

«

»

“ ”

“ ”
_____ .

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ Криптографические методы защиты информации

: 09.04.01

,

:

: 1, : 2

,

		2
1	()	3
2		108
3	, .	47
4	, .	0
5	, .	18
6	, .	18
7	, .	8
8	, .	0
9	, .	2
10	, .	9
11	, .	61
12	(, ()/ ,)	
13		

(): 09.04.01

554 09.11.2009 . : 15743,
: 18.12.2009 .

: 1,

(): 09.04.01

, 6 21.06.2017
, 6 21.06.2017

, 6 21.06.2017

:

, . -

:

,
. . .,

:

. . .

1.

1.1

	: .4
	: .9
	-
	: .2, , ,
	: .2, , ,
	: .2
	: .2
	: .2
	: .2
	: .3
	: .3

2.

,

2.1

.2. 2	; ;
.2. 2 , ,	; ;
.2. 5 , , ,	; ;
.2. 4	; ;
.2. 5 ,	; ;
.2. 6	; ;
.3. 2	; ;

3. 4 (), ,	; ;
4. 1 -	; ;
9. 1 , , , ,	; ;

3.

3.1

		“ .	, .		
: 2					
:					
7. 34.10	6	0	2	4. 1, 9. 1, .2 . -1.2, .2 . 2, .2/ . -1.5, .2 / . 4, . 2/ . 5, .2/ . 6, .3/ . -1. 2, .3/ . 4	
:					
5. DES, AES,	4	0	2	4. 1, 9. 1, .2 . -1.2, .2 . 2, .2/ . -1.5, .2 / . 4, . 2/ . 5, .2/ . 6, .3/ . -1. 2, .3/ . 4	DES, AES,
:					
6. RSA	4	0	2	4. 1, 9. 1, .2 . -1.2, .2 . 2, .2/ . -1.5, .2 / . 4, . 2/ . 5, .2/ . 6, .3/ . -1. 2, .3/ . 4	RSA

8.	RSA	4	0	2	.4. 1, .9. 1, .2 . -1.2, .2 . 2, .2/ . -1.5, .2 / . 4, . 2/ . 5, .2/ . 6, .3/ . -1. 2, .3/ . 4	RSA
----	-----	---	---	---	--	-----

: 2						
:						
1.	DES, , AES	4	0	0	.4. 1, .9. 1, .2 . -1.2, .2 . 2, .2/ . -1.5, .2 / . 4, . 2/ . 5, .2/ . 6, .3/ . -1. 2, .3/ . 4	DES, , AES
2.	RSA	4	0	0	.4. 1, .9. 1, .2 . -1.2, .2 . 2, .2/ . -1.5, .2 / . 4, . 2/ . 5, .2/ . 6, .3/ . -1. 2, .3/ . 4	RSA
3.	34.10	6	0	0	.4. 1, .9. 1, .2 . -1.2, .2 . 2, .2/ . -1.5, .2 / . 4, . 2/ . 5, .2/ . 6, .3/ . -1. 2, .3/ . 4	34.10

3.3

$$- \frac{1}{\sqrt{\pi}} \int_0^x \frac{e^{-t^2}}{t} dt, \quad (3.4).$$

3.4

	-
	e-mail;
	e-mail

4.

(), 15- ECTS.

4.1

: 2	
Лабораторная:	30
() " . . . - ; [. . .]. - , 2010. - 35, [1] . : .. - : http://elibrary.nstu.ru/source?bib_id=vtls000146768	
Практические занятия:	30
() " . . . - ; [. . .]. - , 2010. - 35, [1] . : .. - : http://elibrary.nstu.ru/source?bib_id=vtls000146768	
РГЗ/Реферат:	20
() " . . . - ; [. . .]. - , 2010. - 35, [1] . : .. - : http://elibrary.nstu.ru/source?bib_id=vtls000146768	
Зачет:	20
() " . . . - ; [. . .]. - , 2010. - 35, [1] . : .. - : http://elibrary.nstu.ru/source?bib_id=vtls000146768	

4.2

.

4.2

		/	/	
.4	.4 1. -	+	+	+
.9	.9 1. , , , ,	+	+	+
.2	.2 2.	+	+	+

	.2 2.		+	+	+
.2/	.2/ 5.		+	+	+
	.2/ 4.		+	+	+
	.2/ 5.		+	+	+
	.2/ 6.		+	+	+
.3/	.3/ 2.		+	+	+
	.3/ 4.		+	+	+

1

7.

1. Лапони́на О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : курс лекций : учебное пособие для вузов по специальности 510200 "Прикладная математика и информатика" / О. Р. Лапони́на ; под ред. В. А. Сухомли́на. - М., 2005. - 604, [1] с. : ил., табл.
2. Осипян В. О. Криптография в задачах и упражнениях / В. О. Осипян, К. В. Осипян. - М., 2004. - 143 с.
3. Котов Ю. А. Криптографические методы защиты информации. Шифры : учебное пособие / Ю. А. Котов ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 57, [1] с.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000232326

1. Баричев С. Г. Основы современной криптографии : учебный курс / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. - М., 2002. - 175 с. : ил.
2. Кузьминов Т. В. Криптографические методы защиты информации / Т. В. Кузьминов ; отв. ред. В. А. Евстигнеев. - Новосибирск, 1998. - 185 с. : ил.

8.

8.1

1. Минин И. В. Криптографические методы защиты информации : учебно-методическое пособие / И. В. Минин, О. В. Минин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2009. - 31, [1] с. : табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000121807
2. Методы и средства защиты компьютерной информации. Ч. 1 : методические указания к лабораторным работам для 4 курса АВТФ / Новосиб. гос. техн. ун-т ; [сост. Ю. А. Котов]. - Новосибирск, 2010. - 35, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000146768

8.2

- 1 Операционная система Microsoft Windows
- 2 Пакет офисных приложений Microsoft Office

8.3

9. -

1	(- , ,)	

1	(Internet)	