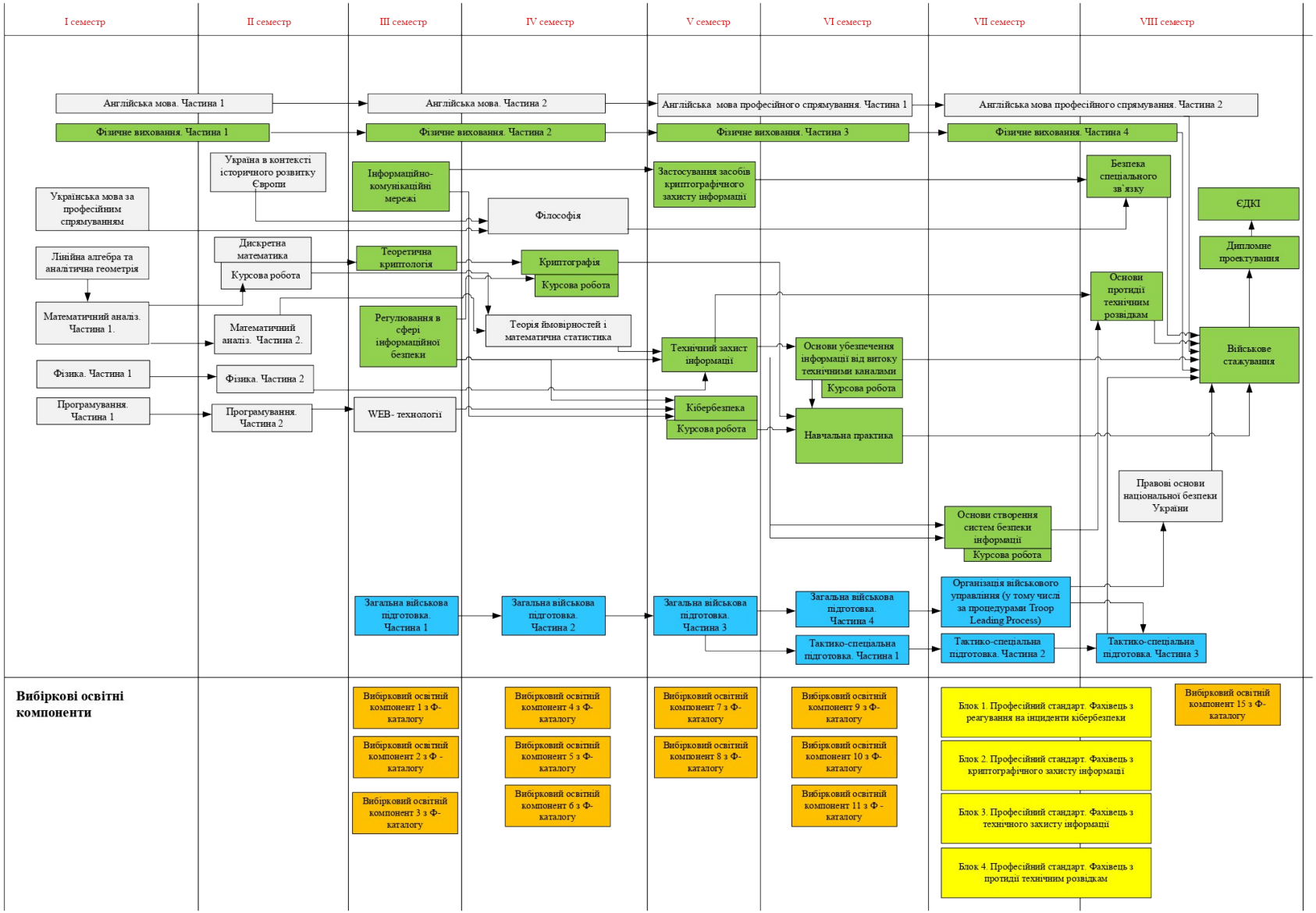
	information from leakage through technical channels. Course work.		
ПО 15	Застосування засобів криптографічного захисту інформації/Application of cryptographic information security tools.	4	залік/test
ПО 16	Безпека спеціального зв'язку/Security of special communications.	4	залік/test
ПО 17	Навчальна практика/ Educational practice.	2	залік/test
ПО 18	Військове стажування/ Military internship	3	залік/test
ПО 19	Дипломне проєктування/ Diploma design	6	захист/defense
Вибіркові освітні компоненти / Elective educational components			
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 communications organization.	4	залік/test
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	залік/test
Вибіркові освітні компоненти / Elective educational components			
Цикл загальної підготовки / General training cycle			
ЗВ 01	Освітній компонент 8 Ф-Каталогу / Educational Component 8 from P-Catalogue	4	залік/test
Цикл професійної підготовки / Professional training cycle			
ПВ 01	Освітній компонент 1 Ф-Каталогу / Educational Component 1 from P-Catalogue	4	залік/test

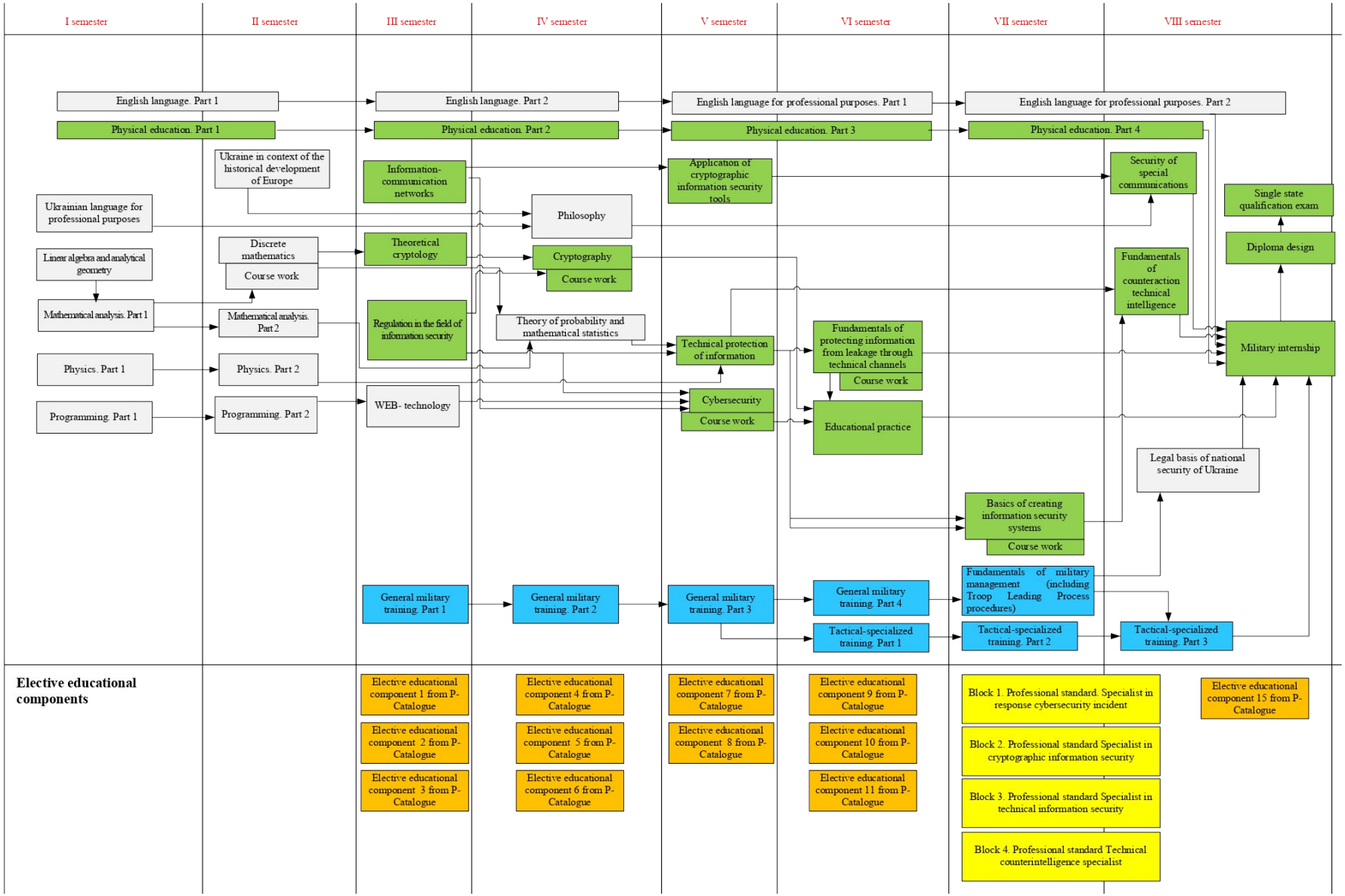
ПВ 02	Освітній компонент 2 Ф-Каталогу / Educational Component 2 from P-Catalogue	4	залік/test
ПВ 03	Освітній компонент 3 Ф-Каталогу / Educational Component 3 from P-Catalogue	4	залік/test
ПВ 04	Освітній компонент 4 Ф-Каталогу / Educational Component 4 from P-Catalogue	4	залік/test
ПВ 05	Освітній компонент 5 Ф-Каталогу / Educational Component 5 from P-Catalogue	4	залік/test
ПВ 06	Освітній компонент 6 Ф-Каталогу / Educational Component 6 from P-Catalogue	4	залік/test
ПВ 07	Освітній компонент 7 Ф-Каталогу / Educational Component 7 from P-Catalogue	4	залік/test
ПВ 09	Освітній компонент 9 Ф-Каталогу / Educational Component 9 from P-Catalogue	4	залік/test
ПВ 10	Освітній компонент 10 Ф-Каталогу / Educational Component 10 from P-Catalogue	4	залік/test
ПВ 11	Освітній компонент 11 Ф-Каталогу / Educational Component 11 from P-Catalogue	4	залік/test
ПВ 15	Освітній компонент 15 Ф-Каталогу / Educational Component 15 from P-Catalogue	4	залік/test
Вибіркові компоненти блочного вибору/ Selective components of the block programme			
Блок 1. Професійний стандарт. Фахівець з реагування на інциденти кібербезпеки / Block 1. Professional standard. Specialist in response cybersecurity incident			
ПВ 12.1	Безпека інформаційно-комунікаційних систем/ Security of information and communication systems.	4	залік/test
ПВ 13.1	Методологічні аспекти захисту інформації (кріптографічний захист інформації, технічний захист інформації, протидія технічним розвідкам)/ Methodological aspects of information security (cryptographic information security, technical information security, organisational and legal information security).	4	залік/test
ПВ 14.1	Аналіз вразливостей інформаційних систем/ Analysis of information system vulnerabilities.	4	залік/test
Блок 2. Професійний стандарт. Фахівець з криптографічного захисту інформації / Block 2. Professional standard Specialist in cryptographic information security			
ПВ 12.2	Криптографічні протоколи/Cryptographic protocols.	4	залік/test
ПВ 13.2	Методологічні аспекти захисту інформації (кіберзахист, технічний захист інформації, протидія технічним розвідкам)/Methodological aspects of information protection (cyber protection, technical protection of information, organisational and legal protection of information).	4	залік/test
ПВ 14.2	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	4	залік/test

	institutions.		
Блок 3. Професійний стандарт. Фахівець з технічного захисту інформації / Block 3. Professional standard Specialist in technical information security			
ПВ 12.3	Основи спеціальних досліджень/Fundamentals of specialised research.	4	залік/test
ПВ 13.3	Методологічні аспекти захисту інформації (кіберзахист, криптографічний захист інформації, протидія технічним розвідкам)/Methodological aspects of information protection (cyber protection, cryptographic information protection, organisational and legal protection of information).	4	залік/test
ПВ 14.3	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
Блок 4. Професійний стандарт. Фахівець з протидії технічним розвідкам/ Block 4. Professional standard. Specialist in countering technical intelligence			
ПВ 12.4	Фізичні основи виникнення демаскувальних ознак об'єктів протидії та можливості технічних розвідок/Physical basis for the emergence of unmasking signs of countermeasures and possibilities for technical reconnaissance.	4	залік/test
ПВ 13.4	Методологічні аспекти захисту інформації (кіберзахист, криптографічний захист інформації, технічний захист інформації)/Methodological aspects of information security (cyber security, cryptographic information security, technical information security).	4	залік/test
ПВ 14.4	Методи та засоби захисту об'єктів протидії та інформації від технічних розвідок/Methods and means of protecting countermeasure facilities and information from technical reconnaissance.	4	залік/test
Загальний обсяг обов'язкових компонентів / Total volume of the required components:			147
Загальний обсяг вибіркових компонентів / Total volume of the elective components:			93
Обсяг освітніх компонентів, що забезпечують здобуття компетентностей визначених стандартом вищої освіти / Total volume of the educational components aimed at acquisition of competencies specified in the Higher Education Standard:			147
Вибіркові освітні компоненти циклів загальної та професійної підготовки / Elective educational components of General and Professional training cycles:			48
Вибіркові компоненти блочного вибору/ Selective components of the block programme:			12
Обсяг освітніх вибіркових компонентів, що забезпечують здобуття компетентностей визначених L-1A, L-1B/ Total scope of the educational elective components aimed at acquisition of competencies specified in the L-1A, L-1B:			33

ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ / TOTAL VOLUME OF THE EDUCATIONAL PROGRAMME :	240

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




I semester
II semester
III semester
IV semester
V semester
VI semester
VII semester
VIII semester
English language. Part 1
English language. Part 2
English language for professional purposes. Part 1
English language for professional purposes. Part 2
Physical education. Part 1
Physical education. Part 2
Physical education. Part 3
Physical education. Part 4
Ukraine in context of the historical development of Europe
Information-communication networks
Application of cryptographic information security tools
Security of special communications
Single state qualification exam
Ukrainian language for professional purposes
Philosophy
Diploma design
Discrete mathematics
Course work
Theoretical cryptology
Cryptography
Course work
Linear algebra and analytical geometry
Fundamentals of counteraction technical intelligence
Mathematical analysis. Part 1
Mathematical analysis. Part 2
Regulation in the field of information security
Theory of probability and mathematical statistics
Technical protection of information
Fundamentals of protecting information from leakage through technical channels
Course work
Military internship
Physics. Part 1
Physics. Part 2
Cybersecurity
Course work
Educational practice
Programming. Part 1
Programming. Part 2
WEB- technology
Legal basis of national security of Ukraine
Basics of creating information security systems
Course work
Fundamentals of military management (including Troop Leading Process procedures)
General military training. Part 1
General military training. Part 2
General military training. Part 3
General military training. Part 4
Tactical-specialized training. Part 1
Tactical-specialized training. Part 2
Tactical-specialized training. Part 3
Elective educational components
Elective educational component 1 from P-Catalogue
Elective educational component 4 from P-Catalogue
Elective educational component 7 from P-Catalogue
Elective educational component 9 from P-Catalogue
Block 1. Professional standard. Specialist in response cybersecurity incident
Elective educational component 15 from P-Catalogue
Elective educational component 2 from P-Catalogue
Elective educational component 5 from P-Catalogue
Elective educational component 8 from P-Catalogue
Elective educational component 10 from P-Catalogue
Block 2. Professional standard Specialist in cryptographic information security
Elective educational component 3 from P-Catalogue
Elective educational component 6 from P-Catalogue
Elective educational component 11 from P-Catalogue
Block 3. Professional standard Specialist in technical information security
Block 4. Professional standard Technical counterintelligence specialist

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 бакалавра, що забезпечує оцінювання досягнутих програмних результатів навчання, визначених стандартом вищої освіти за спеціальністю F5 «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 передбачає розв'язок спеціалізованого завдання теоретичного або практичного спрямування в галузі кібербезпеки та захисту інформації і не може містити академічного плагіату, фальсифікації та фабрикації. З цією метою робота перевіряється на наявність плагіату, фальсифікації та фабрикації 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 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, which provides an assessment of the achieved program learning outcomes defined by the standard of higher education in the specialty F5 "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 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 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 01	ЗО 02	ЗО 03	ЗО 04	ЗО 05	ЗО 06	ЗО 07	ЗО 08	ЗО 09	ЗО 10	ЗО 11	ЗО 12	ЗО 13	ЗО 14	ПО 01	ПО 02	ПО 03	ПО 04	ПО 05	ПО 06	ПО 07	ПО 08	ПО 09	ПО 10	ПО 11	ПО 12	ПО 13	ПО 14	ПО 15	ПО 16	ПО 17	ПО 18	ПО 19
ЗК 01	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК 02	+	+	+		+	+	+	+	+	+				+		+	+	+	+	+	+	+	+		+	+	+	+	+	+			+
ЗК 03	+										+	+			+	+									+	+			+	+	+	+	+
ЗК 04			+	+							+	+	+																			+	+
ЗК 05	+	+			+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+			+	+					+
ЗК 06			+									+																				+	+
ЗК 07	+										+																					+	+
ЗК 08	+	+										+			+																		+
ФК 01			+	+							+							+	+	+	+	+	+	+	+	+			+	+		+	+
ФК 02					+			+	+	+			+			+									+	+			+			+	+
ФК 03																					+	+										+	+
ФК 04																		+						+	+				+	+	+	+	+
ФК 05																+					+	+									+	+	+
ФК 06																								+	+							+	+
ФК 07																							+									+	+
ФК 08						+		+	+				+				+	+	+				+			+			+		+	+	+
ФК 09							+													+			+			+	+	+			+	+	+
ФК 10													+																			+	+	+
ФК 11					+	+	+	+	+	+													+										+
ФК 12												+																					+	+
ФК 13											+																						+	+

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 01	ЗО 02	ЗО 03	ЗО 04	ЗО 05	ЗО 06	ЗО 07	ЗО 08	ЗО 09	ЗО 10	ЗО 11	ЗО 12	ЗО 13	ЗО 14	ПО 01	ПО 02	ПО 03	ПО 04	ПО 05	ПО 06	ПО 07	ПО 08	ПО 09	ПО 10	ПО 11	ПО 12	ПО 13	ПО 14	ПО 15	ПО 16	ПО 17	ПО 18	ПО 19
ПРН 01	+										+	+			+	+									+	+			+	+	+	+	+
ПРН 02			+	+							+	+	+																			+	+
ПРН 03	+		+								+	+																				+	+
ПРН 04		+	+	+		+					+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПРН 05		+	+	+							+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПРН 06		+	+			+						+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			+
ПРН 07		+	+	+				+	+		+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+
ПРН 08		+				+	+	+	+		+	+	+	+		+	+	+	+	+	+	+	+	+			+	+					+
ПРН 09			+	+								+						+	+	+	+		+	+	+	+			+	+		+	+
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											+																						+	+

6.1. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ З ВІЙСЬКОВО-ПРОФЕСІЙНОЇ ТА ВІЙСЬКОВО-СПЕЦІАЛЬНОЇ 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				+				
ПРНВСП 13						+		
ПРНВСП 14							+	
ПРНВСП 15								+
ПРНВСП 16								+