-

23 2022

Рабочая программа дисциплины
Б1.В.ДВ.07.01 Основы криптографии

01.03.02 Прикладная математика и информатика
Математическое и информационное моделирование

4

8

2, 72

-

16

2022

1. Место дисциплины в структуре ОП

.

2. Планируемые результаты обучения по дисциплине

ПК-1. -	**Знает** - **Умеет** - **Владеет** -
ПК-2.	**Знает** - **Умеет**

	Владеет
ПК-3.	**Знает** - ; - **Умеет** **Владеет**

3. Содержание дисциплины

1. **Основные задачи и понятия криптографии.**

2. **Блочные шифры замены.**
   Lucifer DES.
   -28147-89.
3. **Основные понятия математической теории информации.**

4. **Надёжность шифров.**

5. **Методы синтеза шифрсистем.**

6. **Имитостойкость шифров.**

4. Тематический план

1		4	2			2
2		14	4		4	6
3		14	4		4	6
4	.	16	4		6	6
5		12	2		6	4
6		12	2		6	4
		72	18		26	28

5. Виды образовательной деятельности

Лекции

1. **Основные задачи и понятия криптографии.**

2-3. Блочные шифры замены.
Lucifer
DES -28147-89.

4-5. Основные понятия математической теории информации.

.

6-7. Надёжность шифров.

8. Методы синтеза шифрсистем.

9. Имитостойкость шифров.

.

Лабораторные работы

Лабораторное занятие №1-2

Лабораторное занятие №3-4

1. Lucifer.

Лабораторное занятие №5-6

DES.

Лабораторное занятие №7-8

1. AES.

Лабораторное занятие №9-10

1

Лабораторное занятие №11-13

Самостоятельная работа

1. **Основные задачи и понятия криптографии.**

2. **Блочные шифры замены.** -28147-89.

3. **Основные понятия математической теории информации.**

.

4. **Надёжность шифров.**

5. **Методы синтеза шифрсистем.**

9. Имитостойкость шифров. .

6. Критерии оценивания результатов освоения дисциплины (модуля)

6.1. Оценочные средства и критерии оценивания для текущей аттестации

Вопросы к лекциям 1-3

1.
2.
3.
4.
5.

6.
7.
8.
9.
10.
11.
12.
13. s p-

Вопросы к лекциям 2-3

1.
2.
3.
4.
5.
6.
7.

8.
9.
10. m-

Вопросы к лекциям 4-5

1.
2.
3.
4.
5.
6.
7.
8. a b?
9.
10.
11.
12.
13.
14.
15.

Вопросы к лекциям 5-6

1.

2.
3.
4.
5.
6.
7.
8.

9.
10.
11.
12. α β
13.
14.

15.

Вопросы к лекциям 7-9

1.
2.
3.
4.
5.
6.
7.
8.
9.

10.
11.
12.
13.
14.
15.
16.
17.
18.
19.
20.
21.
22.
23.
24.
25.
26. -
27.

Вопросы к лекции 10

1.
2.
3.
4.
5.
6.

Критерии оценивания вопросов

1.

		*)

1		
2		

(*)
2.

3

Задания для лабораторных занятий

(www.moodle.smolgu.ru).

Критерии оценивания выполнения лабораторных работ

1.

		*)
1		
2		

2.

6.2. Оценочные средства и критерии оценивания для промежуточной аттестации

Теоретические вопросы

-ECB.
-CBC.
- -OFB.

-89.

-

Критерии оценивания теоретических вопросов

1.

		*)
1		
2		

(*)
2.

Критерий получения зачета

-
-

7. Перечень основной и дополнительной учебной литературы

7.1. Список основной литературы

1.
2. -
3.

7.2. Список дополнительной литературы

1. -
2. - 002.
3.
4. - - - 2011.
5. 2- -
6. -

7.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. moodle.smolgu.ru).
2. intuit.ru).
3. opened.ru)

8. Материально-техническое обеспечение

Учебная аудитория для проведения занятий лекционного типа,

Учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации -

Помещение для самостоятельной работы

.

9. Программное обеспечение

Kaspersky Endpoint Security
FB6-161215-133553-1-6231.

Microsoft Open License, 49463448 : Microsoft Windows Professional 7 Russian; Microsoft Office 2010 Russian.