**ID 59793**

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**
**БУДІВНИЦТВА І АРХІТЕКТУРИ**

# ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
# «БЕЗПЕКА ІНФОРМАЦІЙНИХ І КОМУНІКАЦІЙНИХ СИСТЕМ»

назва освітньої програми

**(Information and communications systems security)**

**першого бакалаврського рівня вищої освіти**

**за спеціальністю 125 «Кібербезпека та захист інформації»**

**галузі знань 12 «Інформаційні технології»**

**Кваліфікація: Бакалавр з кібербезпеки та захисту інформації**

**ЗАТВЕРДЖЕНО**
*Вченою радою*
*Київського національного університету*
*будівництва і архітектури*
*Протокол №___ від _____.*
*зі змінами*
*Протокол № 20 від 29.03.2024*
*Освітня програма вводиться в дію з 01 вересня 2024 р.*

Голова Вченої ради
_____ Петро КУЛІКОВ
«_29_» _03_ 2024 р.

Київ – 2024

**ЛИСТ ПОГОДЖЕННЯ**

**освітньо-професійної програми підготовки здобувачів вищої освіти**
**на першому (бакалаврському) рівні**
**за спеціальністю 125 «Кібербезпека та захист інформації»**

**1.** Погоджено на засіданні НМК зі спеціальності 125 «Кібербезпека та захист інформації»
(Протокол № _2_ від _27.03. 2024 р.)

**Гарант освітньо-професійної програми** _____ Максим ДЕЛЕМБОВСЬКИЙ

«_27_» _____03_____ 2024 р.

**2.** Перевірено навчально-методичним відділом

**Начальник навчально-методичного відділу** _____ Ігор СКЛЯРОВ

«_28_» _____03_____ 2024 р.

**3.** Погоджено на засіданні Методичної Ради Університету

(Протокол № _7_ від _28.03.2024 р.)

**Проректор з навчально-методичної роботи КНУБА** _____ Андрій ШПАКОВ

«___» _____ 2024 р.

## ПЕРЕДМОВА

**РОЗРОБЛЕНО проектною групою у складі:**

1. Делембовський Максим Михайлович, к.т.н., доцент, доцент кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва та архітектури.
2. Сєлюков Олександр Васильович, д.т.н., с.н.с., професор кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва та архітектури.
3. Ізмайлова Ольга Василівна, к.т.н., доцент, доцент кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва та архітектури.
4. Шабала Євгенія Євгенівна, к.т.н., доцент, доцент кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва та архітектури.
5. Клюєва Вікторія Василівна, старший викладач кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва та архітектури.

**Гарант освітньої програми** – Делембовський Максим Михайлович, к.т.н., доцент., доцент кафедри кібербезпеки та комп'ютерної інженерії, Київського національного університету будівництва та архітектури

**Стейкхолдерів:**

**Академічна спільнота –**

Гайдур Галина Іванівна, д.т.н., професор, завідувач кафедри інформаційної та комп'ютерної безпеки Державного університету телекомунікацій МОН України

Смірнов Олексій Анатолійович – д.т.н., професор, завідувач кафедри кібербезпеки та програмного забезпечення Центрального національного технічного університету м. Кропивницький.

**Роботодавці та/або представники професійної спільноти –**

к.т.н. Ковальов Ігор Генадійович, генеральний директор ТОВ «СВІТ-ІТ»

Долинний Анатолій Степанович, президент Всеукраїнської організації «Українська Федерація Безпеки»

**Здобувачі –**

Дашкевич Олександр Володимирович – бакалавр вищої освіти випуску 2021 року

Мацола Олександр Васильович – бакалавр вищої освіти випуску 2021 року

## 1. Профіль освітньої програми «Безпека інформаційних і комунікаційних систем» зі спеціальності 125 «Кібербезпека та захист інформації»

| 1 - Загальна інформація | |
|---|---|
| **Повна назва вищого навчального закладу та структурного підрозділу** | Київський національний університет будівництва і архітектури, факультет автоматизації і інформаційних технологій, кафедра кібербезпеки та комп'ютерної інженерії |
| **Ступінь вищої освіти та назва кваліфікації мовою оригіналу** | Бакалавр,<br>Бакалавр з кібербезпеки та захист інформації |
| **Офіційна назва освітньої програми** | Безпека інформаційних і комунікаційних систем |
| **Тип диплому та обсяг освітньої програми** | Диплом бакалавра, одиничний.<br>Обсяг кредитів ЄКТС, необхідний для здобуття ступеня бакалавра зі спеціальності 125 Кібербезпека та захист інформації становить:<br>- на базі повної загальної середньої освіти - 240 кредитів ЄКТС;<br>- на базі здобутих освітніх ступенів молодшого бакалавра, фахового молодшого бакалавра (освітньо-кваліфікаційного рівня молодшого спеціаліста) заклад вищої освіти має право визнати та перезарахувати не більше ніж 60 кредитів ЄКТС, отриманих в межах попередньої освітньої програми підготовки фахівців.<br>Мінімум 50% обсягу освітньої програми має бути спрямовано на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю, визначених цим Стандартом вищої освіти. |
| **Наявність акредитації** | Первинна акредитація |
| **Цикл/рівень** | НРК України – 6 рівень,<br>FQ-EHEA – перший цикл,<br>QF-LLL – 6 рівень |
| **Передумови** | Атестат про повну середню освіту або диплом молодшого спеціаліста (молодшого бакалавра) за спеціальністю.<br>Умови вступу визначаються «Правилами прийому до Київського національного університету будівництва і архітектури», затвердженими Вченою радою. |
| **Мова викладання** | українська |
| **Термін дії освітньої програми** | До наступної акредитації |

| | |
|---|---|
| **Інтернет-адреса постійного розміщення опису освітньої програми** | www.knuba.edu.ua |
| **2 - Мета освітньої програми** | |
| Надати освіту в галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека та захист інформації», забезпечити теоретичну та практичну підготовку висококваліфікованих кадрів, які б набули базових фахових знань для виконання професійних завдань та обов'язків прикладного характеру в галузі. Забезпечити умови формування і розвитку програмних компетентностей, що дозволять оволодіти основними знаннями, вміннями, навичками, необхідними для подальшого навчання та подальшої професійної та професійно-наукової діяльності. | |
| **3 - Характеристика освітньої програми** | |
| **Предметна область (галузь знань, спеціальність)** | **Об'єкти професійної діяльності випускників:**<br>– об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології;<br>– технології забезпечення безпеки інформації;<br>– процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту.<br>**Цілі навчання** підготовка фахівців, здатних використовувати і впроваджувати технології інформаційної та/або кібербезпеки.<br>**Теоретичний зміст предметної області**<br>Знання<br>– законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;<br>– принципів супроводу систем та комплексів інформаційної та/або кібербезпеки;<br>– теорії, моделей та принципів управління доступом до інформаційних ресурсів;<br>– теорії систем управління інформаційною та/або кібербезпекою;<br>– методів та засобів виявлення, управління та ідентифікації ризиків;<br>– методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації;<br>методів та засобів технічного та криптографічного захисту інформації;<br>– сучасних інформаційно-комунікаційних технологій; |

| | |
|---|---|
| | – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій; – автоматизованих систем проектування.<br>**Методи, методики та технології:**<br>Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення інформаційної та/ або кібербезпеки.<br>**Інструменти та обладнання:**<br>– системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/ або кібербезпеки; сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. |
| **Орієнтація освітньої програми** | Програма освітньо-професійна;<br>Основна орієнтованість програми - прикладна;<br>Програма базується на загальновідомих наукових результатах із врахуванням сучасного стану галузі інформаційна безпека, орієнтує на актуальні питання спеціальності 125 «Кібербезпека та захист інформації», в рамках яких можлива подальша професійна та наукова кар'єра. |
| **Особливості програми** | Інтеграція виявлення програмно-апаратних засобів, моніторингу та забезпечення інформаційної безпеки, сучасних інформаційних технологій захисту інформації в інформаційно-комунікаційних системах, технологій збереження даних в кіберпросторі та інтелектуалізації функцій протидії кіберзлочинності. Високий рівень практичної підготовки фахівців забезпечується розвиненою міжнародною співпрацею в науковій і освітній сферах, наявністю спеціалізованих лабораторій. Фахівці, залучені до професійної підготовки, пройшли стажування у провідних європейських та українських університетах, мають міжнародний досвід освітньої і наукової діяльності.<br>Мінімум 75% обсягу освітньої програми має бути спрямовано на забезпечення загальних та спеціальних (фахових) компетентностей за спеціальністю визначеною стандартом вищої освіти. |
| **4 - Придатність випускників до працевлаштування та подальшого навчання** | |
| **Придатність до працевлаштування** | Фахівець може займати первинні посади (за ДК 003:2010):<br>- 3439 (24771). Фахівець із організації інформаційної безпеки.<br>International Standard Classification of Occupations 2008 (ISCO-08): |

| | |
|---|---|
| | - 2529 Security specialist (ICT) |
| **Подальше навчання** | Навчання на другому (магістерському) рівні вищої освіти |
| | **5 - Викладання та оцінювання** |
| **Викладання та навчання** | Студентоцентроване навчання, технологія проблемного і диференційованого навчання, технологія інтенсифікації та індивідуалізації навчання, технологія програмованого навчання, інформаційна технологія, технологія розвивального навчання, кредитно-модульна система організації навчання, електронне навчання в системі Moodle, самонавчання, навчання на основі досліджень. Викладання проводиться у вигляді: лекції, мультимедійної лекції, інтерактивної лекції, семінарів, практичних занять, лабораторних робіт, самостійного навчання на основі підручників та конспектів, консультації з викладачами, підготовка кваліфікаційної роботи бакалавра (проекту). |
| **Оцінювання** | Оцінювання навчальних досягнень здійснюється за 100-бальною (рейтинговою) шкалою ЕКТС (ECTS), національною 4-х бальною шкалою:<br>- «відмінно»,<br>- «добре»,<br>- «задовільно»,<br>- «незадовільно»<br>- вербальною («зараховано», «незараховано») системами.<br>Види контролю:<br>- поточний,<br>- тематичний,<br>- періодичний,<br>- підсумковий,<br>- самоконтроль.<br>Форми контролю: усне та письмове опитування, тестові завдання в тому числі комп'ютерне тестування, лабораторні звіти, презентації, захист курсових робіт та проектів, звітів з практик, захист кваліфікаційної роботи бакалавра. |
| | **6 – Програмні компетентності** |
| **Інтегральна Компетентність (ІК)** | Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.. |
| **Загальні компетентності (КЗ)** | **ЗК1.** Здатність застосовувати знання у практичних ситуаціях<br>**ЗК2.** Знання та розуміння предметної області і розуміння професійної діяльності<br>**ЗК3**. Здатність спілкуватися державною мовою як усно, так і |

| | |
|---|---|
| | письмово.<br>**ЗК4.** Здатність спілкуватися іноземною мовою.<br>**ЗК5.** Здатність вчитися і оволодівати сучасними знаннями<br>**ЗК6.** Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні.<br>**ЗК7.** Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.<br>**ЗК8.** 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. |
| **Спеціальні (фахові, предметні) компетентності** | **СК1.** Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.<br>**СК2.** Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.<br>**СК3.** Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.<br>**СК4.** Здатність забезпечувати захист Інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.<br>**СК5.** Здатність відновлювати функціонування Інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.<br>**СК6.** Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)<br>**СК7.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.<br>**СК8.** Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах |

| | |
|---|---|
| | інформаційної діяльності.<br>**СК9.** Здатність застосовувати методи та засоби технічного захисту інформації на об’єктах інформаційної діяльності.<br>**СК10.** Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки. |
| **7 - Програмні результати навчання** | |
| **Програмні результати навчання (ПРН)** | РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов’язків,<br>РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.<br>РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.<br>РН4, Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв’язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.<br>РН5. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.<br>РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.<br>РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.<br>РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.<br>РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації'.<br>РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації |

| | |
|---|---|
| | для здійснення професійної діяльності.<br>РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.<br>РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.<br>РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й Інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.<br>РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.<br>РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.<br>РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах;<br>РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.<br>РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності.<br>РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.<br>РН20. Визначати загрози створення технічних каналів витоку інформації на об’єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації. |

| | |
|---|---|
| | РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах. |
| **8 – Ресурсне забезпечення реалізації програми** | |
| **Кадрове забезпечення** | Всі науково-педагогічні працівники, що забезпечують освітню програму відповідають профілю та напряму дисциплін, що викладаються.<br>90% науково-педагогічних працівників задіяних до викладання професійно-орієнтованих дисциплін зі спеціальності мають наукові ступені та вчені звання, з досвідом практичної роботи за фахом |
| **Матеріально-технічне забезпечення** | Навчальні приміщення дозволяють повністю забезпечити освітній процес протягом усього циклу підготовки за освітньою програмою, оскільки мають достатню кількість комп'ютеризованих та спеціалізованих робочих місць та обладнанні необхідними комп'ютерними засобами та програмним забезпеченням. |
| **Інформаційне та навчально-методичне забезпечення** | Офіційний веб-сайт http://www.knuba.edu.ua містить інформацію про освітні програми, навчальну та наукову діяльність, структурні підрозділи, правила прийому, контакти. Ресурси науково-технічної бібліотеки доступні через сайт: http://library.knuba.edu.ua. Для забезпечення навчального процесу використовується навчальне середовище на базі системи дистанційного навчання Moodle, де розміщені матеріали навчально-методичного забезпечення ОП.<br>Використання дистанційного, навчального середовища університету та авторських розробок науково-педагогічних працівників; підручників та навчальних посібників з грифом Вченої ради КНУБА. |
| **9 - Академічна мобільність** | |
| **Національна кредитна мобільність** | Положенням університету передбачена можливість національної кредитної мобільності. |
| **Міжнародна кредитна мобільність** | Положенням університету передбачена можливість міжнародної кредитної мобільності |
| **Навчання іноземних здобувачів вищої освіт** | Навчання іноземних здобувачів вищої освіти проводиться на загальних умовах з додатковою мовною підготовкою |

## 2. Перелік компонент освітньої програми та їх логічна послідовність

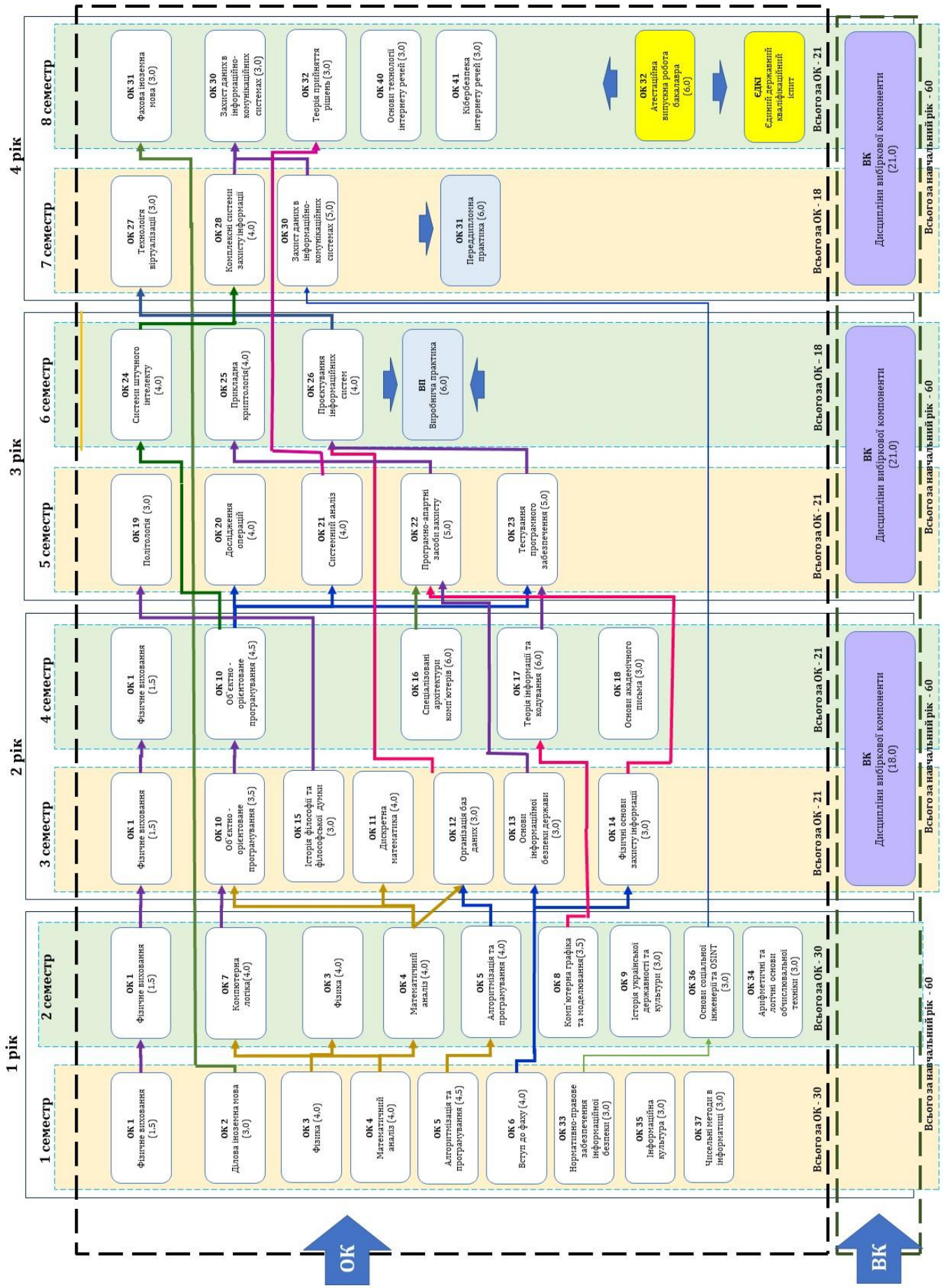
### 2.1 Перелік компонент ОП

| Код н/д | Компоненти освітньої програми | Кількість кредитів | Форма підсумкового контролю |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| **Обов'язкові компоненти ОП** | | | |
| ОК1 | Фізичне виховання | 6 | залік |
| ОК2 | Ділова іноземна мова | 3 | залік |
| ОК3 | Фізика | 8 | залік, іспит |
| ОК4 | Математичний аналіз | 8 | іспит, залік |
| ОК5 | Алгоритмізація та програмування | 8,5 | іспит, залік |
| ОК6 | Вступ до фаху | 4 | іспит |
| ОК7 | Комп`ютерна логіка | 4 | іспит |
| ОК8 | Комп`ютерна графіка та моделювання | 3,5 | іспит |
| ОК9 | Історія української державності та культури | 3 | залік |
| ОК10 | Об`єктно - орієнтоване програмування | 8 | залік, іспит |
| ОК11 | Дискретна математика | 4 | іспит |
| ОК12 | Організація баз даних | 3 | залік |
| ОК13 | Основи інформаційної безпеки держави | 3 | іспит |
| ОК14 | Фізичні основи захисту інформації | 3 | залік |
| ОК15 | Історія філософії та філософської думки | 3 | іспит |
| ОК16 | Спеціалізовані архітектури комп'ютерів | 5 | залік |
| ОК17 | Теорія інформації та кодування | 5 | іспит |
| ОК18 | Основи академічного письма | 3 | залік |
| ОК19 | Політологія | 3 | іспит |
| ОК20 | Дослідження операцій | 4 | іспит |
| ОК21 | Системний аналіз | 5 | залік |
| ОК22 | Програмно-апаратні засоби захисту | 5 | іспит |
| ОК23 | Тестування програмного забезпечення систем | 5 | іспит |
| ОК24 | Системи штучного інтелекту | 4 | іспит |
| ОК25 | Прикладна криптологія | 4 | іспит |
| ОК26 | Проєктування інформаційних систем | 4 | іспит |
| ОК27 | Технології віртуалізації | 3 | іспит |
| ОК28 | Комплексні системи захисту інформації | 4 | іспит |
| ОК30 | Захист даних в інформаційно-комунікаційних системах | 8 | іспит |
| ОК31 | Фахова іноземна мова | 3 | залік |
| ОК32 | Теорія прийняття рішень | 3 | залік |

| | | | |
|---|---|---|---|
| ОК33 | Нормативно-правове забезпечення інформаційної безпеки | 3 | залік |
| ОК34 | Арифметичні та логічні основи обчислювальної техніки | 3 | залік |
| ОК35 | Інформаційна культура | 3 | залік |
| ОК36 | Основи соціальної інженерії та OSINT | 3 | залік |
| ОК37 | Чисельні методи в інформатиці | 3 | залік |
| ОК38 | Виробнича практика | 6 | залік |
| ОК39 | Переддипломна практика | 6 | залік |
| ОК40 | Атестаційна випускна робота бакалавра | 6 | залік |
| ОК41 | Кібербезпека інтернету речей | 4 | залік |
| ОК42 | Основи технології інтернету речей | 3 | залік |
| **Загальний обсяг обов`язкових компонент** | | **180** | |
| **Вибіркові компоненти ОП** | | | |
| ВК | Дисципліни вибіркової компоненти | 60 | Залік |
| **ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ** | | **240** | |

Здобувач вищої освіти самостійно обирає дисципліни вибіркової компоненти з загально університетського каталогу вибіркових дисциплін на офіційному сайті www.knuba.edu.ua

## 2.2. Структурно-логічна схема освітньої програми



## 3. Форма атестації здобувачів вищої освіти освітньої програми

| | |
|---|---|
| **Форми атестації здобувачів вищої освіти** | Атестація здійснюється у формі єдиного державного кваліфікаційного іспиту.<br><br>Додаткова форма атестації є публічний захист кваліфікаційної випускної роботи. |
| **Вимоги до єдиного державного кваліфікаційного іспиту** | Єдиний державний кваліфікаційний іспит передбачає оцінювання досягнень результатів навчання, визначених цим стандартом. |
| **Вимоги до кваліфікаційної роботи (за наявності)** | Кваліфікаційна робота має передбачати розв'язок спеціалізованого завдання теоретичного або практичного спрямування в галузі кібербезпеки та захисту Інформації.<br>У кваліфікаційній роботі не повинно бути академічного плагіату, фальсифікації та фабрикації.<br>Кваліфікаційна робота має бути оприлюднена (за виключенням робіт, що містять інформацію з обмеженим доступом) на офіційному сайті закладу вищої освіти або його структурного підрозділу, або у репозитарії закладу вищої освіти. |

## 4. Вимоги до наявності системи внутрішнього забезпечення якості вищої освіти

У закладі вищої освіти повинна функціонувати система забезпечення ним якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості), яка передбачає здійснення таких процедур і заходів:

1) визначення принципів та процедур забезпечення якості вищої освіти;

2) здійснення моніторингу та періодичного перегляду освітніх програм;

3) щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників закладу вищої освіти та регулярне оприлюднення результатів таких оцінювань на його офіційному веб-сайті, на інформаційних стендах та в будь-який інший спосіб;

4) забезпечення підвищення кваліфікації педагогічних, наукових і науковопедагогічних працівників;

5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів, за кожною освітньою програмою;

6) забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;

7) забезпечення публічності інформації про освітні програми, ступені вищої освіти та кваліфікації;

8) забезпечення ефективної системи запобігання та виявлення академічного плагіату у наукових працях працівників закладів вищої освіти і здобувачів вищої освіти;

9) інших процедур і заходів.

Система забезпечення закладом вищої освіти якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості) за поданням закладу вищої освіти оцінюється Національним агентством із забезпечення якості вищої освіти або акредитованими ним незалежними установами оцінювання та забезпечення якості вищої освіти на предмет її відповідності вимогам до системи забезпечення якості вищої освіти, що затверджуються Національним агентством із забезпечення якості вищої освіти, та міжнародним стандартам і рекомендаціям щодо забезпечення якості вищої освіти.

## 5. Перелік нормативних документів, на яких базується Стандарт вищої освіти

1. Стандарт вищої освіти за спеціальністю 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти затверджений наказом МОН №1074 від 04.10.2018 р.

2. Проект стандарт вищої освіти за спеціальністю 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти оприлюднений МОН

3. International Standard ClassificationofEducation (ISCED 2011). https ://www.datenportal.bmbf.de/portal/en/G294.html# :~:texWSCED%20was%2Qdevelpped%2Oby%2OUNESCO,facilitating%2Onational%2Oand%2Ointernational%20comparis ons ■

4. ISCED FieldsofEducationandTraining 2013 (ISCED-F 2013).: chrome-extension://efaidnbmnnnibpcajpçglclefindmkaj/http://uis.unesco.org/sites/default/files/documents/isced-fields-of-education-and-training-2013-en.pdf;

5. TheEuropeanQualificationsFramework: SupportingLearning, WorkandCrossBorderMobility. URL: http://www.ehea.info/Upload/TPG AQF RQ MK l EQF Brochure.pdf;

6. QF-EHEA - QualificationFrameworkofiheËuropeanHigherÉducationArea.;

7. Стандарта та рекомендації щодо забезпечення якості в Європейському просторі вищої освіта (ESG). Режим доступу: https ://ihed.org.ua/wp-content/uploads/2018/10/04 2016 ESG 2015.pdf;

8. HigherEducationintheWorld 8 - Specialissue.

NewVisionsforHigherEducationtowards 2030. Barcelona, GUNi, May 2022. URL: https://www.guninetwork.org/files/gum _heiw_8 complete_- _new_visîons_for higher_education_towards 2030_l.pdf

9. TUNING Educational StructuresinEurope (Проект Європейської Комісії "Налаштування освітніх систем в Європі (для ознайомлення з прикладами стандартів та вимог до компетентностей для різних предметних областей) http://www.ehea.info/cidl01886/tuning-educational-structures-europe.html.

10. Національний освітній глосарій: вища освіта 2-е вид., перероб. і дол. авт.-уклад. : В. М. Захарченко, С. А. КалашнІкова, В. І. Луговий, А. В. Ставицький, Ю. М. Рашкевич, Ж. В. Таланова / За ред. В.Г.Кременя. - Київ : ТОВ «Видавничий дім «Плеяди», 2014. - 100 с. — Режим доступу: http://onu.edu.ua/pub/bank/userfiles/files/nauk%20method%20rada/glossariy.pdf

11. Бахрушин В.Є. Стандартизація вимог до вищої освіти, як інструмент забезпечення якості вищої освіти: рівні вищої освіти та предметні області. Освітня аналітика України. 2020. № 2(9), С. 50-66. URL: https://science.iea.gov.ua/wp-content/uploads/2020/10/4 Bakhrushin 29 2020, 50 66.pdf.

12. Рашкевич Ю.М. Болонський процес: історія, стан та перспективи. Освітня аналітика України 2018, № 3 (4), С. 5-16 - URL: https://science.iea.gov.ua/w-content/uploads/2018/12/5 16 Rashkevich.pdf

13. Розвиток системи забезпечення якості вищої освіти в Україні:

інформаційно-аналітичний огляд - URL: https://lib.iitta.gov.ua/9412/1/%D0%A0%D0%BE%D0%B7%D0%B2%D0%B8%D1%82%D0%BE%D0%BA%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B8%D0%B7%D0%B0%D0%B5%D0%B7%D0%BF%D1%80%D0%BE%D1%81%D1%82%D0%B8.pdf

14. Розроблення освітніх програм: методичні рекомендації / Авт.: В. М. Захарченко, В. І. Луговий, Ю.М. Рашкевич, Ж.В. Таланова / За ред. В.Г. Кременя. - Київ : ДП «НВЦ «Пріоритети», 2014.- 120 с. - URL: https://core.ac.uk/download/pdf/32308651 .pdf

## 6. Матриця відповідності програмних компетентностей компонентам освітньої програми

| | ОК1 | ОК2 | ОК3 | ОК4 | ОК5 | ОК6 | ОК7 | ОК8 | ОК9 | ОК10 | ОК11 | ОК12 | ОК13 | ОК14 | ОК15 | ОК16 | ОК17 | ОК18 | ОК19 | ОК20 | ОК21 | ОК22 | ОК23 | ОК24 | ОК25 | ОК26 | ОК27 | ОК28 | ОК30 | ОК31 | ОК32 | ОК33 | ОК34 | ОК35 | ОК36 | ОК37 | ОК38 | ОК39 | ОК40 | ОК41 | ОК42 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **ІК** | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • | • |
| **ЗК1** | | | | | | • | | | | | | | | | | | | | | | • | | | | | | | | | • | | | | | | | | | | | |
| **ЗК2** | | | • | • | • | • | • | • | | • | • | | | | | • | • | | | • | • | | | | | | | | | | | | • | | | • | | | | | |
| **ЗК3** | | • | | | | | | | | | | | | | | | | • | | | | | | | | | | | • | | | | | | | | | | | | |
| **ЗК4** | | • | | | | | | | | | | | | | | | | • | | | | | | | | | | | • | | | | | | | | | | | | |
| **ЗК5** | | | • | • | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | • | • | • | | |
| **ЗК6** | | | | | | • | | | • | | | | | | • | | | | • | | | | | | | | | | | | | | | • | | | | | | | |
| **ЗК7** | | | | | | | | | | | | | | | • | | | | • | | | | | | | | | | | | | | | | | | | | | | |
| **ЗК8** | • | | • | | | | | | • | | | | | | | | | | | | | | | | | | | | | | | | | • | | | | | | | |
| **СК1** | | | | | | | | | | | | | • | | | | | | | | | | | | | | | | | | | • | | | | | | | | | |
| **СК2** | | | | • | • | | • | • | | • | • | • | | | | • | • | | | | | | | • | | | | | | | | • | | | • | | | | | |
| **СК3** | | | | | | | | | | | | | | | | | | | | • | • | | | • | | | | | | | • | • | | | | | • | • | • | | |
| **СК4** | | | | | | | | | | | | • | • | | | | | | | | | | • | | | | | • | | | | | | • | | | | | | • | • |
| **СК5** | | | | | | | | | | | | | | • | | | | | | | | | | | | | | • | | | | | | | | | | | • | • |
| **СК6** | | | | | | | | | | | | | | | | | | | | | | • | | | | • | • | • | | | | | | | | | | | | |
| **СК7** | | | | | | | | | | | | | | | | | | | | | | | | | | • | • | • | | | | | | | | | | | | |
| **СК8** | | | | | | | | | | | • | | | | | | • | | | | | | | | • | | | | | | | | | | | | | | | |
| **СК9** | | | | | | | | | | | | | | • | | | | | | | | • | | | • | | | | | | | | | | | | | | | |
| **СК10** | | | | | • | | | | | | | | | | | | | | | | | | • | | | | | | | | | | | | • | | | | • | • |

## 7. Матриця забезпечення програмних результатів навчання (ПРН) відповідним компонентам освітньої програми

| | ОК1 | ОК2 | ОК3 | ОК4 | ОК5 | ОК6 | ОК7 | ОК8 | ОК9 | ОК10 | ОК11 | ОК12 | ОК13 | ОК14 | ОК15 | ОК16 | ОК17 | ОК18 | ОК19 | ОК20 | ОК21 | ОК22 | ОК23 | ОК24 | ОК25 | ОК26 | ОК27 | ОК28 | ОК30 | ОК31 | ОК32 | ОК33 | ОК34 | ОК35 | ОК36 | ОК37 | ОК38 | ОК39 | ОК40 | ОК41 | ОК42 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **РН1** | ● | ● | | | | | | | ● | | | | | | | | | ● | | | | | | | | | | | | ● | | | | ● | | | | | | | | |
| **РН2** | | ● | | | | | | | | | | | | | | | | ● | | | | | | | | | | | | ● | | | | | | | | | | | | |
| **РН3** | | | | | | ● | | | ● | | | | | | ● | | | | ● | | | | | | | | | | | | | | | ● | | | | | | | | |
| **РН4** | | | | | | ● | | | | | | | | | | | | | | | ● | | | | | | | | | | ● | | | | | | | | | | |
| **РН5** | | | | | | ● | | | | | | | | | ● | | | | ● | ● | ● | | | | | | | | | | ● | | | | | | | | | | |
| **РН6** | ● | | ● | ● | | | | | | | | | | | | | | | | | | | | | | | | | | | | | ● | | | ● | ● | ● | | | |
| **РН7** | ● | | | | | ● | | | | | | | | | | | | | | | ● | | | | | | | | | | | | ● | | | | | | | | |
| **РН8** | | | ● | ● | | | ● | ● | | ● | ● | | | | | ● | | | | | | | | | | | | | | | | | | ● | | ● | | | | | |
| **РН9** | | | | | | | | | | | | | ● | | | | | | | | | | | | | | | | | | | | ● | | | | | | | | |
| **РН10** | | | | | ● | | ● | ● | | ● | | ● | | | | ● | ● | | | | | | | ● | | | | | | | | | | ● | | | ● | | | | |
| **РН11** | | | | | | | | | | | | | | | | | | | | ● | ● | | | ● | | | | | | | ● | ● | | | | | ● | ● | ● | | |
| **РН12** | | | | | | | | | | | | ● | ● | | | | | | | | | | ● | | | | | | ● | | | | | | ● | | | | | ● | ● |
| **РН13** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | ● | | | | | | | | | | | | |
| **РН14** | | | | | | | | | | | | | | ● | | | | | | | | | | | | | | | ● | | | | | | | | | | | | |
| **РН15** | | | | | | | | | | | | | | ● | | | | | | | | | | | | | | | | | | | | | | | | | | ● | ● |
| **РН16** | | | | | | | | | | | | | | | | | | | | | | ● | | | | ● | ● | ● | | | | | | | | | | | | | |
| **РН17** | | | | | | | | | | | | | | | | | | | | | | | | | | ● | ● | ● | | | | | | | | | | | | | |
| **РН18** | | | | | | | | | | | ● | | | | | | ● | | | | | | | | ● | | | | | | | | | | | | | | | | |
| **РН19** | | | | | | | | | | | | | | | | | | | | | | | | | ● | | | | | | | | | | | | | | | | |
| **РН20** | | | | | | | | | | | | | | ● | | | | | | ● | ● | ● | | | | | | | | | | | | | | | | | | | |
| **РН21** | | | | | ● | | | | | | | | | | | | | | | | | | ● | | | | | | | | | | | | ● | | | | | ● | ● |