Ф-22.05-04.01/125.00.01/Б-2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«Кібербезпека»

Першого (бакалаврського) рівня вищої освіти
галузі знань 12 «Інформаційні технології»
спеціальності 125 «Кібербезпека та захист інформації»
Кваліфікація: бакалавр з кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО
Вченою радою
Державного університету
«Житомирська політехніка»
Голова Вченої ради
_____ Віктор ЄВДОКИМОВ
(протокол від 28 травня 2024 р.
№ 6)

Освітня програма вводиться в
дію з 01 вересня 2024 р.
Ректор
_____ Віктор ЄВДОКИМОВ
(наказ від 28 травня 2024 р.
№ 296/од)

Житомир – 2024

ПЕРЕДМОВА

Освітньо-професійну програму «Кібербезпека» розроблено відповідно до Стандарту вищої освіти України за спеціальністю 125 «Кібербезпека та захист інформації» для першого (бакалаврського) рівня вищої освіти (затверджено і введено в дію наказом Міністерства освіти і науки України № 1074 від 10 жовтня 2018 р.) робочою групою у складі:

1. ЄФІМЕНКО Андрій., к.т.н., доцент, завідувач кафедри комп'ютерної інженерії та кібербезпеки – гарант освітньої програми.
2. ЛОБАНЧИКОВА Надія, к.т.н., доцент, доцент кафедри інженерії програмного забезпечення.
3. ВОРОТНІКОВ Володимир, д.т.н., доцент, професор кафедри комп'ютерної інженерії та кібербезпеки.
4. ШЕЛУХА Олексій, к.т.н., доцент кафедри комп'ютерної інженерії та кібербезпеки.
5. СЕМЕНЕЦЬ Сергій, д.пед.н., професор, професор кафедри комп'ютерної інженерії та кібербезпеки.
6. БАЙЛЮК Єлизавета, старший викладач кафедри комп'ютерної інженерії та кібербезпеки.
7. ПОКОТИЛО Олександра, старший викладач кафедри комп'ютерної інженерії та кібербезпеки.
8. КРУЧИНСЬКИЙ Ярослав, представник роботодавця, начальник відділу сервісного обслуговування технічної служби, ТОВ «Фрінет».
9. ХАРИТОНЮК Юрій, здобувач вищої освіти, 3 курс, група КБ-21-2
10. СІНІЦИНА Олександра, здобувачка вищої освіти, 4 курс, група КБ-20-1.
11. ШЕВЧИК Дарина, випускниця з ОПП 2023 р.; здобувачка вищої освіти, 1 курс, група КБм-23-1.
12. ГОНЧАРОВ Михайло, випускник з ОПП 2022 р.; Аналітик з інцидентів. ТОВ «МЕТІНВЕСТ ДІДЖИТАЛ».
13. ЛЕЩЕНКО Богдан, випускник з ОПП 2021 р.; адміністратор системи, ТОВ "Сана Комерс Україна".

1. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Державний університет «Житомирська політехніка», факультет інформаційно-комп'ютерних технологій
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Перший (бакалаврський) рівень вищої освіти. Кваліфікація – «бакалавр з кібербезпеки та захисту інформації».
Офіційна назва освітньої програми	Кібербезпека
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців
Наявність акредитації	Сертифікат про акредитацію освітньої програми 5694, дійсний до 01.07.2027
Цикл /рівень	НРК України – 6 рівень, FQ-EHEA – перший цикл, EQF-LLL – 6 рівень
Передумови	Повна загальна середня освіта або наявність освітньо-кваліфікаційного рівня «Молодший спеціаліст», або освітнього ступеня "Молодший бакалавр", або освітньо-професійного ступеня "Фаховий молодший бакалавр"
Мова(и) викладання	Українська
Термін дії освітньої програми	Постійно
Інтернет-адреса постійного розміщення опису освітньої програми	https://ztu.edu.ua
2 – Мета освітньої програми	
Професійна підготовка фахівців з кібербезпеки, набуття ними компетентностей в застосуванні принципів, методів та засобів забезпечення кібербезпеки.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація)	***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 та спеціалізації	Вища освіта в галузі інформаційних технологій. Програма фокусується на питаннях забезпечення кібербезпеки сучасних комп'ютерних систем та мереж. Ключові слова: кібербезпека, комп'ютерна система, комп'ютерна мережа, інформаційна система, інформаційно-телекомунікаційна система, операційна система, адміністрування систем, прикладне та системне програмування, вразливість, атака, ризик, компрометація, протидія, захист інформації, тестування на проникнення, моніторинг, розслідування інциденту, міжмережне екранування, система виявлення та попередження вторгнень, кібероперації, спеціальні системи забезпечення кібербезпеки.

Особливості програми	Тісна співпраця з державними та приватними організаціями з метою отримання практичних навичок безпечної експлуатації, адміністрування, забезпечення захисту комп'ютерних систем та мереж, навичок розробки захищеного прикладного та системного програмного забезпечення, проходження практичної підготовки з розробки нових і вдосконалення існуючих комп'ютерних та інформаційних систем з подальшим впровадженням науково-практичних розробок у діяльність організацій та установ.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Працевлаштування в організаціях та підприємствах будь-якої форми власності на посадах: І. Згідно ДК 003:2010: 1. Адміністратор безпеки мереж і систем 2. Аналітик з безпеки інформаційно-телекомунікаційних систем 3. Аналітик з оцінки вразливостей 4. Аналітик загроз безпеки 5. Аналітик систем захисту інформації та оцінки вразливостей 6. Аудитор інформаційних технологій (з кібербезпеки) 7. Конструктор систем кібербезпеки 8. Розробник систем захисту інформації 9. Уповноважений з авторизації безпеки 10. Фахівець з криптографічного захисту інформації 11. Фахівець з оцінки заходів захисту інформації (кібербезпеки), 12. Фахівець з питань безпеки (інформаційно-комунікаційні технології) 13. Фахівець з підтримки інфраструктури кіберзахисту 14. Фахівець з планування політики та стратегії кібербезпеки 15. Фахівець з реагування на інциденти кібербезпеки 16. Фахівець з тестування систем захисту інформації 17. Фахівець з технічного захисту інформації 18. Фахівець із кібердосліджень та розробок систем безпеки 19. Фахівець сфери захисту інформації

	II. Згідно ECSF (European Cybersecurity Skills Framework): 1. Chief Information Security Officer (CISO) 2. Cyber Incident Responder 3. Cyber Legal, Policy and Compliance Officer 4. Cyber Threat Intelligence Specialist 5. Cybersecurity Educator 6. Cybersecurity Implementer 7. Cybersecurity Auditor 8. Cybersecurity Researcher 9. Cybersecurity Risk Manager 10. Digital Forensics Investigator
Подальше навчання	Можливість навчання за програмою другого (магістерського) рівня
5 – Викладання та оцінювання	
Викладання та навчання	Викладання здійснюється на засадах студентоцентрованого навчання, самонавчання, проблемно-орієнтованого навчання тощо
Оцінювання	Поточне опитування, тестовий контроль, презентація індивідуальних завдань, звіти команд, звіти з практики. Підсумковий контроль – екзамени та заліки з урахуванням накопичених балів поточного контролю. Атестація – підготовка та публічний захист кваліфікаційної роботи, єдиний державний кваліфікаційний іспит.
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 (ЗК)	***Загальні компетентності, визначені стандартом вищої освіти:*** 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 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. ***Загальні компетентності, визначені за освітньою програмою:*** КЗ 8. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.
Спеціальні (фахові, предметні) компетентності (СК)	***Спеціальні компетентності, визначені стандартом вищої освіти:*** 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-телекомунікаційних (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-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (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 і 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-телекомунікаційних (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.
7 - Результати навчання	
Результати навчання, визначені стандартом вищої освіти: РН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. РН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. РН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. РН 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. РН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. РН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. РН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. РН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.	

РН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.
РН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.
РН 11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.
РН 12. Розробляти моделі загроз та порушника.
РН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
РН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
РН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
РН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
РН 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.
РН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
РН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
РН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
РН 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.
РН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
РН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
РН 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).
РН 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.
РН 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.
РН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

РН 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.
РН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
РН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
РН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
РН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
РН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.
РН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
РН 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.
РН 36. Виявляти небезпечні сигнали технічних засобів.
РН 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.
РН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
РН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
РН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.
РН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
РН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
РН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.
РН 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.
РН 45. Застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
РН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.

РН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. РН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах. РН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах. РН 50. Забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних). РН 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах. РН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. РН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз. РН 54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ***Результати навчання, визначені за освітньою програмою:*** РН 55. Вміти ідентифікувати та аналізувати проблеми, пов'язані з корупцією та недоброчесністю, формувати та оцінювати шляхи їх вирішення як у професійній діяльності, так і у суспільному житті на рівні, необхідному для формування нетерпимості до будь-яких проявів недоброчесності задля утвердження цінностей доброчесного суспільства.

8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	У реалізації даної освітньої програми задіяно 5 докторів наук, професорів або доцентів/с.н.с., 10 кандидатів наук, доцентів, 2 кандидати наук/PhD, кожен з яких має виконання не менше 4 пунктів п. 38 Ліцензійних умов провадження освітньої діяльності. Тобто, кадрове забезпечення освітньої програми відповідає ліцензійним вимогам щодо надання освітніх послуг у сфері вищої світи і є достатнім для забезпечення якості освітнього процесу.
Матеріально-технічне забезпечення	Матеріально-технічне забезпечення відповідає ліцензійним вимогам щодо надання освітніх послуг у сфері вищої світи і є достатнім для забезпечення якості освітнього процесу.
Інформаційне та навчально-методичне забезпечення	Інформаційне та навчально-методичне забезпечення освітньої програми з підготовки фахівців зі спеціальності 125 «Кібербезпека та захист інформації» відповідає ліцензійним вимогам, має актуальний змістовий контент, базується на сучасних інформаційно-комунікаційних технологіях.

	В університеті функціонують Мережна академія Cisco, Центр підтримки академій Cisco, Центр підготовки інструкторів Cisco, ресурси яких доступні для студентів (за умови реєстрації). Також в університеті реалізуються партнерські академічні програми від компаній IBM, Microsoft, Fortinet, AWS, Oracle та ін. Здобувачам освіти забезпечується доступ до освітніх платформ Udemy, Coursera тощо.
9 – Академічна мобільність	
Національна кредитна мобільність	Реалізується в межах спільної діяльності з Національним технічним університетом «КПІ імені Ігоря Сікорського», Хмельницьким національним університетом, Запорізьким національним університетом, Житомирським військовим інститутом імені С.П. Корольова, Житомирським державним університетом імені Івана Франка, Національним університетом водного господарства та природокористування, Харківським національним університетом радіоелектроніки, Харківським національним університетом ім. В. Каразіна, Черкаським державним технологічним університетом, Державним університетом інформаційно-комунікаційних технологій, Національним університетом «Одеська юридична академія» згідно укладених договорів про співпрацю.
Міжнародна кредитна мобільність	На основі двосторонніх договорів між Державним університетом «Житомирська політехніка» та зарубіжними закладами вищої освіти.
Навчання іноземних здобувачів вищої освіти	На навчання приймаються іноземні громадяни на умовах контракту, які мають документ про повну загальну середню освіту.

2. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1. Перелік компонент освітньо-професійної програми

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проєкти/роботи, практики кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
Обов'язкові компоненти ОП			
ОК 01	Іноземна мова	18	Заліки, екзамен
ОК 02	Українська мова, професійне та академічне письмо	3	Залік
ОК 03	Фізичне виховання	3	Залік
ОК 04	Лінійна алгебра та аналітична геометрія	3	Екзамен
ОК 05	Фізика	4	Екзамен
ОК 06	Математичний аналіз	8	Залік, екзамен
ОК 07	Антикорупція та доброчесність	3	Залік
ОК 08	Розвиток комунікаційних навичок та групова динаміка	3	Залік
ОК 09	Теорія ймовірностей і математична статистика	4	Екзамен
ОК 10	Комп'ютерна дискретна математика	4	Екзамен
ОК 11	Екологія, безпека життєдіяльності та охорона праці	3	Залік
ОК 12	Українські історико-культурні та політико-соціальні студії	3	Залік
ОК 13	Технології та інструменти електронної документації	3	Залік
ОК 14	Архітектура комп'ютера	4	Екзамен
ОК 15	Програмування	9	Залік, екзамен, курсова робота
ОК 16	Теорія кіл та сигналів	5	Екзамен
ОК 17	Web-технології	3	Залік
ОК 18	Комп'ютерна електроніка та схемотехніка	4	Залік, екзамен
ОК 19	Операційні системи	8	Залік, екзамен
ОК 20	Комп'ютерні мережі	9	Залік, екзамен, курсовий проєкт
ОК 21	Основи кібербезпеки	3	Екзамен
ОК 22	Стандарти та нормативно-правове забезпечення кібербезпеки	3	Екзамен
ОК 23	Прикладна криптологія	5	Залік, екзамен
ОК 24	Бази даних: побудова, адміністрування, захист	6	Залік, екзамен
ОК 25	Мережна безпека	9	Залік, екзамен, курсовий проєкт
ОК 26	Теорія ризиків та її застосування в кібербезпеці	3	Екзамен
ОК 27	Системи технічного захисту інформації	4	Екзамен

ОК 28	Кібероперації	9	Залік, екзамен, курсовий проєкт
ОК 29	Теорія кібербезпеки	3	Залік
ОК 30	Управління кібербезпекою	3	Залік
ОК 31	Комплексні системи захисту інформації	4	Залік
ОК 32	Технологічна практика 1	3	Диф. залік
ОК 33	Технологічна практика 2	3	Диф. залік
ОК 34	Виробнича практика	6	Диф. залік
ОК 35	Переддипломна практика	6	Диф. залік
ОК 36	Кваліфікаційна робота	6	Кваліфікаційна атестація
	Кваліфікаційний іспит	0	ЄДКІ
Загальний обсяг обов'язкових компонент:		**180**	
Вибіркові компоненти ОП			
Вибірковий блок 1 *(вибіркові освітні компоненти університету, перелік освітніх компонент блоку затверджуються наказом ректора щорічно, студенти обирають 3 навчальні дисципліни загальним обсягом 12 кредитів)*			
ВК 1.01	Дисципліна вільного вибору № 01	4	Залік
ВК 1.02	Дисципліна вільного вибору № 02	4	Залік
ВК 1.03	Дисципліна вільного вибору № 03	4	Залік
Вибірковий блок 2 *(обираються навчальні дисципліни загальним обсягом 48 кредитів)*			
ВК 2.01	Дисципліна професійної підготовки № 01	4	Залік
ВК 2.02	Дисципліна професійної підготовки № 02	4	Залік
ВК 2.03	Дисципліна професійної підготовки № 03	4	Залік
ВК 2.04	Дисципліна професійної підготовки № 04	4	Залік
ВК 2.05	Дисципліна професійної підготовки № 05	4	Залік
ВК 2.06	Дисципліна професійної підготовки № 06	4	Залік
ВК 2.07	Дисципліна професійної підготовки № 07	4	Залік
ВК 2.08	Дисципліна професійної підготовки № 08	4	Залік
ВК 2.09	Дисципліна професійної підготовки № 09	4	Залік
ВК 2.10	Дисципліна професійної підготовки № 10	4	Залік
ВК 2.11	Дисципліна професійної підготовки № 11	4	Залік
ВК 2.12	Дисципліна професійної підготовки № 12	4	Залік
Загальний обсяг вибіркових компонент:		**60**	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**240**	

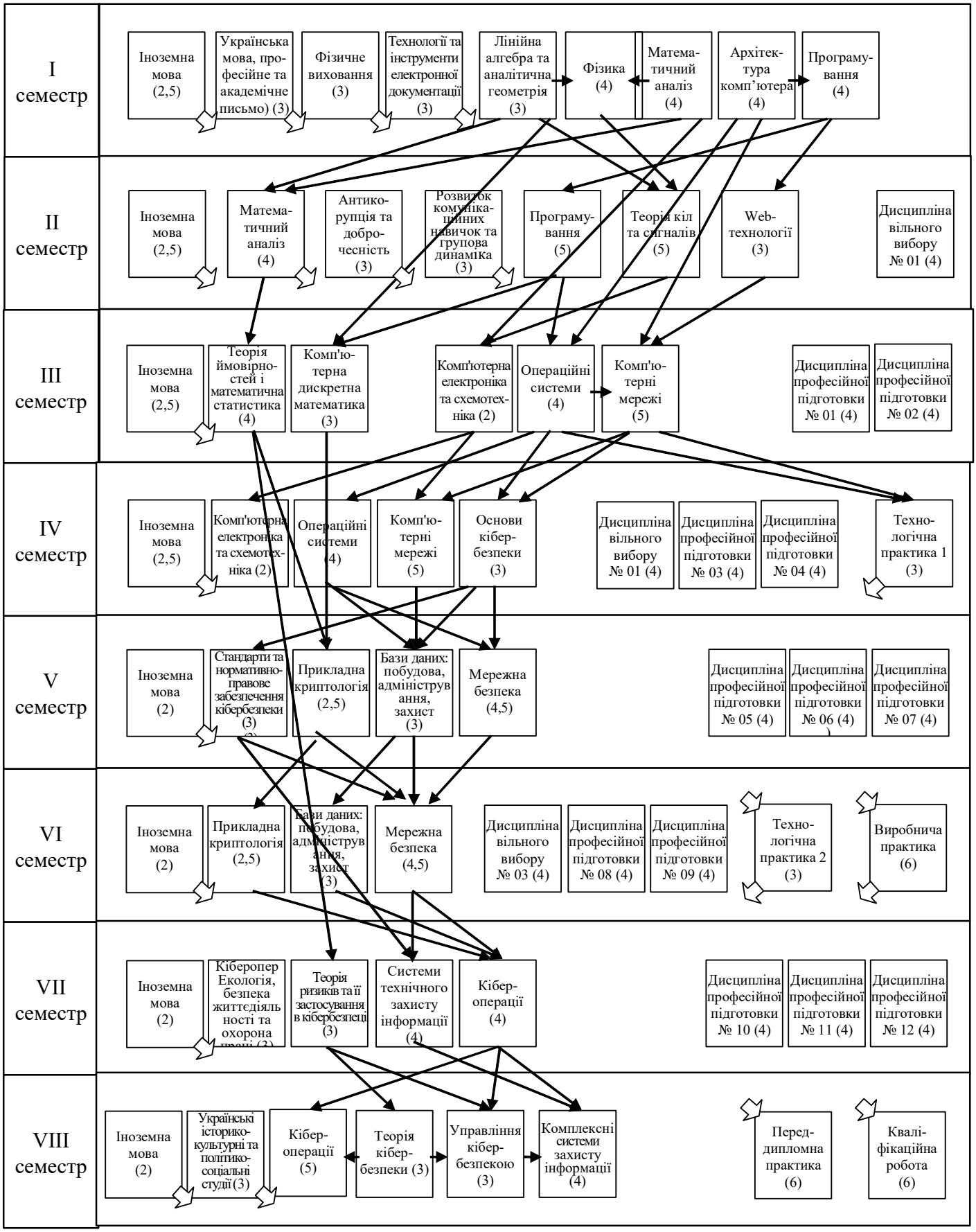
2.2. Структурно-логічна схема освітньо-професійної програми

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проєкти/ роботи, практики кваліфікаційна робота)	Кількість кредитів	Загальний обсяг год.	Форма підсумкового контролю
1	2	3	4	
І курс, І семестр				
ОК 01	Іноземна мова	2,5	75	Залік
ОК 02	Українська мова, професійне та академічне письмо	3	90	Залік
ОК 03	Фізичне виховання	3	90	Залік
ОК 04	Лінійна алгебра та аналітична геометрія	3	90	Екзамен
ОК 05	Фізика	4	120	Екзамен
ОК 06	Математичний аналіз	4	120	Залік
ОК 13	Технології та інструменти електронної документації	3	90	Залік
ОК 14	Архітектура комп'ютера	4	120	Екзамен
ОК 15	Програмування	4	120	Залік
	Разом	**30,5**	**915**	
І курс, ІІ семестр				
ОК 01	Іноземна мова	2,5	75	Залік
ОК 06	Математичний аналіз	4	120	Екзамен
ОК 07	Антикорупція та доброчесність	3	90	Залік
ОК 08	Розвиток комунікаційних навичок та групова динаміка	3	90	Залік
ОК 15	Програмування	5	150	Екзамен, курсова робота
ОК 16	Теорія кіл та сигналів	5	150	Екзамен
ОК 17	Web-технології	3	90	Залік
ВК 1.01	Дисципліна вільного вибору № 01	4	120	Залік
	Разом	**29,5**	**885**	
ІІ курс, І семестр				
ОК 01	Іноземна мова	2,5	75	Залік
ОК 09	Теорія ймовірностей і математична статистика	4	120	Екзамен
ОК 10	Комп'ютерна дискретна математика	4	120	Екзамен
ОК 18	Комп'ютерна електроніка та схемотехніка	2	60	Залік
ОК 19	Операційні системи	4	120	Залік
ОК 20	Комп'ютерні мережі	4	120	Залік
ВК 2.01	Дисципліна професійної підготовки № 01	4	120	Залік
ВК 2.02	Дисципліна професійної підготовки № 02	4	120	Залік
	Разом	**28,5**	**855**	

ІІ курс, ІІ семестр				
ОК 01	Іноземна мова	2,5	75	Залік
ОК 18	Комп'ютерна електроніка та схемотехніка	2	60	Екзамен
ОК 19	Операційні системи	4	120	Екзамен
ОК 20	Комп'ютерні мережі	5	150	Екзамен, курсовий проєкт
ОК 21	Основи кібербезпеки	3	90	Екзамен
ВК 1.02	Дисципліна вільного вибору № 02	4	120	Залік
ВК 2.03	Дисципліна професійної підготовки № 03	4	120	Залік
ВК 2.04	Дисципліна професійної підготовки № 04	4	120	Залік
ОК 32	Технологічна практика 1	3	90	Диф. залік
	Разом	**31,5**	**945**	
ІІІ курс, І семестр				
ОК 01	Іноземна мова	2	60	Залік
ОК 22	Стандарти та нормативно-правове забезпечення кібербезпеки	3	90	Екзамен
ОК 23	Прикладна криптологія	2,5	75	Екзамен
ОК 24	Бази даних: побудова, адміністрування, захист	3	90	Залік
ОК 25	Мережна безпека	4,5	135	Залік
ВК 2.05	Дисципліна професійної підготовки № 05	4	120	Залік
ВК 2.06	Дисципліна професійної підготовки № 06	4	120	Залік
ВК 2.07	Дисципліна професійної підготовки № 07	4	120	Залік
	Разом	**27**	**810**	
ІІІ курс, ІІ семестр				
ОК 01	Іноземна мова	2	60	Залік
ОК 23	Прикладна криптологія	2,5	75	Екзамен
ОК 24	Бази даних: побудова, адміністрування, захист	3	90	Екзамен
ОК 25	Мережна безпека	4,5	135	Екзамен, курсовий проєкт
ВК 1.03	Дисципліна вільного вибору № 03	4	120	Залік
ВК 2.08	Дисципліна професійної підготовки № 08	4	120	Залік
ВК 2.09	Дисципліна професійної підготовки № 09	4	120	Залік
ОК 33	Технологічна практика 2	3	90	Диф. залік
ОК 34	Виробнича практика	6	180	Диф. залік
	Разом	**33**	**990**	

IV курс, I семестр				
ОК 01	Іноземна мова	2	60	Залік
ОК 11	Екологія, безпека життєдіяльності та охорона праці	3	90	Залік
ОК 26	Теорія ризиків та її застосування в кібербезпеці	3	90	Екзамен
ОК 27	Системи технічного захисту інформації	4	120	Екзамен
ОК 28	Кібероперації	4	120	Залік
ВК 2.10	Дисципліна професійної підготовки № 10	4	120	Залік
ВК 2.11	Дисципліна професійної підготовки № 11	4	120	Залік
ВК 2.12	Дисципліна професійної підготовки № 12	4	120	Залік
	Разом	**28**	**840**	
IV курс, II семестр				
ОК 01	Іноземна мова	2	60	Екзамен
ОК 12	Українські історико-культурні та політико-соціальні студії	3	90	Залік
ОК 28	Кібероперації	5	150	Екзамен, курсовий проєкт
ОК 29	Теорія кібербезпеки	3	90	Залік
ОК 30	Управління кібербезпекою	3	90	Залік
ОК 31	Комплексні системи захисту інформації	4	120	Екзамен
ОК 35	Переддипломна практика	6	180	Диф. залік
ОК 36	Кваліфікаційна робота	6	180	Кваліфіка-ційна атестація
	Кваліфікаційний іспит	0	0	ЄДКІ
	Разом	**32**	**960**	
	Загальний обсяг:	**240**	**7200**	

СТРУКТУРНО-ЛОГІЧНА СХЕМА



Вихідна стрілка, яка розміщена в правому чи лівому нижньому кутку, показує, що ОК забезпечує решту ОК поточного і наступних семестрів;
Вхідна стрілка, яка розміщена у правому чи лівому верхньому кутку, показує, що ОК забезпечується ОК попередніх та поточного семестрів.

3. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Поточна атестація студентів здійснюється у формі екзаменів, заліків, диференційованих заліків, захисту курсових робіт та проектів.

Атестація випускників освітньо-професійної програми «Кібербезпека» за спеціальністю 125 «Кібербезпека та захист інформації» проводиться у формі публічного захисту кваліфікаційної роботи, здачі єдиного державного кваліфікаційного іспиту та завершується видачою документу встановленого зразка про присудження здобувачеві вищої освіти освітнього ступеня «бакалавр» з присвоєнням кваліфікації «бакалавр з кібербезпеки та захисту інформації».

У кваліфікаційній роботі не допускається порушень академічної доброчесності, зокрема, наявність академічного плагіату, фабрикації, фальсифікації, списування.

Атестація здійснюється відкрито і публічно.

Кваліфікаційна робота оприлюднюється у репозитарії закладу вищої освіти.

4. ВІДПОВІДНІСТЬ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

4.1. Матриця відповідності програмних компетентностей обов'язковим компонентам освітньо-професійної програми

	КЗ-1	КЗ-2	КЗ-3	КЗ-4	КЗ-5	КЗ-6	КЗ-7	КЗ-8	КФ-1	КФ-2	КФ-3	КФ-4	КФ-5	КФ-6	КФ-7	КФ-8	КФ-9	КФ-10	КФ-11	КФ-12
ОК 01			+																	
ОК 02			+					+												
ОК 03							+													
ОК 04	+				+															
ОК 05	+				+															
ОК 06	+				+															
ОК 07								+												
ОК 08	+		+	+	+		+	+												
ОК 09	+				+															
ОК 10	+				+															
ОК 11	+					+	+													
ОК 12						+	+													
ОК 13	+	+			+					+										
ОК 14		+									+									
ОК 15		+			+					+	+									
ОК 16					+													+		+
ОК 17		+			+					+	+									
ОК 18					+													+		+
ОК 19				+	+					+	+		+	+				+	+	
ОК 20				+	+					+	+	+	+	+				+	+	+
ОК 21		+		+					+	+			+					+		
ОК 22					+				+			+				+				
ОК 23				+	+					+	+		+					+		
ОК 24				+	+					+	+	+	+	+		+		+	+	
ОК 25		+		+	+					+	+	+	+	+				+	+	+
ОК 26					+					+		+				+				+
ОК 27	+	+		+	+					+	+	+		+				+		+
ОК 28		+		+	+					+	+	+	+	+	+	+	+		+	+
ОК 29		+	+	+	+			+		+			+			+	+			+
ОК 30		+		+					+			+				+	+		+	
ОК 31	+	+							+	+	+				+			+		+
ОК 32	+	+		+	+					+	+		+					+		
ОК 33	+	+		+	+					+	+		+					+		
ОК 34	+	+		+	+			+		+	+		+					+		
ОК 35	+	+		+	+			+	+	+	+	+	+	+	+	+	+	+	+	+
ОК 36	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

5. ЗАБЕЗПЕЧЕНІСТЬ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

5.1. Матриця забезпечення програмних результатів навчання відповідними обов'язковими компонентами освітньо-професійної програми

	РН-1	РН-2	РН-3	РН-4	РН-5	РН-6	РН-7	РН-8	РН-9	РН-10	РН-11	РН-12	РН-13	РН-14	РН-15	РН-16	РН-17	РН-18	РН-19	РН-20	РН-21	РН-22	РН-23	РН-24	РН-25	РН-26	РН-27
ОК 01	+																										
ОК 02	+																										
ОК 03																											
ОК 04			+			+																					
ОК 05			+			+																					
ОК 06			+			+																					
ОК 07																											
ОК 08	+	+			+																						
ОК 09		+	+			+																					
ОК 10		+	+			+																					
ОК 11		+				+																					
ОК 12																											
ОК 13															+												
ОК 14										+																	
ОК 15					+										+												
ОК 16					+																						
ОК 17					+										+												
ОК 18			+		+					+	+										+	+	+				
ОК 19		+	+	+						+	+		+	+	+		+		+	+	+	+	+	+	+	+	+
ОК 20		+	+	+						+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	
ОК 21	+	+	+	+	+	+	+			+	+	+		+								+					
ОК 22							+	+																			
ОК 23														+			+		+								+
ОК 24		+	+	+						+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	
ОК 25		+	+	+		+	+			+	+		+	+	+		+	+	+	+	+	+	+	+	+	+	+
ОК 26				+																							
ОК 27		+	+	+										+	+			+			+						
ОК 28		+	+	+		+	+	+	+	+	+	+	+		+	+	+	+	+		+				+		+
ОК 29				+								+							+								
ОК 30		+					+		+													+		+			
ОК 31																+											
ОК 32		+	+	+	+		+			+	+	+	+		+												
ОК 33		+	+	+	+		+			+	+	+	+		+												
ОК 34		+	+	+	+		+		+	+	+	+	+	+	+		+	+	+			+	+				+
ОК 35		+	+		+		+	+	+	+	+	+	+		+	+	+		+	+	+		+	+	+		
ОК 36	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

	РН-28	**РН-29**	**РН-30**	**РН-31**	**РН-32**	**РН-33**	**РН-34**	**РН-35**	**РН-36**	**РН-37**	**РН-38**	**РН-39**	**РН-40**	**РН-41**	**РН-42**	**РН-43**	**РН-44**	**РН-45**	**РН-46**	**РН-47**	**РН-48**	**РН-49**	**РН-50**	**РН-51**	**РН-52**	**РН-53**	**РН-54**	**РН-55**
ОК 01																												
ОК 02																												+
ОК 03																											+	
ОК 04																												
ОК 05																												
ОК 06																												
ОК 07																												+
ОК 08																												+
ОК 09																												
ОК 10																												
ОК 11																											+	
ОК 12																											+	+
ОК 13																												
ОК 14																										+		
ОК 15																							+			+		
ОК 16									+	+	+		+															
ОК 17																							+			+		
ОК 18				+																								
ОК 19				+										+								+	+		+			
ОК 20				+	+			+						+	+							+	+		+			
ОК 21				+																								
ОК 22							+																					
ОК 23				+																+								
ОК 24	+			+	+	+		+						+			+	+		+		+			+			
ОК 25				+	+			+										+		+	+							
ОК 26						+													+									
ОК 27									+	+	+		+															
ОК 28				+		+								+	+	+		+		+	+		+	+		+		
ОК 29	+	+	+																									
ОК 30																	+											
ОК 31		+				+		+				+			+													
ОК 32				+																								
ОК 33				+																								
ОК 34		+	+	+			+	+						+						+								
ОК 35	+			+	+	+	+	+				+											+			+		
ОК 36	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+