МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе

Документ подписан электронной подписью
Сертификат: 1c6cfa0a-52a6-4f49-aef0-5584d3fd4820
Владелец: Троян Павел Ефимович
Действителен: с 19.01.2016 по 16.09.2019

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Математические основы криптологии

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **10.03.01 Информационная безопасность**
Направленность (профиль): **Организация и технология защиты информации**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**
Курс: **3**
Семестр: **5**
Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	5 семестр	Всего	Единицы
1	Лекции	28	28	часов
2	Практические занятия	44	44	часов
3	Всего аудиторных занятий	72	72	часов
4	Из них в интерактивной форме	20	20	часов
5	Самостоятельная работа	36	36	часов
6	Всего (без экзамена)	108	108	часов
7	Подготовка и сдача экзамена	36	36	часов
8	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е

Экзамен: 5 семестр

Томск 2017

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от « 3 » 5 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.03.01 Информационная безопасность, утвержденного 01 декабря 2016 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчик:

доцент каф. БИС _____ О. О. Евсютин

Заведующий обеспечивающей каф.
РЗИ _____ А. В. Фатеев

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами направления подготовки (специальности).

Декан РТФ _____ К. Ю. Попова

Заведующий выпускающей каф.
РЗИ _____ А. В. Фатеев

Эксперт:

доцент каф. РЗИ _____ А. П. Кшнянкин

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью дисциплины «Математические основы криптологии» является изучение студентами математического аппарата, лежащего в основе современных криптографических методов защиты информации.

1.2. Задачи дисциплины

- изучить основные разделы абстрактной алгебры, имеющие криптографические приложения;
- изучить основные разделы теории чисел, имеющие криптографические приложения;
- заложить базовые знания об устройстве современных криптографических алгоритмов.

2. Место дисциплины в структуре ОПОП

Дисциплина «Математические основы криптологии» (Б1.Б.34) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Алгебра и геометрия, Дискретная математика.

Последующими дисциплинами являются: Криптографические методы защиты информации.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОПК-2 способностью применять соответствующий математический аппарат для решения профессиональных задач;
- ПК-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

В результате изучения дисциплины студент должен:

- **знать** элементы теорий групп, колец и полей, основы элементарной теории чисел, базовые алгебраические и теоретико-числовые алгоритмы.
- **уметь** исследовать основные алгебраические структуры; применять полученные знания для компьютерной реализации криптографических алгоритмов.
- **владеть** методами абстрактной алгебры и теории чисел.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 4.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		5 семестр
Аудиторные занятия (всего)	72	72
Лекции	28	28
Практические занятия	44	44
Из них в интерактивной форме	20	20
Самостоятельная работа (всего)	36	36
Проработка лекционного материала	14	14
Подготовка к практическим занятиям, семинарам	22	22
Всего (без экзамена)	108	108
Подготовка и сдача экзамена	36	36
Общая трудоемкость ч	144	144
Зачетные Единицы	4.0	4.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лекции	Практические занятия	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
5 семестр					
1 Множества и отображения	2	2	2	6	ОПК-2
2 Алгебраические операции	2	2	2	6	ОПК-2
3 Группы, подгруппы	2	2	2	6	ОПК-2
4 Циклические группы	2	2	2	6	ОПК-2
5 Различные классы групп	2	2	2	6	ОПК-2
6 Кольца	2	2	2	6	ОПК-2
7 Различные классы колец	2	2	2	6	ОПК-2
8 Поля	2	2	2	6	ОПК-2
9 Поля Галуа	2	2	3	7	ОПК-2
10 Эллиптические кривые	2	4	3	9	ОПК-2, ПК-1
11 Алгоритмы вычисления наибольшего общего делителя целых чисел	2	2	2	6	ОПК-2
12 Китайская теорема об остатках	2	2	2	6	ОПК-2
13 Квадратичные вычеты	2	2	2	6	ОПК-2
14 Сложные вычислительные задачи	2	4	2	8	ОПК-2, ПК-1
15 Проведение контрольных работ	0	12	6	18	ОПК-2, ПК-1
Итого за семестр	28	44	36	108	
Итого	28	44	36	108	

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 - Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины по лекциям	Трудоемкость, ч	Формируемые компетенции
5 семестр			
1 Множества и отображения	Множества, операции над ними. Отображения, их классификация. Бинарные отношения, отношения эквивалентно-	2	ОПК-2

	сти.		
	Итого	2	
2 Алгебраические операции	Алгебраические операции. Свойства алгебраических операций. Алгебраические структуры. Типы алгебраических структур.	2	ОПК-2
	Итого	2	
3 Группы, подгруппы	Группы, подгруппы, критерий подгруппы. Теорема Лагранжа.	2	ОПК-2
	Итого	2	
4 Циклические группы	Целочисленные степени элементов группы. Свойства целочисленных степеней. Циклические группы.	2	ОПК-2
	Итого	2	
5 Различные классы групп	Группы подстановок. Матричные группы.	2	ОПК-2
	Итого	2	
6 Кольца	Кольца, подкольца, примеры колец. Критерий подкольца.	2	ОПК-2
	Итого	2	
7 Различные классы колец	Кольца многочленов. Кольца классов вычетов. Кольца матриц.	2	ОПК-2
	Итого	2	
8 Поля	Поля, подполя, примеры полей. Конечные поля.	2	ОПК-2
	Итого	2	
9 Поля Галуа	Поля Галуа. Исследование мультипликативной группы поля Галуа.	2	ОПК-2
	Итого	2	
10 Эллиптические кривые	Понятие эллиптической кривой над конечным полем. Исследование группы точек эллиптической кривой.	2	ОПК-2, ПК-1
	Итого	2	
11 Алгоритмы вычисления наибольшего общего делителя целых чисел	Наибольший общий делитель. Алгоритм Евклида вычисления наибольшего общего делителя двух чисел. Расширенный алгоритм Евклида. Сравнения первой степени с одним неизвестным.	2	ОПК-2
	Итого	2	
12 Китайская теорема об остатках	Китайская теорема об остатках.	2	ОПК-2
	Итого	2	
13 Квадратичные вычеты	Квадратичные вычеты. Критерий Эйлера. Критерий Гаусса. Символ Лежандра.	2	ОПК-2

	Итого	2	
14 Сложные вычислительные задачи	Задача факторизации целых чисел на множители. Задача дискретного логарифмирования. Задача извлечения квадратного корня по модулю целого числа.	2	ОПК-2, ПК-1
	Итого	2	
Итого за семестр		28	

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 - Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Предшествующие дисциплины															
1 Алгебра и геометрия		+	+	+	+	+	+			+					
2 Дискретная математика	+														
Последующие дисциплины															
1 Криптографические методы защиты информации	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4

Таблица 5.4 – Соответствие компетенций и видов занятий, формируемых при изучении дисциплины

Компетенции	Виды занятий			Формы контроля
	Лекции	Практические занятия	Самостоятельная работа	
ОПК-2	+	+	+	Контрольная работа, Домашнее задание, Экзамен, Проверка контрольных работ, Опрос на занятиях

ПК-1	+	+	+	Контрольная работа, Домашнее задание, Экзамен, Проверка контрольных работ, Опрос на занятиях

6. Интерактивные методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий в часах приведены в таблице 6.1

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий в часах

Методы	Интерактивные практические занятия	Интерактивные лекции	Всего
5 семестр			
Мини-лекция	6		6
IT-методы	6	8	14
Итого за семестр:	12	8	20
Итого	12	8	20

7. Лабораторные работы

Не предусмотрено РУП

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8. 1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
5 семестр			
1 Множества и отображения	Операции над множествами. Исследование свойств отображений.	2	ОПК-2
	Итого	2	
2 Алгебраические операции	Исследование свойств алгебраических операций и алгебраических структур.	2	ОПК-2
	Итого	2	
3 Группы, подгруппы	Исследование свойств алгебраических операций и алгебраических структур.	2	ОПК-2
	Итого	2	
4 Циклические группы	Исследование абстрактных циклических групп.	2	ОПК-2
	Итого	2	
5 Различные классы групп	Исследование групп подстановок. Исследование матричных групп.	2	ОПК-2
	Итого	2	
6 Кольца	Исследование свойств колец.	2	ОПК-2
	Итого	2	
7 Различные классы колец	Исследование групп обратимых эле-	2	ОПК-2

	ментов колец классов вычетов.		
	Итого	2	
8 Поля	Исследование свойств полей.	2	ОПК-2
	Итого	2	
9 Поля Галуа	Построение полей Галуа. Исследование мультипликативных групп полей Галуа.	2	ОПК-2
	Итого	2	
10 Эллиптические кривые	Построение и исследование групп точек эллиптических кривых над конечными полями.	4	ОПК-2, ПК-1
	Итого	4	
11 Алгоритмы вычисления наибольшего общего делителя целых чисел	Нахождение целочисленных линейных комбинаций с помощью расширенного алгоритма Евклида. Решение сравнением первой степени с одним неизвестным.	2	ОПК-2
	Итого	2	
12 Китайская теорема об остатках	Решение систем сравнений первой степени с одним неизвестным.	2	ОПК-2
	Итого	2	
13 Квадратичные вычеты	Установление разрешимости сравнений второй степени.	2	ОПК-2
	Итого	2	
14 Сложные вычислительные задачи	Разложение целых чисел на множители. Нахождение дискретных логарифмов. Извлечение квадратных корней по простым и составным модулям.	4	ОПК-2, ПК-1
	Итого	4	
15 Проведение контрольных работ	Подготовка к контрольным работам по изученному материалу. Проведение контрольных работ.	12	ОПК-2, ПК-1
	Итого	12	
Итого за семестр		44	

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 - Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
5 семестр				
1 Множества и	Подготовка к практиче-	1	ОПК-2	Домашнее задание,

отображения	ским занятиям, семинарам			Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	1		
	Итого	2		
2 Алгебраические операции	Подготовка к практическим занятиям, семинарам	1	ОПК-2	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	1		
	Итого	2		
3 Группы, подгруппы	Подготовка к практическим занятиям, семинарам	1	ОПК-2	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	1		
	Итого	2		
4 Циклические группы	Подготовка к практическим занятиям, семинарам	1	ОПК-2	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	1		
	Итого	2		
5 Различные классы групп	Подготовка к практическим занятиям, семинарам	1	ОПК-2	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	1		
	Итого	2		
6 Кольца	Подготовка к практическим занятиям, семинарам	1	ОПК-2	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	1		
	Итого	2		
7 Различные классы колец	Подготовка к практическим занятиям, семинарам	1	ОПК-2	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	1		
	Итого	2		
8 Поля	Подготовка к практическим занятиям, семинарам	1	ОПК-2	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ,
	Проработка лекционного	1		

	материала			Экзамен
	Итого	2		
9 Поля Галуа	Подготовка к практическим занятиям, семинарам	2	ОПК-2	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	1		
	Итого	3		
10 Эллиптические кривые	Подготовка к практическим занятиям, семинарам	2	ОПК-2, ПК-1	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	1		
	Итого	3		
11 Алгоритмы вычисления наибольшего общего делителя целых чисел	Подготовка к практическим занятиям, семинарам	1	ОПК-2	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	1		
	Итого	2		
12 Китайская теорема об остатках	Подготовка к практическим занятиям, семинарам	1	ОПК-2	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	1		
	Итого	2		
13 Квадратичные вычеты	Подготовка к практическим занятиям, семинарам	1	ОПК-2	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	1		
	Итого	2		
14 Сложные вычислительные задачи	Подготовка к практическим занятиям, семинарам	1	ОПК-2, ПК-1	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	1		
	Итого	2		
15 Проведение контрольных работ	Подготовка к практическим занятиям, семинарам	6	ОПК-2, ПК-1	Контрольная работа, Проверка контрольных работ
	Итого	6		
Итого за семестр		36		
	Подготовка и сдача экзамена	36		Экзамен

Итого	72		

10. Курсовая работа (проект)

Не предусмотрено РУП

11. Рейтинговая система для оценки успеваемости студентов

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
5 семестр				
Домашнее задание	5	5		10
Контрольная работа	10	10	10	30
Опрос на занятиях	10	10	10	30
Итого максимум за период	25	25	20	70
Экзамен				30
Нарастающим итогом	25	50	70	100

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11. 2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11. 3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 - 100	A (отлично)
4 (хорошо) (зачтено)	85 - 89	B (очень хорошо)
	75 - 84	C (хорошо)
	70 - 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 - 69	
	60 - 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Росошек С.К. Специальные главы математики (математические основы криптографии): учебное пособие. Часть 1. — 2012. — 93 с. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/rososhek_sgm_1.pdf
2. Росошек С.К. Специальные главы математики (математические основы криптографии): учебное пособие. Часть 2. — 2012. — 190 с. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/rososhek_sgm_2.pdf
3. Курош А.Г. Курс высшей алгебры: учебник для вузов. — 16-е изд., стереотип. — СПб.: Лань, 2007; М.: Физматкнига, 2007. — 431 с. (наличие в библиотеке ТУСУР - 9 экз.)
4. Сизый С.В. Лекции по теории чисел: учебное пособие для вузов. — М.: Физматлит, 2007. — 190 с. (наличие в библиотеке ТУСУР - 10 экз.)

12.2. Дополнительная литература

1. Смарт Н. Криптография: учебник для вузов.— М. : Техносфера, 2005. — 525 с. (наличие в библиотеке ТУСУР - 11 экз.)

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Евсютин О.О. Криптографические методы защиты информации: методические указания для выполнения практических и самостоятельных работ. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_kmzi.pdf

12.3.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

12.4. Базы данных, информационно-справочные, поисковые системы и требуемое программное обеспечение

1. Не предусмотрено.

13. Материально-техническое обеспечение дисциплины

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория, с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью.

13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических (семинарских) занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория, с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью.

13.1.3. Материально-техническое обеспечение для самостоятельной работы

Для самостоятельной работы используется учебная аудитория (компьютерный класс), рас-

положенная по адресу 634034, г. Томск, ул. Вершинина, 47, 1 этаж, ауд. 126. Состав оборудования: учебная мебель; компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 4 шт.; компьютеры подключены к сети ИНТЕРНЕТ и обеспечивают доступ в электронную информационно-образовательную среду университета.

13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для удаленного просмотра.

При обучении студентов **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах для студентов с нарушениями опорно-двигательного аппарата, мобильной системы обучения для людей с инвалидностью.

14. Фонд оценочных средств

14.1. Основные требования к фонду оценочных средств и методические рекомендации

Фонд оценочных средств и типовые контрольные задания, используемые для оценки сформированности и освоения закрепленных за дисциплиной компетенций при проведении текущей, промежуточной аттестации по дисциплине приведен в приложении к рабочей программе.

14.2 Требования к фонду оценочных средств для лиц с ограниченными возможностями здоровья

Для студентов с инвалидностью предусмотрены дополнительные оценочные средства, перечень которых указан в таблице.

Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью

Категории студентов	Виды дополнительных оценочных средств	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами, исходя из состояния обучающегося на момент проверки

14.3 Методические рекомендации по оценочным средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

– в печатной форме;

– в печатной форме с увеличенным шрифтом;
– в форме электронного документа;
– методом чтения ассистентом задания вслух;
– предоставление задания с использованием сурдоперевода.

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

– письменно на бумаге;
– набор ответов на компьютере;
– набор ответов с использованием услуг ассистента;
– представление ответов устно.

Процедура оценивания результатов обучения инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в форме электронного документа;
– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

– в форме электронного документа;
– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;
– в печатной форме.

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Математические основы криптологии

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки (специальность): **10.03.01 Информационная безопасность**
Направленность (профиль): **Организация и технология защиты информации**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РЗИ, Кафедра радиоэлектроники и защиты информации**
Курс: **3**
Семестр: **5**

Учебный план набора 2013 года

Разработчик:
- доцент каф. БИС О. О. Евсютин

Экзамен: 5 семестр

Томск 2017

1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

Код	Формулировка компетенции	Этапы формирования компетенций
ОПК-2	способностью применять соответствующий математический аппарат для решения профессиональных задач	Должен знать элементы теорий групп, колец и полей, основы элементарной теории чисел, базовые алгебраические и теоретико-числовые алгоритмы.; Должен уметь исследовать основные алгебраические структуры; применять полученные знания для компьютерной реализации криптографических алгоритмов.; Должен владеть методами абстрактной алгебры и теории чисел.;
ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций по этапам

Показатели и критерии	Знать	Уметь	Владеть
Отлично (высокий уровень)	Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости	Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем	Контролирует работу, проводит оценку, совершенствует действия работы
Хорошо (базовый уровень)	Знает факты, принципы, процессы, общие понятия в пределах изучаемой области	Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования	Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем
Удовлетворительно (пороговый уровень)	Обладает базовыми общими знаниями	Обладает основными умениями, требуемыми для выполнения простых задач	Работает при прямом наблюдении

2 Реализация компетенций

2.1 Компетенция ОПК-2

ОПК-2: способностью применять соответствующий математический аппарат для решения профессиональных задач.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 3.

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть

Содержание этапов	элементы теорий групп, колец и полей, основы элементарной теории чисел, базовые алгебраические и теоретико-числовые алгоритмы.	исследовать основные алгебраические структуры;	методами абстрактной алгебры и теории чисел.
Виды занятий	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Самостоятельная работа;
Используемые средства оценивания	• Контрольная работа; • Домашнее задание; • Опрос на занятиях; • Экзамен;	• Контрольная работа; • Домашнее задание; • Опрос на занятиях; • Экзамен;	• Домашнее задание; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Знает разделы абстрактной алгебры и теории чисел, имеющие криптографические приложения, и понимает связи между различными разделами.;	• Умеет исследовать основные алгебраические структуры и анализировать результаты исследования.;	• Владеет основными методами абстрактной алгебры и теории чисел;
Хорошо (базовый уровень)	• Знает основные разделы абстрактной алгебры и теории чисел, имеющие криптографические приложения.;	• Умеет исследовать основные алгебраические структуры.;	• Владеет некоторыми методами абстрактной алгебры и теории чисел.;
Удовлетворительно (пороговый уровень)	• Знает определения основных понятий абстрактной алгебры и теории чисел.;	• Умеет исследовать основные алгебраические структуры.;	• Имеет представление об использовании методов абстрактной алгебры и теории чисел.;

2.2 Компетенция ПК-1

ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 5.

Таблица 5 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание эта-	элементы теорий групп,	исследовать основные	методами абстрактной

пов	колец и полей, основы элементарной теории чисел, базовые алгебраические и теоретико-числовые алгоритмы.	алгебраические структуры; применять полученные знания для компьютерной реализации криптографических алгоритмов.	алгебры и теории чисел.
Виды занятий	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Самостоятельная работа;
Используемые средства оценивания	• Контрольная работа; • Домашнее задание; • Опрос на занятиях; • Экзамен;	• Контрольная работа; • Домашнее задание; • Опрос на занятиях; • Экзамен;	• Домашнее задание; • Экзамен;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 6.

Таблица 6 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Знает влияние параметров алгебраических структуру на свойства криптографических преобразований и стойкость криптографических алгоритмов.;	• Умеет применять аппарат абстрактной алгебры и теории чисел для получения оптимальных компьютерных реализаций криптографических алгоритмов.;	• Владеет основными методами абстрактной алгебры и теории чисел.;
Хорошо (базовый уровень)	• Знает влияние параметров алгебраических структуру на стойкость криптографических алгоритмов.;	• Умеет применять аппарат абстрактной алгебры и теории чисел для получения компьютерных реализаций криптографических алгоритмов.;	• Владеет некоторыми методами абстрактной алгебры и теории чисел.;
Удовлетворительно (пороговый уровень)	• Имеет преставление о влиянии параметров алгебраических структуру на стойкость криптографических алгоритмов.;	• Имеет представление о применении аппарата абстрактной алгебры и теории чисел для компьютерной реализации криптографических алгоритмов.;	• Имеет представление об использовании методов абстрактной алгебры и теории чисел.;

3 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы, в следующем составе.

3.1 Темы домашних заданий

- 1. Исследовать все свойства данной алгебраической структуры.
- 2. Исследовать абстрактную циклическую группу данного порядка.
- 3. Установить, является ли данное множество кольцом относительно данных операций.
- 4. Исследовать данное кольцо классов вычетов.
- 5. Исследовать данное поле Галуа.
- 6. Исследовать данную группу точек эллиптической кривой.
- 7. Найти целочисленную линейную комбинацию данной пары целых чисел.
- 8. Решить данное сравнение первой степени с одним неизвестным.
- 9. Решить данную систему сравнений.

3.2 Темы опросов на занятиях

- Множества, операции над ними. Отображения, их классификация. Бинарные отношения, отношения эквивалентности.
- Алгебраические операции. Свойства алгебраических операций. Алгебраические структуры. Типы алгебраических структур.
- Группы, подгруппы, критерий подгруппы. Теорема Лагранжа.
- Целочисленные степени элементов группы. Свойства целочисленных степеней. Циклические группы.
- Группы подстановок. Матричные группы.
- Кольца, подкольца, примеры колец. Критерий подкольца.
- Кольца многочленов. Кольца классов вычетов. Кольца матриц.
- Поля, подполя, примеры полей. Конечные поля.
- Поля Галуа. Исследование мультипликативной группы поля Галуа.
- Понятие эллиптической кривой над конечным полем. Исследование группы точек эллиптической кривой.
- Наибольший общий делитель. Алгоритм Евклида вычисления наибольшего общего делителя двух чисел. Расширенный алгоритм Евклида. Сравнения первой степени с одним неизвестным.
- Китайская теорема об остатках.
- Квадратичные вычеты. Критерий Эйлера. Критерий Гаусса. Символ Лежандра.
- Задача факторизации целых чисел на множители. Задача дискретного логарифмирования. Задача извлечения квадратного корня по модулю целого числа.

3.3 Темы контрольных работ

- 1. Исследовать все свойства данной алгебраической структуры. 2. Исследовать абстрактную циклическую группу данного порядка. 3. Установить, является ли данное множество кольцом относительно данных операций. 4. Исследовать данное кольцо классов вычетов. 5. Исследовать данное поле Галуа. 6. Исследовать данную группу точек эллиптической кривой. 7. Найти целочисленную линейную комбинацию данной пары целых чисел. 8. Решить данное сравнение первой степени с одним неизвестным. 9. Решить данную систему сравнений.

3.4 Темы контрольных работ

- 1. Исследовать все свойства данной алгебраической структуры. 2. Исследовать абстрактную циклическую группу данного порядка. 3. Установить, является ли данное множество кольцом относительно данных операций. 4. Исследовать данное кольцо классов вычетов. 5. Исследовать данное поле Галуа. 6. Исследовать данную группу точек эллиптической кривой. 7. Найти целочисленную линейную комбинацию данной пары целых чисел. 8. Решить данное сравнение первой степени с одним неизвестным. 9. Решить данную систему сравнений.

3.5 Экзаменационные вопросы

- 1. Понятие алгебраической операции, ее характеристические признаки. Свойства алгебраических операций.
- 2. Понятие алгебраической структуры. Типы алгебраических структур.

– 3. Понятие группы (два определения).
– 4. Определение подгруппы. Критерий подгруппы.
– 5. Целочисленные степени элементов группы. Свойства целочисленных степеней.
– 6. Циклические группы. Прямое произведение групп.
– 7. Группы подстановок.
– 8. Понятие кольца. Простейшие свойства колец.
– 9. Определение подкольца. Критерий подкольца.
– 10. Понятие бинарного отношения. Понятие отношения эквивалентности.
– 11. Кольца классов вычетов.
– 12. Кольца многочленов.
– 13. Понятие поля. Простейшие свойства полей.
– 14. Определение подполя. Критерий подполя.
– 15. Конечные поля.
– 16. Поля Галуа.
– 17. Эллиптические кривые над конечным полем.
– 18. Понятие НОД. Алгоритм Евклида. Расширенный алгоритм Евклида.
– 19. Сравнение первой степени с одним неизвестным.
– 20. Китайская теорема об остатках.
– 21. Функция Эйлера. Теорема Эйлера.
– 22. Квадратичные вычеты. Критерий Эйлера. Критерий Гаусса.
– 23. Символ Лежандра, его свойства.

4 Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие материалы:

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы фор-мирования компетенций, согласно п. 12 рабочей программы.

4.1. Основная литература

1. Росошек С.К. Специальные главы математики (математические основы криптографии): учебное пособие. Часть 1. — 2012. — 93 с. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/rososhek_sgm_1.pdf

2. Росошек С.К. Специальные главы математики (математические основы криптографии): учебное пособие. Часть 2. — 2012. — 190 с. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/rososhek_sgm_2.pdf

3. Курош А.Г. Курс высшей алгебры: учебник для вузов. — 16-е изд., стереотип. — СПб.: Лань, 2007; М.: Физматкнига, 2007. — 431 с. (наличие в библиотеке ТУСУР - 9 экз.)

4. Сизый С.В. Лекции по теории чисел: учебное пособие для вузов. — М.: Физматлит, 2007. — 190 с. (наличие в библиотеке ТУСУР - 10 экз.)

4.2. Дополнительная литература

1. Смарт Н. Криптография: учебник для вузов.— М. : Техносфера, 2005. — 525 с. (наличие в библиотеке ТУСУР - 11 экз.)

4.3. Обязательные учебно-методические пособия

1. Евсютин О.О. Криптографические методы защиты информации: методические указания для выполнения практических и самостоятельных работ. [Электронный ресурс]. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_kmzi.pdf

4.4. Базы данных, информационно справочные и поисковые системы

1. Не предусмотрено.