МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

ЗАТВЕРДЖЕНО
Вченою радою КПІ ім. Ігоря Сікорського
(протокол № 1 від «23» 01 2023 р.)
Голова Вченої ради
_____ Михайло ІЛЬЧЕНКО

Безпека державних інформаційних ресурсів

Security of state information resources

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

першого (бакалаврського) рівня вищої освіти

за спеціальністю	**125 Кібербезпека та захист інформації**
галузі знань	**12 Інформаційні технології**
кваліфікація	**Бакалавр з кібербезпеки та захисту інформації**

Введено в дію з 2023/2024 н.р.
Наказом ректора
КПІ ім. Ігоря Сікорського
від 17.05. 2023р. № НОН/163/2023

Київ – 2023

ПРЕАМБУЛА

РОЗРОБЛЕНО проєктною групою:

Керівник проєктної групи:

Конотопець Микола Миколайович, кандидат технічних наук, доцент, доцент Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського

Члени проєктної групи:

Іванченко Сергій Олександрович, доктор технічних наук, професор, професор Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського

Олексійчук Антон Миколайович, доктор технічних наук, доцент, професор Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського

Самойлов Ігор Володимирович, кандидат технічних наук, доцент, доцент Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського

Сторчак Антон Сергійович, кандидат технічних наук, доцент Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського

За підготовку здобувачів вищої освіти за освітньо-професійною програмою відповідає Спеціальна кафедра № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського

ПОГОДЖЕНО:

Науково-методична комісія КПІ ім. Ігоря Сікорського зі спеціальності 125

Голова НМКУ 125 (для ІСЗЗІ) _____ Сергій ІВАНЧЕНКО

(протокол № 1 від «12» 01 2023 р.)

Методична рада КПІ ім. Ігоря Сікорського

Голова Методичної ради _____ Анатолій МЕЛЬНИЧЕНКО

(протокол № 4 від «19» 01 2023 р.)

ВРАХОВАНО:

1. Постанову 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”;

2. 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;

3. Наказ 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;

4. Постанову 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;

5. Наказ 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”.

Освітньо-професійну програму обговорено після надходження всіх пропозицій, побажань і зауважень від здобувачів вищої освіти, випускників та стейкхолдерів і схвалено на засіданні Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського (протокол № 5/1 від 05 січня 2023 року).

ЗМІСТ

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ

1 – Загальна інформація	
Повна назва ЗВО та інституту/факультету	Національний технічний університет України “Київський політехнічний інститут імені Ігоря Сікорського”, Інститут спеціального зв’язку та захисту інформації
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь ВО – бакалавр Кваліфікація – бакалавр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Безпека державних інформаційних ресурсів
Тип диплому та обсяг освітньої програми	Диплом бакалавра, освітня складова 240 кредитів ЄКТС, термін навчання 3 роки і 10 місяців
Наявність акредитації	Програма акредитована до 1.07.2026, подача програми на акредитацію до Національного агентства із забезпечення якості вищої освіти планується у 2026 році
Цикл/рівень вищої освіти	НРК України – 6 рівень QF-EHEA – перший цикл EQF-LLL – 6 рівень
Передумови	Наявність повної загальної середньої освіти
Мова(и) викладання	Українська
Термін дії освітньої програми	До наступної акредитації
Інтернет-адреса постійного розміщення освітньої програми	https://osvita.kpi.ua/ (розділ “Освітні програми”)
2 – Мета освітньої програми	
Метою освітньо-професійної програми “Безпека державних інформаційних ресурсів” є підготовка висококваліфікованих фахівців ступеня бакалавра в галузі кібербезпеки та захисту інформації, здатних самостійно розв’язувати складні спеціалізовані задачі у галузі відповідної професійної діяльності на посадах органів та підрозділів Держспецзв’язку, що передбачає здійснення розробки, впровадження й дослідження у різних галузях людської діяльності, національної економіки та виробництва в умовах: – науково-технічного прогресу та сталого розвитку суспільства; – інтернаціоналізації освіти; – урахування трансформації посадових обов’язків випускників шляхом взаємодії з Адміністрацією Держспецзв’язку; всебічного професійного, інтелектуального, соціального та творчого розвитку особистості в освітньо-професійному середовищі. Мета освітньо-професійної програми відповідає стратегії розвитку КПІ ім. Ігоря Сікорського на 2020-2025 роки щодо формування суспільства майбутнього на засадах концепції сталого розвитку.	
3 – Характеристика освітньої програми	
Предметна область	Об’єкти професійної діяльності випускників: – об’єкти інформатизації, включаючи комп’ютерні, автоматизовані, комунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-комунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою об’єктів, що підлягають захисту.

	Цілі навчання підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. Теоретичний зміст предметної області Знання – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення – інформаційно-комунікаційних технологій; – автоматизованих систем проектування. Методи, методики та технології: Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/або кібербезпеки. Інструменти та обладнання: – системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
Орієнтація освітньої програми	Освітньо-професійна
Основний фокус освітньої програми	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.

Особливості програми	Особливості освітньої програми полягають в наступному: – освітня програма розроблена з урахуванням вимог професійних стандартів військового фахівця Держспецзв'язку, що визначені замовником на підготовку військових фахівців Держспецзв'язку; – до викладання освітніх компонент освітньої програми залучаються фахівців Держспецзв'язку, інших навчальних закладів та провідних компаній відповідного сектору економіки; – навчальна практика проводиться в територіальних підрозділах Держспецзв'язку або в закладі освіти Держспецзв'язку науково-педагогічними працівниками закладу освіти Держспецзв'язку, як практичні заняття, відповідно до навчального плану та складається з: – військове стажування в восьмому семестрі відбувається в територіальних підрозділах Держспецзв'язку у формі індивідуальної самостійної роботи (виконання здобувачами обов'язків на первинних посадах у підрозділах Держспецзв'язку) під керівництвом науково-педагогічних працівників закладу освіти Держспецзв'язку або посадових осіб підрозділів Держспецзв'язку, на базі яких воно проводиться. – 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 місяців.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Відповідно до Державного класифікатору професій ДК 003:2010 зі Зміною №10 та Зміною №11 випускники можуть працювати на посадах, що відповідають професійній назві роботи: 2139.2 Адміністратор мереж і систем; 2139.2 Фахівець з криптографічного захисту інформації; 2139.2 Фахівець з технічного захисту інформації; 2139.2 Фахівець сфери захисту інформації. Замовником фахівців зі спеціальності 125 Кібербезпека та захист інформації виступає Державна служба спеціального зв'язку та захисту інформації України.
Подальше навчання	Мають право продовжити навчання на другому (магістерському) рівні вищої освіти. Набуття додаткових кваліфікацій в системі післядипломної освіти.
5 – Викладання та оцінювання	

Викладання та навчання	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, 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.
Оцінювання	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.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі або практичні завдання у галузі кібербезпеки та захисту інформаціїі характеризується комплексністю та невизначеністю умов, що передбачає глибоке переосмислення наявних цілісних знань та/або професійної практики.
Загальні компетентності (КЗ)	
КЗ 1	Здатність застосовувати знання у практичних ситуаціях.
КЗ 2	Знання та розуміння предметної області та розуміння професії.
КЗ 3	Здатність професійно спілкуватися державною та іноземною мовою як усно, так і письмово.
КЗ 4	Вміння виявляти,ставити та вирішувати проблеми за професійним спрямуванням.
КЗ 5	Здатність до пошуку, оброблення та аналізу інформації.
КЗ 6	Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
КЗ 7	Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
Фахові компетентності (КФ)	

КФ 1	Здатність застосовувати законодавчу та нормативно правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
КФ 2	Здатність до використання інформаційно-комунікаційних технологій , сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
КФ 3	Здатність до використання програмних та програмно апаратних комплексів засобів захисту інформації в інформаційно-комунікаційних (автоматизованих) системах.
КФ 4	Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
КФ 5	Здатність забезпечувати захист інформації, що обробляється в інформаційно-комунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
КФ 6	Здатність відновлювати штатне функціонування інформаційних, інформаційно-комунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
КФ 7	Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів и методів, процедур, практичних прийомів та ін.)
КФ 8	Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
КФ 9	Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.
КФ 10	Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.
КФ 11	Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-комунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
КФ 12	Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
КФ 13	Здатність аналізувати, інтегрувати і використовувати кращі світові практики, міжнародні стандарти при розробці криптографічних систем захисту спеціальних інформаційно-комунікаційних систем.
КФ 14	Здатність проводити дослідження, перевірку, оцінювання об’єктів інформаційної діяльності щодо їх відповідності вимогам нормативних документів із технічного захисту інформації.
КФ 15	Здатність засвоювати загальні принципи побудови та функціонування засобів та комплексів криптографічного захисту інформації, принципи, їх схемотехнічної реалізації.
КФ 16	Здатність забезпечувати успішне впровадження та функціональність вимог безпеки та відповідних політик і процедур та використовувати автоматизовані можливості для оновлення або виправлення системного програмного забезпечення.
КФ 17	Здатність обґрунтовано впроваджувати заходи з безпеки спеціального зв’язку в підпорядкованому органі.
7 – Програмні результати навчання	
ПРН 1	Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.
ПРН 2	Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язання складних спеціалізованих задач та практичних проблем у професійної діяльності, оцінювати їхню ефективність.

ПРН 3	Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
ПРН 4	Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
ПРН 5	Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.
ПРН 6	Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
ПРН 7	Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки.
ПРН 8	Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки.
ПРН 9	Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.
ПРН 10	Виконувати аналіз та декомпозицію інформаційно-комунікаційних систем.
ПРН 11	Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.
ПРН 12	Розробляти моделі загроз та порушника.
ПРН 13	Аналізувати проекти інформаційно-комунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
ПРН 14	Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-комунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
ПРН 15	Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
ПРН 16	Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємств) відповідно до вимог нормативно-правових документів.
ПРН 17	Забезпечувати процеси захисту та функціонування інформаційно-комунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектор та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
ПРН 18	Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
ПРН 19	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-комунікаційних системах.
ПРН 20	Забезпечувати функціонування спеціального програмного забезпечення щодо захисту інформації від руйнуючих програмних впливів,руйнуючих кодів в інформаційно-комунікаційних системах.
ПРН 21	Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-комунікаційних (автоматизованих) системах.

ПРН 22	Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної та/або кібербезпеки.
ПРН 23	Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-комунікаційних (автоматизованих) системах.
ПРН 24	Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-комунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
ПРН 25	Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-комунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур їх захисту.
ПРН 26	Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу та захисту інформаційних та інформаційно-комунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
ПРН 27	Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-комунікаційних (автоматизованих) системах.
ПРН 28	Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-комунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки.
ПРН 29	Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-комунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
ПРН 30	Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-комунікаційних систем.
ПРН 31	Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-комунікаційних систем.
ПРН32	Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
ПРН 33	Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.
ПРН 34	Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
ПРН 35	Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-комунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.
ПРН 36	Виявляти небезпечні сигнали технічних засобів.
ПРН 37	Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН 38	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-комунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН 39	Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
ПРН 40	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІКС відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН 41	Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
ПРН 42	Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
ПРН 43	Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.
ПРН 44	Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.
ПРН 45	Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
ПРН 46	Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-комунікаційних системах.
ПРН 47	Вирішувати задачі захисту інформації, що обробляється в інформаційно-комунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
ПРН 48	Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-комунікаційних системах.
ПРН 49	Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
ПРН 50	Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
ПРН 51	Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-комунікаційних системах.
ПРН 52	Використовувати інструментарій для моніторингу процесів в інформаційно-комунікаційних системах.
ПРН 53	Вирішувати задачі аналізу програмного коду на наявність можливих загроз.
ПРН 54	Усвідомлювати цінності громадського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
ПРН 55	Проводити аналіз та синтез криптографічних алгоритмів; розробляти рекомендації впровадження інноваційних проектів, використовуючи базові методи дослідницької діяльності.
ПРН 56	Застосовувати методи та методики щодо оцінювання захищеності об’єктів інформаційної діяльності та державних інформаційних ресурсів від несанкціонованого доступу
ПРН 57	Будувати системи протидії технічним розвідкам.
ПРН 58	Організація та практична реалізація заходів безпеки інформаційно-комунікаційних технологій.

ПРН 59	Організовувати, здійснювати на контролювати безпеку спеціального зв'язку в органах спеціального зв'язку у відповідності до вимог нормативно-правових актів та нормативних документів з криптографічного захисту інформації
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	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).
Матеріально-технічне забезпечення	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). Лабораторія технічного захисту інформації, 4 навчальні станції спеціального зв'язку, комп'ютерний клас.
Інформаційне та навчально-методичне забезпечення	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.
9 – Академічна мобільність	
Національна кредитна мобільність	Можлива за наявності двосторонніх договорів між ІСЗЗІ КПІ ім. Ігоря Сікорського та закладами вищої освіти України.
Міжнародна кредитна мобільність	Можливість укладання угод про академічну мобільність, про тривалі міжнародні проекти, які передбачають включене навчання здобувачів вищої освіти (за рішенням Голови Держспецзв'язку).
Навчання іноземних здобувачів вищої освіти	Навчання іноземних здобувачів вищої освіти за даною освітньо-професійною програмою не передбачено.

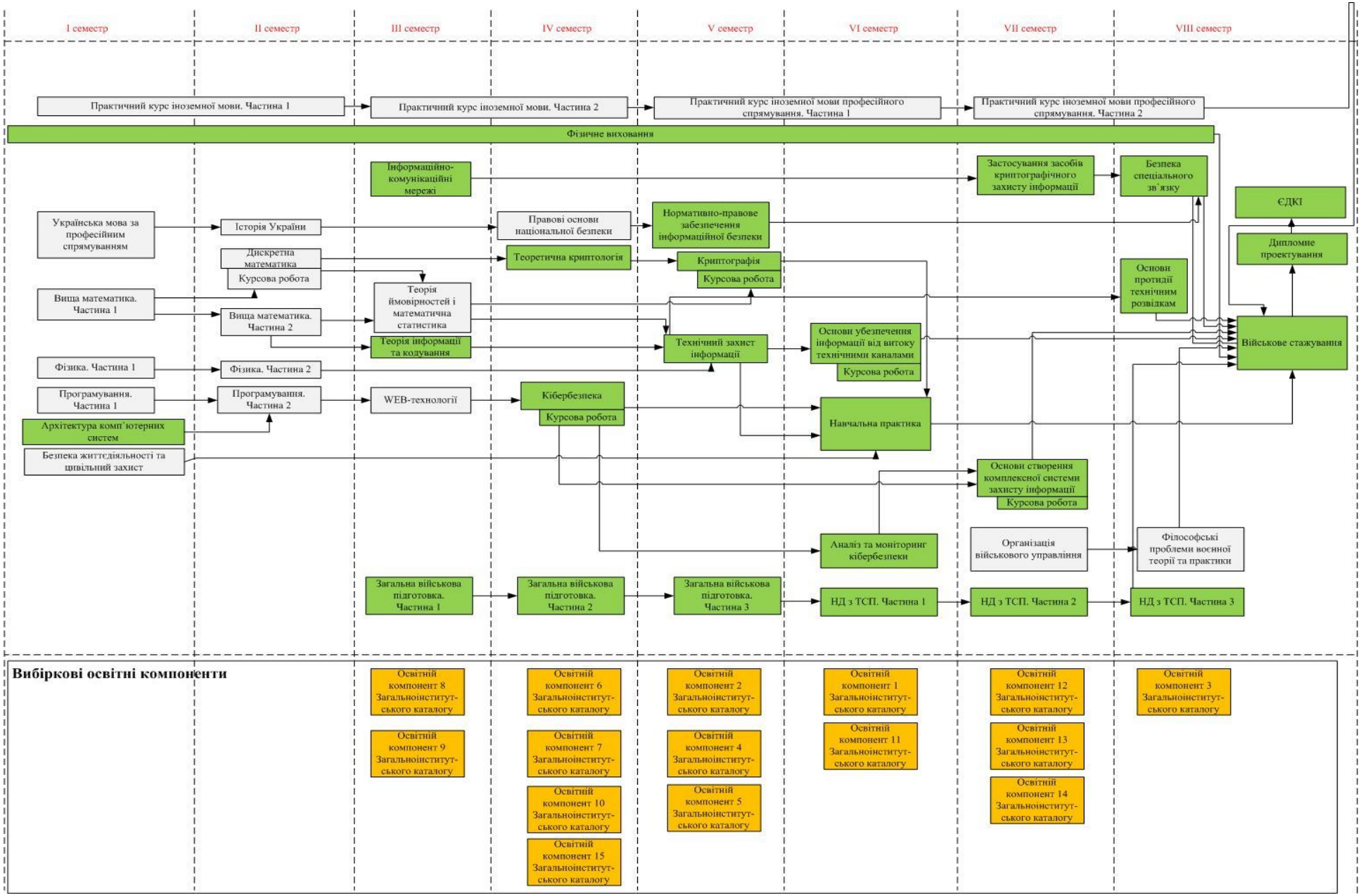
2. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬОЇ ПРОГРАМИ

Код	Компоненти освітньої програми (навчальні дисципліни, курсові проекти/роботи, практики)	Кількість кредитів ЄКТС	Форма підсумкового контролю
1	**2**	**3**	**4**
1. НОРМАТИВНІ освітні компоненти			
1.1. Цикл загальної підготовки			
ЗО 1	Українська мова за професійним спрямуванням	2	залік
ЗО 2	Історія України	2	залік
ЗО 3.1	Практичний курс іноземної мови. Частина 1	3	залік
ЗО 3.2	Практичний курс іноземної мови. Частина 2	3	залік
ЗО 4.1	Практичний курс іноземної мови професійного спрямування. Частина 1	3	залік
ЗО 4.2	Практичний курс іноземної мови професійного спрямування. Частина 2	3	екзамен
ЗО 5	Організація військового управління	3	залік
ЗО 6	Безпека життєдіяльності та цивільний захист	2	залік
ЗО 7.1	Вища математика. Частина 1. Лінійна алгебра. Аналітична геометрія. Диференціальне числення однієї та кількох змінних.	8	екзамен
ЗО 7.2	Вища математика. Частина 2. Інтегральне числення функції однієї змінної. Диференціальні рівняння. Числові і функціональні ряди і інтеграл Фур'є.	7	екзамен
ЗО 8.1	Фізика. Частина 1. Електромагнетизм. Коливання та хвилі. Оптика.	5	екзамен
ЗО 8.2	Фізика. Частина 2. Основи квантової фізики. Фізика твердого тіла. Основи квантової електроніки.	5	екзамен
ЗО 9	Дискретна математика	6	екзамен
ЗО 10	Дискретна математика. Курсова робота	1	залік
ЗО 11.1	Програмування. Частина 1. Алгоритмізація та програмування.	4	залік
ЗО 11.2	Програмування. Частина 2. Об'єктно-орієнтоване програмування.	6	залік
ЗО 12	WEB-технології.	3	залік
ЗО 13	Правові основи національної безпеки	3	залік
ЗО 14	Філософські проблеми воєнної теорії та практики	2	залік
ЗО 15	Теорія ймовірностей і математична статистика	4	екзамен
1.2. Цикл професійної підготовки			
ПО 1	Архітектура комп'ютерних систем	3	залік
ПО 2.1	Фізичне виховання. Частина 1	2	залік
ПО 2.2	Фізичне виховання. Частина 2	2	екзамен
ПО 2.3	Фізичне виховання. Частина 3	2	залік

1	2	3	4
ПО 2.4	Фізичне виховання. Частина 4	2	екзамен
ПО 2.5	Фізичне виховання. Частина 5	2	залік
ПО 2.6	Фізичне виховання. Частина 6	2	екзамен
ПО 2.7	Фізичне виховання. Частина 7	2	залік
ПО 2.8	Фізичне виховання. Частина 8	2	екзамен
ПО 3	Інформаційно-комунікаційні мережі	4	екзамен
ПО 4	Теорія інформації та кодування	3	залік
ПО 5	Теоретична криптологія	3	залік
ПО 6	Криптографія.	4	екзамен
ПО 7	Криптографія. Курсова робота	1	залік
ПО 8	Технічний захист інформації	3	залік
ПО 9	Кібербезпека	4	екзамен
ПО 10	Кібербезпека. Курсова робота	1	залік
ПО 11.1	Загальна військова підготовка. Частина 1	3	залік
ПО11.2	Загальна військова підготовка. Частина 2	5	залік
ПО 11.3	Загальна військова підготовка. Частина 3	5	екзамен
ПО 12.1	Тактико-спеціальна підготовка. Частина 1	4	залік
ПО12.2	Тактико-спеціальна підготовка. Частина 2	4	залік
ПО12.3	Тактико-спеціальна підготовка. Частина 3	5	екзамен
ПО 13	Основи протидії технічним розвідкам	3	залік
ПО 14	Нормативно-правове забезпечення інформаційної безпеки	3	залік
ПО 15	Основи створення комплексних систем захисту інформації.	4	екзамен
ПО 16	Основи створення комплексних систем захисту інформації. Курсова робота	1	залік
ПО 17	Аналіз та моніторинг кібербезпеки	4	екзамен
ПО 18	Основи убезпечення інформації від витоку технічними каналами.	4	екзамен
ПО 19	Основи убезпечення інформації від витоку технічними каналами. Курсова робота	1	залік
ПО 20	Застосування засобів криптографічного захисту інформації.	3	екзамен
ПО 21	Безпека спеціального зв'язку	3,5	залік
ПО 22	Навчальна практика	1,5	залік
ПО 23	Військове стажування	3	залік
ПО 24	Дипломне проектування	6	захист
2. ВИБІРКОВІ освітні компоненти			
2.1. Вибіркові освітні компоненти з Загальноінститутського Каталогу			
ПВ 1	Освітній компонент 1 Загальноінститутського Каталогу	4	залік
ПВ 2	Освітній компонент 2 Загальноінститутського Каталогу	4	залік
ПВ 3	Освітній компонент 3 Загальноінститутського Каталогу	4	залік

1	2	3	4
ПВ 4	Освітній компонент 4 Загальноінститутського Каталогу	4	залік
ПВ 5	Освітній компонент 5 Загальноінститутського Каталогу	4	залік
ПВ 6	Освітній компонент 6 Загальноінститутського Каталогу	4	залік
ПВ 7	Освітній компонент 7 Загальноінститутського Каталогу	4	залік
ПВ8	Освітній компонент 8 Загальноінститутського Каталогу	4	залік
ПВ9	Освітній компонент 9 Загальноінститутського Каталогу	4	залік
ПВ10	Освітній компонент 10 Загальноінститутського Каталогу	4	залік
ПВ 11	Освітній компонент 11 Загальноінститутського Каталогу	4	залік
ПВ 12	Освітній компонент 12 Загальноінститутського Каталогу	4	залік
ПВ 13	Освітній компонент 13 Загальноінститутського Каталогу	4	залік
ПВ 14	Освітній компонент 14 Загальноінститутського Каталогу	4	залік
ПВ 15	Освітній компонент 15 Загальноінститутського Каталогу	4	залік
Загальний обсяг **нормативних освітніх компонентів циклу загальної підготовки:**		**75**	
Загальний обсяг **нормативних освітніх компонентів циклу професійної підготовки:**		**105**	
Загальний обсяг **вибіркових освітніх компонентів:**		**60**	
Обсяг освітніх компонентів, що забезпечують здобуття компетентностей, визначених СВО:		**180**	
ЗАГАЛЬНИЙ ОБСЯГ:		**240**	

3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬОЇ ПРОГРАМИ



4. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація здобувачів вищої освіти за освітньо-професійною програмою “Безпека державних інформаційних ресурсів” здійснюється у формі єдиного державного кваліфікаційного іспиту та захисту кваліфікаційної роботи/проекту бакалавра, що забезпечує оцінювання досягнутих програмних результатів навчання, визначених стандартом вищої освіти за спеціальністю 125 “Кібербезпека та захист інформації” для першого (бакалаврського) рівня вищої освіти та освітньо-професійною програмою.

До атестації допускаються здобувачі, які в повному обсязі виконали вимоги програми підготовки. Кваліфікаційна робота/проект має передбачати розв’язання складної задачі дослідницького та/або інноваційного характеру у сфері кібербезпеки та захисту інформації і не може бути академічного плагіату та фальсифікації. З цією метою робота перевіряється на наявність плагіату згідно з процедурою, визначеною системою забезпечення якості освітньої діяльності та якості вищої освіти Університетом.

Після захисту кваліфікаційна робота розміщується в навчальній бібліотеці ІСЗЗІ КПІ ім. Ігоря Сікорського в архіві наукових та освітніх матеріалів для вільного доступу.

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

5. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

	ЗО 1	ЗО 2	ЗО 3	ЗО 4	ЗО 5	ЗО 6	ЗО 7	ЗО 8	ЗО 9	ЗО 10	ЗО 11	ЗО 12	ЗО 13	ЗО 14	ЗО 15	ПО 1	ПО 2	ПО 3	ПО 4	ПО 5	ПО 6	ПО 7	ПО 8	ПО 9	ПО 10	ПО 11	ПО 12	ПО 13	ПО 14	ПО 15	ПО 16	ПО 17	ПО 18	ПО 19	ПО 20	ПО 21	ПО 22	ПО 23	ПО 24
КЗ 1	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+					+	+	+	+	+	+		+	+	+
КЗ 2	+	+	+			+	+	+	+	+								+	+	+	+	+	+	+	+					+	+	+	+	+	+		+	+	+
КЗ 3	+		+	+				+				+	+	+										+						+	+				+		+	+	+
КЗ 4		+				+	+		+				+	+	+	+		+		+	+		+									+	+	+			+	+	+
КЗ 5		+					+			+	+	+	+	+					+						+		+			+	+	+			+			+	+
КЗ 6			+		+	+							+	+																		+						+	+
КЗ 7		+											+	+												+													+
КФ 1			+	+																+	+	+	+	+	+			+	+	+	+	+	+	+	+	+	+	+	+
КФ 2	+						+		+	+					+	+		+	+					+	+					+	+	+			+		+	+	+
КФ 3																								+	+					+	+	+			+		+	+	+
КФ4																								+	+					+		+					+	+	+
КФ5																				+	+	+		+	+				+		+				+			+	+
КФ 6								+										+	+					+	+							+						+	+
КФ 7							+	+									+													+	+	+	+					+	+
КФ 8																																+						+	+
КФ 9																											+	+							+		+	+	+
КФ 10							+	+							+				+	+		+	+				+				+	+	+	+	+	+	+	+	+
КФ 11																																						+	+
КФ 12								+							+													+	+	+					+		+	+
КФ 13																						+																	+
КФ 14																							+																+
КФ 15																								+															+
КФ 16																									+					+									+
КФ 17																																			+				+

6. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

	ЗО 1	ЗО 2	ЗО 3	ЗО 4	ЗО 5	ЗО 6	ЗО 7	ЗО 8	ЗО 9	ЗО 10	ЗО 11	ЗО 12	ЗО 13	ЗО 14	ЗО 15	ПО 1	ПО 2	ПО 3	ПО 4	ПО 5	ПО 6	ПО 7	ПО 8	ПО 9	ПО 10	ПО 11	ПО 12	ПО 13	ПО 14	ПО 15	ПО 16	ПО 17	ПО 18	ПО 19	ПО 20	ПО 21	ПО 22	ПО 23	ПО 24
ПРН 1	+	+	+	+								+	+	+										+	+				+	+	+	+			+	+	+	+	+
ПРН 2		+					+		+		+				+	+			+	+	+	+			+			+	+						+	+		+	+
ПРН 3		+					+			+		+			+	+			+	+	+	+			+			+	+	+	+				+		+	+
ПРН 4		+				+	+		+		+				+	+			+	+	+	+		+			+	+	+						+	+	+	+	+
ПРН 5		+					+					+			+				+					+				+	+						+	+	+	+	+
ПРН 6		+			+		+		+				+	+	+	+																					+	+
ПРН 7				+									+	+						+	+	+		+	+			+	+	+			+	+	+	+	+	+	+
ПРН 8													+																				+	+				+	+
ПРН 9				+																				+	+						+				+	+		+	+
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																				+		+		+	+						+	+					+	+	+

	ЗО 1	ЗО 2	ЗО 3	ЗО 4	ЗО 5	ЗО 6	ЗО 7	ЗО 8	ЗО 9	ЗО 10	ЗО 11	ЗО 12	ЗО 13	ЗО 14	ЗО 15	ПО 1	ПО 2	ПО 3	ПО 4	ПО 5	ПО 6	ПО 7	ПО 8	ПО 9	ПО 10	ПО 11	ПО 12	ПО 13	ПО 14	ПО 15	ПО 16	ПО 17	ПО 18	ПО 19	ПО 20	ПО 21	ПО 22	ПО 23	ПО 24
ПРН 23																				+		+		+	+			+		+	+						+		+
ПРН 24																						+		+	+												+	+
ПРН 25																								+	+													+
ПРН 26																														+	+					+		+
ПРН 27																			+	+										+	+			+			+	+
ПРН 28															+															+							+	+
ПРН 29																														+							+	+
ПРН 30																																					+	+
ПРН 31															+															+	+		+	+			+	+
ПРН 32																		+						+	+												+	+
ПРН 33																																					+	+
ПРН 34																												+							+		+	+
ПРН 35																				+		+								+	+						+	+
ПРН 36								+											+				+										+			+		+
ПРН 37								+															+										+			+		+
ПРН 38								+															+										+	+			+	+
ПРН 39																																					+	+
ПРН 40								+															+								+	+	+			+		+
ПРН 41																															+					+		+
ПРН 42																				+		+									+						+	+
ПРН 43																												+									+	+
ПРН 44																																					+	+
ПРН 45																																					+	+
ПРН 46																			+																		+	+
ПРН 47																				+		+												+	+	+		+

	ЗО 1	ЗО 2	ЗО 3	ЗО 4	ЗО 5	ЗО 6	ЗО 7	ЗО 8	ЗО 9	ЗО 10	ЗО 11	ЗО 12	ЗО 13	ЗО 14	ЗО 15	ПО 1	ПО 2	ПО 3	ПО 4	ПО 5	ПО 6	ПО 7	ПО 8	ПО 9	ПО 10	ПО 11	ПО 12	ПО 13	ПО 14	ПО 15	ПО 16	ПО 17	ПО 18	ПО 19	ПО 20	ПО 21	ПО 22	ПО 23	ПО 24
ПРН 48																				+		+										+				+	+		+
ПРН 49																																+						+	+
ПРН 50																																				+			+
ПРН 51																																				+			+
ПРН 52																																+				+			+
ПРН 53											+	+																				+				+			+
ПРН 54			+										+	+			+								+		+	+							+				+
ПРН 55					+																+	+							+										+
ПРН 56																							+						+				+						+
ПРН 57																								+					+			+							+
ПРН 58																									+				+	+									+
ПРН 59																													+	+						+			+