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

СИСТЕМИ, ТЕХНОЛОГІЇ ТА МАТЕМАТИЧНІ МЕТОДИ КІБЕРБЕЗПЕКИ

SYSTEMS, TECHNOLOGIES AND MATHEMATICAL METHODS OF CYBER SECURITY

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 навч. року
наказом ректора
КПІ ім. Ігоря Сікорського
від 17.05. 2023 р. № НОН/165/2023

Київ – 2023

ПРЕАМБУЛА

РОЗРОБЛЕНО проектною групою:

Керівник проектної групи:

Ланде Дмитро Володимирович, доктор технічних наук, професор, завідувач кафедри інформаційної безпеки, Навчально-науковий Фізико-технічний інститут

Члени проектної групи:

Новіков Олексій Миколайович, доктор технічних наук, професор, директор Навчально-Наукового Фізико-Технічного інституту

Грайворонський Микола Владленович, кандидат фізико-математичних наук, доцент, доцент кафедри інформаційної безпеки, Навчально-науковий Фізико-технічний інститут

Литвинова Тетяна Василівна, кандидат технічних наук, доцент, доцент кафедри інформаційної безпеки, Навчально-науковий Фізико-технічний інститут

Стьопочкіна Ірина Валеріївна, кандидат технічних наук, доцент кафедри інформаційної безпеки, Навчально-науковий Фізико-технічний інститут

ПОГОДЖЕНО:

Науково-методичною комісією КПІ ім. Ігоря Сікорського зі спеціальності 125

Голова НМКУ 125

_____ Дмитро ЛАНДЕ

(протокол №1/2023 від «10» січня 2023 р.)

Методичною радою КПІ ім. Ігоря Сікорського

Голова Методичної ради

_____ Анатолій МЕЛЬНИЧЕНКО

(протокол № 4 від «19» 01 2023 р.)

ВРАХОВАНО:

Пропозиції стейкхолдерів:

Представники роботодавців:
Жора Віктор Володимирович, заступник голови Державної служби спеціального зв'язку та захисту інформації України

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

Кудін Антон Михайлович,
головний експерт Департаменту безпеки НБУ,
д.т.н., професор

Представники студентських організацій:

Зібаров Дмитро,
студент 4 курсу бакалаврату за
спеціальністю 125 Кібербезпека

Курганський Леонід, студент
4 курсу бакалаврату за спеціальністю 125 Кібербезпека

Чалий Олексій, студент 1 курсу магістратури
за спеціальністю 125 Кібербезпека

Внесено наступні зміни:
Освітню програму оновлено у зв'язку зі зміною назви спеціальності. Внесено корективи у відповідності з вимогами Постанови Кабінету Міністрів України від 16.12.2022 № 1392 "Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти"

Освітню програму обговорено на засіданнях НМКУ та ухвалено на засіданні кафедри інформаційної безпеки, протокол №10/2022 від 28.12.2022.

ЗМІСТ

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ
зі спеціальності 125 Кібербезпека та захист інформації
за освітньою програмою «Системи, технології та математичні методи кібербезпеки»

1 – Загальна інформація	
Повна назва ЗВО та інституту/ факультету	Національний технічний університет України “Київський політехнічний інститут імені Ігоря Сікорського”, Навчально-науковий Фізико-технічний інститут
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь – бакалавр Кваліфікація – бакалавр з кібербезпеки та захисту інформації
Рівень з НРК	НРК України – 6 рівень, QF-EHEA – перший цикл, EQF-LLL – 6 рівень
Офіційна назва освітньої програми	Системи, технології та математичні методи кібербезпеки
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів, термін навчання 3 роки 10 місяці
Наявність акредитації	Сертифікат акредитації спеціальності УД 11010979 дійсний до 01.07.2028
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/node/103, (розділ «Освітні програми»), http://is.ipt.kpi.ua/navchalni-programi-2
2 – Мета освітньої програми	
Підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки та захисту інформації; а також новітні технології та математичні методи, проводити інноваційну діяльність в галузі захисту інформації і кібернетичної безпеки; забезпечення поглибленої фундаментальної підготовки; гармонійність, багатовимірність освіти; інтеграція науково-інноваційної та практичної діяльності і навчального процесу; орієнтація на міжнародні вимоги в сфері кібербезпеки; орієнтація на вимоги ринку праці та дуальну освіту. Мета освітньої програми відповідає стратегії розвитку КПІ імені Ігоря Сікорського 2020-2025 років 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, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно- телекомунікаційні системи, інформаційні ресурси і технології; – технології забезпечення безпеки інформації; – процеси управління інформаційною та/або кібербезпекою об’єктів, що підлягають захисту. Цілі навчання підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки. Теоретичний зміст предметної області Знання – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів інформаційної та/або кібербезпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною та/або кібербезпекою; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення – інформаційно-комунікаційних технологій; – автоматизованих систем проектування. Методи, методики та технології: – Методи, методики, 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 ОП – системи та процеси кіберпростору, засоби та заходи захисту. Ключові слова: кібернетична безпека, захист інформації, інформаційно- телекомунікаційні системи, програмні та апаратні засоби захисту інформації, системи і технології кібербезпеки, математичні методи кібербезпеки, аудит кіберінцидентів, технічний аудит
Особливості програми	1) ґрунтовна фундаментальна підготовка у поєднанні із сучасною професійною підготовкою, яка дозволяє проводити інноваційну діяльність і працювати з наукоємними технологіями кібербезпеки; 2) проходження переддипломної практики на базі підприємств- партнерів та участь студентів у виконанні спільних науково- дослідних проектів на замовлення установ та провідних ІТ- компаній України за фахом; 3) підготовка до дуальної освіти в магістратурі.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Відповідно до Державного класифікатору професій ДК 003:2010 зі Зміною №10 випускники можуть працювати на посадах, що відповідають класифікаційним угрупованням: 3139 Фахівець із організації захисту інформації з обмеженим доступом; Фахівець із організації інформаційної безпеки 3121 Фахівець з інформаційних технологій. 2139.2 Аналітик систем захисту інформації та оцінки вразливостей 2139.2 Аналітик загроз безпеки 2132.2 Розробник систем захисту інформації. 2149 Професіонали із організації інформаційної безпеки.
Подальше навчання	Продовження освіти за другим (освітньо-професійним, освітньо- науковим) рівнем вищої освіти
5 – Викладання та оцінювання	
Викладання та навчання	Програмою передбачено студентоцентроване навчання. Викладання проводиться у таких формах: лекції, практичні та семінарські заняття, комп'ютерні практикуми і лабораторні роботи; курсові роботи і індивідуальні завдання; технологія змішаного навчання за деякими освітніми компонентами, практики; виконання дипломної роботи (бакалаврської дипломної роботи)
Оцінювання	Оцінювання знань студентів здійснюється у відповідності до Положення про систему оцінювання результатів навчання КПІ ім. Ігоря Сікорського за усіма видами аудиторної та позааудиторної роботи (вхідний, поточний, календарний, підсумковий контроль); усних та письмових екзаменів, заліків

6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
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 мовами 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 зако-номірностей 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 (ФК)	
ФК 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.
ФК 2	Здатність до використання інформаційно- комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/ або кібербезпеки.
ФК 3	Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно- телекомунікаційних (автоматизованих) системах.
ФК 4	Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
ФК 5	Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки..

ФК 6	Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.
ФК 7	Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно- правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)
ФК 8	Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
ФК 9	Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою
ФК 10	Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.
ФК 11	Здатність виконувати моніторинг процесів функціонування інформаційних інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/ або кібербезпеки.
ФК 12	Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки
ФК 13	Здатність розв’язувати задачі за фахом із використанням математичних методів, алгоритмів, прикладних та системних програмних рішень та технологій
ФК 14	Здатність розв’язувати задачі із забезпечення конфіденційності, цілісності, доступності та спостережності інформації та керування нею із використанням сучасних технологій, моделей та методів кібербезпеки із врахуванням вимог нормативних документів та Стандартів
ФК 15	Здатність до аудиту кібербезпеки інформаційних систем, та управління інформаційною та кібернетичною безпекою
ФК 16	Здатність до проектування та розробки захищених інформаційних систем
ФК 17	Здатність до зворотної розробки та аналізу програмного забезпечення
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’язування складних спеціалізованих задач та практичних проблем у професійній 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, щобазуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки
ПРН 10	Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних 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-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних
ПРН 14	Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних 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 (підприємства) відповідно до вимог нормативно-правових документів
ПРН 17	Забезпечувати процеси захисту та функціонування інформаційно- телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент

ПРН 18	Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів
ПРН 19	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах
ПРН 20	Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних 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-телекомунікаційних (автоматизованих) системах
ПРН 22	Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно- телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки
ПРН 23	Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах
ПРН 24	Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових)
ПРН 25	Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту
ПРН 26	Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем

ПРН 27	Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах
ПРН 28	Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно- телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки
ПРН 29	Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційних та інформаційно- телекомунікаційних системах, ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів
ПРН 30	Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем
ПРН 31	Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем
ПРН 32	Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних 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- телекомунікаційних (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-телекомунікаційних 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 ІТС 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-телекомунікаційних системах
ПРН 47	Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних 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-телекомунікаційних системах
ПРН 49	Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;

ПРН 50	Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення втрогнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних)
ПРН 51	Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах
ПРН 52	Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах
ПРН 53	Вирішувати задачі аналізу програмного коду на наявність можливих загроз
ПРН 54	Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні
ПРН 55	Здійснювати зворотну розробку та аналіз шкідливого програмного забезпечення із застосуванням сучасних технологій та математичних методів
ПРН 56	Застосовувати сучасні методи та технології аналізу та моніторингу кібернетичної безпеки для забезпечення управління інформаціною безпекою
ПРН 57	Здійснювати управління інцидентами безпеки із застосуванням ризик-орієнтованого підходу
ПРН 58	Володіти принципами проектування та системної інженерії захищених систем
ПРН 59	Здійснювати технічний аудит кібербезпеки, аудит кіберінцидентів

8 – Ресурсне забезпечення реалізації програми	
Кадрове Забезпечення	Відповідно до кадрових вимог щодо забезпечення провадження освітньої діяльності для відповідного рівня ВО (Ліцензійні умови, затверджені Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 (в чинній редакції))
Матеріально-технічне забезпечення	Відповідно до технологічних вимог щодо матеріально-технічного забезпечення освітньої діяльності відповідного рівня ВО (Ліцензійні умови, затверджені Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 (в чинній редакції)), 3 комп'ютерних класи, полігон з Кібербезпеки Матеріально-технічна база Samsung R&D Institute Ukraine
Інформаційне та навчально-методичне забезпечення	Відповідно до вимог щодо навчально-методичного та інформаційного забезпечення освітньої діяльності відповідного рівня ВО (Ліцензійні умови, затверджені Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 (в чинній редакції)) Ресурси науково-технічної бібліотеки КПІ імені Ігоря Сікорського, бібліотеки Навчально-наукового Фізико-технічного інституту
9 – Академічна мобільність	
Національна кредитна мобільність	Участь студентів у програмах академічної мобільності
Міжнародна кредитна мобільність	Можливість укладення угод про міжнародну академічну мобільність, про тривалі міжнародні проекти
Навчання іноземних здобувачів вищої освіти	Навчання іноземних здобувачів ВО, які опановують ОП за програмами міжнародної академічної мобільності, навчання може проводитись англійською або українською мовою, за умови володіння здобувачем мовою навчання на рівні не нижче В2.

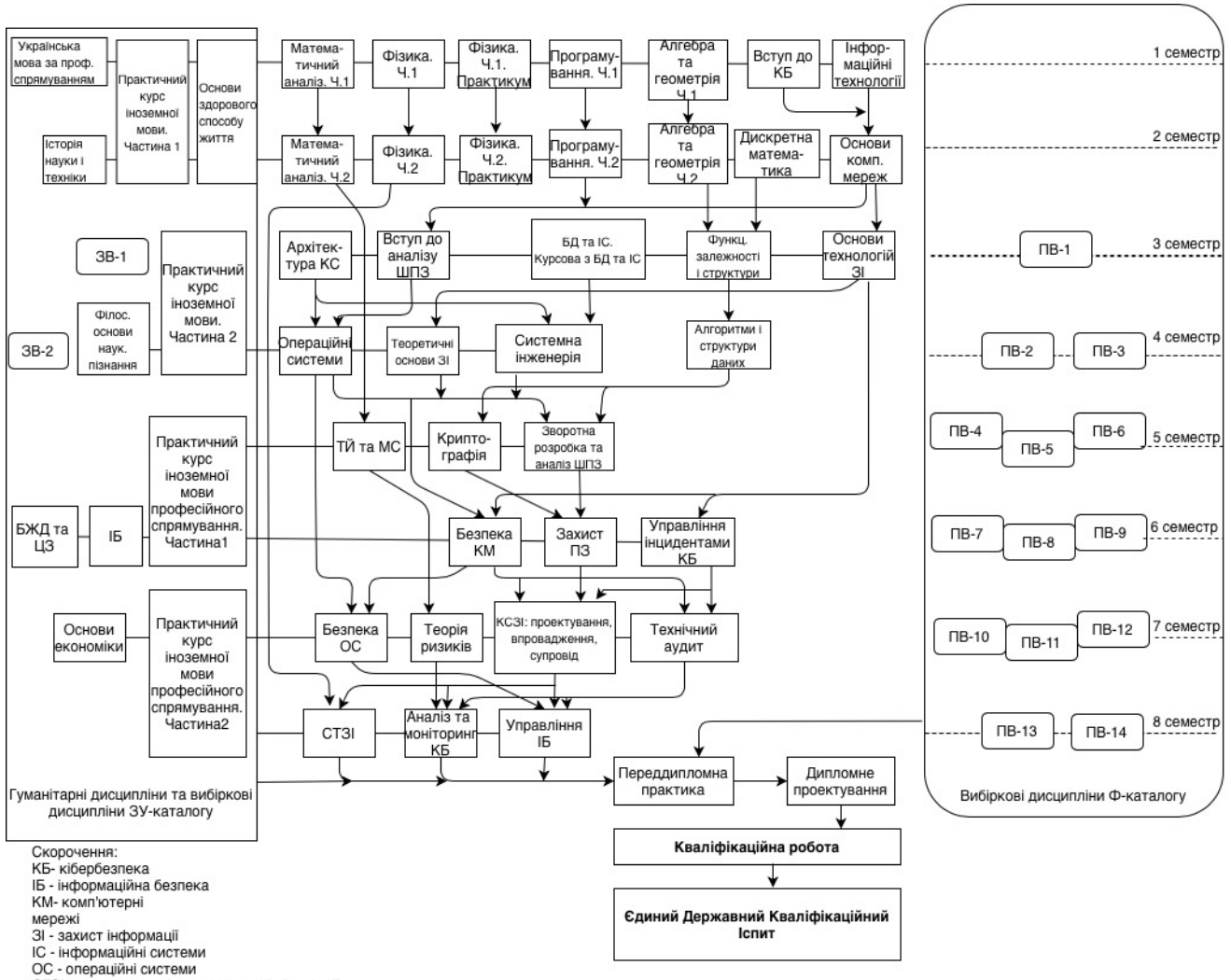
2. ПЕРЕЛІК КОМПОНЕНТІВ ОСВІТНЬОЇ ПРОГРАМИ

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кільк. кредитів	Форма підсумков. контролю
1. Нормативні освітні компоненти			
1.1 Цикл загальної підготовки			
ЗО 1	Українська мова за професійним спрямуванням	2	Залік
ЗО 2	Історія науки і техніки	2	Залік
ЗО 3	Основи здорового способу життя	3	Залік
ЗО 4.1	Практичний курс іноземної мови. Частина 1	3	Залік
ЗО 4.2	Практичний курс іноземної мови. Частина 2	3	Залік
ЗО 5	Основи економіки	2	Залік
ЗО 6	БЖД та цивільний захист	2	Залік
ЗО 7.1	Математичний аналіз. Частина 1	6,5	Екзамен
ЗО 7.2	Математичний аналіз. Частина 2	5,5	Екзамен
ЗО 8.1	Фізика. Частина 1	4,5	Залік
ЗО 8.2	Фізика. Частина 2	5,5	Екзамен
ЗО 9	Теорія ймовірностей та математична статистика	5,5	Екзамен
ЗО 10	Дискретна математика	4,5	Екзамен
ЗО 11.1	Програмування. Частина 1. Структурний підхід	4,5	Екзамен
ЗО 11.2	Програмування. Частина 2. Об’єктно-орієнтований підхід	3,5	Залік
ЗО 12.1	Алгебра та геометрія. Частина 1	4.5	Екзамен
ЗО 12.2	Алгебра та геометрія. Частина 2	3	Залік
ЗО 13	Вступ до кібернетичної безпеки	2	Залік
ЗО 14	Інформаційні технології	3	Залік
ЗО 15	Основи комп’ютерних мереж	3	Залік
ЗО 16	Архітектура комп'ютерних систем	4	Екзамен
ЗО 17	Операційні системи	5	Екзамен
ЗО 18	Теоретичні основи захисту інформації	3	Екзамен
ЗО 19	Системна інженерія	5	Екзамен
ЗО 20	Криптографія	6	Екзамен
ЗО 21	Комплексні системи захисту інформації: проектування, впровадження, супровід	3,5	Залік
ЗО 22.1	Практичний курс іноземної мови професійного спрямування. Частина 1	3	Залік
ЗО 22.2	Практичний курс іноземної мови професійного спрямування. Частина 2	3	Екзамен
ЗО 23	Філософські основи наукового пізнання	2	Залік
ЗО 24	Інформаційна безпека	2	Залік

ЗО 25	Переддипломна практика	6	Залік
ЗО 26	Дипломне проектування	6	Захист
1. 2 Цикл професійної підготовки			
ПО 1	Алгоритми та структури даних	3,5	Залік
ПО 2	Вступ до аналізу шкідливого програмного забезпечення	5	Екзамен
ПО 3	Функціональні залежності та структури	4	Екзамен
ПО 4	Бази даних та інформаційні системи	4	Залік
ПО 5	Основи технологій захисту інформації	4,5	Залік
ПО 6	Зворотна розробка та аналіз шкідливого програмного забезпечення	5	Екзамен
ПО 7	Безпека комп'ютерних мереж	4,5	Екзамен
ПО 8	Системи технічного захисту інформації	3	Залік
ПО 9	Захист програмного забезпечення	4	Екзамен
ПО 10	Управління інцидентами комп’ютерної безпеки	4	Екзамен
ПО 11	Безпека операційних систем	4	Екзамен
ПО 12	Теорія ризиків	3	Екзамен
ПО 13	Технічний аудит	4	Екзамен
ПО 14	Бази даних та інформаційні системи. Курсова робота	1	Залік
ПО 15	Аналіз та моніторинг кібернетичної безпеки	3	Екзамен
ПО 16	Управління інформаційною безпекою	2,5	Залік
2. Вибіркові освітні компоненти			
2.1. Цикл загальної підготовки (Вибіркові освітні компоненти із загальноуніверситетського Каталогу)			
ЗВ 1	Освітній компонент 1 ЗУ-Каталогу	2	Залік
ЗВ 2	Освітній компонент 2 ЗУ-Каталогу	2	Залік
2.2. Цикл професійної підготовки (Вибіркові освітні компоненти з факультетського/кафедрального Каталогів)			
ПВ 1	Освітній компонент 1 Ф-Каталогу	4	Залік
ПВ 2	Освітній компонент 2 Ф-Каталогу	4	Залік
ПВ 3	Освітній компонент 3 Ф-Каталогу	4	Залік
ПВ 4	Освітній компонент 4 Ф-Каталогу	4	Залік
ПВ 5	Освітній компонент 5 Ф-Каталогу	4	Залік
ПВ 6	Освітній компонент 6 Ф-Каталогу	4	Залік
ПВ 7	Освітній компонент 7 Ф-Каталогу	4	Залік
ПВ 8	Освітній компонент 8 Ф-Каталогу	4	Залік
ПВ 9	Освітній компонент 9 Ф-Каталогу	4	Залік
ПВ 10	Освітній компонент 10 Ф-Каталогу	4	Залік
ПВ 11	Освітній компонент 11 Ф-Каталогу	4	Залік
ПВ 12	Освітній компонент 12 Ф-Каталогу	4	Залік
ПВ 13	Освітній компонент 13 Ф-Каталогу	4	Залік
ПВ 14	Освітній компонент 14 Ф-Каталогу	4	Залік

Загальний обсяг обов'язкових компонентів	**180**
Загальний обсяг вибіркових компонентів	**60**
Обсяг освітніх компонентів, що забезпечують здобуття компетентностей, визначених СВО	**180**
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ	**240**

3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬОЇ ПРОГРАМИ



Скорочення:
КБ- кібербезпека
ІБ - інформаційна безпека
КМ- комп'ютерні мережі
ЗІ - захист інформації
ІС - інформаційні системи
ОС - операційні системи
СТЗІ - системи технічного захисту інформації
КСЗІ - комплексні системи захисту інформації
ТЙ та МС- теорія ймовірностей та математична статистика
ПЗ -програмне забезпечення
ШПЗ - шкідливе ПЗ

4. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація здобувачів вищої освіти за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки» спеціальності 125 Кібербезпека та захист інформації здійснюється у формі Єдиного державного кваліфікаційного іспиту та публічного захисту кваліфікаційної роботи, яка завершується видачею документу встановленого зразка про присвоєння кваліфікації бакалавра з кібербезпеки та захисту інформації.

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

5. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ НОРМАТИВНИМ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

	КЗ1	**КЗ2**	**КЗ3**	**КЗ4**	**КЗ5**	**КЗ6**	**КЗ7**	**ФК1**	**ФК2**	**ФК3**	**ФК4**	**ФК5**	**ФК6**	**ФК7**	**ФК8**	**ФК9**	**ФК10**	**ФК11**	**ФК12**	**ФК13**	**ФК14**	**ФК15**	**ФК16**	**ФК17**
	1	2	3	4	5	6	7	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
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	+	+		+					+	+								+		+	+	+		
ЗО 16	+	+		+					+	+										+				+
ЗО 17	+	+			+				+									+		+		+		+
ЗО 18		+		+					+			+							+		+		+	
ЗО 19	+	+		+					+	+										+			+	

	КЗ1	**КЗ2**	**КЗ3**	**КЗ4**	**КЗ5**	**КЗ6**	**КЗ7**	**ФК1**	**ФК2**	**ФК3**	**ФК4**	**ФК5**	**ФК6**	**ФК7**	**ФК8**	**ФК9**	**ФК10**	**ФК11**	**ФК12**	**ФК13**	**ФК14**	**ФК15**	**ФК16**	**ФК17**
ЗО 20	+	+		+				+									+		+		+			
ЗО 21		+		+				+		+		+		+							+		+	
ЗО 22	+		+																					
ЗО 23						+	+																	
ЗО 24						+																		
ЗО 25	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗО 26	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПО1	+	+			+				+					+					+	+				
ПО2		+		+						+		+							+					+
ПО3	+	+		+					+								+		+	+				
ПО4	+	+		+	+			+	+	+		+								+			+	
ПО5	+	+		+					+	+		+	+								+		+	
ПО6	+	+								+									+		+			+
ПО7	+	+							+	+		+	+					+			+			
ПО8	+	+						+		+		+		+			+				+			
ПО9	+			+				+	+	+		+							+	+			+	+
ПО10	+	+						+			+				+	+		+	+		+	+		
ПО11	+							+	+	+		+						+	+		+			
ПО12		+		+				+							+	+			+	+				
ПО13	+			+				+							+	+		+	+		+	+		
ПО14	+	+		+	+			+	+	+		+								+			+	

	КЗ1	**КЗ2**	**КЗ3**	**КЗ4**	**КЗ5**	**КЗ6**	**КЗ7**	**ФК1**	**ФК2**	**ФК3**	**ФК4**	**ФК5**	**ФК6**	**ФК7**	**ФК8**	**ФК9**	**ФК10**	**ФК11**	**ФК12**	**ФК13**	**ФК14**	**ФК15**	**ФК16**	**ФК17**
ПО15	+	+		+	+	+		+	+	+	+		+	+	+	+	+	+	+		+	+		
ПО16	+	+		+		+		+			+					+		+			+	+		

6. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ НОРМАТИВНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

ПРН	**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**	**ЗО 16**	**ЗО 17**	**ЗО 18**	**ЗО 19**	**ЗО 20**	**ЗО 21**	**ЗО 22**	**ЗО 23**	**ЗО 24**	**ЗО25**	**ЗО 26**	**ПО 1**	**ПО2**	**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**
ПРН1	+	+		+					+	+				+								+			+	+	+														
ПРН2		+			+		+		+	+	+	+	+	+		+			+	+	+				+	+	+	+	+	+		+							+	+	
ПРН3		+					+		+	+	+	+	+	+	+	+	+			+			+		+	+	+												+		
ПРН 4		+			+		+		+	+		+	+	+	+	+		+	+	+					+	+	+		+								+			+		+

ПРН 11	ПРН 10	ПРН 9	ПРН 8	ПРН 7	ПРН 6	ПРН 5	ПРН
							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
	+	+			+		ЗО 16
	+						ЗО 17
	+			+	+		ЗО 18
+	+				+	+	ЗО 19
	+	+	+	+	+		ЗО 20
+	+			+			ЗО 21
				+			ЗО 22
					+		ЗО 23
		+	+	+			ЗО 24
+	+	+	+	+	+	+	ЗО25
+	+	+	+	+	+	+	ЗО 26
	+				+	+	ПО 1
	+						ПО2
	+				+	+	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

ПРН 18	ПРН 17	ПРН 16	ПРН 15	ПРН 14	ПРН 13	ПРН 12	ПРН
							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
							ЗО 16
			+				ЗО 17
						+	ЗО 18
						+	ЗО 19
				+			ЗО 20
		+		+	+	+	ЗО 21
							ЗО 22
							ЗО 23
							ЗО 24
+	+	+	+	+	+	+	ЗО25
+	+	+	+	+	+	+	ЗО 26
			+				ПО 1
+							ПО2
							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

ПРН 25	ПРН 24	ПРН 23	ПРН 22	ПРН 21	ПРН 20	ПРН 19	ПРН
							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
							ЗО 16
							ЗО 17
+	+		+	+		+	ЗО 18
							ЗО 19
		+	+			+	ЗО 20
	+			+		+	ЗО 21
							ЗО 22
							ЗО 23
							ЗО 24
+	+	+	+	+	+	+	ЗО25
+	+	+	+	+	+	+	ЗО 26
							ПО 1
		+			+		ПО2
						+	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

ПРН 32	ПРН 31	ПРН 30	ПРН 29	ПРН 28	ПРН 27	ПРН 26	ПРН
							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
							ЗО 16
							ЗО 17
	+						ЗО 18
							ЗО 19
					+		ЗО 20
	+	+	+	+			ЗО 21
							ЗО 22
							ЗО 23
							ЗО 24
+	+	+	+	+	+	+	ЗО25
+	+	+	+	+	+	+	ЗО 26
							ПО 1
		+					ПО2
							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

ПРН 39	ПРН 38	ПРН 37	ПРН 36	ПРН 35	ПРН 34	ПРН 33	ПРН
							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
							ЗО 16
							ЗО 17
					+		ЗО 18
					+		ЗО 19
				+			ЗО 20
				+	+	+	ЗО 21
							ЗО 22
							ЗО 23
							ЗО 24
+	+	+	+	+	+	+	ЗО25
+	+	+	+	+	+	+	ЗО 26
							ПО 1
							ПО2
							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

ПРН 46	ПРН 45	ПРН 44	ПРН 43	ПРН 42	ПРН 41	ПРН 40	ПРН
							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
							ЗО 16
							ЗО 17
	+						ЗО 18
							ЗО 19
				+			ЗО 20
+		+					ЗО 21
							ЗО 22
							ЗО 23
							ЗО 24
+	+	+	+	+	+	+	ЗО25
+	+	+	+	+	+	+	ЗО 26
							ПО 1
							ПО2
							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

ПРН 53	ПРН 52	ПРН 51	ПРН 50	ПРН 49	ПРН 48	ПРН 47	ПРН
							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
							ЗО 16
							ЗО 17
							ЗО 18
							ЗО 19
+					+	+	ЗО 20
							ЗО 21
							ЗО 22
							ЗО 23
							ЗО 24
+	+	+	+	+	+	+	ЗО25
+	+	+	+	+	+	+	ЗО 26
+							ПО 1
+							ПО2
							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

ПРН 59	ПРН 58	ПРН 57	ПРН 56	ПРН 55	ПРН 54	ПРН
						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
	+			+		ЗО 16
				+		ЗО 17
	+					ЗО 18
	+					ЗО 19
						ЗО 20
	+					ЗО 21
						ЗО 22
						ЗО 23
						ЗО 24
+	+	+	+	+	+	ЗО25
+	+	+	+	+	+	ЗО 26
						ПО 1
				+		ПО2
				+		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