

# ІНСТИТУТ КІБЕРНЕТИКИ ІМЕНІ В.М.ГЛУШКОВА НАН УКРАЇНИ

«ЗАТВЕРДЖУЮ»

Директор Інституту кібернетики  
імені В.М. Глушкова НАН України  
академік НАН України



*Сергієнко* І.В. Сергієнко

«*22*» *07* 2020 року

## РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ КОМП'ЮТЕРНА КРИПТОГРАФІЯ (ДВА.3.02.05)

для здобувачів освітньо-наукового рівня «доктор філософії»

галузь знань	11 “Математика та статистика”
спеціальність	113 “Прикладна математика”
освітній рівень	третій (освітньо-науковий)
освітньо-наукова програма	“Прикладна математика”
вид дисципліни	вибіркова

Форма навчання	денна / заочна
Навчальний рік	2020/2021
Рік навчання	2
Кількість кредитів ECTS	4
Мова викладання, навчання та оцінювання	українська
Форма заключного контролю	екзамен

Викладачі: **Задірака Валерій Костянтинович**, академік НАН України, д.ф.-м.н., професор

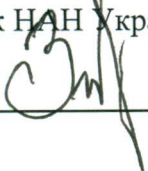
Пролонговано Вченою радою Інституту кібернетики імені В.М. Глушкова НАН України

Навчальні роки пролонгації	Учений секретар	Підпис	№ протоколу	Дата протоколу
20___/20___ р.	_____	_____	_____	_____
20___/20___ р.	_____	_____	_____	_____
20___/20___ р.	_____	_____	_____	_____
20___/20___ р.	_____	_____	_____	_____

**КИЇВ – 2020**

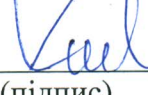
**РОЗРОБНИК:**

Завідувач відділу оптимізації  
чисельних методів  
академік НАН України, д.ф.-м.н., професор

  
Задірака Валерій Костянтинович


**Робочу програму розглянуто та схвалено на засіданні відділу чисельних методів та комп'ютерного моделювання**

Протокол від "08" 07 2020 року № 7

Завідувач відділу  
член-кор. НАН України, д.ф.-м.н.  О.М. Хіміч  
(підпис)

**Робочу програму ухвалено науково-методичною радою**

Протокол від "15" 07 2020 року № 3

Голова науково-методичної ради  
академік НАН України  І.В. Сергієнко  
(підпис)


**Робочу програму затверджено Вченою радою Інституту кібернетики імені В.М. Глушкова НАН України**

Протокол від "28" 07 2020 року № 13

Учений секретар  А.І. Куляс  
(підпис)

**Робочу програму погоджено з гарантом освітньої програми 113 «Прикладна математика»**

"15" 07 2020 року

Гарант освітньої програми  
академік НАН України  І.В. Сергієнко  
(підпис)

1.

，  
；  
，

2.

:

1.

:

，

2.

:

，

3.

:

“ ”

，

，

，

，

，

，

，

，

，

3.

(

):

，

，

(

)

«

».

；

：

，

5.

:

(1. ; 2. ; 3. ; 4. )		( / )	( )	
1.1		，	，	20%
1.2				
1.3				20%
1.4				
2.1		，	，	20%

2.2				20%
2.3				5%
3.1				5%
4.1				5%
4.2				5%

**6.**

	1.1	1.2	1.3	1.4	2.1	2.2	2.3	3.1	4.1	4.2
( )										
-2. -	+	+	+	+	+	+	+			
-5. ,	+	+	+	+	+	+	+			
-6. , , , , -			+	+	+	+	+	+		
-8. , -				+	+	+	+	+	+	+
-13. i	+	+	+	+	+					
-16. , ( , - ) ,						+	+	+	+	+

**7.**

**7.1.**

-

- 1. : PH1.1, PH1.2, PH1.3, PH1.4– 10 /6 ;
- 2. : PH2.1, PH2.2 – 20 /12 ;
- 3. : PH2.1, PH2.2, PH3.1, PH4.1, PH4.2 – 30 /18 ;

-

- : 40 ;
- : PH1.1, PH1.2, PH1.3, PH1.4;
- :

**7.2.**

1 1-3, 2– 4–6 3– 7–9.

- 1. ;
- 2. ;
- 3. : 9 .

**7.3.**

/ Excellent	90-100
/ Good	75-89
/ Satisfactory	60-74
/ Fail	0-59

8.

<b>1. „ ’ ”</b>				
1	<b>1.</b> : DES, -28147, SKIPJACK.	2		8
2	<b>2.</b> : RSA.	2		12
3	<b>3.</b> :	2		8
4	<b>4.</b> :	2		12
5	<b>5.</b> :	2		8
<b>2. „ ’ ”</b>				
6	<b>6.</b> :	2		12
7	<b>7.</b> :	2		12
<b>3. „ ’ ”</b>				
8	<b>8.</b> :	2		12
9	<b>9.</b> :	2		12
			4	
		18	4	96

120 , :  
 -18 ,  
 -4 ,  
 -2 ,  
 -96 .

**9.**

1. :  
« », 2002.
2. :  
, 2000.
3. :  
« », 2003.

1. . - . « », 2002.
2. :  
. - , « », 2010.