

«

»

“

”

“ ”
_____ .

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ Программные средства защиты информации

: 02.04.03

, :

: 2, : 3

,

		3
1	()	3
2		108
3	, .	68
4	, .	18
5	, .	0
6	, .	36
7	, .	0
8	, .	0
9	, .	2
10	, .	12
11	, .	40
12	(, ()/ ,)	
13		

(): 02.04.03

0 . 812 22.12.2009 ., : , :

: 1,

(): 02.04.03

, 4 21.06.2017

, 6 21.06.2017

:

:

,

:

. . .

		" .	, .		
:3					
:					
1.	2	0	0	.10. 7, .11. 1, .4. -1.1, .4. -1.5	, , , . .2 . , , , , , ,

2.	2	0	0	.11. 1	" " " , " " " " ? 3 ,4 . . . 4 (). .
:					
3.	3	0	0	.10. 7, .4. -1.5, .1/ . 1	AES, DES.

:					
2					
4.	2	0	0	.11. 1, .1/ . 1	.
5.	3	0	0	.10. 7, .11. 1, .4. -1.1, .4. -1.5, .1/ . 1	RSA.
:					
6.	2	0	0	.10. 7, .11. 1, .4. -1.1, .4. -1.5	. 4 - . 3
:					

7.	2	0	0	.10. 7, .11. 1, .4. -1.1, .4. -1.5, .1/ . 1	(MAC).
----	---	---	---	---	--------

:					
8.	2	0	0	.11. 1, .4. -1.1, .4. -1.5, .1/ . 1	5

		„ .	, .		
: 3					
: 1					
1. n-	5	0	0	.4. -1.1, .1/ . 1	

2. ()	5	0	0	.4. -1.1, .1/ . 1	,
3. (DES 28147-89)	5	0	0	.4. -1.1, .1/ . 1	DES 28147 89.
4. .	5	0	0	.4. -1.1, .1/ . 1	DES 28147 89.
: 2					
5. . n. -	6	0	0	.4. -1.1, .1/ . 1	, n. -
6. DES/ RSA (RSA)	5	0	0	.4. -1.1, .1/ . 1	RSA. ,
:					

7.	5	0	0	.4. -1.1, .1/ . 1	,
----	---	---	---	----------------------	---

3.2

3.3

: 3				
1		.10. 7, .11. 1, .4. -1.5, .1/ . 1	30	6
<p>, []:</p> <p>- , [2017]. - : http://elibrary.nstu.ru/source?bib_id=vtls000234876. -</p> <p>2 02.04.03 -</p> <p>, -</p> <p>/ . . - ;[. . . ,</p> <p>. . .]. - , 2017. - 96 . : .. -</p> <p>http://elibrary.nstu.ru/source?bib_id=vtls000235031</p> <p>5</p> <p>" / . . . - ;[. . .]. -</p> <p>, 2005. - 68, [1] . : .. -</p> <p>http://elibrary.nstu.ru/source?bib_id=vtls000043534</p> <p>[]: - / . . , . . ,</p> <p>; . . . - . - , [2011]. -</p> <p>http://elibrary.nstu.ru/source?bib_id=vtls000160644. -</p>				
2		.10. 7, .11. 1, .4. -1.5, .1/ . 1	10	6

« : . - » []: -
/ . . ; . . - , [2011]. - :
http://elibrary.nstu.ru/source?bib_id=vtls000162770. - . .
[]: - /
. . ; . . - , [2017]. -
: http://elibrary.nstu.ru/source?bib_id=vtls000234876. -
: 2
02.04.03 -
,
/
. . . - ; [: . . , . .
]. - , 2017. - 96 .: .. - :
http://elibrary.nstu.ru/source?bib_id=vtls000235031 :
5
" / . . - ; [. . .]. -
, 2005. - 68, [1] .: ., .. - :
http://elibrary.nstu.ru/source?bib_id=vtls000043534 . .
[]: - / . . , . . ,
. . ; . . - , [2011]. - :
http://elibrary.nstu.ru/source?bib_id=vtls000160644. - .

3.3

, (. 3.4).

3.4

	-
	: http://ami.nstu.ru/~gulyaeva
	e-mail: t.gulyaeva@corp.nstu.ru
	: http://ami.nstu.ru/~gulyaeva

4.

(),

15-

ECTS.

. 4.1.

4.1

	.	
: 3		
Лабораторная:	30	60
2 () " 02.04.03 - : / . . - ; [: . . , . . .]. - , 2017. - 96 .: .. - : http://elibrary.nstu.ru/source?bib_id=vtls000235031 "		
Экзамен:	20	40
() " . . . []: - / . . , . . . - ; . . . - , [2017]. - : http://elibrary.nstu.ru/source?bib_id=vtls000234876 . - .		

.10	.10 7.	+
.11	.11 1.	+
.4	.4 1.	+
	.4 5.	+
.1/	.1/ 1.	+

1

7.

1. Нортроп Т. Основы разработки приложений на платформе Microsoft .NET Framework : экзамен-536 MCTS / Тони Нортроп, Шон Уилдермьюс, Билл Райан ; [пер. с англ. А. Е. Соловченко]. - М. СПб., 2007.- 842 с. : ил. + 1 CD-ROM.

2. Грибунин В. Г. Комплексная система защиты информации на предприятии : [учебное пособие для вузов по специальностям "Организация и технология защиты информации", "Комплексная защита объектов информации" направления подготовки "Информационная безопасность"] / В. Г. Грибунин, В. В. Чудовский. - Москва, 2009. - 411, [1] с. : ил., табл.

3. ЭБС Издательство «Лань» [Электронный ресурс] : электронно-библиотечная система. - [Россия], 1993. - Режим доступа: <http://e.lanbook.com>. - Загл. с экрана.

4. Долозов Н. Л. Программные средства защиты информации : конспект лекций для 2 курса ФПМИ по направлению "Математическое обеспечение и администрирование информационных систем" (02.04.03), магистерская программа, "Математическое и программное обеспечение информационных технологий" / Н. Л. Долозов, Т. А. Гуляева ; Новосиб. гос. техн. ун-т. - Новосибирск, 2015. - 60, [2] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000222753

1. Галатенко В. А. Основы информационной безопасности : курс лекций : учебное пособие для студентов вузов, обучающихся по специальностям в области информационных технологий / В. А. Галатенко ; под ред. В. Б. Бетелина. - Москва, 2006. - 205 с. : ил.

2. Галатенко В. А. Стандарты информационной безопасности : курс лекций : учебное пособие для студентов вузов, обучающихся по специальностям в области информационных технологий / В. А. Галатенко ; под ред. В. Б. Бетелина. - Москва, 2006. - 262, [1] с. : табл.

3. Столлингс В. Основы защиты сетей. Приложения и стандарты / Вильямс Столлингс ; [пер. с англ. и ред. А. Г. Сивака]. - М. ; СПб. ; Киев, 2002.- 429 с. : ил.

4. Галицкий А. В. Защита информации в сети - анализ технологий и синтез решений / Галицкий А. В., Рябко С. Д., Шаньгин В. Ф.. - М., 2004.- 613 с. : ил.

5. Мао В. Современная криптография : теория и практика / Венбо Мао ; [пер. с англ. и ред. Д. А. Ключина]. - М. [и др.], 2005. - 763 с. : ил., табл.

6. Зензин О. С. Стандарт криптографической защиты - AES. Конечные поля / О. С. Зензин, М. А. Иванов. - М., 2002. - 174 с. : ил.
7. 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.
8. Столлингс В. Криптография и защита сетей. Принципы и практика : пер. с англ. / Вильямс Столлингс. - М., 2001. - 669 с. : ил.
9. Фомичев В. М. Методы дискретной математики в криптологии / В. М. Фомичев. – М. : Диалог-МИФИ, 2010. – 424 с.
10. Баричев С. Г. Основы современной криптографии : учебный курс / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. - М., 2002. - 175 с. : ил.
11. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко. – 2-е изд., доп. – М. : МЦНМО, 2006 – 336 с.
12. Фергюсон Нильс. Практическая криптография : [пер. с англ.] / Нильс Фергюсон, Брюс Шнайер. - М. : Диалектика : Вильямс, 2005. - 421 с.
13. Криптография. Скоростные шифры / А. А. Молдовян, Н. А. Молдовян, Н. Д. Гуц, Б. В. Изотов. – СПб. : БХВ-Петербург, 2002. – 493 с.
14. Вельшенбах М. Криптография на Си и С++ в действии : [учеб. пособие] / М. Вельшенбах. – М. : Триумф, 2004. – 461 с. : ил.; 24 см + компакт-диск. - (Практика программирования).
15. Шнайер Б. Прикладная криптография : Протоколы, алгоритмы, исход. тексты на яз. Си / Б. Шнайер. – М. : Триумф, 2002. – 815 с. : ил. – (Знания и опыт экспертов).

8.

,

8.1

1. Программные средства защиты информации : методические указания к выполнению лабораторных работ для 5 курса по специальности "Прикладная математика и информатика" / Новосиб. гос. техн. ун-т ; [сост. Н. Л. Долозов]. - Новосибирск, 2005. - 68, [1] с. : ил., табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000043534
2. Курлаев С. А. Программные средства защиты информации [Электронный ресурс] : учебно-методическое пособие / С. А. Курлаев, Т. А. Гультяева, Н. Л. Долозов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2011]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000160644. - Загл. с экрана.
3. Гультяева Т. А. Расчетно-графическая работа по курсу «Программные средства защиты информации» [Электронный ресурс] : учебно-методическое пособие / Т. А. Гультяева ; Новосиб. гос. техн. ун-т. - Новосибирск, [2011]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000162770. - Загл. с экрана.
4. Гультяева Т. А. Программные средства защиты информации [Электронный ресурс] : электронный учебно-методический комплекс / Т. А. Гультяева, Н. Л. Долозов, С. А. Курлаев ; Новосиб. гос. техн. ун-т. - Новосибирск, [2017]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234876. - Загл. с экрана.
5. Программные средства защиты информации : методические указания к выполнению лабораторных работ для 2 курса ФПМИ образовательной программы 02.04.03 - Математическое обеспечение и администрирование информационных систем, магистерские программы - Математическое и программное обеспечение информационных технологий и Математическое обеспечение информационных систем в экономике / Новосиб. гос. техн. ун-т ; [сост.: Н. Л. Долозов, С. А. Курлаев, Т. А. Гультяева]. - Новосибирск, 2017. - 96 с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000235031

8.2

- 1 Пакет офисных приложений Microsoft Office
- 2 Интегрированная среда разработки Microsoft Visual Studio
- 3 Design Science MathType

8.3

,
- .

9. -

1	(- , ,)	

1	(Internet)	