МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

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

_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Математические основы криптологии

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.02 Информационная безопасность телекоммуникационных систем**
Направленность (профиль) / специализация: **Безопасность телекоммуникационных систем информационного взаимодействия**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РСС, Кафедра радиоэлектроники и систем связи**
Курс: **3**
Семестр: **5**
Учебный план набора 2012 года

Распределение рабочего времени

№	Виды учебной деятельности	5 семестр	Всего	Единицы
1	Лекции	36	36	часов
2	Практические занятия	48	48	часов
3	Всего аудиторных занятий	84	84	часов
4	Самостоятельная работа	60	60	часов
5	Всего (без экзамена)	144	144	часов
6	Подготовка и сдача экзамена	36	36	часов
7	Общая трудоемкость	180	180	часов
		5.0	5.0	З.Е.

Экзамен: 5 семестр

Томск 2018

Согласована на портале №

35380

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.02 Информационная безопасность телекоммуникационных систем, утвержденного 16.11.2016 года, рассмотрена и одобрена на заседании кафедры РСС «___» _____ 20__ года, протокол №_____.

Разработчик:

Доцент каф. БИС _____ О. О. Евсютин

Заведующий обеспечивающей каф. РСС _____ А. В. Фатеев

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан РТФ _____ К. Ю. Попова

Заведующий выпускающей каф. РСС _____ А. В. Фатеев

Эксперты:

Доцент кафедры безопасности информационных систем (БИС) _____ А. Ю. Исхаков

Старший преподаватель кафедры радиоэлектроники и систем связи (РСС) _____ Ю. В. Зеленецкая

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.В.ОД.4) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: 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:

– ПСК-12.5 способностью применять стандартные средства для анализа программного кода кода с целью оценки уровня его защиты от исследования и поиска несанкционированного или вредоносного вмешательства в работу телекоммуникационных систем информационного взаимодействия;

В результате изучения дисциплины обучающийся 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 5.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		5 семестр
Аудиторные занятия (всего)	84	84
Лекции	36	36
Практические занятия	48	48
Самостоятельная работа (всего)	60	60
Проработка лекционного материала	17	17
Подготовка к практическим занятиям, семинарам	43	43
Всего (без экзамена)	144	144
Подготовка и сдача экзамена	36	36
Общая трудоемкость, ч	180	180
Зачетные Единицы	5.0	5.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Согласована на портале №

35380

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лек., ч	Прак.	Сам. раб	Всего	Формируем
5 семестр					
1 Множества и отображения	2	2	3	7	ПСК-12.5
2 Алгебраические операции	2	2	3	7	ПСК-12.5
3 Группы, подгруппы	2	2	3	7	ПСК-12.5
4 Циклические группы	2	2	3	7	ПСК-12.5
5 Различные классы групп	2	2	3	7	ПСК-12.5
6 Кольца	2	2	3	7	ПСК-12.5
7 Различные классы колец	4	4	6	14	ПСК-12.5
8 Поля	2	2	3	7	ПСК-12.5
9 Поля Галуа	4	4	6	14	ПСК-12.5
10 Эллиптические кривые	4	4	3	11	ПСК-12.5
11 Алгоритмы вычисления наибольшего общего делителя целых чисел	4	2	3	9	ПСК-12.5
12 Китайская теорема об остатках	2	2	3	7	ПСК-12.5
13 Квадратичные вычеты	2	2	3	7	ПСК-12.5
14 Сложные вычислительные задачи	2	4	6	12	ПСК-12.5
15 Проведение контрольных работ	0	12	9	21	ПСК-12.5
Итого за семестр	36	48	60	144	
Итого	36	48	60	144	

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)	Трудое	Формир
5 семестр			
1 Множества и отображения	Множества, операции над ними. Отображения, их классификация. Бинарные отношения, отношения эквивалентности.	2	ПСК-12.5
	Итого	2	
2 Алгебраические операции	Алгебраические операции. Свойства алгебраических операций. Алгебраические структуры. Типы алгебраических структур.	2	ПСК-12.5
	Итого	2	
3 Группы, подгруппы	Группы, подгруппы, критерий подгруппы. Теорема Лагранжа.	2	ПСК-12.5
	Итого	2	
4 Циклические группы	Целочисленные степени элементов группы. Свойства целочисленных степеней. Циклические группы.	2	ПСК-12.5
	Итого	2	

Согласована на портале №

35380

5 Различные классы групп	Группы подстановок. Матричные группы.	2	ПСК-12.5
	Итого	2	
6 Кольца	Кольца, подкольца, примеры колец. Критерий подкольца.	2	ПСК-12.5
	Итого	2	
7 Различные классы колец	Кольца многочленов. Кольца классов вычетов. Кольца матриц.	4	ПСК-12.5
	Итого	4	
8 Поля	Поля, подполя, примеры полей. Конечные поля.	2	ПСК-12.5
	Итого	2	
9 Поля Галуа	Поля Галуа. Исследование мультипликативной группы поля Галуа.	4	ПСК-12.5
	Итого	4	
10 Эллиптические кривые	Понятие эллиптической кривой над конечным полем. Исследование группы точек эллиптической кривой.	4	ПСК-12.5
	Итого	4	
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.	4	ПСК-12.5
	Итого	4	
12 Китайская теорема об остатках	Китайская теорема об остатках.	2	ПСК-12.5
	Итого	2	
13 Квадратичные вычеты	Квадратичные вычеты. Критерий Эйлера. Критерий Гаусса. Символ Лежандра.	2	ПСК-12.5
	Итого	2	
14 Сложные вычислительные задачи	Задача факторизации целых чисел на множители. Задача дискретного логарифмирования. Задача извлечения квадратного корня по модулю целого числа.	2	ПСК-12.5
	Итого	2	
Итого за семестр		36	

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, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий			Формы контроля
	Лек.	Практ. зан.	Сам. раб.	
ПСК-12.5	+	+	+	Контрольная работа, Домашнее задание, Экзамен, Проверка контрольных работ, Опрос на занятиях, Тест

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

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)	Трудое	Формир
5 семестр			
1 Множества и отображения	Операции над множествами. Исследование свойств отображений.	2	ПСК-12.5
	Итого	2	
2 Алгебраические операции	Исследование свойств алгебраических операций и алгебраических структур.	2	ПСК-12.5
	Итого	2	
3 Группы, подгруппы	Исследование свойств алгебраических операций и алгебраических структур.	2	ПСК-12.5
	Итого	2	
4 Циклические группы	Исследование абстрактных циклических групп.	2	ПСК-12.5
	Итого	2	
5 Различные классы групп	Исследование групп подстановок. Исследование матричных групп.	2	ПСК-12.5
	Итого	2	
6 Кольца	Исследование свойств колец.	2	ПСК-12.5
	Итого	2	

Согласована на портале №

35380

7 Различные классы колец	Исследование групп обратимых элементов колец классов вычетов.	4	ПСК-12.5
	Итого	4	
8 Поля	Исследование свойств полей.	2	ПСК-12.5
	Итого	2	
9 Поля Галуа	Построение полей Галуа. Исследование мультипликативных групп полей Галуа.	4	ПСК-12.5
	Итого	4	
10 Эллиптические кривые	Построение и исследование групп точек эллиптических кривых над конечными полями.	4	ПСК-12.5
	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	ПСК-12.5
	Итого	2	
12 Китайская теорема об остатках	Решение систем сравнений первой степени с одним неизвестным.	2	ПСК-12.5
	Итого	2	
13 Квадратичные вычеты	Установление разрешимости сравнений второй степени.	2	ПСК-12.5
	Итого	2	
14 Сложные вычислительные задачи	Разложение целых чисел на множители. Нахождение дискретных логарифмов. Извлечение квадратных корней по простым и составным модулям.	4	ПСК-12.5
	Итого	4	
15 Проведение контрольных работ	Подготовка к контрольным работам по изученному материалу. Проведение контрольных работ.	12	ПСК-12.5
	Итого	12	
Итого за семестр		48	

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	Формируемые	Формы контроля
5 семестр				
1 Множества и отображения	Подготовка к практическим занятиям, семинарам	2	ПСК-12.5	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	1		

Согласована на портале №

35380

	Итого	3		
2 Алгебраические операции	Подготовка к практическим занятиям, семинарам	2	ПСК-12.5	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	1		
	Итого	3		
3 Группы, подгруппы	Подготовка к практическим занятиям, семинарам	2	ПСК-12.5	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	1		
	Итого	3		
4 Циклические группы	Подготовка к практическим занятиям, семинарам	2	ПСК-12.5	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	1		
	Итого	3		
5 Различные классы групп	Подготовка к практическим занятиям, семинарам	2	ПСК-12.5	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	1		
	Итого	3		
6 Кольца	Подготовка к практическим занятиям, семинарам	2	ПСК-12.5	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	1		
	Итого	3		
7 Различные классы колец	Подготовка к практическим занятиям, семинарам	4	ПСК-12.5	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	2		
	Итого	6		
8 Поля	Подготовка к практическим занятиям, семинарам	2	ПСК-12.5	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	1		
	Итого	3		
9 Поля Галуа	Подготовка к практическим занятиям,	4	ПСК-12.5	Домашнее задание, Контрольная работа,

	семинарам			Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	2		
	Итого	6		
10 Эллиптические кривые	Подготовка к практическим занятиям, семинарам	2	ПСК-12.5	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	2	ПСК-12.5	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	1		
	Итого	3		
12 Китайская теорема об остатках	Подготовка к практическим занятиям, семинарам	2	ПСК-12.5	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	1		
	Итого	3		
13 Квадратичные вычеты	Подготовка к практическим занятиям, семинарам	2	ПСК-12.5	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	1		
	Итого	3		
14 Сложные вычислительные задачи	Подготовка к практическим занятиям, семинарам	4	ПСК-12.5	Домашнее задание, Контрольная работа, Опрос на занятиях, Проверка контрольных работ, Экзамен
	Проработка лекционного материала	2		
	Итого	6		
15 Проведение контрольных работ	Подготовка к практическим занятиям, семинарам	9	ПСК-12.5	Контрольная работа, Проверка контрольных работ
	Итого	9		
Итого за семестр		60		
	Подготовка и сдача экзамена	36		Экзамен
Итого		96		

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

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		20
Тест			10	10
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] - Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/rososhek_sgm_1.pdf (дата обращения: 28.06.2018).
2. Росошек С.К. Специальные главы математики (математические основы криптографии): учебное пособие. Часть 2. — 2012. — 190 с. [Электронный ресурс] - Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/rososhek_sgm_2.pdf (дата обращения: 28.06.2018).
3. Гречников Е.А. Вычислительно сложные задачи теории чисел: учебное пособие для вузов / Е.А. Гречников, С.В. Михайлов, Ю.В. Нестеренко И.А. Поповян. — М.: Издательство Московского университета, 2012. — 312 с. (наличие в библиотеке ТУСУР - 30 экз.)

12.2. Дополнительная литература

1. Основы криптографии: учебное пособие для вузов / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. — 3-е изд., испр. и доп. — М.: Гелиос АРВ, 2005. — 479 [1] с. (наличие в библиотеке ТУСУР - 30 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] - Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/evsutin_kmzi.pdf (дата обращения: 28.06.2018).

12.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и 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. Профессиональные базы данных и информационные справочные системы

1. https://edu.tusur.ru/ – Научно-образовательный портал ТУСУР.
2. http://fgosvo.ru – Портал Федеральных государственных образовательных стандартов высшего образования.
3. eLIBRARY.RU – Российская научная электронная библиотека, интегрированная с Российским индексом научного цитирования (РИНЦ).
4. Scopus – библиографическая и реферативная база данных.
5. SpringerLink – хранилище электронных копий научных книг и журналов, издаваемых компанией Springer.
6. IEEE Xplore – электронная платформа, содержащая полные тексты публикаций из журналов, материалов конференций, стандартов, издаваемых IEEE и IEE (Institution of Electrical Engineers).

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

13.1. Общие требования к материально-техническому и программному обеспечению дисциплины

13.1.1. Материально-техническое и программное 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. Имеются демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

13.1.2. Материально-техническое и программное обеспечение для практических занятий

Учебная аудитория

учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий семинарского типа, помещение для проведения групповых и индивидуальных консультаций, помещение для проведения текущего контроля и промежуточной аттестации

634034, Томская область, г. Томск, Вершинина улица, д. 47, 310 ауд.

Описание имеющегося оборудования:

- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение не требуется.

13.1.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Состав оборудования:

- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

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

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в

Согласована на портале №

35380

которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися **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 комфортного просмотра.

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

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

14.1.1. Тестовые задания

1. Что из перечисленного не относится к признакам алгебраической операции?

а) Всюдуопределенность
б) Обратимость
в) Однозначность
г) Замкнутость

2. Какой тип алгебраических структур наиболее часто используется для построения криптографических алгоритмов?

а) Группы
б) Полугруппы
в) Моноиды
г) Квазигруппы

3. Каким свойством должна обладать алгебраическая операция, чтобы на ее основе мог быть построен алгоритм зашифрования?

а) Ассоциативность
б) Коммутативность
в) Обратимость
г) Дистрибутивность

4. Какое из перечисленных свойств алгебраических структур не является обязательным для группы?

а) Ассоциативность
б) Коммутативность
в) Обратимость элементов
г) Существование нейтрального элемента

5. В каком случае группа называется циклической?

а) Если она состоит из конечного числа элементов
б) Если она содержит образующий элемент
в) Если она содержит обратимые элементы
г) Если групповая операция является коммутативной

6. Какие алгебраические операции задаются на множестве, имеющем структуру кольца?

а) Сложение и умножение
б) Сложение и вычитание
в) Сложение, умножение и деление

Согласована на портале №

35380

г) Умножение и деление

7. Какие числа образуют класс вычетов *a* по модулю *n*?
а) Все целые числа, которые меньше *n*
б) Все целые числа, которые больше *n*
в) Все целые числа, которые делятся нацело на *n*
г) Все целые числа, имеющие тот же остаток при делении на *n*, что и *a*

8. 112 mod 33 = ?
а) 13
б) 23
в) 112
г) 33

9. Каким свойством обладают элементы *a* и a^{-1} в кольце классов вычетов по модулю *n*?
а) $a \cdot a^{-1} = 0 \pmod{n}$
б) $a \cdot a^{-1} = -1 \pmod{n}$
в) $a \cdot a^{-1} = 1 \pmod{n}$
г) $a \cdot a^{-1} = n \pmod{n}$

10. В каком случае существует значение a^{-1} по модулю *n*?
а) Если *a* делит *n*
б) Если *n* делит *a*
в) Если НОД(a, n) = 1
г) Если НОД(a, n) > 1

11. Как выглядит группа обратимых элементов кольца Z_{12}?
а) {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11}
б) {1, 5, 7, 11}
в) {0, 2, 4, 6, 8, 10}
г) {1, 3, 5, 7, 11}

12. В каком случае кольцо классов вычетов по модулю *n* является полем?
а) Если *n* — четное число
б) Если *n* — нечетное число
в) Если *n* — простое число
г) Если *n* — составное число

13. Что представляют собой элементы поля Галуа?
а) Многочлены
б) Целые числа
в) Функции
г) Векторы

14. Какое поле Галуа соответствует множеству значений байта?
а) $GF(2^8)$
б) $GF(2^2)$
в) $GF(3^2)$
г) $GF(3^4)$

15. Сколько элементов содержит мультипликативная группа поля $GF(5^2)$?
а) 2
б) 5
в) 24

г) 25

16. Поставьте в соответствие двоичной последовательности 11001101 элемент поля Галуа $GF(2^8)$, в виде которого можно представить данную последовательность для проведения над ней криптографических преобразований.

а) $x^8 + x^7 + x^4 + x^3 + x$
б) $x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$
в) $x^7 + x^6 + x^3 + x^2 + 1$
г) $x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$

17. Как называется групповая операция в группе точек эллиптической кривой?

а) Сложением
б) Умножение
в) Деление
г) Конкатенация

18. Для чего служит расширенный алгоритм Евклида?

а) Для нахождения целочисленной линейной комбинации
б) Для нахождения наибольшего общего делителя
в) Для нахождения наименьшего общего делителя
г) Для факторизации чисел

19. Чему равное значение функции Эйлера φ(26)?

а) 2
б) 12
в) 13
г) 26

20. Что из перечисленного относится к сложным вычислительным операциям, на которых основывается стойкость некоторых криптографических алгоритмов?

а) Дискретное логарифмирование
б) Приведение по модулю
в) Умножение в кольце классов вычетов
г) Нахождение модулярно обратного элемента

14.1.2. 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.

Согласована на портале №

35380

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.

14.1.3. 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.

14.1.4. 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.

14.1.5. 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.

14.2. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 14.

Таблица 14 – Дополнительные материалы оценивания для лиц с ограниченными возможностями

здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	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 материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов 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.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся 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 лиц с ограниченными возможностями здоровья и 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 лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.