

**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)

Введено в дію наказом ректора від

_____ 20 __ № _____

КПІ ім. Ігоря Сікорського

Математичні методи криптографічного захисту інформації

(Mathematical Methods of Cryptographic Security)

**ОСВІТНЬО-НАУКОВА ПРОГРАМА
другого (магістерського) рівня вищої освіти**

за спеціальністю	113 Прикладна математика
галузь знань	11 Математика і статистика
кваліфікація	Магістр з прикладної математики

Київ
КПІ ім. Ігоря Сікорського
2020

ПЕРЕДМОВА

Розроблено проектною групою:

Голова проектної групи

Савчук Михайло Миколайович, член-кореспондент НАН України,
доктор фізико-математичних наук, в.о. зав. кафедри математичних
методів захисту інформації _____

Члени проектної групи:

Смирнов Сергій Анатолійович, кандидат фізико-математичних наук,
с.н.с., заступник директора ФТІ _____

Завадська Людмила Олексіївна, кандидат фізико-математичних наук,
с.н.с., доцент кафедри математичних методів захисту інформації,
гарант освітньої програми _____

Яковлев Сергій Володимирович, кандидат технічних наук,
доцент кафедри математичних методів захисту інформації _____

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

ПОГОДЖЕНО:

Науково-методична комісія КПІ ім. Ігоря Сікорського зі спеціальності
113 Прикладна математика

Голова НМКУ _____ Михайло САВЧУК
(протокол № ___ від «___» _____ 2020 р.)

Методична рада КПІ ім. Ігоря Сікорського

Голова Методичної ради _____ Юрій ЯКИМЕНКО
(протокол № ___ від «___» _____ 2020 р.)

ВРАХОВАНО

фахову експертизу стейкхолдерів:

Кудін Антон Михайлович,
заступник директора департаменту, начальник 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

Пархотік Дмитро Іванович,
начальник Департаменту банківських технологій ТОВ «Автор»

Мелько Марія Андріївна,
Голова Профбюро ФТІ, студентка 4 курсу бакалаврату
за спеціальністю 113 Прикладна математика

Ядуха Дарія Вікторівна,
студентка 2 курсу магістратури за спеціальністю 113 Прикладна математика

Курінний Олег Вікторович,
студент 2 курсу магістратури за спеціальністю 113 Прикладна математика

Рецензії-відгуки стейкхолдерів додаються.

Освітню програму обговорено після надходження всіх побажань та пропозицій від студентів та випускників ОП та схвалено на розширеному засіданні кафедри математичних методів захисту інформації
(протокол № 02/2020 від 19.02.2020 р.).

ЗМІСТ

1. Профіль освітньої програми	5
2. Перелік компонент освітньої програми	10
3. Структурно-логічна схема освітньої програми	11
4. Форма атестації здобувачів вищої освіти	11
5. Матриця відповідності програмних компетентностей компонентам освітньої програми	12
6. Матриця забезпечення програмних результатів навчання відповідними компонентами освітньої програми	12

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ

зі спеціальності 113 Прикладна математика за спеціалізацією «Математичні методи криптографічного захисту інформації»

1 – Загальна інформація	
Повна назва ЗВО та інституту/факультету	Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь – магістр Кваліфікація – магістр з прикладної математики
Рівень з НРК	НРК України – 8 рівень QF-EHEA – другий цикл EQF-LLL – 7 рівень
Офіційна назва освітньої програми	«Математичні методи криптографічного захисту інформації» другого (магістерського) рівня
Тип диплому та обсяг освітньої програми	Диплом магістра, одиничний; 120 кредитів, термін навчання 1 рік 9 місяців
Наявність акредитації	Сертифікат МОН серія НД № 1192616 (070918) від 25.09.2017. Термін дії – до 01.07.2023 р.
Передумови	Наявність ступеня бакалавра
Мова(и) викладання	Українська / англійська
Термін дії освітньої програми	До наступної акредитації
Інтернет-адреса постійного розміщення освітньої програми	https://osvita.kpi.ua/node/103 http://mmis.ipt.kpi.ua
2 – Мета освітньої програми	
Мета освітньої програми полягає у підготовці професіоналів у галузі математики, статистики, інформаційних технологій, інформаційної безпеки та криптології, здатних формулювати, аналізувати та розв'язувати складні спеціалізовані задачі, а також теоретичні та практичні проблеми прикладної математики 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.	

3 – Характеристика освітньої програми

Предметна область	<p><i>Об’єкт діяльності:</i> математичні методи, моделі, алгоритми та програмне забезпечення, що призначені для дослідження, аналізу, проектування процесів та систем в різноманітних конкретних предметних областях.</p> <p><i>Цілі навчання:</i> підготовка спеціалістів, здатних:</p> <ul style="list-style-type: none"> – використовувати та впроваджувати математичні методи та технології в галузі прикладної математики; – формулювати, розв’язувати й узагальнювати теоретичні та практичні задачі з використанням фундаментальних та спеціальних прикладних методів математичних та комп’ютерних наук; – розв’язувати задачі математичного моделювання процесів і явищ в умовах невизначеності та неповноти інформації щодо функціонування системи об’єктів; – будувати, досліджувати та застосовувати математичні моделі, що ґрунтуються на даних та на знаннях, створювати та експлуатувати програмне забезпечення. <p><i>Теоретичний зміст предметної області:</i> математичні методи, що застосовуються в науці, інженерії, бізнесі та промисловості, а також алгоритми і програмні засоби їх реалізації.</p> <p><i>Методи, методика та технології:</i> прикладні математичні методи та алгоритми; методики вирішення інженерних, наукових, соціально-економічних задач за допомогою спеціалізованих програмних засобів; інформаційні технології проведення комп’ютерного моделювання та обчислювального експерименту, інтелектуального аналізу даних.</p> <p><i>Інструменти та обладнання:</i> спеціалізовані програмні, апаратні та програмно-апаратні засоби та комплекси для моделювання об’єктів та систем, проведення обчислювальних експериментів тощо; комп’ютеризовані системи у професійній та навчальній діяльності.</p>
Орієнтація освітньої програми	Освітньо-наукова
Основний фокус освітньої програми та спеціалізації	<p><i>Базовий фокус ОП</i> – математичні моделі, методи, алгоритми для задач комп’ютерних наук та криптографічного захисту інформації</p> <p><i>Ключові слова:</i> математичні методи, алгоритми, криптологія, криптографія, шифрування, цифровий підпис, геш-функція, криптографічний захист інформації</p>
Особливості програми	Проходження науково-дослідної практики та виконання спільних проектів на замовлення державних, науково-дослідних установ та провідних ІТ-компаній України за фахом, дуальна освіта

4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Відповідно до Державного класифікатору професій ДК 003:2010, випускники можуть працювати на посадах, що відповідають таким класифікаційним угрупованням: 2121.2 Математик (прикладна математика); 2132.2 Програміст прикладний; 2139.1 Науковий співробітник (галузь обчислень); 2121.1 Науковий співробітник-консультант (математика). Випускники ОП можуть працювати спеціалістами з криптографічного захисту інформації та/або ІТ-технологій, аналітиками даних, розробниками програмних засобів, прикладними програмістами, консультантами із застосування методів математики і статистики для розв'язання прикладних задач широкого спектру, науковими співробітниками.
Подальше навчання	Продовження освіти за третім (освітньо-науковим) 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 (індивідуальні та у малих групах); курсові проекти та роботи; технологія змішаного навчання за окремими освітніми компонентами; науково-дослідна практика; виконання дипломної роботи (магістерської дисертації).
Оцінювання	Оцінювання знань студентів здійснюється у відповідності до Положення про рейтингову систему оцінювання результатів навчання студентів КПІ ім. Ігоря Сікорського за усіма видами аудиторної та позааудиторної роботи (вхідний, поточний, рубіжний, підсумковий контроль): усні та письмові екзамени, тестування, колоквиуми тощо. Рівень знань по кожній дисципліні оцінюється згідно критеріїв, визначених у Рейтинговій системі оцінювання даної дисципліни.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати складні задачі та проблеми у галузі математики та статистики або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.
Загальні компетентності (ЗК)	
ЗК1	Здатність до абстрактного мислення, аналізу і синтезу
ЗК2	Здатність до самонавчання; пошуку, оброблення, співставлення та аналізу інформації з різних джерел
ЗК3	Здатність розробляти рішення у відповідності з нормами інтелектуальної власності
ЗК4	Здатність керувати проектами, забезпечувати рішення задач у відповідності із принципами сталого розвитку суспільства
ЗК5	Міжособистісні навички та вміння, здатність до наукової комунікації іноземною мовою
ЗК6	Здатність прийняття обґрунтованих рішень, представлення та донесення знань та ідей до широкого загалу
ЗК7	Здатність здійснювати науково-дослідну діяльність

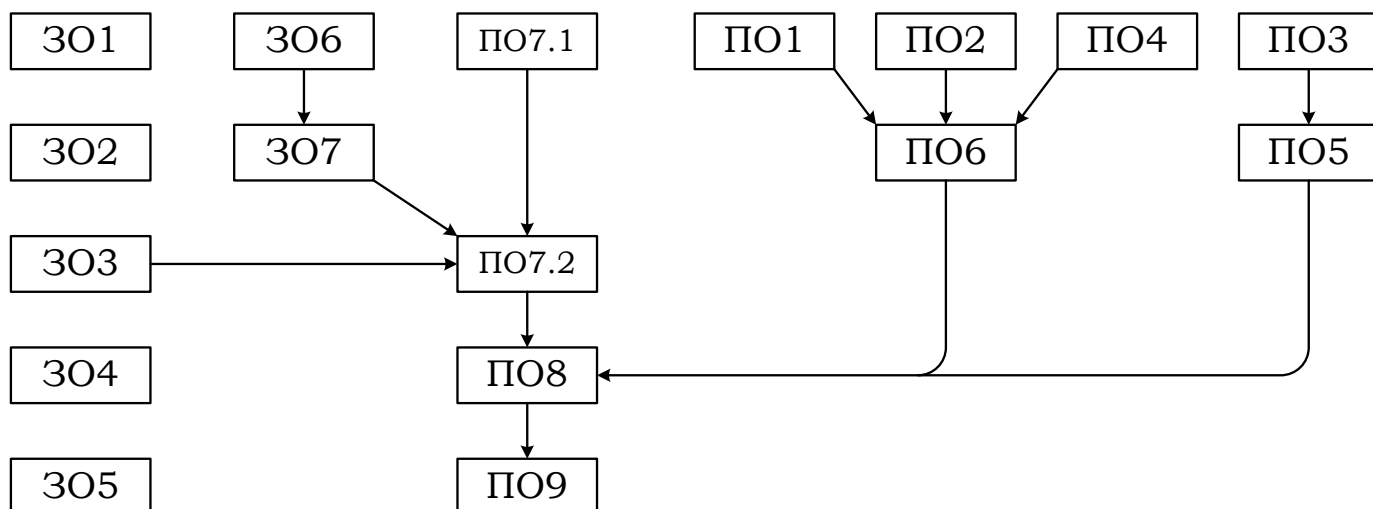
ЗК8	Здатність готувати та здійснювати публічні виступи з презентацією отриманих результатів, готувати науково-технічні публікації (звіти, статті тощо) за результатами виконаних досліджень, в тому числі іноземною мовою
Фахові компетентності спеціальності (ФК)	
ФК1	Здатність використовувати математичний апарат, розробляти моделі та методи для розв'язання задач широкого спектру з обробки інформації та моделювання складних систем.
ФК2	Здатність провадити теоретичний та практичний аналіз сучасних криптографічних систем
ФК3	Здатність розроблювати новітні механізми криптографічного захисту
ФК4	Здатність проектувати, розроблювати та реалізовувати системи криптографічного захисту з урахуванням сучасних досягнень науки та існуючої правової та нормативної бази
ФК5	Здатність використовувати та впроваджувати існуючі механізми, протоколи та системи криптографічного захисту інформації
ФК6	Розуміння основ організації наукової діяльності, здатність досліджувати наукові проблеми за фахом
ФК7	Здатність пропонувати практичні рішення за фахом з урахуванням сучасних досягнень науки
ФК8	Здатність провадити педагогічну діяльність у вищій освіті
7 – Програмні результати навчання	
РН 1	Використовувати математичний апарат, розробляти моделі та методи для розв'язання задач широкого спектру з обробки інформації та моделювання складних систем.
РН 2	Знаходити, вивчати та аналізувати науково-технічну інформацію, вітчизняний й іноземний досвід, пов'язаний із професійною проблематикою; керуватись в професійній діяльності принципами інтелектуальної власності
РН 3	Складати наукові звіти із виконаних науково-дослідних робіт та впроваджувати на практиці результати проведених досліджень і розробок, доповідати та публікувати результати досліджень (у тому числі іноземними мовами), проводити патентний пошук, здійснювати патентування.
РН 4	Керувати проектами, організовувати власну професійну діяльність згідно із принципами сталого розвитку суспільства
РН 5	Проводити аналіз криптографічних алгоритмів, протоколів та систем
РН 6	Орієнтуватись у останніх досягненнях криптології
РН 7	Розроблювати нові криптографічні алгоритми, механізми та системи захисту
РН 8	Керуватись законами, стандартами, технічними специфікаціями та нормативними документами у галузі
РН 9	Розроблювати та аналізувати алгоритми у класичній та квантовій моделях обчислень
РН 10	Проводити педагогічну діяльність у вищій освіті
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Відповідно до кадрових вимог щодо забезпечення провадження освітньої діяльності для відповідного рівня ВО (додаток 2 до Ліцензійних умов), затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 із змінами, внесеними згідно з Постановою Кабінету Міністрів України №347 від 10.05.2018 р.

Матеріально-технічне забезпечення	Відповідно до технологічних вимог щодо матеріально-технічного забезпечення освітньої діяльності відповідного рівня ВО (додаток 4 до Ліцензійних умов), затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 із змінами, внесеними згідно з Постановою Кабінету Міністрів України №347 від 10.05.2018 р.
Інформаційне та навчально-методичне забезпечення	Відповідно до технологічних вимог щодо навчально-методичного та інформаційного забезпечення освітньої діяльності відповідного рівня ВО (додаток 5 до Ліцензійних умов), затверджених Постановою Кабінету Міністрів України від 30.12.2015 р. № 1187 із змінами, внесеними згідно з Постановою Кабінету Міністрів України №347 від 10.05.2018 р. Користування Науково-технічною бібліотекою КПІ ім. Ігоря Сікорського
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	Викладання іноземною мовою

2. ПЕРЕЛІК КОМПОНЕНТІВ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
1. Нормативні освітні компоненти			
1.1. Цикл загальної підготовки			
ЗО 1	Інтелектуальна власність та патентознавство	3	Залік
ЗО 2	Навчальна дисципліна з проблем сталого розвитку*	2	Залік
ЗО 3	Практикум іншомовного наукового спілкування	4,5	Залік
ЗО 4	Навчальна дисципліна з менеджменту*	3	Залік
ЗО 5	Навчальна дисципліна з педагогіки*	2	Залік
ЗО 6	Інтелектуальний аналіз даних	4	Екзамен
ЗО 7	Моделювання складних систем	4	Екзамен
1.2. Цикл професійної підготовки			
ПО 1	Методи криптоаналізу	7	Екзамен
ПО 2.1	Методи реалізації криптографічних механізмів	4	Екзамен
ПО 2.2	Методи реалізації криптографічних механізмів (курсова робота)	1	Залік
ПО 3	Сучасні алгебраїчні криптосистеми	3	Залік
ПО 4	Організаційні аспекти криптографії	3,5	Залік
ПО 5	Квантові обчислення та квантова криптографія	4	Екзамен
ПО 6.1	Проектування, розробка і реалізація криптографічних систем	4	Екзамен
ПО 6.2	Проектування, розробка і реалізація криптографічних систем (курсова робота)	1	Залік
Дослідницький (науковий) компонент			
ПО 7	Наукова робота за темою магістерської дисертації:		
ПО 7.1	1. Основи наукових досліджень	2	Залік
ПО 7.2	2. Науково-дослідна робота за темою магістерської дисертації	7,5	Залік
ПО 8	Науково-дослідна практика	9	Залік
ПО 9	Робота над магістерською дисертацією	21	Захист
2. Вибіркові освітні компоненти			
2.2. Цикл професійної підготовки			
(Вибіркові освітні компоненти з факультетського каталогу)			
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	Екзамен
ПВ 4	Освітній компонент 4 Ф-Каталогу	5	Екзамен
ПВ 5	Освітній компонент 5 Ф-Каталогу	5,5	Екзамен
ПВ 6	Освітній компонент 6 Ф-Каталогу	5	Залік
ПВ 7	Освітній компонент 7 Ф-Каталогу	3	Залік
Загальний обсяг обов'язкових компонентів:		89,5	
Загальний обсяг вибірових компонентів:		30,5	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ:		120	

3. СТРУКТУРНО-ЛОГІЧНА СХЕМА ОСВІТНЬОЇ ПРОГРАМИ



Розгорнута структура освітньої програми розташована на сайті кафедри ММЗІ за адресою <http://mmis.ipt.kpi.ua/navchalni-plani>

4. ФОРМА ВИПУСКНОЇ АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Випускна атестація здобувачів вищої освіти за освітньою програмою спеціальності 113 Прикладна математика проводиться у формі захисту магістерської дисертації та завершується видачею документа встановленого зразка про присудження йому ступеня магістра з присвоєнням кваліфікації «Магістр з прикладної математики».

Випускна атестація здійснюється відкрито і публічно. Кваліфікаційні роботи (магістерські дисертації) перевіряються на ознаки порушення академічної доброчесності та після захисту публікуються в репозиторії НТБ Університету для вільного доступу.

5. МАТРИЦЯ ВІДПОВІДНОСТІ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

	ЗК								ФК							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
ЗО 1		+	+													
ЗО 2		+		+												
ЗО 3		+			+	+		+								
ЗО 4		+		+												
ЗО 5		+														+
ЗО 6	+	+				+			+							
ЗО 7	+	+							+							
ПО 1	+	+			+				+	+	+					
ПО 2		+		+	+					+	+	+	+		+	
ПО 3	+	+			+				+	+	+		+			
ПО 4		+						+			+	+				
ПО 5	+	+							+	+	+					
ПО 6		+		+	+					+	+	+	+		+	
ПО 7.1	+	+						+	+					+		
ПО 7.2	+	+				+	+	+			+			+		
ПО 8	+	+						+	+		+				+	
ПО 9	+	+						+	+		+				+	

6. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ ВІДПОВІДНИМИ КОМПОНЕНТАМИ ОСВІТНЬОЇ ПРОГРАМИ

	РН									
	1	2	3	4	5	6	7	8	9	10
ЗО 1		+	+							
ЗО 2				+						
ЗО 3		+								
ЗО 4				+						
ЗО 5										+
ЗО 6	+									
ЗО 7	+									
ПО 1	+				+	+			+	
ПО 2		+	+		+	+	+			
ПО 3	+				+	+				
ПО 4		+			+	+		+		
ПО 5	+				+	+			+	
ПО 6		+	+		+	+	+			
ПО 7.1		+								
ПО 7.2		+								
ПО 8		+	+				+			
ПО 9		+	+				+			