**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**
**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ**
**імені Ігоря Сікорського»**

ЗАТВЕРДЖЕНО
Вченою радою КПІ ім. Ігоря Сікорського
(протокол № ___ від «___» _____ 20__ р.)

Голова Вченої ради

_____ Михайло ІЛЬЧЕНКО

# КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ КІБЕРБЕЗПЕКИ (APPLIED CRYPTOGRAPHY IN CYBERSECURITY SYSTEMS)

## ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

**Перший (бакалаврський) рівень вищої освіти**

**Спеціальність:** F5 Кібербезпека та захист інформації
**Галузь знань:** F Інформаційні технології
**Кваліфікація:** бакалавр з кібербезпеки та захисту інформації

Введено в дію з 2026/2027 навч. року
наказом ректора КПІ ім. Ігоря Сікорського
від _____ № _____

Київ – 2026

# ПРЕАМБУЛА

**РОЗРОБЛЕНО:**

**Керівник робочої групи**

ЯКОВЛЄВ Сергій Володимирович, кандидат технічних наук, зав. кафедрою математичних методів захисту інформації, гарант освітньої програми

**Члени робочої групи:**

ФЕСЕНКО Андрій В'ячеславович, кандидат фізико-математичних наук, старший викладач кафедри математичних методів захисту інформації

ЗАВАДСЬКА Людмила Олексіївна, кандидат фізико-математичних наук, старший науковий співробітник, доцент кафедри математичних методів захисту інформації

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

ЯКИМЧУК Олексій Петрович, аспірант 4 курсу

**ПОГОДЖЕНО:**

Науково-методична комісія КПІ ім. Ігоря Сікорського зі спеціальності F5 Кібербезпека та захист інформації

(протокол № __ від «__» грудня 2025 р.)

Голова НМКУ – F5

_____ Дмитро ЛАНДЕ

Методична рада КПІ ім. Ігоря Сікорського

(протокол № __ від «__» _____ 2026 р.)

Голова Методичної ради

_____ Тетяна ЖЕЛЯСКОВА

**ВРАХОВАНО**

Стандарт вищої освіти для першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека та захист інформації

Положення про освітні програми КПІ ім. Ігоря Сікорського https://osvita.kpi.ua/node/137.

Наказ КПІ ім. Ігоря Сікорського №НОД/215/26 від 18.03.2026 «Про планування та організацію освітнього процесу 2026/2027 н.р.».

фахову експертизу стейкхолдерів:

Кудін Антон Михайлович, головний експерт управління безпеки інформації Департаменту безпеки НБУ, д.т.н., проф.

Фісуненко Андрій Леонідович, віце-президент з розробок і досліджень ТОВ Самсунг Електронікс Україна Компані, Центр розробок і досліджень

Грубіян Євген Олександрович, провідний дослідник Distributed Labs

Агамалян Мирон Каренович, студент 3 курсу навчання першого (бакалаврського) рівня

Бондар Петро Олександрович, студент 2 курсу навчання другого (магістерського) рівня

Паршин Олександр Юрійович, аспірант 2 курсу навчання третього (доктор філософії) рівня

Освітню програму обговорено після надходження всіх побажань та пропозицій від стейкхолдерів та схвалено на розширеному засіданні кафедри математичних методів захисту інформації (протокол № ____ від «___» _____ 2026 р.).

## ЕВОЛЮЦІЯ ОСВІТНЬОЇ ПРОГРАМИ

Міждисциплінарна освітньо-професійна програма «Криптографічний захист інформації в системах кібербезпеки» впроваджується в дію з 2026-2027 навчального року з метою підготовки висококваліфікованих та конкурентоспроможних фахівців, інтегрованих у європейський та світовий науково-освітній простір. Освітня програма є нащадком освітніх програм «Прикладна криптологія» (2016-2018) та «Математичні методи криптографічного захисту інформації» (2019-2025), які відносились до спеціальності «Прикладна математика», і продовжує багаторічні традиції кафедри ММЗІ з підготовки фахівців у галузі прикладної математики, комп'ютерних наук та криптології, з акцентом як на глибинній теоретичній підготовці, так і на практичних навичках, необхідних для створення та аналізу систем криптографічного захисту інформації.

Запровадження освітньої програми здійснюється для задоволення потреб держави, суспільства, фізичних і юридичних осіб у висококваліфікованих фахівцях для виконання замовлення ринку праці, забезпечення професійної успішності випускників, зростання ролі Університету у наданні освітніх послуг на міжнародному та державному рівні. Згідно з Законом України "Про основні засади забезпечення кібербезпеки України" (№2163-VIII, зі змінами, внесеними Законом України №№ 4336-IX від 27.03.2025), криптографічний захист інформації є невід'ємною частиною кіберзахисту. Згідно з Методичними рекомендаціями щодо відповідності освітніх програм спеціальностям (Наказ МОН №1734 від 31.12.2025), освітні програми, основний зміст яких стосується криптографічного захисту інформації, відносяться до спеціальності F5 Кібербезпека та захист інформації. Однак фахівці з криптографічних методів захисту інформації, які здатні не тільки реалізовувати, але й створювати та аналізувати криптографічні механізми, повинні мати ґрунтовну обізнаність у моделях і методах аналізу та синтезу криптографічних алгоритмів, примітивів та протоколів. Відповідні навички відносяться до фундаментальних засад дискретної математики та комп'ютерних наук.

Освітня програма «Криптографічний захист інформації в системах кібербезпеки» робить сильний акцент на математичному апараті комп'ютерних наук, який корисний не тільки фахівцям з кібербезпеки, але й програмістам-розробникам, інженерам-дослідникам, аналітикам безпеки. У порівнянні з попередниками, у програмі закладається більша практична орієнтованість у галузі кібербезпеки, суттєво посилена складова з алгоритмики, а також додана складова з опанування технологій Web3, в першу чергу, блокчейнів та смарт-контрактів.

# 1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ

| 1 – Загальна інформація | |
|---|---|
| Повна назва закладу вищої освіти та навчального підрозділу | Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»,<br>Навчально-науковий фізико-технічний інститут |
| Ступінь вищої освіти та назва кваліфікації | Ступінь – бакалавр<br>Кваліфікація – бакалавр з кібербезпеки та захисту інформації |
| Офіційна назва освітньої програми | «Криптографічний захист інформації в системах кібербезпеки» |
| Тип диплому та обсяг освітньої програми | Диплом бакалавра;<br>240 кредитів, термін навчання 3 роки 10 місяців |
| Інформація про акредитацію | Не акредитовано |
| Цикл, рівень вищої освіти | НРК України – 6 рівень<br>QF-EHEA – перший цикл<br>EQF-LLL – 6 рівень |
| Передумови | Наявність повної загальної середньої освіти |
| Форма здобуття освіти | Очна (денна) |
| Мова(и) викладання | Українська |
| Інтернет-адреса постійного розміщення освітньої програми | |
| **2 – Мета освітньої програми** | |
| Мета освітньої програми полягає у підготовці фахівців у галузі інформаційних технологій, кібербезпеки та криптології, здатних розв’язувати складні спеціалізовані задачі та практичні проблеми криптографічного захисту інформації у професійній діяльності або у процесі навчання, здійснювати і забезпечувати міжкультурну фахову взаємодію представників науково-технічної спільноти, спрямовану на інтеграцію університетської освіти в європейський освітньо-науковий простір шляхом інтернаціоналізації освітнього процесу в умовах сталого інноваційного науково-технічного розвитку суспільства та формування високої адаптивності здобувачів вищої освіти в умовах трансформації ринку праці через взаємодію з роботодавцями та іншими стейкхолдерами.<br><br>Мета освітньої програми відповідає стратегії розвитку КПІ імені Ігоря Сікорського 2025-2030 років щодо досягнення цілей сталого розвитку суспільства, високотехнологічної трансформації держави та зміцнення її обороноздатності, формування якісного людського капіталу для відновлення та стійкого розвитку України | |

| 3 – Характеристика освітньої програми | |
|---|---|
| Предметна область | *Об'єкти вивчення та діяльності*: технології кібербезпеки та захисту інформації, математичні методи, моделі, алгоритми та програмне забезпечення, що призначені для дослідження, аналізу, проектування процесів управління кібербезпекою та захистом інформації та інформаційних систем і ресурсів.<br><br>*Цілі навчання:* підготовка фахівців, здатних:<br>– використовувати та впроваджувати технології кібербезпеки та захисту інформації, математичні методи та технології в галузі прикладної математики;<br>– формулювати, розв'язувати й узагальнювати складні теоретичні та практичні задачі в галузі кібербезпеки та захисту інформації з використанням фундаментальних та спеціальних прикладних методів математичних та комп'ютерних наук;<br>– будувати, досліджувати та застосовувати математичні моделі, що ґрунтуються на даних та на знаннях, створювати та експлуатувати програмне забезпечення для задач криптографічного захисту інформації.<br><br>*Теоретичний зміст предметної області:* принципи, концепції, теорії та математичні методи захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору; алгоритми і програмні засоби їх реалізації; своєчасне виявлення, запобігання і нейтралізація загроз національній безпеці України у кіберпросторі.<br><br>*Методи, методики та технології*: прикладні математичні методи, алгоритми, методики та технології вирішення теоретичних і прикладних задач кібербезпеки та захисту інформації, зокрема, за допомогою комп'ютерного моделювання та спеціалізованих програмних засобів<br><br>*Інструменти та обладнання*: спеціалізовані програмні, апаратні та програмно-апаратні засоби, пристрої, комп'ютерні та соціальні мережі, інформаційні системи та комплекси для проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків). |
| Орієнтація освітньої програми | Освітньо-професійна |
| Основний фокус освітньої програми | *Базовий фокус ОП* – математичні моделі, методи, алгоритми для задач комп'ютерних наук, кібербезпеки та криптографічного захисту інформації<br><br>*Ключові слова:* кібербезпека, захист інформації, алгоритми, криптологія, криптографія, шифрування, цифровий підпис, геш-функція |
| Особливості програми | Багатопрофільна підготовка фахівців. Поглиблена фундаментальна підготовка з дискретної математики, прикладної алгебри, теорії алгоритмів та теорії імовірностей, орієнтована на розв'язування прикладних задач у галузях комп'ютерних наук, кібербезпеки, захисту інформації та криптології. Поєднання теоретичної підготовки та практичних навичок (зокрема, з програмування) у циклі професійної підготовки.<br>Проходження переддипломної практики та виконання спільних проектів на замовлення державних, науково-дослідних установ та провідних ІТ-компаній України за фахом. Орієнтація на дуальну освіту. |

| 4 – Придатність випускників до працевлаштування та подальшого навчання | |
|---|---|
| Придатність до працевлаштування | Відповідно до національного Класифікатору професій ДК 003:2010, випускники можуть працювати на посадах, що відповідають таким класифікаційним угрупованням:<br>3139 Фахівець із організації захисту інформації з обмеженим доступом; Фахівець із організації інформаційної безпеки<br>3121 Фахівець з інформаційних технологій.<br>2139.2 Аналітик систем захисту інформації та оцінки вразливостей<br>2139.2 Аналітик загроз безпеки<br>2132.2 Розробник систем захисту інформації<br>Компетентності, одержані завдяки циклу професійної підготовки освітньої програми, дозволяють працювати на посадах, що відповідають класифіційним угрупованням<br>2149 Професіонали із організації інформаційної безпеки<br>2139.2 Професіонали в інших галузях обчислень (комп'ютеризація):<br>Фахівець з криптографічного захисту інформації<br>за наявності другого рівня вищої освіти відповідного спрямування (у галузі математики та статистики або інформаційних технологій).<br><br>Випускники ОП можуть працювати спеціалістами з криптографічного захисту інформації та/або ІТ-технологій, розробниками програмних засобів, прикладними програмістами, аналітиками безпеки, аналітиками даних, адміністраторами програмних систем та баз даних. |
| Подальше навчання | Продовження освіти за другим (освітньо-науковим, освітньо-професійним) рівнем вищої освіти; набуття додаткових кваліфікацій у системі післядипломної 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 та лабораторні роботи (індивідуальні та у малих групах), курсові роботи; технології змішаного та перевернутого навчання за окремими освітніми компонентами; дослідницькі практики; виконання дипломної роботи (бакалаврської дипломної роботи) |
| Оцінювання | Оцінювання знань студентів здійснюється у відповідності до Положення про систему оцінювання результатів навчання КПІ ім. Ігоря Сікорського за усіма видами аудиторної та позааудиторної роботи (вхідний, поточний, календарний, підсумковий контроль): усні та письмові екзамени, тестування, колоквіуми тощо. Рівень знань по кожній дисципліні оцінюється згідно критеріїв, визначених у Рейтинговій системі оцінювання даної дисципліни. |
| **6 – Програмні компетентності** | |
| Інтегральна компетентність | Здатність розв'язувати спеціалізовані задачі і практичні проблеми у галузі кібербезпеки та криптографічного захисту інформації, що передбачає застосування математичних методів, розробку нових рішень та застосування існуючих |
| **Загальні компетентності (ЗК)** | |
| ЗК01 | Здатність застосовувати знання у практичних ситуаціях |
| ЗК02 | Знання та розуміння предметної області та розуміння професії |
| ЗК03 | Здатність спілкуватися державною мовою як усно, так і письмово |
| ЗК04 | Здатність спілкуватися іноземною мовою |
| ЗК05 | Здатність вчитися і оволодівати сучасними знаннями |

| | |
|---|---|
| ЗК06 | 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 |
| ЗК07 | Здатність ухвалювати рішення та діяти, дотримуючи принципу неприпустимості корупції та будь-яких проявів недоброчесності |
| ЗК08 | 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. |
| ЗК09 | Здатність до виконання свого конституційного обов'язку щодо захисту Вітчизни, національно-патріотичної налаштованості, відданості українському народові |
| ЗК10 | Здатність до абстрактного мислення, аналізу та синтезу; здатність генерувати нові ідеї, бути критичним і самокритичним. |
| ЗК11 | Навички у використанні інформаційних і комунікаційних технологій. |
| **Фахові компетентності спеціальності (ФК)** | |
| ФК01 | Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності |
| ФК02 | Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації |
| ФК03 | Здатність забезпечувати неперервність бізнесу згідно встановленої політики кібербезпеки та захисту інформації |
| ФК04 | Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої политики кібербезпеки й захисту інформації |
| ФК05 | Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження |
| ФК06 | Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекс нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо) |
| ФК07 | Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою |
| ФК08 | Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності |
| ФК09 | Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності |
| ФК10 | Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки |
| ФК11 | Здатність виконувати завдання, сформульовані у математичній формі, використовуючи та адаптуючи математичні теорії, моделі та методи |
| ФК12 | Здатність обирати та застосовувати математичні методи для розв'язання прикладних задач (зокрема, тих, які виникають при розробці, реалізації та аналізі криптографічних систем), проводити математичне і комп'ютерне моделювання, аналіз та обробку даних, обчислювальні експерименти, розв'язувати формалізовані задачі за допомогою спеціалізованих програмних засобів |
| ФК13 | Здатність до ефективної професійної письмової й усної комунікації українською мовою та однією з офіційних мов ЄС, складання наукових звітів із виконаних робіт та впровадження результатів проведених досліджень і розробок |

| 7 – Програмні результати навчання | |
|---|---|
| ПРН01 | Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків |
| ПРН02 | Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації |
| ПРН03 | Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності |
| ПРН04 | 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 |
| ПРН05 | 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 |
| ПРН06 | Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат |
| ПРН07 | Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, теорії чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчальній та професійній діяльності |
| ПРН08 | 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 |
| ПРН09 | Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації |
| ПРН10 | Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності |
| ПРН11 | Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації |
| ПРН12 | Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки |
| ПРН13 | 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 |
| ПРН14 | Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування |
| ПРН15 | Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи |
| ПРН16 | Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах |
| ПРН17 | Забезпечувати функціонування систем 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 |
| ПРН18 | Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності |

| | |
|---|---|
| ПРН19 | Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів |
| ПРН20 | 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 |
| ПРН21 | 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 |
| ПРН22 | Володіти основними положеннями та методами математичного аналізу, лінійної та прикладної алгебри, теорії ймовірностей |
| ПРН23 | Володіти основними методами розробки дискретних математичних моделей об'єктів та процесів, аналітичного дослідження властивостей цих моделей |
| ПРН24 | Знати та вміти використовувати основні засоби захисту та оборони держави, співвітчизників, матеріальних цінностей та територіальної цілісності держави, зокрема, у разі військових дій та надзвичайних ситуацій |
| ПРН25 | Володіти основними принципами та методами побудови симетричних та асиметричних криптографічних систем у різних моделях обчислення, а також методами їх аналізу |
| ПРН26 | Знати та вміти використовувати блокчейн-технології та інструменти Web3 |

| **8 – Ресурсне забезпечення реалізації програми** | |
|---|---|
| Кадрове забезпечення | Відповідно до кадрових вимог щодо забезпечення провадження освітньої діяльності для відповідного рівня ВО , затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 у чинній редакції |
| Матеріально-технічне забезпечення | Відповідно до технологічних вимог щодо матеріально-технічного забезпечення освітньої діяльності відповідного рівня ВО, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 у чинній редакції<br>Використання обладнання для проведення лекцій у форматі презентацій, мережевих технологій, зокрема на платформі дистанційного навчання Sikorsky, демонстраційного галузевого обладнання в ході виконання лабораторних практик та комп'ютерних практикумів |
| Інформаційне та навчально-методичне забезпечення | Відповідно до технологічних вимог щодо навчально-методичного та інформаційного забезпечення освітньої діяльності відповідного рівня ВО, затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 в чинній редакції.<br>Ресурси Науково-технічної бібліотеки КПІ ім. Ігоря Сікорського, бібліотеки Навчально-наукового фізико-технічного інституту |
| **9 – Академічна мобільність** | |
| Національна кредитна мобільність | Участь студентів у програмах академічної мобільності, можливість укладення угод про академічну мобільність |
| Міжнародна кредитна мобільність | Можливість укладення угод про міжнародну академічну мобільність, про тривалі міжнародні проекти |
| Навчання іноземних здобувачів вищої освіти | Навчання іноземних здобувачів ВО, які опановують ОП за програмами міжнародної академічної мобільності; може проводитись англійською або українською мовою, за умови володіння здобувачем мовою навчання на рівні не нижче В2. |
| **10 – Процедура присвоєння професійних кваліфікацій** | |
| Не передбачено присвоєння професійної кваліфікації | |

## 2. ПЕРЕЛІК КОМПОНЕНТІВ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

| Код | Освітні компоненти програми | Кількість кредитів ЄКТС | Форма підсумкового контролю |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| **Нормативні освітні компоненти** | | | |
| **Обов'язкові компоненти циклу загальної підготовки** | | | |
| ЗО 1 | Українська мова за професійним спрямуванням | 2 | Залік |
| ЗО 2 | Історія науки і техніки | 2 | Залік |
| ЗО 3 | Основи здорового способу життя | 3 | Залік |
| ЗО 4 | Англійська мова | 5 | Залік |
| ЗО 5 | Англійська мова професійного спрямування | 5 | Залік |
| ЗО 6 | Основи економіки | 2 | Залік |
| ЗО 7 | Філософські основи наукового пізнання | 2 | Залік |
| ЗО 8 | Вступ до кібернетичної безпеки | 2 | Залік |
| ЗО 9 | Правові основи інформаційної безпеки | 2 | Залік |
| ЗО 10 | Теоретична підготовка базової загальновійськової підготовки / Цивільний захист, оборона та патріотичне виховання | 3 | Залік |
| **Обов'язкові компоненти циклу професійної підготовки** | | | |
| ПО 1.1 | Математичний аналіз. Частина 1 | 5 | Екзамен |
| ПО 1.2 | Математичний аналіз. Частина 2 | 5 | Екзамен |
| ПО 2 | Алгебра та геометрія | 5 | Екзамен |
| ПО 3.1 | Дискретна математика. Частина 1 | 3 | Залік |
| ПО 3.2 | Дискретна математика. Частина 2 | 5 | Екзамен |
| ПО 4 | Математична логіка та теорія алгоритмів | 5 | Екзамен |
| ПО 5 | Теорія імовірностей | 5 | Екзамен |
| ПО 6 | Математична статистика | 5 | Екзамен |
| ПО 7.1 | Фізика. Частина 1 | 5 | Залік |
| ПО 7.2 | Фізика. Частина 2 | 6 | Екзамен |
| ПО 8.1 | Програмування. Частина 1 | 4 | Залік |
| ПО 8.2 | Програмування. Частина 2 | 4 | Залік |
| ПО 9 | Основи комп'ютерних мереж | 4 | Залік |
| ПО 10 | Архітектура комп'ютерних систем | 5 | Екзамен |
| ПО 11 | Бази даних та інформаційні системи | 4 | Залік |
| ПО 12 | Операційні системи | 4 | Залік |
| ПО 13 | Методи та засоби технічного захисту інформації | 4 | Залік |
| ПО 14 | Комплексні системи захисту інформації: проектування, впровадження, супровід | 4 | Залік |
| ПО 15 | Управління інформаційною безпекою | 4 | Залік |
| ПО 16.1 | Прикладна алгебра. Частина 1 | 4 | Залік |
| ПО 16.2 | Прикладна алгебра. Частина 2 | 5 | Екзамен |
| ПО 17 | Прикладні алгоритми та структури даних | 6 | Екзамен |
| ПО 18 | Прикладні алгоритми та структури даних. Курсова робота | 1 | Залік |
| ПО 19 | Спеціальні розділи обчислювальної математики | 5 | Екзамен |
| ПО 20 | Теорія інформації та кодування | 4 | Залік |
| ПО 21 | Теоретико-числові алгоритми у криптології | 4 | Залік |
| ПО 22 | Симетрична криптографія | 6 | Екзамен |
| ПО 23 | Симетрична криптографія. Курсова робота | 1 | Залік |

| | | | |
|---|---|---|---|
| ПО 24.1 | Асиметричні криптосистеми та протоколи. Частина 1 | 5 | Екзамен |
| ПО 24.2 | Асиметричні криптосистеми та протоколи. Частина 2 | 3 | Залік |
| ПО 25 | Асиметричні криптосистеми та протоколи. Курсова робота | 1 | Залік |
| ПО 26 | Геш-функції та коди автентифікації | 5 | Екзамен |
| ПО 27 | Вступ до технології блокчейн та криптовалют | 4 | Залік |
| ПО 28 | Переддипломна практика | 6 | Залік |
| ПО 29 | Дипломне проектування | 6 | Захист |
| **Вибіркові освітні компоненти** | | | |
| **Вибіркові компоненти циклу загальної підготовки** | | | |
| ЗВ 1 | Освітній компонент 1 ЗУ-Каталогу | 2 | Залік |
| ЗВ 2 | Освітній компонент 2 ЗУ-Каталогу | 2 | Залік |
| **Вибіркові компоненти циклу професійної підготовки** | | | |
| ПВ 1 | Освітній компонент 1 Ф-Каталогу | 4 | Залік |
| ПВ 2 | Освітній компонент 2 Ф-Каталогу | 4 | Залік |
| ПВ 3 | Освітній компонент 3 Ф-Каталогу | 4 | Залік |
| ПВ 4 | Освітній компонент 4 Ф-Каталогу | 4 | Залік |
| ПВ 5 | Освітній компонент 5 Ф-Каталогу | 4 | Залік |
| ПВ 6 | Освітній компонент 6 Ф-Каталогу | 4 | Залік |
| ПВ 7 | Освітній компонент 7 Ф-Каталогу | 4 | Залік |
| ПВ 8 | Освітній компонент 8 Ф-Каталогу | 4 | Залік |
| ПВ 9 | Освітній компонент 9 Ф-Каталогу | 4 | Залік |
| ПВ 10 | Освітній компонент 10 Ф-Каталогу | 4 | Залік |
| ПВ 11 | Освітній компонент 11 Ф-Каталогу | 4 | Залік |
| ПВ 12 | Освітній компонент 12 Ф-Каталогу | 4 | Залік |
| ПВ 13 | Освітній компонент 13 Ф-Каталогу | 4 | Залік |
| ПВ 14 | Освітній компонент 14 Ф-Каталогу | 4 | Залік |
| | | | |
| **Загальний обсяг обов'язкових компонентів:** | | **180** | |
| **Загальний обсяг вибіркових компонентів:** | | **60** | |
| **Обсяг освітніх компонентів, що забезпечують здобуття компетентностей, визначених СВО за спеціальністю 125 Кібербезпека та захист інформації:** | | **135** | |
| **Обсяг освітніх компонентів, що забезпечують здобуття компетентностей, визначених СВО за спеціальністю 113 Прикладна математика:** | | **125** | |
| **ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ:** | | **240** | |

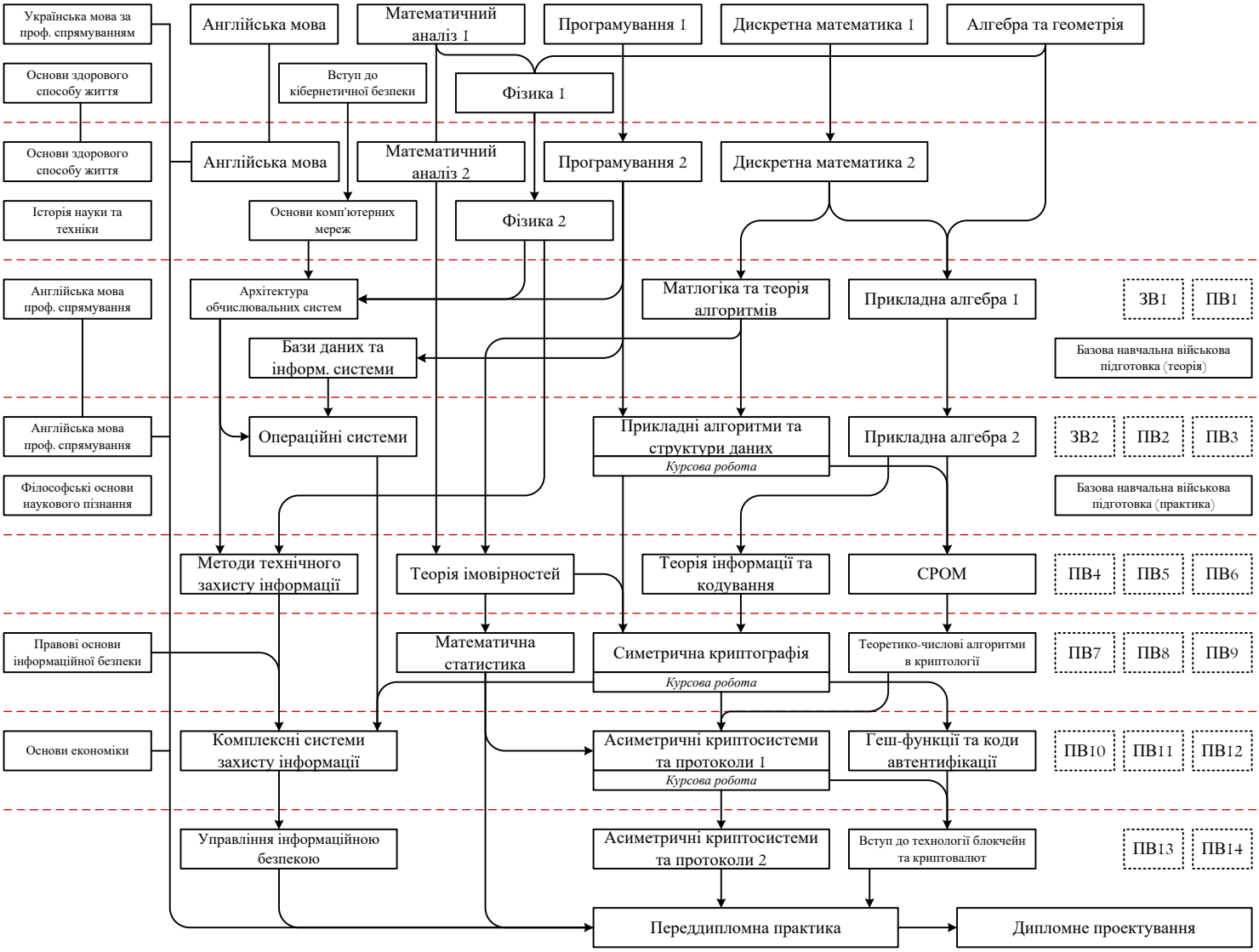
Примітки / Notes:

1) Навчальна дисципліна «Базова загальновійськова підготовка», яка складається з освітнього компоненту «Теоретична підготовка базової загальновійськової підготовки» обсягом 3 кредити ЄКТС та освітнього компоненту «Практична підготовка базової загальновійськової підготовки» обсягом 7 кредитів ЄКТС, включається до індивідуальних навчальних планів здобувачів вищої освіти – громадян України чоловічої статі (жіночої статі – добровільно), які навчаються за денною або дуальною формою здобуття освіти, згідно з Порядком проведення базової загальновійськової підготовки громадян України, які здобувають вищу освіту, та поліцейських, затвердженого постановою Кабінету Міністрів України від 21 червня 2024 р. № 734 / The academic discipline «Basic General Military Training», which consists educational component «Theoretical Course of Basic General Military Training» in the amount of 3 ECTS credits and educational component «Practical Course of Basic General Military Training» in the amount of 7 ECTS credits, is included in the individual study plans of higher education students – male citizens of Ukraine (female citizens – voluntarily), who study full-time or dual form of education, in accordance with the Procedure for Conducting Basic General Military Training for Citizens of Ukraine Pursuing Higher Education and for Police Officers, approved by the Resolution of the Cabinet of Ministers of Ukraine № 734 of 21 June 2024.

2) Освітній компонент «Практична підготовка базової загальновійськової підготовки» організовується і проводиться Міністерством оборони України, а його обсяг (7 кредитів ЄКТС) не враховується в загальному обсязі кредитів ЄКТС, необхідному для опанування освітньо-професійної програми / The educational component «Practical Course of Basic General Military Training» is organized and conducted by the Ministry of Defence of Ukraine, and its amount (7 ECTS credits) is not taken into account in the total volume of ECTS credits of the educational and professional programme.

3) Освітній компонент «Цивільний захист, оборона та патріотичне виховання» обсягом 3 кредити ЄКТС включається до індивідуальних навчальних планів здобувачів вищої освіти, звільнених від проходження базової загальновійськової підготовки згідно з Порядком проведення базової загальновійськової підготовки громадян України, які здобувають вищу освіту, та поліцейських, затвердженого постановою Кабінету Міністрів України від 21 червня 2024 р. № 734, та здобувачів вищої освіти, до індивідуальних навчальних планів яких не включено освітній компонент «Теоретична підготовка базової загальновійськової підготовки» / The educational component «Civil Protection, Defence and Patriotic Education» in the amount of 3 ECTS credits is included in the individual study plans of higher education students exempted from basic military training in accordance with the Procedure for Conducting Basic General Military Training for Citizens of Ukraine Pursuing Higher Education and for Police Officers, approved by the Resolution of the Cabinet of Ministers of Ukraine № 734 of 21 June 2024, and of higher education students whose individual study plans do not include the educational component «Theoretical Course of Basic General Military Training»

# 3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬОЇ ПРОГРАМИ




Додаткову інформацію про структуру навчального плану та можливі індивідуальні освітні траєкторії можна знайти тут: https://mmis.ipt.kpi.ua/education/educational-plans/

# 4. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація здобувачів вищої освіти за освітньою програмою «Криптографічний захист інформації в системах кібербезпеки» проводиться у формі складання Єдиного державного кваліфікаційного іспиту та захисту кваліфікаційної бакалаврської роботи. Атестація завершується видачею документа встановленого зразка про присудження здобувачу ступеня бакалавра з присвоєнням кваліфікації «Бакалавр з кібербезпеки та захисту інформації».

Атестація здійснюється відкрито і публічно. Кваліфікаційні бакалаврські роботи перевіряються на ознаки порушення академічної доброчесності та після захисту публікуються в репозиторії Науково-технічної бібліотеки Університету для вільного доступу (за виключенням робіт, які містять інформацію з обмеженим доступом).

## 5. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

| | ЗО 1 | ЗО 2 | ЗО 3 | ЗО 4 | ЗО 5 | ЗО 6 | ЗО 7 | ЗО 8 | ЗО 9 | ЗО 10 | ПО 1 | ПО 2 | ПО 3 | ПО 4 | ПО 5 | ПО 6 | ПО 7 | ПО 8 | ПО 9 | ПО 10 | ПО 11 | ПО 12 | ПО 13 | ПО 14 | ПО 15 | ПО 16 | ПО 17 | ПО 18 | ПО 19 | ПО 20 | ПО 21 | ПО 22 | ПО 23 | ПО 24 | ПО 25 | ПО 26 | ПО 27 | ПО 28 | ПО 29 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ЗК 01 | + | + | | + | + | + | | + | | | + | + | + | | + | + | + | + | + | + | + | + | + | + | | + | + | + | | + | + | + | + | + | | | + | + |
| ЗК 02 | + | + | | + | + | | + | + | | | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | | + | + | + | + | | + | | | + | + |
| ЗК 03 | + | | | + | + | + | + | | + | | | | | | | | + | | | | | | | | | | | | | | | | | | | | + | + |
| ЗК 04 | | | | + | + | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | + | + |
| ЗК 05 | + | + | | + | + | + | + | | + | | + | + | + | + | + | + | + | + | + | + | + | + | + | | | + | + | | + | + | + | + | + | + | | | + | + |
| ЗК 06 | | | | | | + | + | | + | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ЗК 07 | + | | | | | | | | + | | | | | | | | | | | | | | | | | | | + | | | | | + | | + | | | | + |
| ЗК 08 | + | + | + | | | + | + | | | | | | | | | | + | | | | | | | | | | | | | | | | | | | | | |
| ЗК 09 | | | | | | | | | | + | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ЗК 10 | | | | | | | + | | | | + | + | + | + | + | + | + | + | | | | | | | | + | + | | | | | | | | | | + | + |
| ЗК 11 | | | | | | | | | + | | | | | | | | | + | | + | + | | | | | | + | | + | + | + | + | + | + | + | | + | + |
| ФК 01 | + | | | + | + | | | | + | | | | | | | | | | | | | + | | + | + | | | + | | | | | + | | + | | | + | + |
| ФК 02 | | | | | | | | + | + | | | | + | | | | | + | + | | + | + | + | + | + | | + | | + | + | + | + | | + | | | + | + |
| ФК 03 | | | | | | + | | + | + | | | | | | | | | + | + | | | + | | + | + | | | | | | | | | | | | + | + |
| ФК 04 | | | | | | + | | + | + | | | | | | | | | + | | | | + | + | + | + | | | | + | + | + | + | + | + | + | | + | + |
| ФК 05 | | | | | | | | + | | | | | | | | | | | + | + | + | + | | | | | | | | | | | | | | | + | + |
| ФК 06 | | | | | | | | | | | | | | | | | | + | | + | + | + | + | + | | | + | | | | | | | | | | + | + |
| ФК 07 | | | | | | | | + | | | + | + | + | + | + | + | + | + | | | | + | | + | + | + | + | | + | + | + | + | + | + | + | + | + | + |
| ФК 08 | | | | | | | | | | | + | + | | | + | + | | | | | | | | | | | | | | | + | + | + | + | + | + | + | + |
| ФК 09 | | | | | | | | | | | | | | | | | | | | | | | + | + | | | | | | | | | | | | | + | + |
| ФК 10 | | | | | | | | | | | | | | | | | | | + | | | + | | + | + | | | | | | | | | | | | + | + |
| ФК 11 | + | + | | + | + | + | + | | + | | + | + | + | + | + | + | + | + | | | | | | | | + | + | + | + | + | + | + | + | + | + | + | + | + |
| ФК 12 | + | | | + | + | + | + | | + | | + | + | + | + | + | + | | + | | | | | | | | + | + | | + | + | + | + | | + | | + | + | + |
| ФК 13 | + | | | + | + | | | | | | | | | | | | | | | | | | | | | | | + | | | | | + | | + | | | + | + |

## 6. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

| | ЗО 1 | ЗО 2 | ЗО 3 | ЗО 4 | ЗО 5 | ЗО 6 | ЗО 7 | ЗО 8 | ЗО 9 | ЗО 10 | ПО 1 | ПО 2 | ПО 3 | ПО 4 | ПО 5 | ПО 6 | ПО 7 | ПО 8 | ПО 9 | ПО 10 | ПО 11 | ПО 12 | ПО 13 | ПО 14 | ПО 15 | ПО 16 | ПО 17 | ПО 18 | ПО 19 | ПО 20 | ПО 21 | ПО 22 | ПО 23 | ПО 24 | ПО 25 | ПО 26 | ПО 27 | ПО 28 | ПО 29 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ПРН 01 | + | | | | | | + | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | + | + |
| ПРН 02 | | | | + | + | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | + | + |
| ПРН 03 | + | | | | | | | | + | | | | | | | | | | | | | | | | | | + | | | | | + | | + | | | + | + |
| ПРН 04 | | | + | | | + | + | + | | | | | | | | | | | | | | | | | | + | + | | | | | | | | | | + | + |
| ПРН 05 | | | | | | | + | | | | + | + | + | + | + | + | | + | | | + | | | | + | + | + | + | + | + | + | + | + | + | + | + | + |
| ПРН 06 | + | + | + | + | + | + | + | | + | | | | | | | | | | | | | | | | | | | | | | | | | | | | + | + |
| ПРН 07 | | | | | | | | + | | | | | + | + | + | + | | + | | | + | | | | | + | + | | + | | | + | | + | | | + | + |
| ПРН 08 | | | | | | + | | | | | + | + | + | | + | + | + | | | | | | + | | | + | + | | + | + | + | + | | + | | | + | + |
| ПРН 09 | | | | | | | | | + | | | | | | | | | | | | | + | | + | + | | | | | | | | | | | | + | + |
| ПРН 10 | | | | | | | | + | + | | | | + | | | | | + | + | | + | + | + | + | + | | + | | + | + | + | + | | + | | | + | + |
| ПРН 11 | | | | | | + | | + | + | | | | | | | | | + | + | | + | + | | + | + | | | | | | | | | | | | + | + |
| ПРН 12 | | | | | | | | + | + | | | | + | | | | | + | + | | + | + | + | + | + | | | | | | | | | | | | + | + |
| ПРН 13 | | | | | | | | | | | | | | | | | | | + | + | + | + | + | | | | | | | | | | | | | | + | + |
| ПРН 14 | | | | | | | | | | | | | | | | | | | + | + | + | + | | + | | | | | | | | | | | | | + | + |
| ПРН 15 | | | | | | | | | | | | | | | | | | | + | + | + | + | | | | | | | | | | | | | | | + | + |
| ПРН 16 | | | | | | | | | | | | | | | | | | | | | + | | + | + | | | | | | | | | | | | | + | + |
| ПРН 17 | | | | | | | | | | | | | | | | | | | | | | | | | + | | | | | | | | | | | | + | + |
| ПРН 18 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | + | | + | | + | | + | + |
| ПРН 19 | | | | | | | | | | | | | | | | | | | | | | | | + | | | | | | | + | + | + | + | + | + | + | + |
| ПРН 20 | | | | | | | | | | | | | | | | | | | | | | | + | + | | | | | | | | | | | | | + | + |
| ПРН 21 | | | | | | | | | | | | | | | | | | | | | | | | + | | | | | | | | | | | | | + | + |
| ПРН 22 | | | | | | | | | | | + | + | + | | + | + | | + | | | | | | | | | + | | | | + | | | | | | | |
| ПРН 23 | | | | | | | | | | | + | + | + | + | + | + | + | | | | | | | | | | | | | + | + | | | | | | | |
| ПРН 24 | | | | | | | | | | + | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ПРН 25 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | + | + | + | + | | | + | + |
| ПРН 26 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | + | + | + | + |