Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра вычислительной техники
Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н. Рева И. Л.
“___ ”_____ _____ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Криптографические методы защиты информации

Образовательная программа: 09.04.01 Информатика и вычислительная техника, магистерская программа: Кибербезопасность информационных систем

Курс: 1, семестр : 2

Факультет автоматики и вычислительной техники,

		Семестр
№	**Вид деятельности**	**2**
1	Всего зачетных единиц (кредитов)	3
2	Всего часов	108
3	Всего занятий в контактной форме, час.	47
4	Лекции, час.	0
5	Практические занятия, час.	18
6	Лабораторные занятия, час.	18
7	из них в активной и интерактивной форме, час.	8
8	Аттестация, час.	2
9	Консультации, час.	9
10	Самостоятельная работа, час.	61
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	РГЗ
12	Вид аттестации	ДЗ

Новосибирск 2017

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 09.04.01 Информатика и вычислительная техника

ФГОС введен в действие приказом №1420 от 30.10.2014 г. , дата утверждения: 25.11.2014 г.

Место дисциплины в структуре учебного плана: Блок 1, вариативная

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 09.04.01 Информатика и вычислительная техника

Рабочая программа обсуждена на заседании кафедры

ВТ, протокол заседания кафедры №6 от 20.06.2017
ЗИ, протокол заседания кафедры №6 от 20.06.2017

Утверждена на совете факультета автоматики и вычислительной техники, протокол № 6 от 21.06.2017

Программу разработал:

доцент, к.ф-м.н. Котов Ю. А.

Заведующий кафедрой:

доцент, к.т.н. Якименко А. А.
с.н.с., к.т.н. Трушин В. А.

Ответственный за образовательную программу:

доцент Якименко А. А.

1. Внешние требования

Таблица 1.1

***Компетенция ФГОС*: ОК.4 способность заниматься научными исследованиями; *в части следующих результатов обучения*:**
у1. способность осуществлять научно-исследовательскую деятельность в области задач математического моделирования объектов профессиональной деятельности
***Компетенция ФГОС*: ОК.9 умение оформлять отчеты о проведенной научно-исследовательской работе и подготавливать публикации по результатам исследования; *в части следующих результатов обучения*:**
у1. составлять аналитические отчеты по результатам эксперимента, моделирования, сбора и обработки данных, содержащих постановку задачи, анализ и интерпретацию результатов, выводы и рекомендации
***Компетенция ФГОС*: ОПК.2 культурой мышления, способность выстраивать логику рассуждений и высказываний, основанных на интерпретации данных, интегрированных из разных областей науки и техники, выносить суждения на основании неполных данных; *в части следующих результатов обучения*:**
з2. знать основные методы научного познания
у2. анализировать и интерпретировать в терминах решаемой задачи результаты, полученные в процессе моделирования, сбора и обработки данных
***Компетенция ФГОС*: ПК.2 знанием методов научных исследований и владение навыками их проведения; *в части следующих результатов обучения*:**
з5. основные методы, области использования, ограничения, достоинства и недостатки, инструментальные средства математического моделирования объектов профессиональной деятельности
у4. выполнять сравнительный анализ эффективности применения различных методов математического моделирования в рамках решаемой задачи
у5. планировать и проводить машинные эксперименты с имитационными моделями объектов профессиональной деятельности, статистически обрабатывать и интерпретировать полученные результаты
у6. разрабатывать математические модели объектов профессиональной деятельности с использованием специализированных инструментальных средств
***Компетенция ФГОС*: ПК.3 знанием методов оптимизации и умение применять их при решении задач профессиональной деятельности; *в части следующих результатов обучения*:**
з2. знать основные математические методы оптимизации процесса функционирования объектов профессиональной деятельности
у4. уметь осуществлять математическую постановку задачи оптимизации процесса функционирования объектов профессиональной деятельности (ОПД), решать ее с помощью специализированных инструментальных средств, анализировать полученные результаты, выдавать практические рекомендации по оптимизации работы ОПД.

2. Требования НГТУ к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	**Формы организации занятий**
Криптографические методы защиты информации	
ОПК.2.з2 знать основные методы научного познания	
1.знать основные методы научного познания	Практические занятия; Лабораторные работы; Самостоятельная работа
ОПК.2.у2 анализировать и интерпретировать в терминах решаемой задачи результаты, полученные в процессе моделирования, сбора и обработки данных	
2.анализировать и интерпретировать в терминах решаемой задачи результаты, полученные в процессе моделирования, сбора и обработки данных	Практические занятия; Лабораторные работы; Самостоятельная работа
ПК.2.з5 основные методы, области использования, ограничения, достоинства и недостатки, инструментальные средства математического моделирования объектов профессиональной деятельности	

3.основные методы, области использования, ограничения, достоинства и недостатки, инструментальные средства математического моделирования объектов профессиональной деятельности	Практические занятия; Лабораторные работы; Самостоятельная работа
ПК.2.у4 выполнять сравнительный анализ эффективности применения различных методов математического моделирования в рамках решаемой задачи	
4.выполнять сравнительный анализ эффективности применения различных методов математического моделирования в рамках решаемой задачи	Практические занятия; Лабораторные работы; Самостоятельная работа
ПК.2.у5 планировать и проводить машинные эксперименты с имитационными моделями объектов профессиональной деятельности, статистически обрабатывать и интерпретировать полученные результаты	
5.планировать и проводить машинные эксперименты с имитационными моделями объектов профессиональной деятельности, статистически обрабатывать и интерпретировать полученные результаты	Практические занятия; Лабораторные работы; Самостоятельная работа
ПК.2.у6 разрабатывать математические модели объектов профессиональной деятельности с использованием специализированных инструментальных средств	
6.разрабатывать математические модели объектов профессиональной деятельности с использованием специализированных инструментальных средств	Практические занятия; Лабораторные работы; Самостоятельная работа
ПК.3.з2 знать основные математические методы оптимизации процесса функционирования объектов профессиональной деятельности	
7.знать основные математические методы оптимизации процесса функционирования объектов профессиональной деятельности	Практические занятия; Лабораторные работы; Самостоятельная работа
ПК.3.у4 уметь осуществлять математическую постановку задачи оптимизации процесса функционирования объектов профессиональной деятельности (ОПД), решать ее с помощью специализированных инструментальных средств, анализировать полученные результаты, выдавать практические рекомендации по оптимизации работы ОПД.	
8.уметь осуществлять математическую постановку задачи оптимизации процесса функционирования объектов профессиональной деятельности (ОПД), решать ее с помощью специализированных инструментальных средств, анализировать полученные результаты, выдавать практические рекомендации по оптимизации работы ОПД.	Практические занятия; Лабораторные работы; Самостоятельная работа
ОК.4.у1 способность осуществлять научно-исследовательскую деятельность в области задач математического моделирования объектов профессиональной деятельности	
9.способность осуществлять научно-исследовательскую деятельность в области задач математического моделирования объектов профессиональной деятельности	Практические занятия; Лабораторные работы; Самостоятельная работа
ОК.9.у1 составлять аналитические отчеты по результатам эксперимента, моделирования, сбора и обработки данных, содержащих постановку задачи, анализ и интерпретацию результатов, выводы и рекомендации	
10.составлять аналитические отчеты по результатам эксперимента, моделирования, сбора и обработки данных, содержащих постановку задачи, анализ и интерпретацию результатов, выводы и рекомендации	Практические занятия; Лабораторные работы; Самостоятельная работа

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лабораторных работ	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 2				
Дидактическая единица: Криптоанализ				
7. ЭЦП ГОСТ Р 34.10	2	6	1, 10, 2, 3, 4, 5, 6, 7, 8, 9	Криптоанализ классических шифров
Дидактическая единица: Стандартные шифры				

5. Шифры DES, AES, ГОСТ	2	4	1, 10, 2, 3, 4, 5, 6, 7, 8, 9	Шифры DES, AES, ГОСТ
Дидактическая единица: Приложения шифров				
6. Шифр с открытым ключом RSA	2	4	1, 10, 2, 3, 4, 5, 6, 7, 8, 9	Шифр с открытым ключом RSA
8. Электронная цифровая подпись RSA	2	4	1, 10, 2, 3, 4, 5, 6, 7, 8, 9	Электронная цифровая подпись RSA

Таблица 3.2

Темы практических занятий	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 2				
Дидактическая единица: Шифры				
1. Шифры DES,ГОСТ, AES	0	4	1, 10, 2, 3, 4, 5, 6, 7, 8, 9	Шифры DES,ГОСТ, AES
2. Шифр RSA	0	4	1, 10, 2, 3, 4, 5, 6, 7, 8, 9	Шифр RSA
3. ЭЦП ГОСТ Р 34.10	0	6	1, 10, 2, 3, 4, 5, 6, 7, 8, 9	ЭЦП ГОСТ Р 34.10
4. ЭЦП RSA	0	4	1, 10, 2, 3, 4, 5, 6, 7, 8, 9	ЭЦП RSA

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 2				
1	РГЗ	1, 10, 2, 3, 4, 5, 6, 7, 8, 9	20	7
РГЗ: 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				
2	Подготовка к занятиям	1, 10, 2, 3, 4, 5, 6, 7, 8, 9	21	0
Подготовка к занятиям: 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				
3	Подготовка к аттестации	1, 10, 2, 3, 4, 5, 6, 7, 8, 9	20	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				

5. Технология обучения

Для организации и контроля самостоятельной работы обучающихся, а также проведения консультаций применяются информационно-коммуникационные технологии (табл. 5.1).

Таблица 5.1

Деятельность	Информационно-коммуникационные технологии
Информирование	e-mail; Социальные сети

Консультирование	e-mail
Контроль	Портал НГТУ
Размещение учебных материалов	Портал НГТУ

6. Правила аттестации обучающихся по учебной дисциплине

Для аттестации обучающихся по дисциплине используется балльно-рейтинговая система (БРС), позволяющая выставлять оценки по традиционной шкале и 15-уровневой ECTS. Краткая информация о БРС приведена в табл. 6.1.

Таблица 6.1

Оцениваемые виды деятельности обучающихся	**Максимальный балл**
Семестр: 2	
Лабораторная:	30
Контролирующие материалы (список вопросов) приводятся в "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"	
Практические занятия:	30
Контролирующие материалы (список вопросов) приводятся в "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"	
РГЗ:	20
Контролирующие материалы (список вопросов) приводятся в "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"	
Зачет:	20
Контролирующие материалы (список вопросов) приводятся в "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"	

В таблице 6.2 представлено соответствие форм контроля заявляемым требованиям к результатам освоения дисциплины.

Таблица 6.2

Коды компетенций ФГОС	**Результаты обучения**	**Формы контроля**		
		Защита Л/Р	**Защита РГЗ**	**Зачет**
ОК.4	у1. способность осуществлять научно-исследовательскую деятельность в области задач математического моделирования объектов профессиональной деятельности	+	+	+
ОК.9	у1. составлять аналитические отчеты по результатам эксперимента, моделирования, сбора и обработки данных, содержащих постановку задачи, анализ и интерпретацию результатов, выводы и рекомендации	+	+	+
ОПК.2	з2. знать основные методы научного познания	+	+	+
	у2. анализировать и интерпретировать в терминах решаемой задачи результаты, полученные в процессе моделирования, сбора и обработки данных	+	+	+
ПК.2	з5. основные методы, области использования, ограничения, достоинства и недостатки, инструментальные средства математического моделирования объектов профессиональной деятельности	+	+	+
	у4. выполнять сравнительный анализ эффективности применения различных методов математического моделирования в рамках решаемой задачи	+	+	+

	у5. планировать и проводить машинные эксперименты с имитационными моделями объектов профессиональной деятельности, статистически обрабатывать и интерпретировать полученные результаты	+	+	+
	у6. разрабатывать математические модели объектов профессиональной деятельности с использованием специализированных инструментальных средств	+	+	+
ПК.3	з2. знать основные математические методы оптимизации процесса функционирования объектов профессиональной деятельности	+	+	+
	у4. уметь осуществлять математическую постановку задачи оптимизации процесса функционирования объектов профессиональной деятельности (ОПД), решать ее с помощью специализированных инструментальных средств, анализировать полученные результаты, выдавать практические рекомендации по оптимизации работы ОПД.	+	+	+

Фонд оценочных средств по дисциплине представлен в приложении № 1 к рабочей программе.

7. Литература

Основная литература

1. Лапонина 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. Лапонина ; под ред. В. А. Сухомлина. - 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

Дополнительная литература

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.

Интернет-ресурсы

1. ЭБС НГТУ : http://elibrary.nstu.ru/

2. ЭБС «Издательство Лань» : https://e.lanbook.com/

3. ЭБС IPRbooks : http://www.iprbookshop.ru/

4. ЭБС "Znanium.com" : http://znanium.com/

5. :

8. Методическое и программное обеспечение

8.1 Методическое обеспечение

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 Специализированное программное обеспечение

1 Microsoft Windows
2 Microsoft Office

9. Материально-техническое обеспечение

Презентационное оборудование

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Применяется при проведении лекций

Компьютерный класс

№	Наименование	Назначение
1	Компьютерный класс (Компьютеры объединены в локальную сеть с выходом в Internet)	Применяется при проведении лабораторных работ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра вычислительной техники
Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н., доцент И.Л. Рева
“___”_____ _____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ

Криптографические методы защиты информации

Образовательная программа: 09.04.01 Информатика и вычислительная техника, магистерская программа: Кибербезопасность информационных систем

Новосибирск 2017

1. **Обобщенная структура фонда оценочных средств учебной дисциплины**

Обобщенная структура фонда оценочных средств по **дисциплине** Криптографические методы защиты информации приведена в Таблице.

Таблица

Формируемые компетенции	**Показатели сформированности компетенций (знания, умения, навыки)**	**Темы**	**Этапы оценки компетенций**	
			Мероприятия текущего контроля (курсовой проект, РГЗ(Р) и др.)	**Промежуточная аттестация (экзамен, зачет)**
ОК.4 способность заниматься научными исследованиями	у1. способность осуществлять научно-исследовательскую деятельность в области задач математического моделирования объектов профессиональной деятельности	Шифр RSA Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры DES,ГОСТ, AES Электронная цифровая подпись RSA ЭЦП RSA ЭЦП ГОСТ Р 34.10	Отчет по лабораторной работе РГЗ, разделы 1-2	Зачет, вопросы 1-5
ОК.9 умение оформлять отчеты о проведенной научно-исследовательской работе и подготавливать публикации по результатам исследования	у1. составлять аналитические отчеты по результатам эксперимента, моделирования, сбора и обработки данных, содержащих постановку задачи, анализ и интерпретацию результатов, выводы и рекомендации	Шифр RSA Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры DES,ГОСТ, AES Электронная цифровая подпись RSA ЭЦП RSA ЭЦП ГОСТ Р 34.10	Отчет по лабораторной работе РГЗ, разделы 2-3	Зачет, вопросы 6-9
ОПК.2 культурой мышления, способность выстраивать логику рассуждений и высказываний, основанных на интерпретации данных, интегрированных из разных областей науки и техники, выносить суждения на основании неполных данных	з2. знать основные методы научного познания	Шифр RSA Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры DES,ГОСТ, AES Электронная цифровая подпись RSA ЭЦП RSA ЭЦП ГОСТ Р 34.10	Отчет по лабораторной работе РГЗ, разделы 1-3	Зачет, вопросы 10-15
ОПК.2	у2. анализировать и интерпретировать в терминах решаемой задачи результаты, полученные в процессе моделирования, сбора и обработки данных	Шифр RSA Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры DES,ГОСТ, AES Электронная цифровая подпись RSA ЭЦП RSA ЭЦП ГОСТ Р 34.10	Отчет по лабораторной работе РГЗ, разделы 4	Зачет, вопросы 16-18

ПК.2/НИ знанием методов научных исследований и владение навыками их проведения	з5. основные методы, области использования, ограничения, достоинства и недостатки, инструментальные средства математического моделирования объектов профессиональной деятельности	Шифр RSA Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры DES,ГОСТ, AES Электронная цифровая подпись RSA ЭЦП RSA ЭЦП ГОСТ Р 34.10	Отчет по лабораторной работе РГЗ, разделы 2-4	Зачет, вопросы 19-22
ПК.2/НИ	у4. выполнять сравнительный анализ эффективности применения различных методов математического моделирования в рамках решаемой задачи	Шифр RSA Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры DES,ГОСТ, AES Электронная цифровая подпись RSA ЭЦП RSA ЭЦП ГОСТ Р 34.10	Отчет по лабораторной работе РГЗ, разделы 1-4	Зачет, вопросы 22-25
ПК.2/НИ	у5. планировать и проводить машинные эксперименты с имитационными моделями объектов профессиональной деятельности, статистически обрабатывать и интерпретировать полученные результаты	Шифр RSA Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры DES,ГОСТ, AES Электронная цифровая подпись RSA ЭЦП RSA ЭЦП ГОСТ Р 34.10	Отчет по лабораторной работе РГЗ, разделы 1-4	Зачет, вопросы 26-28
ПК.2/НИ	у6. разрабатывать математические модели объектов профессиональной деятельности с использованием специализированны х инструментальных средств	Шифр RSA Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры DES,ГОСТ, AES Электронная цифровая подпись RSA ЭЦП RSA ЭЦП ГОСТ Р 34.10	Отчет по лабораторной работе РГЗ, разделы 1-4	Зачет, вопросы 18-21
ПК.3/НИ знанием методов оптимизации и умение применять их при решении задач профессиональной деятельности	з2. знать основные математические методы оптимизации процесса функционирования объектов профессиональной деятельности	Шифр RSA Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры DES,ГОСТ, AES Электронная цифровая подпись RSA ЭЦП RSA ЭЦП ГОСТ Р 34.10	Отчет по лабораторной работе РГЗ, разделы 1-4	Зачет, вопросы 22-24
ПК.3/НИ	у4. уметь осуществлять математическую постановку задачи оптимизации процесса функционирования объектов	Шифр RSA Шифр с открытым ключом RSA Шифры DES, AES, ГОСТ Шифры DES,ГОСТ, AES Электронная цифровая подпись RSA ЭЦП RSA ЭЦП ГОСТ Р 34.10	Отчет по лабораторной работе РГЗ, разделы 1-4	Зачет, вопросы 25-28

	профессиональной деятельности (ОПД), решать ее с помощью специализированных инструментальных средств, анализировать полученные результаты, выдавать практические рекомендации по оптимизации работы ОПД.			

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по **дисциплине** проводится в 2 семестре - в форме дифференцированного зачета, который направлен на оценку сформированности компетенций ОК.4, ОК.9, ОПК.2, ПК.2/НИ, ПК.3/НИ.

Зачет проводится в устной форме, по билетам.

Кроме того, сформированность компетенций проверяется при проведении мероприятий текущего контроля, указанных в таблице раздела 1.

В 2 семестре обязательным этапом текущей аттестации является расчетно-графическое задание (работа) (РГЗ(Р)). Требования к выполнению РГЗ(Р), состав и правила оценки сформулированы в паспорте РГЗ(Р).

Общие правила выставления оценки по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе учебной дисциплины.

На основании приведенных далее критериев можно сделать общий вывод о сформированности компетенций ОК.4, ОК.9, ОПК.2, ПК.2/НИ, ПК.3/НИ, за которые отвечает дисциплина, на разных уровнях.

Общая характеристика уровней освоения компетенций.

Ниже порогового. Уровень выполнения работ не отвечает большинству основных требований, теоретическое содержание курса освоено частично, пробелы могут носить существенный характер, необходимые практические навыки работы с освоенным материалом сформированы не достаточно, большинство предусмотренных программой обучения учебных заданий не выполнены или выполнены с существенными ошибками.

Пороговый. Уровень выполнения работ отвечает большинству основных требований, теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые виды заданий выполнены с ошибками.

Базовый. Уровень выполнения работ отвечает всем основным требованиям, теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые из выполненных заданий, возможно, содержат ошибки.

Продвинутый. Уровень выполнения работ отвечает всем требованиям, теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра вычислительной техники
Кафедра защиты информации

Паспорт зачета

по дисциплине «Криптографические методы защиты информации», 2семестр

1. Методика оценки

Зачет проводится в устной форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов 1-6, второй вопрос из диапазона вопросов 7-12 (список вопросов приведен ниже). В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы из общего перечня (п. 4).

Форма билета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____
к зачету по дисциплине «Криптографические методы защиты информации»

---

1. Длина ключа и стойкость шифра.
2. Отечественные стандарт хэш-функции ГОСТ Р 34.11-2012.

Утверждаю: зав. кафедрой ____ _____ должность, ФИО
(подпись)
(дата)

2. **Критерии оценки**

- Ответ на зачетный билет считается **неудовлетворительным**, если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений, при решении задачи допускает принципиальные ошибки, оценка составляет *_5_ баллов.*
- Ответ на зачетный билет засчитывается на **пороговом** уровне, если студент при ответе на вопросы дает определение основных понятий, может показать причинно-следственные связи явлений, при решении задачи допускает непринципиальные ошибки, например, вычислительные,
  оценка составляет *10 баллов.*
- Ответ на зачетный билет засчитывается на **базовом** уровне, если студент при ответе на вопросы формулирует основные понятия, законы, дает характеристику процессов,

явлений, проводит анализ причин, условий, может представить качественные характеристики процессов, не допускает ошибок при решении задачи, оценка составляет *_15_ баллов.*

- Ответ на зачетный билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы проводит сравнительный анализ подходов, проводит комплексный анализ, выявляет проблемы, предлагает механизмы решения, способен представить количественные характеристики определенных процессов, приводит конкретные примеры из практики, не допускает ошибок и способен обосновать выбор метода решения задачи, оценка составляет _20_ *баллов.*

3. Шкала оценки

В общей оценке по дисциплине зачетные баллы учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. **Вопросы к** зачету **по дисциплине** «Криптографические методы защиты информации»

1	Криптографическая защита информации. Классификация шифров. Требования к средствам криптографической защиты информации.
2	Шифры и шифрование. Основные понятия и определения
3	Шифры перестановки
4	Шифры замены
5	Шифр гаммирования
6	Шифр гаммирования с обратной связью
7	Совершенные, идеально стойкие, абсолютно стойкие шифры
8	Длина ключа и стойкость шифра
9	Фундаментальные ограничения криптографических преобразований
10	Проблемы массового использования шифров. Стандартные схемы и приемы реализации массовых шифров.
11	Стандартные шифры (DES, ГОСТ, AES).
12	Стандарт шифрования DES.
13	Режимы использования шифра DES
14	Стандарт шифрования ГОСТ 28147-89
15	Стандарт шифрования AES
16	Генераторы псевдослучайных чисел в шифровании
17	Основные подходы и методики криптоанализа.
18	Криптоанализ с использованием открытого текста.
19	Криптосистемы с открытым ключем. Принцип Шеннона. Основные особенности и характеристики криптосистем с открытым ключем
29	Структура системы секретной связи при использовании симметричных шифров и шифров с открытым ключом
21	Система Диффи-Хелмана
22	Шифр RSA
23	Шифр Эль Гаммаля
24	Гибридные криптосистемы
25	Основные проблемы криптографической защиты и способы их решения

26	Применение шифров для идентификации и аутентификации субъектов и данных. Хэш-функции. Электронно-цифровая подпись. Схемы цифровой подписи.
27	Отечественные стандарт хэш-функции ГОСТ Р 34.11-2012
28	Отечественные стандарт шифрования с открытым ключом и электронно-цифровой подписи ГОСТ Р 34.10-2012

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра вычислительной техники
Кафедра защиты информации

Паспорт
расчетно-графической работы

по дисциплине «Криптографические методы защиты информации», 2 семестр

1. **Методика оценки.**

Задание: Шифр Виженера.

Структура:1. Цель работы. 2. Постановка задачи. 3.Результаты выполнения. 4. Заключение. 5. Список литературы.

Этапы выполнения и защиты: в соответствии со структурой

Оцениваемые позиции: работа в целом.

2. **Критерии оценки.**

- работа считается **не выполненной,** если оценка составляет менее 49 баллов.
- работа считается выполненной **на пороговом** уровне, если оценка составляет 50-72 баллов.
- работа считается выполненной **на базовом** уровне, если оценка составляет 73-88 баллов.
- работа считается выполненной **на продвинутом** уровне, если оценка составляет более 88 баллов.

3. **Шкала оценки.**

В общей оценке по дисциплине баллы за работы учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. **Примерный перечень тем РГР.**

1. Шифр одиночной перестановка по ключу.
2. Шифр двойной перестановка по ключу.
3. Шифр перестановки с запретом записи.
4. Шифр перестановки на основе «магического» квадрата.
5. Шифр перестановки «по маршрутам».
6. Шифр перестановки с различными размерами блоков.
7. Шифр простой перестановки с изменением направления записи/чтения.
8. Шифры замены. Система Цезаря.
9. Шифры замены. Система Полибия.
10. Шифры замены. Простая замена.
11. Шифр Гронсфельда.
12. Шифр Виженера.
13. Шифр многоалфавитной замены.

14. Шифр монофонической замены.

15. Шифр гаммирования.

5. Перечень вопросов к защите РГР.

Вопросы для защиты РГР по дисциплине
«Криптографические методы защиты информации»

Минимальное количество вопросов – 2, по одному из каждой части.

Часть 1

1.
1. Дайте определение шифра, ключа.
2. Чем шифрование отличается от кодирования.
3. Что такое тайнопись.
4. Для чего применяются шифры.
5. Что такое алфавит.
6. Какое значение имеет буква.
7. Что такое (k. –граммы.
8. Что такое индекс совпадения и как он вычисляется.
   Как в закодированном тексте выделить с помощью биграмм:
9. Символы (О,Е,А,И);
10. Символы (Ь,Ы).
11. Символ (Э);
12. Символы (С,Т);
13. Символ (Л);
14. Символ (Н);
15. Символы (О,В).

2.
1. Какие шифры называются симметричными.
2. Особенность секретной связи при использовании симметричных шифров.
3. Какие шифры называются перестановкой.
4. Определение функциональной эквивалентности шифров.
5. В чем заключается единственность шифра перестановки.
   Приведите схему перестановки:
6. простой;
7. одиночной по ключу;
8. двойной по ключу;
9. с запретом записи;
10. с использованием магических квадратов;
11. по «маршрутам»;
12. со сменой направления записи/чтения;
13. использующей разные размеры блоков;
14. повторной перестановки.
15. Как определить размер блока линейной перестановки для повторных перестановок.
16. В чем заключаются фундаментальные особенности шифров перестановки.
17. Что называется циклом или раундом при шифровании.
18. Что такое характеристическая функция ключа и для чего она может быть использована.
19. Какому шифру перестановки функционально эквивалентны остальные шифры перестановки.

3.
1. Как определяется стойкость шифра.
2. В каких единицах измеряется длина ключа.
3. В каких единицах измеряется стойкость шифра.
4. Что такое расстояние единственности.
5. В каких единицах измеряется переборная стойкость шифра.
6. В чем различие между длиной и размером ключа.
7. Что такое период ключа.
8. В чем заключаются фундаментальные особенности перестановки.
9. Приведите примеры чувствительности перестановки к специально подобранному тексту.
10. В чем заключается зависимости длины ключа перестановки от шифруемого текста.

11. В чем особенность шифрования перестановкой не полностью заполненного блока текста.
12. Какими способами можно повысить эффективность шифра перестановки.
13. Что такое защищенная кодировка и в чем ее смысл.
14. Как и в каких единицах измеряется переборная стойкость шифра.

4.
1. Какие шифры называются шифрами замены.
2. Опишите шифр:
а. Цезаря;
б. Полибия;
в. простой замены;
г. Гронсфельда;
д. Виженера.
3. Чем системы Цезаря, Полибия и простой замены отличаются от других шифров замены.
4. Приведите формулу общей математической модели шифров Цезаря, Гронсфелда, Виженера.
5. Какие шифры называются шифрами Бофора.
6. Какой шифр называется шифром Вернама.
7. Постройте собственный пример шифрования и расшифрования по формулам (4.2., отличающийся от приведенного в пособии.
8. Какой шифр называется шифром гаммирования, с какими известными шифрами и как он связан.
9. Что называется инфляцией алфавита.
10. В чем основная особенность шифра гаммирования.
11. Какой условие должно выполняться для обратимого шифрования композицией замен.
12. Какой алфавит называется входным (исходным) для шифра, а какой – выходным алфавитом.
13. Какие шифры называются одноалфавитными, моноалфавитными, полиалфавитными, многоалфавитными.
14. Как получить ключ шифра замены при шифровании перестановкой.
15. Частным случаем каких шифров является шифр перестановки.
16. Какой шифр называется шифром гаммирования с обратной связью.
17. Что общего у шифров монофонической замены, перестановки и гаммирования с обратной связью.
18. Как объединяются повторные применения шифров:
а. Цезаря;
б. Виженера;
в. простой замены и Виженера.

Часть 2.

5.
1. Размер блока и ключа шифра DES.
2. Размер блока и ключа шифра AES.
3. Размер блока и ключа шифра ГОСТ.
4. Режимы работы шифра DES.
5. Режимы работы шифра ГОСТ.
6. Количество базовых циклов шифрования в шифре DES.
7. Количество базовых циклов шифрования в шифре AES.
8. Количество базовых циклов шифрования в шифре ГОСТ.
9. Что называется имитовставкой в шифре ГОСТ.
10. Как определяется размер имитовставки.
11. Что называется синхропосылкой в шифре ГОСТ.
12. Что называется сетью Фейстейля.
13. Что называется SP-сетью.
14. Где в сообщении должна располагаться имитовставка шифра ГОСТ.
15. Какой шифр называется 3DES.

6.
1. Назначение и ограничения метода полного перебора.
2. Что называется переборным пространством.
3. Теоретическая оценка сокращения переборного пространства при поиске по образцу.
4. Чем отличается направленный случайный поиск от простого случайного поиска.
5. В каком случае при случайном поиске число просмотров будет минимальным.
6. В чем заключается метод проб и ошибок, с каким разделом математической статистики он связан.

7. Что называется «парадоксом дней рождения».
8. Каким требованиям (по Шеннону. должен отвечать «хороший» статистический метод криптоанализа.
9. Определите два основных класса методов криптоанализа.

В ответах на контрольные вопросы 10-16 дайте определение и опишите основные элементы для указанного в вопросе метода.

10. Метод вероятных слов.
11. Тест Казиски.
12. Метод «встречи посередине».
13. Метод линейного криптоанализа.
14. Метод дифференциального криптоанализа
15. Слайдовый метод.
16. Метод криптоанализа на связанных ключах.