МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ
Проректор по учебной работе

_____ С.Т. Князев
«___» _____ 2018 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ
СПЕЦИАЛЬНЫЕ ГЛАВЫ МАТЕМАТИКИ

Перечень сведений о рабочей программе модуля	**Учетные данные**
Модуль **Специальные главы математики**	Код модуля **1139533** **Учебный план № 5347**
Образовательная программа **Компьютерная безопасность**	Код ОП **10.05.01/01.02**
Траектория образовательной программы	**Не предусмотрена**
Направление подготовки **Компьютерная безопасность**	Код направления и уровня подготовки **10.05.01**
Уровень подготовки **Специалитет**	
ФГОС ВО	Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО: **1 декабря 2016 г., № 1512**

Екатеринбург, 2018

Программа модуля составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Кафедра	Подпись
1	Ананичев Дмитрий Сергеевич	К. ф.-м. н., доцент	доцент	Кафедра алгебры и дискретной математики	

Руководитель модуля Д.С. Ананичев

Рекомендовано учебно-методическим советом института математики и компьютерных наук

Председатель учебно-методического совета А.Ю. Коврижных
Протокол № 12 от 15 декабря 2016 г.

Согласовано:

Дирекция образовательных программ Р.Х. Токарева

Руководитель образовательной программы (ОП), для которой реализуется модуль
В.А. Баранский

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ СПЕЦИАЛЬНЫЕ ГЛАВЫ МАТЕМАТИКИ

1.1. Объем модуля, 6 з.е.

1.2. Аннотация содержания модуля

Модуль входит в состав базовой части образовательной программы, состоит из трех дисциплин «Теория кодирования», «Методы алгебраической геометрии» и «Теория псевдослучайных генераторов». Цель изучения данных дисциплин — дать студентам фундаментальные знания о математических понятиях, конструкциях, алгоритмах и алгоритмических проблемах, на основе которых строятся современные технологии защиты информации.

2. СТРУКТУРА МОДУЛЯ И РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ ПО ДИСЦИПЛИНАМ

Наименования дисциплин с указанием, к какой части образовательной программы они относятся: базовой (Б), вариативной – по выбору вуза (ВВ), вариативной - по выбору студента (ВС).		Семестр изучения	Объем времени, отведенный на освоение дисциплин модуля							
			Аудиторные занятия, час.				Самостоятельная работа, включая все виды текущей аттестации, час.	Промежуточная аттестация (зачет, экзамен), час.	Всего по дисциплине	
			Лекции	Практические занятия	Лабораторные работы	Всего			Час.	Зач. ед.
1.	**(Б)** Теория псевдослучайных генераторов	8	17	17		34	34	4(З)	72	2
2.	**(Б)** Методы алгебраической геометрии в криптографии	9	17	17		34	34	4(З)	72	2
3.	**(Б)** Теория кодирования	9	17	17		34	34	4(З)	72	2
Всего на освоение модуля			**51**	**51**		**102**	**102**	**12**	**216**	**6**

3. ПОСЛЕДОВАТЕЛЬНОСТЬ ОСВОЕНИЯ ДИСЦИПЛИН В МОДУЛЕ

3.1.	**Пререквизиты и постреквизиты в модуле**	
3.2.	**Кореквизиты**	Теория псевдослучайных генераторов Методы алгебраической геометрии в криптографии, Теория кодирования (дисциплины независимы)

4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ МОДУЛЯ

4.1. Планируемые результаты освоения модуля и составляющие их компетенции

Коды ОП, для которых реализуется модуль	**Планируемые в ОХОП результаты обучения -РО, которые формируются при освоении модуля**	**Компетенции в соответствии с ФГОС ВО, а также дополнительные из ОХОП, формируемые при освоении модуля**
10.05.01/01.02	РО2. Способность применять основополагающие принципы и современные достижения физико-математических наук, математического описания и построения компьютерных систем, а также современные информационные технологии в разработке технологических решений с использованием программного кода.	ПК-4, способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем; ОПК-1, способность анализировать физические явления и процессы при решении профессиональных задач; ОПК-2, способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов; ОПК-8, способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач; ПСК-2.2, способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах; ПСК-2.3, способностью строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов; ПСК-2.5, способность проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации.
10.05.01/01.02	РО3. Способность осуществлять проектирование систем защиты информации с учётом актуальных информационных угроз и с использованием	ОК-2, способность использовать основы экономических знаний в различных сферах деятельности; ОПК-4, способность применять методы научных исследований в

	современных достижений науки и техники.	профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами; ОПК-7, способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения; ОПК-9, способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации; ОПК-10, способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах; ПК-5, способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации; ПК-6, способность участвовать в разработке проектной и технической документации; ПК-7, способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем; ПК-8, способность участвовать в разработке подсистемы информационной безопасности компьютерной системы; ПСК-2.2, способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах; ПСК-2.3, способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием

		современных математических методов.
10.05.01/01.02	РО8. Способность к разработке, анализу и обоснованию адекватности математических моделей процессов, возникающих при функционировании программно-аппаратных средств защиты информации, а также к разработке математических моделей для оценки безопасности компьютерных систем.	ОПК-2, способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов; ОПК-7, способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения; ОПК-8, способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач; ОПК-9, способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации; ОПК-10, способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах; ПК-4, способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем; ПК-5, способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации; ПК-6, способность участвовать в разработке проектной и технической документации; ПК-8, способность участвовать в

		разработке подсистемы информационной безопасности компьютерной системы; ПСК-2.1, способностью разрабатывать вычислительные алгоритмы, реализующие современные методы защиты информации; ПСК-2.2, способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах; ПСК-2.3, способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов; ПСК-2.4, способность разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации; ПСК-2.5, способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации.

4.2.Распределение формирования компетенций по дисциплинам модуля

	Дисциплины модуля	ОК 2	ОПК 1,2,4,7, 8,9,10	ПК 4,5,6,7,8	ПСК 2.1,2.2,2.3, 2.4, 2.5
1	**(Б)** Теория псевдослучайных генераторов	*	*	*	*
2	**(Б)** Методы алгебраической геометрии в криптографии	*	*	*	*
3	**(Б)** Теория кодирования	*	*	*	*

5. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО МОДУЛЮ

Не предусмотрено

6. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В РАБОЧЕЙ ПРОГРАММЕ МОДУЛЯ

Номер листа изменений	Номер протокола заседания проектной группы модуля	Дата заседания проектной группы модуля	Всего листов в документе	Подпись руководителя проектной группы модуля

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
МЕТОДЫ АЛГЕБРАИЧЕСКОЙ ГЕОМЕТРИИ

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Модуль **Специальные главы математики**	Код модуля **1139533** **Учебный план № 5347**
Образовательная программа **Компьютерная безопасность**	Код ОП **10.05.01/01.02**
Направление подготовки **Компьютерная безопасность**	Код направления и уровня подготовки **10.05.01**
Уровень подготовки **Специалитет**	
ФГОС ВО	Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО: **1 декабря 2016 г., № 1512**

Екатеринбург, 2018

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Кафедра	Подпись
1	Ананичев Дмитрий Сергеевич	К. ф.-м. н., доцент	доцент	Кафедра алгебры и дискретной математики	

Руководитель модуля Д.С. Ананичев

Рекомендовано учебно-методическим советом института математики и компьютерных наук

Председатель учебно-методического совета А.Ю. Коврижных
Протокол № 12 от 15 декабря 2016 г.

Согласовано:

Дирекция образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ МЕТОДЫ АЛГЕБРАИЧЕСКОЙ ГЕОМЕТРИИ

1.1.Аннотация содержания дисциплины

Дисциплина «Методы алгебраической геометрии» является одной из трех дисциплин модуля «Специальные главы математики». Она независима от других дисциплин модуля. Изучается в девятом семестре.

Курс «Методы алгебраической геометрии» посвящен изучению свойств кубических кривых над полями простой характеристики. Подробно рассматриваются нормальные формы кривой и операция сложения ее точек над полями различных простых характеристик.

Изучение дисциплины предполагает 17 часов лекций и 17 часов практических занятий и зачет в качестве промежуточной аттестации.

.

1.2. Язык реализации программы - русский

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

ОК-2, способность использовать основы экономических знаний в различных сферах деятельности;

ОПК-1, способность анализировать физические явления и процессы при решении профессиональных задач;

ОПК-2, способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов;

ОПК-4, способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами;

ОПК-7, способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения;

ОПК-8, способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач;

ОПК-9, способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации;

ОПК-10, способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах;

ПК-4, способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем;

ПК-5, способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

ПК-6, способность участвовать в разработке проектной и технической документации;

ПК-7, способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем;

ПК-8, способность участвовать в разработке подсистемы информационной безопасности компьютерной системы;

ПСК-2.1, способностью разрабатывать вычислительные алгоритмы, реализующие современные методы защиты информации;
ПСК-2.2, способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах;
ПСК-2.3, способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов;
ПСК-2.4, способность разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации;
ПСК-2.5, способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации.

В результате освоения дисциплины студент должен:

Знать основные понятия и результаты теории кодирования.

Уметь решать задачи на кодирование и декодирование с исправлением ошибок для наиболее известных кодов.

Владеть методами построения кодов и оценки их качества.

1.4.Объем дисциплины

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	9 семестр
1.	**Аудиторные занятия**	**34**	**34**	**34**
2.	Лекции	17	17	17
3.	Практические занятия	17	17	17
4.	Лабораторные работы			
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	**34**	**5,1**	**34**
6.	**Промежуточная аттестация**	**4**	**0,25**	**Зачет(4)**
7.	**Общий объем по учебному плану, час.**	**72**	**39,35**	**72**
8.	**Общий объем по учебному плану, з.е.**	**2**		**2**

*Контактная работа составляет:

в п/п 2,3,4 - количество часов, равное объему соответствующего вида занятий;

в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в группе (15% от объема аудиторных занятий) и объема времени, выделенного преподавателю на руководство курсовой работой/проектом одного студента, если она предусмотрена.

в п.6 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного студента и объема времени, выделенного в рамках дисциплины на руководство проектом по модулю (если он предусмотрен) одного студента.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины	Содержание
Р1	**Кубическая кривая на плоскости.**	Определения. Сложение точек. Теорема о 9 точках.
Р2	**Проективная плоскость.**	Определения п.плоскости и геометрических объектов в ней. Особые точки кривой и их влияние на операцию сложения точек. Формула Эйлера.
Р3	**Нормальные формы неособой кубической кривой.**	Вывод нормальных форм над полем характеристики >3. Выводы нормальных форм над полями характеристик 2 и 3. Вывод условия отсутствия особых точек для кривых в нормальной форме.
Р4	**Сложение точек.**	Вывод формул для сложения точек на кривых в нормальных формах.
Р5	**Теорема Хассе.**	Доказательство Манина теоремы Хассе.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

5 семестр

Объем модуля (зач.ед.): 6
Объем дисциплины (зач.ед.): 2

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																						
								Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)												Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	**Всего (час.)**	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иноязы. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
Р1	Кубическая кривая на плоскости.	**2,4**	**2**	2	0		**0,4**	**0,4**	0,4	0,0																				
Р2	Проективная плоскость.	**9,2**	**7**	4	3		**2,2**	**2**	0,8	1,4																				
Р3	Нормальные формы неособой кубической кривой.	**19**	**8**	2	4		**11**	**3**	0,4	2,6			8					1												
Р4	Сложение точек.	**29**	**10**	2	10		**19**	**3**	0,4	2,6			16					2												
Р5	Теорема Хассе.	**8,4**	**7**	7	0		**1,4**	**1,4**	1,4	0,0																				
	Всего (час), без учета промежуточной аттестации**:**	**68**	**34**	**17**	**17**	**0**	**34**	**10**	**3,4**	**6,6**	**0**	**0**	**24**	**0**	**0**	**0**	**0**	**24**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**				
	Всего по дисциплине (час.):	**72**	**34**				**38**	В т.ч. промежуточная аттестация																			**4**	**0**	**0**	**0**

*Суммарный объем в часах на мероприятие
указывается в строке «Всего (час.) без учета промежуточной аттестации

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1. Лабораторные работы

«не предусмотрено»

4.2. Практические занятия

Код раздела, темы	Номер занятия	Тема занятия	Время на проведение занятия (час.)
P2	1	Построение проективных плоскостей.	3
P3	2	Построение кубических кривых над простыми полями.	2
P3	3	Построение кубических кривых над полями характеристики 2.	2
P4	4	Сложение и умножение точек над простыми полями	4
P4	5	Сложение и умножение точек над полями характеристики 2.	6
		Всего:	17

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

«не предусмотрено»

4.3.2. Примерный перечень тем графических работ

«не предусмотрено»

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

«не предусмотрено»

4.3.4 Примерная тематика индивидуальных или групповых проектов

«не предусмотрено»

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

1. Построение множества точек кубической кривой над полем характеристики 2.
2. Сложение и умножение точек над простыми полями.
3. Сложение и умножение точек над полями характеристики 2.

4.3.6. Примерный перечень тем расчетно-графических работ

«не предусмотрено»

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

«не предусмотрено»

4.4.1. Примерная тематика контрольных работ

«не предусмотрено»

4.3.9. Примерная тематика коллоквиумов

«не предусмотрено»

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
Р1		+		+	+							
Р2		+		+	+							
Р3		+		+	+							
Р4		+		+	+							
Р5		+		+	+							

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1.Основная литература

1. J.H.Silverman, The Arithmetic of Elliptic Curves.- Spriger 2009.
   DOI: 10.1007/978-0-387-09494-6
   https://www.springer.com/gp/book/9780387094939#otherversion=9781441918581
2. Ю.Г.Прохоров, Эллиптические кривые и криптография.
   www.mi.ras.ru/~prokhoro/teach/crypt.pdf

9.1.2.Дополнительная литература

1. Ю. И. Манин, О сравнениях третьей степени по простому модулю, Изв. АН СССР. Сер. матем., 1956, том 20, выпуск 5, 673–678
   http://mi.mathnet.ru/izv3844
2. FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Digital Signature Standard (DSS) NIST FIPS PUB 186-4
http://dx.dopi.org/10.6028/NIST.FIPS.186-4.

9.2. Методические разработки

Не используются

9.3.Программное обеспечение

Не используется

9.4. Базы данных, информационно-справочные и поисковые системы

Общероссийский математический портал http://www.mathnet.ru/
Научная электронная библиотека eLibrary.ru http://www.elibrary.ru/
Сайт издательства Elsevier http://www.sciencedirect.com/
Сайт кафедры: http://kma.imkn.urfu.ru
Сайт кафедры: http://kadm.imkn.urfu.ru/pages.php?id=index
Сайт библиотеки университета http://lib.urfu.ru/

9.5.Электронные образовательные ресурсы

Не используются

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Аудитория с проектором

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0,6		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Конспект литературного источника № 1	**9, 1-17**	**50**
Конспект литературного источника № 2	**9, 1-17**	**50**
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – *зачет* **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0,4		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Расчетная работа № 1	**1, 1-10**	**40**
Расчетная работа № 2	**1, 1-14**	**30**
Расчетная работа № 3	**1, 1-17**	**30**
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям–1		
Промежуточная аттестация по практическим/семинарским занятиям– не предусмотрено **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –не предусмотрены		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Не предусмотрены

6.4. Коэффициент значимости семестровых результатов освоения дисциплины

Порядковый номер семестра по учебному плану, в котором осваивается дисциплина	**Коэффициент значимости результатов освоения дисциплины в семестре**
Семестр 9	1

*В случае проведения промежуточной аттестации по дисциплине (экзамена, зачета) методом тестирования используются официально утвержденные ресурсы: АПИМ УрФУ, СКУД УрФУ, имеющие статус ЭОР УрФУ; ФЭПО (www.фэпо.рф); Интернет-тренажеры (www.i-exam.ru).

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Не применяется

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной дея-	Студент имеет выраженную мотивацию	Студент имеет развитую мотивацию учеб-

	тельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	ной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

НТК не проводится

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий

«не предусмотрено»

8.3.2. Примерные контрольные задачи в рамках учебных занятий

«не предусмотрено»

8.3.3. Примерные контрольные кейсы

«не предусмотрено»

8.3.4. Перечень примерных вопросов для зачета

«не предусмотрено»

8.3.5. Перечень примерных вопросов для экзамена

1. Пересечение проективной кубической кривой и проективной прямой.
2. Особые точки кривой и их влияние на операцию сложения точек.
3. Формула Эйлера.
4. Вывод нормальных форм над полем характеристики >3.
5. Выводы нормальных форм над полями характеристик 2 и 3.
6. Вывод формул для сложения точек на кривых в нормальных формах.
7. Теорема Хассе. Общая структура.
8. Теорема Хассе. Лемма о связи числа точек со степенями числителей абсцисс точек.
9. Теорема Хассе. Лемма о соотношении степеней числителя и знаменателя абсциссы точки.
10. Теорема Хассе. Лемма о произведении знаменателей.
11. Теорема Хассе. Леммы о рекуррентных соотношениях.

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

«не используются»

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

«не используются»

8.3.8. Интернет-тренажеры

«не используются»

8.3.9. Примерные задания для расчетных работ (программный продукт)

Расчетная работа № 1.

Задание. Создать программу порождения множества точек эллиптической кривой.

Расчетная работа № 2.

Задание. Создать программу сложения и умножения точек эллиптической кривой над простым полем с длинной арифметикой.

Расчетная работа № 3.

Задание. Создать программу сложения и умножения точек эллиптической кривой над полем характеристики 2 с длинной арифметикой.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ТЕОРИЯ КОДИРОВАНИЯ

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Модуль **Специальные главы математики**	Код модуля **1139533** **Учебный план № 5347**
Образовательная программа **Компьютерная безопасность**	Код ОП **10.05.01/01.02**
Направление подготовки **Компьютерная безопасность**	Код направления и уровня подготовки **10.05.01**
Уровень подготовки **Специалитет**	
ФГОС ВО	Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО: **1 декабря 2016 г., № 1512**

Екатеринбург, 2018

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Кафедра	Подпись
1	Ананичев Дмитрий Сергеевич	К. ф.-м. н., доцент	доцент	Кафедра алгебры и дискретной математики	

Руководитель модуля Д.С. Ананичев

Рекомендовано учебно-методическим советом института математики и компьютерных наук

Председатель учебно-методического совета А.Ю. Коврижных
Протокол № 12 от 15 декабря 2016 г.

Согласовано:

Дирекция образовательных программ Р.Х. Токарева

Руководитель образовательной программы (ОП), для которой реализуется модуль
В.А. Баранский

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ ТЕОРИЯ КОДИРОВАНИЯ

1.1.Аннотация содержания дисциплины

Дисциплина «Теория кодирования» является одной из трех дисциплин модуля «Специальные главы математики». Она независима от других дисциплин модуля. Изучается в девятом семестре.

Курс «Теория кодирования» посвящен изучению с теоретической и алгоритмической точек зрения задач защиты информации от случайного шума. Подробно рассматриваются базовые понятия теории кодирования, а также некоторые серии кодов имеющих эффективные алгоритмы декодирования.

Изучение дисциплины предполагает 17 часов лекций и 17 часов практических занятий и зачет в качестве промежуточной аттестации.

1.2. Язык реализации программы - русский

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

ОК-2, способность использовать основы экономических знаний в различных сферах деятельности;

ОПК-1, способность анализировать физические явления и процессы при решении профессиональных задач;

ОПК-2, способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов;

ОПК-4, способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами;

ОПК-7, способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения;

ОПК-8, способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач;

ОПК-9, способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации;

ОПК-10, способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах;

ПК-4, способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем;

ПК-5, способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

ПК-6, способность участвовать в разработке проектной и технической документации;

ПК-7, способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем;

ПК-8, способность участвовать в разработке подсистемы информационной безопасности компьютерной системы;

ПСК-2.1, способностью разрабатывать вычислительные алгоритмы, реализующие современные методы защиты информации;

ПСК-2.2, способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах;
ПСК-2.3, способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов;
ПСК-2.4, способность разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации;
ПСК-2.5, способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации.

В результате освоения дисциплины студент должен:

Знать основные понятия и результаты теории кодирования.

Уметь решать задачи на кодирование и декодирование с исправлением ошибок для наиболее известных кодов.

Владеть методами построения кодов и оценки их качества.

1.4.Объем дисциплины

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	9 семестр
1.	**Аудиторные занятия**	**34**	**34**	**34**
2.	Лекции	17	17	17
3.	Практические занятия	17	17	17
4.	Лабораторные работы			
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	**34**	**5,1**	**34**
6.	**Промежуточная аттестация**	**4**	**0,25**	**Зачет (4)**
7.	**Общий объем по учебному плану, час.**	**72**	**39,35**	**72**
8.	**Общий объем по учебному плану, з.е.**	**2**		**2**

*Контактная работа составляет:

в п/п 2,3,4 - количество часов, равное объему соответствующего вида занятий;

в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в группе (15% от объема аудиторных занятий) и объема времени, выделенного преподавателю на руководство курсовой работой/проектом одного студента, если она предусмотрена.

в п.6 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного студента и объема времени, выделенного в рамках дисциплины на руководство проектом по модулю (если он предусмотрен) одного студента.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины	Содержание
Р1	**Модель канала без памяти.**	Математическая модель, изучаемая теорией кодирования: двоичный симметричный канал без памяти. Обсуждение модели. Теорема Шеннона.
Р2	**Основные параметры кодов, исправляющих ошибки.**	Длина, скорость, минимальное расстояние. Связь между минимальным расстоянием и корректирующими возможностями кода. Граница Хэмминга. Совершенные коды.
Р3	**Линейные коды.**	Порождающая матрица. Граница Синглтона. Граница Плоткина. Граница Элайса. Дуальный код. Контрольная матрица. Код Хэмминга. Характеризация минимального расстояния в терминах контрольной матрицы. Граница Гильберта-Варшамова. Коды Рида-Маллера. Коды Гоппы. NP-полнота задачи декодирования общего линейного кода по синдрому.
Р4	**Циклические коды.**	Связь с идеалами кольца многочленов. Коды, исправляющие пакеты ошибок. Граница Рейджера. Алгоритм исправления пакетов ошибок. Обзор кодов, исправляющих пакеты ошибок. Перемежение. Коды Файра.
Р5	**Коды Боуза-Чоудхури-Хоквингема (БЧХ).**	Граница БЧХ. Алгоритм Питерсона декодирования кодов БЧХ. Алгоритм Берлекэмпа. . Коды Рида-Соломона. Укороченные и каскадные коды. Алгоритм Форни.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

5 семестр

Объем модуля (зач.ед.): 6
Объем дисциплины (зач.ед.): 2

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																					
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)											Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Ни семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иностр. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
Р1	Модель канала без памяти.	**2,4**	**2**	2			**0,4**	**0,4**	0,4																					
Р2	Основные параметры кодов, исправляющих ошибки.	**9**	**6**	4	2		**3**	**3**	0,8	2,2																				
Р3	Линейные коды.	**20,2**	**10**	4	6		**10,2**	**2,2**	0,8	1,4			8					1												
Р4	Циклические коды.	**18,2**	**8**	4	4		**10,2**	**2,2**	0,8	1,4			8					1												
Р5	Коды БЧХ.	**18,2**	**8**	3	5		**10,2**	**2,2**	0,8	1,4			8					1												
	Всего (час), без учета промежуточной аттестации**:**	**68**	**34**	**17**	**17**	**0**	**34**	**10**	**3,6**	**6,4**	**0**	**0**	**24**	**0**	**0**	**0**	**0**	**24**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**				
	Всего по дисциплине (час.):	**72**	**34**				**38**	В т.ч. промежуточная аттестация																			**4**	**0**	**0**	**0**

*Суммарный объем в часах на мероприятие
указывается в строке «Всего (час.) без учета промежуточной аттестации

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1. Лабораторные работы

«не предусмотрено»

4.2. Практические занятия

Код раздела, темы	Номер заня-тия	Тема занятия	Время на проведение занятия (час.)
P1	1	Вычисление кодового расстояния.	2
P3	2	Порождающая и проверочная матрицы.	2
P3	3	Коды Рида-Малера.	2
P3	4	Коды Гоппы.	2
P4	5	Порождающий многочлен и матрица циклического кода.	2
P4	6	Коды Файра	2
P4	7	Коды БЧХ.	3
P5	8	Укороченные и каскадные коды.	2
		Всего:	17

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

«не предусмотрено»

4.3.2. Примерный перечень тем графических работ

«не предусмотрено»

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

«не предусмотрено»

4.3.4 Примерная тематика индивидуальных или групповых проектов

«не предусмотрено»

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

1. Решение задачи декодирования кода Гоппы.
2. Построение циклического кода с заданными параметрами.
3. Решение задачи декодирования кода БЧХ.

4.3.6. Примерный перечень тем расчетно-графических работ

«не предусмотрено»

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

«не предусмотрено»

4.4.1. Примерная тематика контрольных работ

«не предусмотрено»

4.3.9. Примерная тематика коллоквиумов

«не предусмотрено»

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
Р1		+		+	+							
Р2		+		+	+							
Р3		+		+	+							
Р4		+		+	+							
Р5		+		+	+							

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1.Основная литература

1. Сидельников, В.М. Теория кодирования [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : Физматлит, 2008. — 320 с. <URL: http://www.biblioclub.ru/book/68384/>.
2. Штарьков, Ю.М. Универсальное кодирование. Теория и алгоритмы [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : Физматлит, 2013. — 288 с. — Режим доступа: https://e.lanbook.com/book/59667.
3. Лидл, Рудольф. Прикладная абстрактная алгебра : Учеб. пособие / Р. Лидл, Г. Пильц ; Пер. с англ. — Екатеринбург : Изд-во Урал. ун-та, 1996. — 744 с. — ISBN 5-7525-0483-X : 40000-00. 50 экз

9.1.2.Дополнительная литература

Ромащенко А. Е., Румянцев А. Ю., Шень А. Р47 Заметки по теории кодирования. | М.: МЦНМО, 2011. | 80 с. ISBN 978-5-94057-750-8

https://www.mccme.ru/~anromash/courses/coding-theory-05-2016.pdf

9.2. Методические разработки

Не используются

9.3.Программное обеспечение

Не используется

9.4. Базы данных, информационно-справочные и поисковые системы

Общероссийский математический портал http://www.mathnet.ru/
Научная электронная библиотека eLibrary.ru http://www.elibrary.ru/
Сайт издательства Elsevier http://www.sciencedirect.com/
Сайт кафедры: http://kma.imkn.urfu.ru
Сайт кафедры: http://kadm.imkn.urfu.ru/pages.php?id=index
Сайт библиотеки университета http://lib.urfu.ru/

9.5.Электронные образовательные ресурсы

Не используются

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Аудитория с проектором

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины –

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0,6		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Конспект литературного источника № 1	**9, 1-17**	**50**
Конспект литературного источника № 2	**9, 1-17**	**50**
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – *зачет* **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0,4		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Расчетная работа № 1	**1, 1-10**	**40**
Расчетная работа № 2	**1, 1-14**	**30**
Расчетная работа № 3	**1, 1-17**	**30**
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям–1		
Промежуточная аттестация по практическим/семинарским занятиям– не предусмотрено **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –не предусмотрены		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта
Не предусмотрены

6.4. Коэффициент значимости семестровых результатов освоения дисциплины

Порядковый номер семестра по учебному плану, в котором осваивается дисциплина	**Коэффициент значимости результатов освоения дисциплины в семестре**
Семестр 9	1

*В случае проведения промежуточной аттестации по дисциплине (экзамена, зачета) методом тестирования используются официально утвержденные ресурсы: АПИМ УрФУ, СКУД УрФУ, имеющие статус ЭОР УрФУ; ФЭПО (www.фэпо.рф); Интернет-тренажеры (www.i-exam.ru).

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Не применяется

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной дея-	Студент имеет выраженную мотивацию	Студент имеет развитую мотивацию учеб-

	тельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	ной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

НТК не проводится

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий
«не предусмотрено»

8.3.2. Примерные контрольные задачи в рамках учебных занятий
«не предусмотрено»

8.3.3. Примерные контрольные кейсы
«не предусмотрено»

8.3.4. Перечень примерных вопросов для зачета

1. Теорема Шеннона.
2. Граница Хэмминга. Совершенные коды.
3. Граница Синглтона.
4. Граница Плоткина.
5. Граница Гильберта-Варшамова.
6. Коды Рида-Маллера.
7. Циклические коды. Связь с идеалами кольца многочленов.
8. Граница Рейджера.
9. Алгоритм исправления пакетов ошибок.
10. Перемежение.
11. Коды Файра.
12. Граница БЧХ.
13. Алгоритм декодирования кодов БЧХ.
14. Коды Рида-Соломона.
15. Коды Гоппы.
16. Укороченные и каскадные коды.
17. Алгоритм Форни.
18. NP-полнота задачи декодирования.

8.3.5. Перечень примерных вопросов для экзамена
«не предусмотрено»

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации
«не используются»

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля
«не используются»

8.3.8. Интернет-тренажеры
«не используются»

8.3.9. Примерные задания для расчетных работ (программный продукт)

Расчетная работа № 1.
Задание. Создать программу декодирования кода Гоппы.
Расчетная работа № 2.
Задание. Создать программу поиска двоичного циклического кода с заданной длиной кода и длиной исправляемого пакета.
Расчетная работа № 3.
Задание. Создать программу декодирования кода БЧХ**.**

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ТЕОРИЯ ПСЕВДОСЛУЧАЙНЫХ ГЕНЕРАТОРОВ

Перечень сведений о рабочей программе модуля	**Учетные данные**
Модуль **Специальные главы математики**	Код модуля **1139533** **Учебный план № 5347**
Образовательная программа **Компьютерная безопасность**	Код ОП **10.05.01/01.02**
Направление подготовки **Компьютерная безопасность**	Код направления и уровня подготовки **10.05.01**
Уровень подготовки **Специалитет**	
ФГОС ВО	Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО: **1 декабря 2016 г., № 1512**

Екатеринбург, 2018

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Департамент	Подпись
1	Попов Владимир Юрьевич	д.ф.-м.н., доцент	Профессор	Кафедра алгебры и фундаментальной информатики	

Руководитель модуля Д.С. Ананичев

Рекомендовано учебно-методическим советом института математики и компьютерных наук

Председатель учебно-методического совета А.Ю. Коврижных
Протокол № 12 от 15 декабря 2016 г.

Согласовано:

Дирекция образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ «ТЕОРИЯ ПСЕВДОСЛУЧАЙНЫХ ГЕНЕРАТОРОВ»

1.1.Аннотация содержания дисциплины

Дисциплина «Теория псевдослучайных генераторов» является одной из трех дисциплин модуля «Специальные главы математики». Она независима от других дисциплин модуля. Изучается в восьмом семестре.

Дисциплина посвящена изучению математических основ и основных типов псевдослучайных генераторов, а также рассмотрению вопросов криптографической надежности псевдослучайных генераторов.

Изучение дисциплины предполагает 17 часов лекций и 17 часов практических занятий и зачет в качестве промежуточной аттестации.

1.2. Язык реализации программы – *русский*

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

ОК-2, способность использовать основы экономических знаний в различных сферах деятельности;

ОПК-1, способность анализировать физические явления и процессы при решении профессиональных задач;

ОПК-2, способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов;

ОПК-4, способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами;

ОПК-7, способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения;

ОПК-8, способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач;

ОПК-9, способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации;

ОПК-10, способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах;

ПК-4, способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем;

ПК-5, способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства крипто-графической защиты информации;

ПК-6, способность участвовать в разработке проектной и технической документации;

ПК-7, способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем;

ПК-8, способность участвовать в разработке подсистемы информационной безопасности компьютерной системы;

ПСК-2.1, способностью разрабатывать вычислительные алгоритмы, реализующие современные методы защиты информации;
ПСК-2.2, способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах;
ПСК-2.3, способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов;
ПСК-2.4, способность разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации;
ПСК-2.5, способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации.

В результате освоения дисциплины студент должен:

Знать:
- классификацию и общую характеристику основных типов псевдослучайных генераторов;
- основные принципы построения псевдослучайных генераторов;
- особенности реализации псевдослучайных генераторов.

Уметь:
- применять механизмы защиты, реализующие псевдослучайные генераторы;
- оценивать и контролировать эффективность псевдослучайных генераторов;
- разрабатывать компоненты псевдослучайных генераторов.

Владеть (демонстрировать навыки и опыт деятельности):
- методикой разработки и применения псевдослучайных генераторов.

1.4.Объем дисциплины

Очная форма обучения

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	*9*
1.	**Аудиторные занятия**	**34**	**34**	**34**
2.	Лекции	17	17	17
3.	Практические занятия	17	17	17
4.	Лабораторные работы			
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	**34**	**5,1**	**34**
6.	**Промежуточная аттестация**	**4**	**0,25**	**Зачет(4)**
7.	**Общий объем по учебному плану, час.**	**72**	**39,35**	**72**
8.	**Общий объем по учебному плану, з.е.**	**2**		**2**

*Контактная работа составляет:

в п/п 2,3,4 - количество часов, равное объему соответствующего вида занятий;

в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в группе (15% от объема аудиторных занятий) и объема времени, выделенного преподавателю на руководство курсовой работой/проектом одного студента, если она предусмотрена.

в п.6 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного студента и объема времени, выделенного в рамках дисциплины на руководство проектом по модулю (если он предусмотрен) одного студента.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины	Содержание
1	**Теория псевдослучайных генераторов на основе машин Тьюринга**	Парадокс метода Монте-Карло. Понятие машины Тьюринга как псевдослучайного генератора. Применение универсальных машин Тьюринга. Применение простейших клеточных автоматов. Игра "Жизнь" как модель для порождения псевдослучайных последовательностей. Использование моделей управления при помощи глобальных сигналов для порождения псевдослучайных последовательностей. Применение Redcode для порождения псевдослучайных последовательностей. Использование эзотерических языков для порождения псевдослучайных последовательностей. Порождение псевдослучайных последовательностей на основе машины Минского. Недетерминированные машины Тьюринга для порождения псевдослучайных последовательностей.
2	**Варианты определения случайной последовательности**	Определения по Лехмеру и Франклину. Понятие к-распределенности. Понятие конечной случайной последовательности.
3	**Тесты на случайность**	Алгоритм Кнута. Простейшие тесты на случайность. Chi-test. Тест Колмогорова - Смирнова. Gap test. Покерный тест. Тесты на количество значений на интервале. Перестановочные тесты. Тесты на возрастание и убывание. Распределение максимальных значений на интервале. Тестирование подпоследовательностей. Коэффициент корреляции. Линейные конгруэнтные последовательности. Спектральный тест. Постулаты Голомба. NIST.
4	**Использование криптографических алгоритмов для генерации псевдослучайных чисел**	Блочные алгоритмы. Потоковые шифры. Алгоритмы с открытым ключем.
5	**Генераторы псевдослучайных последовательностей и потоковые шифры**	Линейные конгруэнтные генераторы. Регистры сдвига с обратной связью. Генератор Геффе. Генератор Дженнингса. Генератор Бета-Пайпера. Пороговый генератор. Генератор Голлмана. Сжимающий генератор. Самосжимающий генератор. A5. Hughes. Nanoteq. Rambutan. Fish. Pike. Mush. M. RC4. SEAL. WAKE. Генератор Плесса.
6	**Генераторы истинно случайных**	Таблицы. Шум. Таймеры. Задержки. Извлеченная случайность.

	последовательностей	
7	**Сплетения псевдослучайных генераторов**	Основные свойства апериодических последовательностей с точки зрения теории псевдослучайных генераторов. Последовательность Туэ - Морса. Последовательность Фибоначчи. Механические последовательности. Методы представления информации при использовании апериодических последовательностей для генерации псевдослучайных чисел. Порождение сплетений псевдослучайных генераторов.
8	**Интеллектуальные методы для порождения и тестирования псевдослучайных последовательностей**	Нейросетевые методы. Обобщение линейных конгруэнтных генераторов на основе нейронных сетей. Применение генетических алгоритмов для порождения и тестирования псевдослучайных последовательностей.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

Очная форма обучения

Объем модуля (зач.ед.): 19
Объем дисциплины (зач.ед.): 3

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																	Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)																	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод инояз. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
1	Теория псевдослучайных генераторов на основе машин Тьюринга	13	6	3	3		7	3	0,6	2,4														4	1					
2	Варианты определения случайной последовательности	9	4	2	2		5	2	0,4	1,6			3	1																
3	Тесты на случайность	9	4	2	2		5	2	0,4	1,6			3	1																
4	Использование криптографических алгоритмов для генерации псевдослучайных чисел	6	4	2	2		2	2	0,4	1,6																				
5	Генераторы псевдослучайных последовательностей и потоковые шифры	9	4	2	2		5	2	0,4	1,6			3	1																
6	Генераторы истинно случайных последовательностей	6	4	2	2		2	2	0,4	1,6																				
7	Сплетения псевдослучайных генераторов	10	4	2	2		6	2	0,4	1,6														4	1					
8	Интеллектуальные методы для порождения и тестирования псевдослучайных последовательностей	6	4	2	2		2	2	0,4	1,6																				
	Всего (час), без учета промежуточной аттестации**:**	**68**	**34**	**17**	**17**		**34**	**17**	**3,4**	**13,6**			**9**	**9**										**8**	**8**					
	Всего по дисциплине (час.):	**72**	**34**				**38**	В т.ч. промежуточная аттестация																			4	0	**0**	**0**

*Суммарный объем в часах на мероприятие
указывается в строке «Всего (час.) без учета промежуточной аттестации

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1 Лабораторные работы

Не предусмотрено

4.2 Практические занятия

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
1	1	Теория псевдослучайных генераторов на основе машин Тьюринга	3
2	2	Варианты определения случайной последовательности	2
3	3	Тесты на случайность	2
4	4	Использование криптографических алгоритмов для генерации псевдослучайных чисел	2
5	5	Генераторы псевдослучайных последовательностей и потоковые шифры	2
6	6	Генераторы истинно случайных последовательностей	2
7	7	Сплетения псевдослучайных генераторов	2
8	8	Интеллектуальные методы для порождения и тестирования псевдослучайных последовательностей	2
Всего:			17

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

- Программирование псевдослучайных генераторов на основе клеточных автоматов
- Применение тестов на случайность
- Порождение истинно случайных последовательностей

4.3.2. Примерный перечень тем графических работ

Не предусмотрено

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

Не предусмотрено

4.3.4 Примерная тематика индивидуальных или групповых проектов

Не предусмотрено

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

Не предусмотрено

4.3.6. Примерный перечень тем расчетно-графических работ

Не предусмотрено

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

Не предусмотрено

4.3.8. Примерная тематика контрольных работ

1. Теория псевдослучайных генераторов на основе машин Тьюринга.
2. Сплетения псевдослучайных генераторов.

4.3.9. Примерная тематика коллоквиумов

Не предусмотрено

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
Теория псевдослучайных генераторов на основе машин Тьюринга	*											
Варианты определения случайной последовательности	*											
Тесты на случайность	*											
Использование криптографических алгоритмов для генерации псевдослучайных чисел	*											
Генераторы псевдослучайных последовательностей и потоковые шифры	*											
Генераторы истинно случайных последовательностей	*											
Сплетения псевдослучайных генераторов	*											
Интеллектуальные методы для порождения и тестирования псевдослучайных последовательностей	*											

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

ДИСЦИПЛИНЫ

9.1. Рекомендуемая литература

9.1.1. Основная литература

Дональд Кнут. Искусство программирования. Т.3. 1-е,2-е,3-е изд. — Москва: Вильямс, 2000—2009 гг 17 экз.

9.1.2. Дополнительная литература

1. Press, WH; Teukolsky, SA; Vetterling, WT; Flannery, BP Numerical Recipes: The Art of Scientific Computing (2rd ed.). New York: Cambridge University Press 1997 http://alvand.basu.ac.ir/~dezfoulian/files/Numericals/Cambridge%20-%20Numerical%20Recipes%20in%20C_%20The%20Art%20of%20Scientific%20Computing,%202nd%20Ed.,%20Press%20W.H.,%20Teukols.pdf
2. Шнайер, Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер; Предисл. У. Диффи; Науч.-техн. ред. пер. П. В. Семьянов .— М. : Триумф, 2003 .— 816 с. : ил. ; 24 см .— Пер. кн.: Applied cryptography. Protocols, Algorithms, and Source Code in C / B. Schneier. - New York a. o., 1996. — Библиогр.: с. 741-796 (1653 назв.). — ISBN 0-471-11709-9 : 356.07 6 экз

9.2. Методические разработки

Отсутствуют

9.3. Программное обеспечение

Операционные системы семейства MS Windows (лицензии по числу рабочих мест).

9.4. Базы данных, информационно-справочные и поисковые системы

Сайт библиотеки университета http://lib.urfu.ru/

9.5.Электронные образовательные ресурсы

Отсутствуют

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Не предусмотрено

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0,6		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Контрольная работа № 1	*8,1-14*	*50*
Контрольная работа № 2	*8,1-17*	*50*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – зачет **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий –0,4		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Домашняя работа №1	*8,1-10*	*30*
Домашняя работа №2	*8,1-14*	*30*
Домашняя работа №3	*8,1-17*	*40*
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям–1		
Промежуточная аттестация по практическим/семинарским занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий – не предусмотрены		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

не предусмотрено

6.4. Коэффициент значимости семестровых результатов освоения дисциплины

не предусмотрено

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте ФЭПО http://fepo.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на сайте Интернет-тренажеры http://training.i-exam.ru.

Дисциплина и ее аналоги, по которым возможно тестирование, отсутствуют на портале СМУДС УрФУ.

В связи с отсутствием Дисциплины и ее аналогов, по которым возможно тестирование, на сайтах ФЭПО, Интернет-тренажеры и портале СМУДС УрФУ, тестирование в рамках НТК не проводится.

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

При проведении независимого тестового контроля как формы промежуточной аттестации применяется методика оценивания результатов, предлагаемая разработчиками тестов. Процентные показатели результатов независимого тестового контроля переводятся в баллы промежуточной аттестации по 100-балльной шкале в БРС:

– в случае балльной оценки по тесту (блокам, частям теста) переводится процент набранных баллов от общего числа возможных баллов по тесту;
– при отсутствии балльной оценки по тесту переводится процент верно выполненных заданий теста, от общего числа заданий.

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий *Не предусмотрено*

8.3.2. Примерные контрольные задачи в рамках учебных занятий

Контрольная работа № 1.
Построить удовлетворяющий тесту Колмогорова – Смирнова генератор псевдослучайных чисел на основе машины Минского. Проверить для построенного генератора выполнимость постулатов Голомба.

Контрольная работа № 2.
Построить удовлетворяющий перестановочному тесту генератор псевдослучайных чисел на основе правила 30. Рассмотреть сплетение построенного генератора и линейного регистра сдвига с обратной связью и проверить для полученного сплетения выполнимость тестов на возрастание и убывание.

8.3.3. Примерные контрольные кейсы

Не предусмотрено

8.3.4. Перечень примерных вопросов для зачета

1. Парадокс метода Монте-Карло.
2. Понятие машины Тьюринга как псевдослучайного генератора.
3. Применение универсальных машин Тьюринга.
4. Применение простейших клеточных автоматов.
5. Игра "Жизнь" как модель для порождения псевдослучайных последовательностей.
6. Использование моделей управления при помощи глобальных сигналов для порождения псевдослучайных последовательностей.
7. Применение Redcode для порождения псевдослучайных последовательностей.
8. Использование эзотерических языков для порождения псевдослучайных последовательностей.
9. Порождение псевдослучайных последовательностей на основе машины Минского.
10. Недетерминированные машины Тьюринга для порождения псевдослучайных последовательностей.
11. Определения случайной последовательности по Лехмеру и Франклину.
12. Понятие к-распределенности.
13. Понятие конечной случайной последовательности.
14. Алгоритм Кнута.
15. Простейшие тесты на случайность.
16. Chi-test.
17. Тест Колмогорова - Смирнова.

18. Gap test.
19. Покерный тест.
20. Тесты на количество значений на интервале.
21. Перестановочные тесты.
22. Тесты на возрастание и убывание.
23. Распределение максимальных значений на интервале.
24. Тестирование подпоследовательностей.
25. Линейные конгруэнтные последовательности.
26. Спектральный тест.
27. Постулаты Голомба.
28. Тесты NIST.
29. Использование криптографических алгоритмов для генерации псевдослучайных чисел.
30. Регистры сдвига с обратной связью.
31. Генератор Геффе.
32. Генератор Дженнингса.
33. Генератор Бета-Пайпера.
34. Пороговый генератор.
35. Генератор Голлмана.
36. Сжимающий генератор.
37. Самосжимающий генератор.
38. A5.
39. Hughes.
40. Nanoteq.
41. Rambutan.
42. Fish.
43. Pike.
44. Mush.
45. M.
46. RC4.
47. SEAL.
48. WAKE.
49. Генератор Плесса.
50. Генераторы истинно случайных последовательностей.
51. Сплетения псевдослучайных генераторов.
52. Интеллектуальные методы для порождения и тестирования псевдослучайных последовательностей.

8.3.5. Перечень примерных вопросов для экзамена

Не предусмотрено

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

Не предусмотрено

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

Не предусмотрено

8.3.8. Интернет-тренажеры

Не предусмотрено

8.3.9. Примерные задания для домашних работ

Домашняя работа № 1.

Построить генератор псевдослучайных чисел на основе модели управления при помощи глобальных сигналов, удовлетворяющий покерному тесту и тесту на количество значений на интервале.

Домашняя работа № 2.

Тесты NIST для генератора Плесса.

Домашняя работа № 3.

Разработать генератор псевдослучайных чисел на основе сигналов компьютерной мыши. Настройку параметров осуществить на основе генетического алгоритма, рассматривая в качестве меры приспособленности соответствие постулатам Голомба.