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 «20» 01 2020 р.)

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**
галузі знань	**12 Інформаційні технології**
кваліфікація	**бакалавр з кібербезпеки**

Зміни та доповнення погоджено НМКУ 125
(протокол № 3 від «8» 06 2020 р.)
Освітню програму зі змінами та доповненнями
введено в дію з 2020 /2021 навч. року
(наказ № 1/231 від «08» 07 2020 р.)

Київ -2020

ПРЕАМБУЛА

РОЗРОБЛЕНО проєктною групою:

Керівник проєктної групи:
Новіков Олексій Миколайович, директор Фізико-технічного інституту, професор, доктор технічних наук

Члени проєктної групи:

Грайворонський Микола Владленович, в.о. завідувача кафедри інформаційної безпеки, доцент, кандидат фізико-математичних наук

Барановський Олексій Миколайович, доцент кафедри інформаційної безпеки, доцент, кандидат технічних наук

Стьопочкіна Ірина Валеріївна, доцент кафедри інформаційної безпеки, кандидат технічних наук

За підготовку здобувачів вищої освіти за освітньою програмою відповідає кафедра інформаційної безпеки

ПОГОДЖЕНО:

Першу редакцію освітньої програми ухвалено Методичною радою КПІ ім. Ігоря Сікорського (протокол № 7 від 29.03.2018 р.)

Попередню редакцію затверджено Методичною радою КПІ ім. Ігоря Сікорського (протокол № 5 від 16.01.2020 р.)

Зміни та доповнення до освітньої програми погоджені Науково-методичною комісією університету зі спеціальності 125 Кібербезпека (протокол № 3 від «8» 06 2020 р.)

Голова НМКУ зі спеціальності 125 Кібербезпека
Олексій НОВІКОВ

ВРАХОВАНО:
фахову експертизу стейкхолдерів:

Представники роботодавців:

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

Жора Віктор Володимирович,
керівник ТОВ «Інфосейф»

Кудін Антон Михайлович,
заступник директора департаменту, начальник управління
безпеки інформації Департаменту безпеки НБУ
д.т.н., професор

Представники студентських організацій:

Ракович Дар'я, в.о. голови Профбюро ФТІ,
студентка 3 курсу бакалаврату за
спеціальністю 125 Кібербезпека

Михалко Дмитро, голова Студради ФТІ, студент
3 курсу бакалаврату за спеціальністю 125 Кібербезпека

Дубас Антон, студент 3 курсу бакалаврату
за спеціальністю 125 Кібербезпека

Враховано такі пропозиції стейкхолдерів:

- збільшити різноманітність професійно-орієнтованих дисциплін (студенти) при збереженні насиченої фундаментальної складової (роботодавці).
- доповнити план сучасними актуальними дисциплінами за фахом, зокрема "Управління інцидентами комп'ютерної безпеки ", "Зворотна розробка та аналіз шкідливого програмного забезпечення", "Захист програмного забезпечення" (стейкхолдери-роботодавці, студенти).

В ОП було внесено також наступні зміни:

- зробити обовя'зковими дисципліни, які передбачають надбання компетентностей, передбачених Стандартом Вищої освіти за 125 Кібербезпека (серед них Комплексні системи захисту інформації: проектування, впровадження, супровід).
- частину природничих та фундаментальних дисциплін перенести до блоків вибіркових дисиплін, модернізувавши їх наповнення згідно профілю 125 Кібербезпека. запропонувати список вибіркових дисциплін до Факультетського/кафедрального каталогів.

Освітню програму обговорено після надходження всіх побажань та пропозицій від здобувачів вищої освіти і випускників освітньої програми та схвалено на розширеному засіданні кафедри інформаційної безпеки (протокол № 11/2020 від 20.05.2020 р.).

.

ЗМІСТ

1. ПРОФІЛЬ ОСВІТНЬОЇПРОГРАМИ
зі спеціальності 125 Кібербезпека
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”,Фізико-технічний інститут
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь – бакалавр Кваліфікація – бакалавр з кібербезпеки
Рівень з НРК	НРК України – 7 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 УД на спеціальність № 11002216 (078011) від 06.04.2018, дійсний до01.07.2028
Передумови	Наявність повної загальної середньої освіти
Мова(и) викладання	Українська/англійська
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	
Забезпечення поглибленої фундаментальної підготовки фахівців, здатних використовувати технології інформаційної та/або кібербезпеки; а також новітні технології та математичні методи, в галузі захисту інформації і кібернетичної безпеки; гармонійність, багатовимірність освіти; інтеграція інноваційної та практичної діяльності і навчального процесу; орієнтація на міжнародні вимоги в сфері кібербезпеки; орієнтація на вимоги ринку праці та дуальнуосвіту. 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 (галузь знань, спеціальність)	Галузь знань – 12 Інформаційні технології Спеціальність – 125 Кібербезпека Освітня програма– **Системи, технології та математичні методи кібербезпеки** 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 криптографічногозахисту 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 – 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 та спеціалізації	1) Базовий фокус ОП – системи та процеси кіберпростору, засоби та заходи захисту. 2) Ключові слова: кібернетична безпека, інформаційно-телекомунікаційні системи, програмні та апаратні засоби захисту інформації, системи і технології кібербезпеки, математичні методи 3) кібербезпеки, аудит кіберінцидентів, технічний аудит
Особливості програми	4) ґрунтовна фундаментальна підготовка у поєднанні із сучасною професійною підготовкою, яка дозволяє проводити інноваційну діяльність і працювати з наукоємними технологіямикібербезпеки; 5) проходження переддипломної практики на базі підприємств- партнерів та участь студентів у виконанні спільних науково- дослідних проектів на замовлення установ та провідних ІТ- компаній України зафахом; 6) підготовка до дуальної освіти вмагістратурі.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Відповідно до Державного класифікатору професій ДК 003:2010 випускники можуть працювати на посадах, що відповідають класифікаційним угрупованням: 3439 “Фахівець із захисту інформації в інформаційних і комунікаційних системах”, “Фахівець із організації інформаційної безпеки” 3121 Фахівець з інформаційних технологій. Випускники ОП можуть працювати фахівцями із захисту інформації та кібербезпеки в складі відповідних департаментів організацій, підприємств та банків, розробниками та тестувальниками застосунків, що потребують виконання особливих вимог щодо інформаційної та кібернетичної безпеки; співробітниками служб захисту інформації; адміністраторами інформаційної та кібернетичної безпеки, проектувальниками систем захисту в кіберпросторі; розробниками програмних та програмно-апаратних засобів захисту інформації в кіберпросторі, консультантами-інструкторами з кібербезпеки, спеціалістами в галузі кібербезпеки в складі правоохоронних органів, спеціалістами з забезпечення кібербезпеки в кіберпросторі (зокрема, об’єктах критичної інфраструктури)
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 дипломноїроботи (бакалаврської дипломної роботи)
Оцінювання	Оцінювання знань студентів здійснюється у відповідності до Положення про рейтингову систему оцінювання результатів навчання студентів КПІ ім. Ігоря Сікорського за усіма видами аудиторної та позааудиторної роботи (вхідний, поточний, рубіжний, підсумковий контроль); усних та письмових екзаменів, заліків

6 – Програмні компетентності	
Інтегральна компетентність	Здатність вирішувати складні спеціалізовані задачі та практичні проблеми в області кібернетичної безпеки, що передбачає застосування певних теорій, моделей та методів і характеризуєтьсякомплексністю та невизначеністю умов.
Загальні компетентності (ЗК)	
ЗК1	Здатність застосовувати знання у практичних ситуаціях.
ЗК2	Знання та розуміння предметної області та розуміння професії.
ЗК3	Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
ЗК4	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
ЗК5	Здатність до пошуку, оброблення та аналізу інформації.
ЗК6	Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенстваправа, прав і свобод людини і громадянина в Україні;
ЗК7	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 способужиття.

Фахові компетентності (ФК)	
ФК 1	Здатність застосовувати законодавчу та нормативно- правову базу, атакож державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі.
ФК 2	Здатність до використання інформаційно- комунікаційних технологій, сучасних методів і моделей інформаційної безпеки.
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 інформаційноїбезпеки.
ФК 5	Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системахз метою реалізації встановленої політики інформаційної безпеки.
ФК 6	Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класівта 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 політикиінформаційної 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 їхнюефективність
ПРН 3	Використовувати результати самостійного пошуку, аналізу тасинтезу інформації з різних джерел для ефективного рішенняспеціалізованих задач
ПРН 4	Аналізувати, аргументувати приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю танеповною 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 поняттяу навчанні та професійній діяльності
ПРН 7	Діяти на основі законодавчої та нормативно-правової бази Українита вимог відповідних стандартів, у тому числі міжнародних вгалузіінформаційної 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 тареагування на інциденти інформаційної та/або кібербезпеки
ПРН 10	Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем
ПРН 11	Виконувати аналіз зв'язків між інформаційними процесами навіддалених 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 результативностіякості прийнятих рішень
ПРН 15	Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій
ПРН 16	Реалізовувати комплексні системи захисту інформації вавтоматизованих 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 інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; та моделей захисту електронних даних
ПРН 18	Використовувати програмні та програмно-апаратні комплексизахисту 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 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 отриманнюнесанкціонованого доступудоінформаційнихресурсівіпроцесіввінформаційнихта 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)системнаосновіеталонноїмоделівзаємодії 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 встановленоїполітикиінформаційної та\або кібербезпеки;
ПРН 29	Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційних та інформаційно- телекомунікаційних системах, ефективності використаннякомплексів 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 цілейі завдань організації
ПРН 35	Вирішувати задачі забезпечення та супроводукомплексних 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 режимусекретності 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 ріні 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

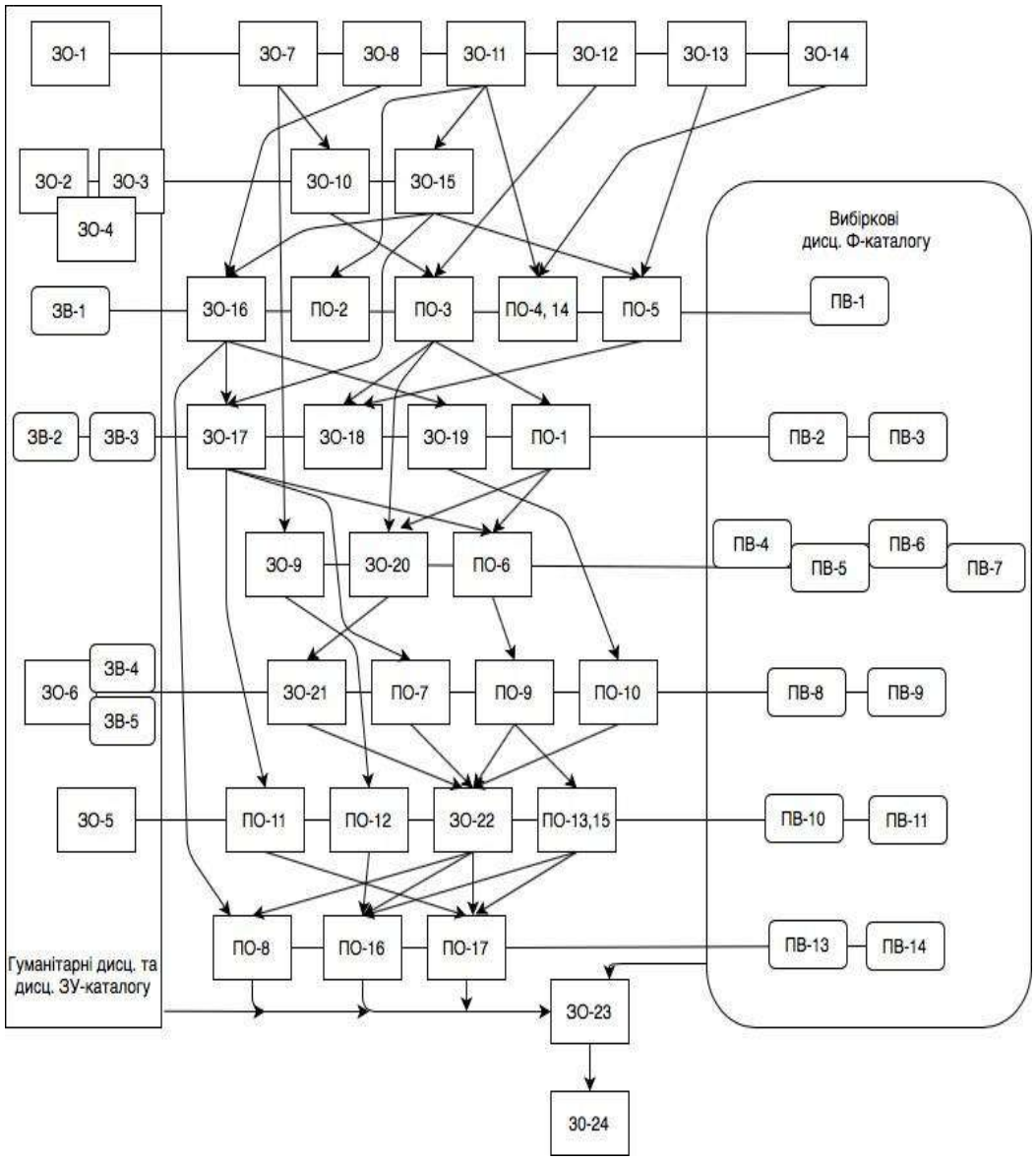
8 – Ресурсне забезпечення реалізації програми	
Кадрове Забезпечення	Відповідно до кадрових вимог щодо забезпечення провадження освітньої діяльності для відповідного рівня ВО (додаток 3 до Ліцензійних умов, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187, за текстом постанови КабінетуМіністрів України від 10.05.2018 р. № 347, п. 28-32)
Матеріально-технічне забезпечення	Відповідно до технологічних вимог щодо матеріально-технічного забезпечення освітньої діяльності відповідного рівня ВО (додаток 4 до Ліцензійних умов, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187, за текстом постанови КабінетуМіністрів України від 10.05.2018 р. № 347, п. 34-35), 3 комп'ютерних класи, полігон з Кібербезпеки Матеріально-технічна базаSamsung R&D Institute Ukraine
Інформаційне та навчально-методичне забезпечення	Відповідно до вимог щодо навчально-методичного та інформаційного забезпечення освітньої діяльності відповідного рівня ВО (додаток 5 до Ліцензійних умов, затверджених Постановою Кабінету МіністрівУкраїни від 30.12.2015 р. № 1187, за текстом постанови Кабінету Міністрів України від 10.05.2018 р. № 347, п.36). Ресурси науково-технічної бібліотеки КПІ імені Ігоря Сікорського, бібліотеки 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	Для іноземних громадян навчання здійснюється українською або англійською мовами

2. ПЕРЕЛІК ОБОВ'ЯЗКОВИХ КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇПРОГРАМИ

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового 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	Фізичне виховання	5	Залік
ЗО 4	Іноземна мова	6	Залік
ЗО 5	Економіка і організація виробництва	4	Залік
ЗО 6	БЖД та цивільний захист	2	Залік
ЗО 7	Математичний аналіз	12	Екзамен
ЗО 8	Фізика	10,5	Екзамен
ЗО 9	Теорія ймовірностей та математична статистика	5,5	Екзамен
ЗО 10	Дискретна математика	4,5	Екзамен
ЗО 11	Програмування	8	Екзамен
ЗО 12	Алгебра та геометрія	7,5	Екзамен
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	Теорія інформації та кодування	4	Екзамен
ЗО 22	Комплексні системи захисту інформації: проектування, впровадження, супровід	4	Залік
ЗО 23	Переддипломна практика	6	Залік
ЗО 24	Дипломне проектування	6	Захист
1. 2 Цикл професійної підготовки			
ПО 1	Алгоритми та структури даних	3,5	Залік
ПО 2	Web-програмування	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	3	Залік

ПО 6	Зворотна розробка та аналіз шкідливого програмного забезпечення	4	Екзамен
ПО 7	Безпека комп'ютерних мереж	5	Екзамен
ПО 8	Системи технічного захисту інформації	4	Екзамен
ПО 9	Захист програмного забезпечення	4	Екзамен
ПО 10	Управління інцидентами комп’ютерної безпеки	3,5	Залік
ПО 11	Безпека операційних систем	4	Екзамен
ПО 12	Теорія ризиків	3,5	Екзамен
ПО 13	Технічний аудит	4	Екзамен
ПО 14	Курсова робота з баз даних та інформаційних систем	1	Залік
ПО 15	Курсова робота з технічного аудиту	1	Залік
ПО 16	Аналіз та моніторинг кібернетичної безпеки	3	Екзамен
ПО 17	Управління інформаційною безпекою	3,5	Залік
2. Вибіркові освітні компоненти			
2.1. Цикл загальної підготовки (Вибіркові освітні компоненти із загальноунівер- ситетського Каталогу)			
ЗВ 1	Освітній компонент 1 з ЗУ-Каталогу	2	Залік
ЗВ 2	Освітній компонент 2 з ЗУ-Каталогу	2	Залік
ЗВ 3	Освітній компонент 3 з ЗУ-Каталогу	2	Залік
ЗВ 4	Освітній компонент 4 з ЗУ-Каталогу	2	Залік
ЗВ 5	Іноземна мова професійного спрямування	6	Екзамен, Залік
2.2. Цикл професійної підготовки (Вибіркові освітні компоненти з факультетського/кафедральногоКаталогів)			
ПВ 1	Освітній компонент 1 з Ф-Каталогу	4	Залік
ПВ 2	Освітній компонент 2 з Ф-Каталогу	4	Залік
ПВ 3	Освітній компонент 3 з Ф-Каталогу	3	Залік
ПВ 4	Освітній компонент 4 з Ф-Каталогу	3	Залік
ПВ 5	Освітній компонент 5 з Ф-Каталогу	3	Залік
ПВ 6	Освітній компонент 6 з Ф-Каталогу	3	Залік
ПВ 7	Освітній компонент 7 з Ф-Каталогу	4	Залік
ПВ 8	Освітній компонент 8 з Ф-Каталогу	4	Залік
ПВ 9	Освітній компонент 9 з Ф-Каталогу	4	Залік
ПВ 10	Освітній компонент 10 з Ф-Каталогу	4	Залік
ПВ 11	Освітній компонент 11 з Ф-Каталогу	4	Залік
ПВ 12	Освітній компонент 12 з Ф-Каталогу	3	Залік
ПВ 13	Освітній компонент 13 з Ф-Каталогу	3	Залік
ПВ 14	Освітній компонент 14 з 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 ОСВІТНЬОЇПРОГРАМИ



4. ФОРМА ВИПУСКНОЇ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇОСВІТИ

Випускна атестація здобувачів вищої освіти здійснюється у формі публічного захисту кваліфікаційного проекту/роботи та завершується видачею документу встановленого зразка про присвоєння кваліфікації: «бакалавр з кібербезпеки» за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки».

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

	ЗК1	**ЗК2**	**ЗК3**	**ЗК4**	**ЗК5**	**ЗК6**	**ЗК7**	**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		+		+					+			+							+		+		+	

	ЗК1	**ЗК2**	**ЗК3**	**ЗК4**	**ЗК5**	**ЗК6**	**ЗК7**	**ФК1**	**ФК2**	**ФК3**	**ФК4**	**ФК5**	**ФК6**	**ФК7**	**ФК8**	**ФК9**	**ФК10**	**ФК11**	**ФК12**	**ФК13**	**ФК14**	**ФК15**	**ФК16**	**ФК17**
ЗО 19	+	+		+					+	+									+			+	
ЗО 20	+	+		+				+									+		+		+			
ЗО 21		+		+													+			+				
ЗО 22		+		+				+		+		+		+							+		+	
ЗО 23	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ЗО 24	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ПО1	+	+			+				+					+					+	+				
ПО2	+	+		+	+			+	+	+						+		+		+				
ПО3	+	+		+					+								+		+	+				
ПО4	+	+		+	+			+	+	+		+								+			+	
ПО5	+	+		+					+	+		+	+								+		+	
ПО6	+	+								+									+		+			+
ПО7	+	+							+	+		+	+					+			+			
ПО8	+	+						+		+		+		+			+				+			
ПО9	+			+				+	+	+		+							+	+			+	+
ПО10	+	+						+			+				+	+		+	+		+	+		
ПО11	+							+	+	+		+						+	+		+			
ПО12		+		+				+							+	+			+	+				
ПО13	+			+				+							+	+		+	+		+	+		
ПО14	+	+		+	+			+	+	+		+								+			+	
ПО15	+			+	+			+	+						+	+		+	+		+	+		

	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ФК1	ФК2	ФК3	ФК4	ФК5	ФК6	ФК7	ФК8	ФК9	ФК10	ФК11	ФК12	ФК13	ФК14	ФК15	ФК16	ФК17
ПО16	+	+		+	+	+		+	+	+	+		+	+	+	+	+	+	+		+	+		
ПО17	+	+		+		+		+			+					+		+			+	+		

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	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
ПРН1	+	+		+					+	+				+									+	+	+															
ПРН2		+			+		+		+	+	+	+	+	+		+			+	+	+	+	+	+	+	+	+	+		+							+		+	
ПРН3		+					+		+	+	+	+	+	+	+	+	+			+			+	+	+													+			
ПРН4		+			+		+		+	+		+	+	+	+	+		+	+	+			+	+	+		+								+			+			+

ПРН11	ПРН10	ПРН9	ПРН8	ПРН7	ПРН6	ПРН5	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
	+				+	+	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

ПРН18	ПРН17	ПРН16	ПРН15	ПРН14	ПРН13	ПРН12	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
			+				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

ПРН25	ПРН24	ПРН23	ПРН22	ПРН21	ПРН20	ПРН19	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
							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

ПРН32	ПРН31	ПРН30	ПРН29	ПРН28	ПРН27	ПРН26	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
							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

ПРН39	ПРН38	ПРН37	ПРН36	ПРН35	ПРН34	ПРН33	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
							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

ПРН46	ПРН45	ПРН44	ПРН43	ПРН42	ПРН41	ПРН40	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
							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

ПРН53	ПРН52	ПРН51	ПРН50	ПРН49	ПРН48	ПРН47	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
+							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

ПРН 59	ПРН 58	ПРН 57	ПРН 56	ПРН 55	ПРН54	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
						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