МИНОБРНАУКИ РОССИИ
ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Утверждено:
на заседании кафедры программирования и экономической информатики
протокол от «25» июня 2018 г. № 7
Зав. кафедрой _____/Юлмухаметов Р.С.

Согласовано:
Председатель УМК факультета математики и информационных технологий
_____/Ефимов А.М.

"Направление
Направленность (профиль) подготовки -

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

дисциплина *Теория кодирования, защита информации*

Вариативная часть

программа бакалавриата

Направление подготовки (специальность)
02.03.03 Математическое обеспечение и администрирование информационных систем
(указывается код и наименование направления подготовки (специальности))

Направленность (профиль) подготовки
"Системное и интернет-программирование"

Квалификация
Бакалавр

Разработчик (составитель) доцент кафедры ПиЭИ, к.ф.-м.н.	_____/ Луценко В.И.

Для приема: 2018 года

Уфа 2018 г.

Составитель: Доцент кафедры ПиЭИ, к.ф.-м.н. Луценко В.И..

Рабочая программа дисциплины утверждена на заседании кафедры программирования и экономической протокол информатики от «25» июня 2018 г. № 7.

Заведующий кафедрой _____/ Юлмухаметов Р.С./

Список документов и материалов

Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

(с ориентацией на карты компетенций)

В результате освоения образовательной программы обучающийся должен овладеть следующими результатами обучения по дисциплине:

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	1.Знать современные языки программирования и языки баз данных, сетевые технологии, библиотеки и пакеты программ, современные профессиональные стандарты информационных технологий.	ОПК-3 - способность к разработке алгоритмических и программных решений в области системного и прикладного программирования, математических, информационных и имитационных моделей, созданию информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных, тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям.	
	2. Знать основные понятия и теоремы теории информации и кодирования	ПК-7 - способность к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения.	
Умения	1. Уметь применять в профессиональной деятельности современные языки программирования и языки баз данных, системы автоматизированного проектирования, электронные библиотеки и	ОПК-3 - способность к разработке алгоритмических и программных решений в области системного и прикладного программирования, математических, информационных и имитационных моделей, созданию информационных ресурсов глобальных сетей,	

	коллекции, сетевые технологии, библиотеки и пакеты прикладных программ.	образовательного контента, прикладных баз данных, тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям.	
	2. Уметь использовать основные теоретические принципы теории информации и кодирования для обеспечения эффективной и надежной передачи информации	ПК-7 - способность к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения	
Владения (навыки/ опыт деятельности)	1. Владеть методикой работы с электронными библиотеками, сетевыми технологиями, библиотеками и пакетами прикладных программ; навыками разработки прикладных программ	ОПК-3 - способность к разработке алгоритмических и программных решений в области системного и прикладного программирования, математических, информационных и имитационных моделей, созданию информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных, тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям.	
	2. Владеть методами получения количественных оценок информации, расчета информационных характеристик основных элементов систем передачи информации, построения кодов.	ПК-7 - способность к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения	

2. Цель и место дисциплины в структуре образовательной программы

. Дисциплина (модуль) «Теория кодирования, защита информации» относится к вариативной части, дисциплины по выбору.

Дисциплина (модуль) изучается на 3 курсе в 6 семестре.

Цель изучения дисциплины –формирование у обучающихся фундаментальных теоретических знаний в области применения наиболее эффективных методов кодирования, позволяющих осуществлять передачу определенного количества информации по каналу связи с помощью минимального количества символов, как при отсутствии, так и при наличии помех.

Для изучения данной дисциплины студент должен получить необходимые знания, умения и компетенции, которые формируются в результате изучения перечисленных ниже дисциплин.

Перечень дисциплин, изучение которых должно предшествовать изучению данной дисциплины:

- Иностранный (английский) язык;
- Математический анализ (функции одной переменной);
- Математический анализ (функции многих переменных, теория комплексных чисел);
- Алгебра и геометрия;
- Дифференциальные уравнения;
- Вычислительные методы;
- Языки и методы программирования;

Знания и умения, полученные в результате освоения данной дисциплины, будут использоваться при прохождении обучающийся предквалификационной практики, подготовке им выпускной квалификационной работы, а также в научной и практической деятельности после окончания университета.

3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)

Содержание рабочей программы представлено в Приложении № 1.

4. Фонд оценочных средств по дисциплине

4.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

В результате освоения дисциплины должны быть сформированы следующие компетенции:

ОПК-3 - способность к разработке алгоритмических и программных решений в области системного и прикладного программирования, математических, информационных и имитационных моделей, созданию информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных, тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям.

Этап (уровень) освоения компетенции	**Планируемые результаты обучения** (показатели достижения заданного уровня освоения компетенций)	**Критерии оценивания результатов обучения**			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	1.Знать современные языки программирования и языки баз данных, сетевые технологии, библиотеки и пакеты программ, современные профессиональные стандарты информационных технологий.	Отсутствие знаний или фрагментарные представления об основных концепциях современных языков программирования и языков баз данных, сетевых технологий, библиотек и пакетов программ, современных профессиональных стандартов информационных технологий.	Неполные представления об основных концепциях современных языков программирования и языков баз данных, сетевых технологий, библиотек и пакетов программ, современных профессиональных стандартов информационных технологий.	Сформированные, но содержащие отдельные пробелы представления об основных концепциях современных языков программирования и языков баз данных, сетевых технологий, библиотек и пакетов программ, современных профессиональных стандартов информационных технологий.	Сформированные систематические представления об основных концепциях современных языков программирования и языков баз данных, сетевых технологий, библиотек и пакетов программ, современных профессиональных стандартов информационных технологий.
Второй этап (уровень)	Уметь применять в профессиональной деятельности современные языки программирования и языки баз данных, системы автоматизированного проектирования, электронные	Отсутствие умений или фрагментарные умения применять в профессиональной деятельности современные языки программирования и языки баз данных, системы автоматизиров	В целом успешное, но не систематическое использование умения применять в профессиональной деятельности современные языки программирования и языки	В целом успешное, но содержащее отдельные пробелы использования умения понимать, применять в профессиональной деятельности современные языки программиров	Сформированное умение понимать, применять в профессиональной деятельности современные языки программирования и языки баз данных, системы автоматизированного

	библиотеки и коллекции, сетевые технологии, библиотеки и пакеты прикладных программ.	анного проектировани я, электронные библиотеки и коллекции, сетевые технологии, библиотеки и пакеты прикладных программ.	баз данных, системы автоматизиров анного проектировани я, электронные библиотеки и коллекции, сетевые технологии, библиотеки и пакеты прикладных программ.	ания и языки баз данных, системы автоматизиров анного проектировани я, электронные библиотеки и коллекции, сетевые технологии, библиотеки и пакеты прикладных программ.	проектировани я, электронные библиотеки и коллекции, сетевые технологии, библиотеки и пакеты прикладных программ.
Третий этап (уровень)	Владеть методикой работы с электронными библиотеками, сетевыми технологиями, библиотеками и пакетами прикладных программ; навыками разработки прикладных программ	Отсутствие владения или фрагментарное владение методикой работы с электронными библиотеками, сетевыми технологиями, библиотеками и пакетами прикладных программ; навыками разработки прикладных программ	В целом успешное, но не систематическ ое владение методикой работы с электронными библиотеками, сетевыми технологиями, библиотеками и пакетами прикладных программ; навыками разработки прикладных программ	В целом успешное, но содержащее отдельные пробелы владение методикой работы с электронными библиотеками, сетевыми технологиями, библиотеками и пакетами прикладных программ; навыками разработки прикладных программ	Успешное и систематическ ое владение методикой работы с электронными библиотеками, сетевыми технологиями, библиотеками и пакетами прикладных программ; навыками разработки прикладных программ

ПК-7: способностью к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения.

Этап (уровень) освоения компетенции	**Планируемые результаты обучения** (показатели достижения заданного уровня освоения компетенций)	**Критерии оценивания результатов обучения**			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать основные понятия и теоремы теории информации и кодирования	Отсутствие знаний или фрагментарные представления об основных понятиях и теоремах теории информации и кодирования	Неполные представления об основных понятиях и теоремах теории информации и кодирования	Сформированные, но содержащие отдельные пробелы представления об основных понятиях и теоремах теории информации и кодирования	Сформированные систематические представления об основных понятиях и теоремах теории информации и кодирования
Второй этап (уровень)	Уметь использовать основные теоретические принципы теории информации и кодирования для обеспечения эффективной и надежной передачи информации	Отсутствие умений или фрагментарные умения понимать, применять и совершенствовать аппарат теории информации и кодирования для обеспечения эффективной и надежной передачи информации	В целом успешное, но не систематическое использование умения понимать, применять и совершенствовать аппарат теории информации и кодирования для обеспечения эффективной и надежной передачи информации	В целом успешное, но содержащее отдельные пробелы использования умения понимать, применять и совершенствовать аппарат теории информации и кодирования для обеспечения эффективной и надежной передачи информации	Сформированное умение понимать, применять и совершенствовать аппарат теории информации и кодирования для обеспечения эффективной и надежной передачи информации
Третий этап (уровень)	Владеть методами получения количественных оценок информации,	Отсутствие владения или фрагментарное владение методами получения	В целом успешное, но не систематическое владение методами получения	В целом успешное, но содержащее отдельные пробелы владение	Успешное и систематическое владение методами получения количественн

	расчета информационных характеристик основных элементов систем передачи информации, построения кодов.	количественных оценок информации, расчета информационных характеристик основных элементов систем передачи информации, построения кодов.	количественных оценок информации, расчета информационных характеристик основных элементов систем передачи информации, построения кодов.	методами получения количественных оценок информации, расчета информационных характеристик основных элементов систем передачи информации, построения кодов.	ых оценок информации, расчета информационных характеристик основных элементов систем передачи информации, построения кодов.

Показатели сформированности компетенции:

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (*для экзамена:* текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10; *для зачета:* текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

Экзамены:

- отлично – от 80 до 110 баллов (включая 10 поощрительных баллов),
- хорошо – от 60 до 79 баллов,
- удовлетворительно – от 45 до 59 баллов,
- неудовлетворительно – менее 45 баллов.

4.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций

Этапы освоения	Результаты обучения	Компетенция	Оценочные средства
1-й этап Знания	1.Знать современные языки программирования и языки баз данных, сетевые технологии, библиотеки и пакеты программ, современные профессиональные стандарты информационных технологий.	ОПК-3 - способность к разработке алгоритмических и программных решений в области системного и прикладного программирования, математических, информационных и имитационных моделей,	Лабораторные работы, курсовая работа, экзамен

		созданию информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных, тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям.	
	2. Знать основные понятия и теоремы теории информации и кодирования	ПК-7: способностью к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения.	Лабораторные работы, курсовая работа, экзамен
2-й этап Умения	1.Знать современные языки программирования и языки баз данных, сетевые технологии, библиотеки и пакеты программ, современные профессиональные стандарты информационных технологий.	ОПК-3 - способность к разработке алгоритмических и программных решений в области системного и прикладного программирования, математических, информационных и имитационных моделей, созданию информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных, тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям.	Лабораторные работы, курсовая работа, экзамен
	2. Уметь использовать основные теоретические принципы теории информации и кодирования для обеспечения эффективной и надежной передачи информации	ПК-7: способностью к разработке и применению алгоритмических и программных решений в области системного и прикладного программного	Лабораторные работы, курсовая работа, экзамен

		обеспечения.	
3-й этап Владеть навыками	1. Владеть методикой работы с электронными библиотеками, сетевыми технологиями, библиотеками и пакетами прикладных программ; навыками разработки прикладных программ	ОПК-3 - способность к разработке алгоритмических и программных решений в области системного и прикладного программирования, математических, информационных и имитационных моделей, созданию информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных, тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям.	Лабораторные работы, курсовая работа, экзамен
	2. Владеть методами получения количественных оценок информации, расчета информационных характеристик основных элементов систем передачи информации, построения кодов.	ПК-7: способностью к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения.	Лабораторные работы, курсовая работа, экзамен

4.3. Рейтинг-план дисциплины

Рейтинг–план дисциплины представлен в приложении 2.

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Введение в теоретико-числовые методы криптографии [Электронный ресурс] : учебное пособие / М.М. Глухов [и др.]. — Электрон. дан. — Санкт-Петербург : Лань, 2011. — 400 с. — Режим доступа: https://e.lanbook.com/book/68466.
2. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / С.А. Нестеров. — Электрон. дан. — Санкт-Петербург : Лань, 2019. — 324 с. — Режим доступа: https://e.lanbook.com/book/114688.

3. Березкин, Е.Ф. Основы теории информации и кодирования [Электронный ресурс] : учебное пособие / Е.Ф. Березкин. — Электрон. дан. — Санкт-Петербург : Лань, 2018. — 320 с. — Режим доступа: https://e.lanbook.com/book/108326.

Дополнительная литература:

4. Мытник, К.Я. Смарт-карты и информационная безопасность [Электронный ресурс] / К.Я. Мытник, С.П. Панасенко ; под ред. В.Ф. Шаньгина. — Электрон. дан. — Москва : ДМК Пресс, 2018. — 516 с. — Режим доступа: https://e.lanbook.com/book/116128.

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины

1	Электронно-библиотечная система «ЭБ БашГУ»	Собственная электронная библиотека учебных и научных электронных изданий, которая включает издания преподавателей БашГУ	Авторизованный доступ по паролю из любой точки сети Интернет	Регистрация в Библиотеке БашГУ, дальнейший доступ из любой точки сети Интернет	https://elib.bashedu.ru/
2	Электронно-библиотечная система «Университетская библиотека online»	Полнотекстовая БД учебных и научных электронных изданий	Авторизованный доступ по паролю из любой точки сети Интернет	Регистрация из сети БашГУ, дальнейший доступ из любой точки сети Интернет	http://www.biblioclub.ru/
3	Электронно-библиотечная система издательства «Лань»	Полнотекстовая БД учебных и научных электронных изданий	Авторизованный доступ по паролю из любой точки сети Интернет	Регистрация из сети БашГУ, дальнейший доступ из любой точки сети Интернет	http://e.lanbook.com/

2018/2019	Договор на ЭБС между БашГУ и издательством «Лань» № 848 от 03.09.2018	С 01.10.2018 по 30.09.2019
	Соглашение на бесплатные коллекции в ЭБС между БашГУ и издательством «Лань» № 961 от 01.10.2018	С 01.10.2018 по 30.09.2019
	Договор на доступ к электронным научным периодическим изданиям между БашГУ и РУНЭБ № 1262 от 11.12.2018	С 11.12.2018 по 31.12.2019
	Договор на БД диссертаций между БашГУ и РГБ №095040040 от 27.02.2019	С 27.02.2019 по 26.02.2020

6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

1. ***учебная аудитория для проведения занятий лекционного типа:*** аудитория № 520а (Физмат корпус - учебное), № 521 (Физмат корпус - учебное), аудитория № 522 (Физмат корпус - учебное), аудитория № 524 (Физмат корпус - учебное), аудитория № 525 (Физмат корпус - учебное) **2.** ***учебная аудитория для проведения занятий семинарского типа:*** аудитория № 520а (Физмат корпус - учебное), № 521 (Физмат корпус - учебное), аудитория № 522 (Физмат корпус - учебное), аудитория № 524 (Физмат корпус - учебное), аудитория № 525 (Физмат корпус - учебное) **3.** ***учебная аудитория для курсового проектирования (выполнения курсовых работ):*** аудитория № 520а (Физмат корпус - учебное), № 521 (Физмат корпус - учебное), аудитория № 522 (Физмат корпус - учебное), аудитория № 524 (Физмат корпус - учебное), аудитория № 525 (Физмат корпус - учебное) **4.** ***учебная аудитория для проведения групповых и индивидуальных консультаций:*** аудитория № 520а (Физмат корпус - учебное), № 521 (Физмат корпус - учебное), аудитория № 522 (Физмат корпус - учебное), аудитория № 524 (Физмат корпус - учебное), аудитория № 525 (Физмат корпус - учебное) **5.** ***учебная аудитория для текущего контроля и промежуточной аттестации:*** аудитория № 520а (Физмат корпус - учебное), № 521 (Физмат корпус - учебное), аудитория № 522 (Физмат корпус - учебное), аудитория № 524 (Физмат корпус - учебное), аудитория № 525 (Физмат корпус - учебное) **6.** ***помещения для самостоятельной работы:*** аудитория № 426 (Физмат корпус - учебное), читальный зал №2 (Физмат корпус - учебное) **7.** ***помещение для хранения и профилактического обслуживания учебного оборудования:***аудитория № 522 (Физмат корпус - учебное)	**Аудитория №426** Учебная мебель, доска, персональные компьютеры LenovoThinkCentreA70zIntelPentiumE 5800, 320 Gb, 19" – 13 шт., шкаф TLKTWP-065442-G-GY **Аудитория №520а** Учебная мебель, доска, монитор LG 19 L1942S SF 1280 x 1024,5ms,8000:1,black (3,4 кг,VGA,19"(48,3см)5mc, мониторы LG 19" L1942SBF 1280x1024,5ms,8000:1,black 10 шт., системный блок HPPavilionSlimlineS3500FAMDAthlon64 X2 5400+/2.8GHz,4Gb,500Gb 12шт.,доска аудитор. ДА36. **Аудитория № 521** Учебная мебель, доска, коммутатор HP V1905-24 Switch 24*10/100+2*10/100/1000, персональные компьютеры в комплекте DEPO Neos 460MDi5 2300/4GDDR1333/T500G/DVD W – 12 шт., проектор Optoma EX542i.DLP3D.XGA(1024*768).2700 ANSI Lm.3000 1.Lamp5000+/-40 ver, шкаф TLKTWP-065442-G-GY, экран на штативе DraperDiplomat (1:1) 84/84* 213*213 MW, доска аудитор. ДА36. **Аудитория №522** Учебная мебель, доска, персональный компьютер LenovoThinkCentre A70z IntelPentium E 5800, 320 Gb, 19" – 13 шт., кондиционер LessarLS/LU-H24KB2. **Аудитория № 524** Учебная мебель, доска настенная меловая, коммутатор HP V1905-24 Switch 24*10/100+2*10/100/1000, персональный компьютер в комплекте HP AiO 20"CQ 100 eu – 27 шт., экран ScreeMediaGolgview 274*206 NW 4:3, универсальное потолочное крепление ScreeMedia для проектора, регулировка высоты , шкаф TLKTWP-065442-G-GY, патч-корд (1296), доска аудитор. ДА32. **Аудитория № 525** Учебная мебель, доска, персональные компьютеры в комплекте DEPONeos 460MDi5 2300/4GDDR1333/T500G/DVDW/ - 13 шт., доска аудитор. ДА32. **Читальный зал №2** Учебная мебель, учебно-наглядные пособия, стенд по пожарной безопасности, моноблоки стационарные – 8 шт, принтер – 1 шт., сканер – 1 шт.

Приложение № 1

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины «*Теория кодирования, защита информации*» на 6 семестр
очная
форма обучения

Рабочую программу осуществляют:

Лекции: доцент каф. ПиЭИ, к.ф.-м.н. Луценко В.И.

Практические занятия: доцент каф. ПиЭИ, к.ф.-м.н. Луценко В.И.

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ)	4
Учебных часов на контактную работу с преподавателем:	51.2
Лекций	16
практических/ семинарских	
Лабораторных	32
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем)	3,2
Учебных часов на самостоятельную работу обучающихся (СРС) включая подготовку к экзамену/зачету	58

Форма контроля:
экзамен 6 семестр
В том числе:
курсовая работа 6 семестр, контактных часов – 2, часов на самостоятельную работу – 20

№п/п	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)					Основная и дополнительная литература, рекомендуемая студентам (номера из списка)	Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		Всего	ЛК	ПР/СЕМ	ЛР	СРС			
1	2	3	4	5	6	7	8	9	10
	6- й семестр	144	16		32	58			
1	Модуль 1. Теория информации. Базовые понятия теории информации. 1.1. Теория информации рассматривается как существенная часть кибернетики. Характеристики непрерывной и дискретной информации. 1.2. Принципы хранения, измерения, обработки и передачи информации. Схема передачи информации. Сущность работы ЦВМ и АВМ и их применение на практике. 1.3. Базовые понятия: информация, канал связи, шум, кодирование.		2		4	4	1-2	Отчет по лабораторной работе №1	отчеты по лабораторным работам, экзамен
2	Модуль 2. Энтропия Шеннона.		2		4	4	1-2	Отчет по	отчеты по

	2.1 Энтропия дискретной случайной величины. Понятие префиксного кодирования. 2.2 Сжатие информации. Основная теорема о кодировании при отсутствии помех. 2.3 Метод блокирования.							лабораторной работе №2	лабораторным работам, экзамен
3	Модуль 3. Математическая модель системы связи. 3.1 Коды с исправлением ошибок. Коды с обнаружением ошибок. 3.2 Понятие сигнала и его модели. Различные формы представления детерминированных сигналов.		2		4	4	1-2	Отчет по лабораторной работе №3	отчеты по лабораторным работам, экзамен
4	Модуль 4. Кодирование информации. 4.1 Основные задачи кодирования. 4.2 Эффективное и помехоустойчивое кодирование. Основные теоремы Шеннона о кодировании. 4.3 Эффективные коды: код Шеннона - Фано, код Хаффмана, и их характеристики.		2		4	4	1-2	Отчет по лабораторной работе №4	отчеты по лабораторным работам, экзамен

5	Модуль 5. Методики построения помехоустойчивых кодов. 5.1 Код с проверкой четности. 5.2 Код с тройным повторением. 5.3 Код Хэмминга..		2		4	4	1,2	Отчет по лабораторной работе №5	отчеты по лабораторным работам, экзамен
6	Модуль 6. Математические основы шифрования с открытым ключом. 6.1 Сравнения. 6.2. Функция Эйлера 6.3 Теорема Эйлера.		2		4	6	1-2	Отчет по лабораторной работе №6	отчеты по лабораторным работам, экзамен
7	Модуль 7. Математические основы шифрования с открытым ключом. 7.1 Теорема малая Ферма. 7.2. Алгоритм генерации длинных простых чисел.		2		4	6	1-2	Отчет по лабораторной работе №7	отчеты по лабораторным работам, экзамен
8	Модуль 8. Моделирование цифровой подписи.		2		4	6	1-2	Отчет по лабораторной работе №8	отчеты по лабораторным работам, экзамен
	Курсовая работа	0	0	0	0	20	1-2		
	Всего часов:	144	16		32	58			3,2

0

Приложение № 2

Рейтинг – план дисциплины

Теория кодирования, защита информации

направление подготовки *02.03.03 Математическое обеспечение и администрирование информационных систем*
курс 3, семестр 6,
Количество часов по учебному плану 144, в т.ч. контактная работа 55,2, самостоятельная работа 58.
Преподаватель: *к.ф.-м.н.* Луценко В.И.

Кафедра: *Программирования и экономической информатики*

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	баллы	
			минимальный	максимальный
Текущий контроль				**50**
Отчеты по лабораторным работам	5	10	0	50
Рубежный контроль				**20**
Защита отчетов	2	10	0	20
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение лабораторных занятий			0	-10
Итоговый контроль				**30**
1. Экзамен	10	2	0	30
ИТОГО				**100**

Приложение № 3

Вопросы для самостоятельной проработки
Раздел 1 Информация и ее свойства

При изучении раздела 1 необходимо:
1. Читать лекции, содержащие основы образовательной программы по дисциплине «теория информации и кодирования».
Акцентировать внимание на следующих понятиях:
 данные, информация;
 свойства информации;
 формы адекватности информации.
Определить основные особенности информационных коммуникаций.
Уяснить основные особенности и сферы применения синтаксической, семантической, прагматической адекватности.
2. Для самооценки по разделу 1 необходимо ответить на следующие вопросы:
1.Каким образом измеряется объем данных в сообщение, привести пример;
2. Дайте определение понятию «количество информации».
3. Напишите и разъясните формулу Шеннона, Хартли, приведите пример;
4. Что такое тезаурусная мера, тезаурус;
5. Как можно определить ценность информации;
6. Перечислите качества информации;
7. Перечислите единицы измерения информации и приведите примеры;
8. Характеристики для оценки качества информации.
Раздел 2. Классификация и кодирование информации
При изучении раздела 2 необходимо:
1. Читать лекции, содержащие основы образовательной программы по дисциплине «теория информации и кодирование».
Акцентировать внимание на следующих понятиях:
 иерархическая система классификации информации;
 фасетная система классификации информации;
 дескрипторная система классификации информации.
Определить основные особенности системы кодирования.
36
Уяснить основные особенности и сферы применения последовательного кодирования, параллельного кодирования, регистрационного кодирования

(порядковая система кодирования, серийно-порядковая система кодирования).

2. Для самооценки по разделу 2 необходимо ответить на следующие вопросы:

1. Иерархическая система кодирования.
2. Фасетная система кодирования.
3. Дескрипторная система кодирования.
4. Назначение системы кодирования.
5. Основные идеи классификационного и регистрационного кодирования.
6. Классификация информации, циркулирующей в организации.

Раздел 3. Информационно-логические основы построения

При изучении раздела 3 необходимо:

1. Читать лекции, содержащие основы образовательной программы по дисциплине «*Теория кодирования, защита информации*».

Акцентировать внимание на следующих понятиях:

- позиционные системы счисления;
- законы алгебры-логики;
- представление информации в ПК.

Определить основные особенности процесса логического синтеза вычислительных схем.

Уяснить основные особенности и сферы применения алгоритмов решения задач.

2. Для самооценки по разделу 3 необходимо ответить на следующие вопросы:

1. Непозиционные системы счисления
2. Позиционные системы счисления
3. Охарактеризуйте перевод числа из десятичной системы счисления в любую другую систему счисления
4. Охарактеризуйте перевод дробного числа из любой системы счисления в десятичную систему счисления
5. Определите поля постоянной длины
6. Упакованный формат двоично-кодированного десятичного числа
7. Распокованный формат двоично-кодированного десятичного числа
8. ASCII-код для представления символьной информации
9. Определение алгебры логики
10. Простейшие операции алгебры-логики

37

11. Перечислите законы алгебры-логики. Приведите примеры

12. Рассмотрите логический синтез вычислительных систем на примере одноразрядного двоичного сумматора
13. Определите логическую схему сумматора
14. Поясните логические блоки сумматора

Для самостоятельной проверки знаний необходимо ответить на следующие вопросы:

1. Формы представления информации в персональном компьютере
2. Основные понятия алгебры логики
3. Отличие информации от данных
4. Формы адекватности информации и их особенности
5. Меры информации
6. Характеристики для оценки качества информации
7. Виды классификации информации
8. Иерархическую систему классификации
9. Фасетную систему классификации
10. Дескрипторную систему классификации
11. Назначение системы кодирования информации
12. Основные идеи классификационного и регистрационного кодирования
13. Классификацию информации, циркулирующей в организации

Экзаменационные билеты

Экзамен является оценочным средством для всех этапов освоения компетенций.

Структура экзаменационного билета: 2 вопроса.

Примерные вопросы для экзамена:

1. Понятие информации.
2. Системы передачи информации.
3. Различные подходы к измерению информации и их применение.
4. Структурные меры информации.
5. Статистический подход к измерению информации.
6. Энтропия и ее свойства.
7. Понятие сигнала и его модели.
8. Основные преобразования сигналов.
9. Информационные характеристики источника сообщений.
10. Основные задачи кодирования.
11. Эффективное кодирование. Теорема Шеннона о кодировании для канала без шума.
12. Код Шеннона-Фано.
13. .Код Хаффмана.
14. Помехоустойчивое кодирование. Теорема Шеннона о кодировании для канала с шумом.
15. Код с проверкой четности. Код с тройными повторениями.
16. Код Хэмминга.
17. .Информационные характеристики канала связи.
18. Принципы построения криптосистем
19. Уровни криптосистем
20. Компоненты Криптосистем
21. Функции Криптосистем
22. Методы получения “случайности”
23. Архивация. Алгоритмы архивации
24. Генерация ключей. Распределение ключей. Главный ключ.
25. Восстановление системы при компрометации ключей
26. Классификация криптоалгоритмов
27. Симметричные криптоалгоритмы
28. Асимметричные криптоалгоритмы
29. Технология Хэш-функций

Образец экзаменационного билета:

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
КАФЕДРА МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Экзаменационный билет №1
по курсу «Программное обеспечение в научных и инженерных исследованиях»
(2018-2019 у.г.)

1. Понятие информации.
2. Эффективное кодирование. Теорема Шеннона о кодировании для канала без шума..

Преподаватель Луценко В.И.. /_____/

Зав. кафедрой Юлмухаметов Р.С. /_____/

Перевод оценки из 100-балльной в четырехбалльную производится следующим образом:

- отлично – от 80 до 110 баллов (включая 10 поощрительных баллов);
- хорошо – от 60 до 79 баллов;
- удовлетворительно – от 45 до 59 баллов;
- неудовлетворительно – менее 45 баллов.

Критерии оценки (в баллах):

- **25-30 баллов** выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание функциональных возможностей, терминологии, основных элементов. Студент без затруднений ответил на все дополнительные вопросы.

-**17-24 баллов** выставляется студенту, если студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности.

- 10-16 баллов выставляется студенту, если при ответе на теоретические вопросы студентом допущено несколько существенных ошибок в толковании основных понятий. Логика и полнота ответа страдают заметными изъянами. Заметны пробелы в знании основных методов. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос.

- 1-10 баллов выставляется студенту, если ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Студент не смог ответить ни на один дополнительный вопрос.

Курсовая работа

Курсовая работа является оценочным компетенций. Тема выбирается студентом самостоятельно, утверждается на заседании кафедры.

Примерные темы курсовых работ

1 Разработка алгоритма и программы решения линейных уравнений с целыми коэффициентами большой размерности.
2. Разработка алгоритма и программы генерации простых чисел большой размерности.
3. Разработка алгоритма программы для генерации ключей алгоритма RSA.
4/ Разработка алгоритма программы быстрого возведения больших чисел в большие степени.
5. Разработка алгоритма программы реализация цифровой подписи.
6. Разработка алгоритма программы для генерации и проверки подписи Эль-Гамаля.
7. Разработка алгоритма программы для реализации электронных денег.
8. Выполнить программную реализацию протокола Нидхама-Шредера.
9. Выполнить программную реализацию шифра Эль-Гамаля на эллиптической кривой..
10. Выполнить программную реализацию алгоритма генерации и проверки цифровой подписи на эллиптической кривой.

Критерии оценки при защите курсовой работы

Оценка	Описание
5 «отлично»	выставляется студенту, если студент дал полное, развернутое описание всех теоретических аспектов темы, продемонстрировал возможностей, терминологии, основных элементов, умение применять теоретические знания при формировании и выполнении практической части темы. Студент без затруднений ответил на все дополнительные вопросы. выполнена полностью без неточностей и ошибок;
4 «хорошо»	теоретических аспектов темы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности. При выполнении практической части работы допущены несущественные ошибки.
3 «удовлетво-рительно»	выставляется студенту, если студент дал полное, развернутое описание всех теоретических аспектов темы, однако допущены несколько существенных ошибок в толковании основных понятий. Логика и полнота курсовой работы страдают заметными изъянами. Заметны пробелы в знании основных методов. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответов на дополнительные вопросы. Практическая часть отсутствует или при в ней допущены грубые ошибки
2 «неудовлетворительно»	выставляется студенту, если курсовая работа свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Обнаруживается отсутствие навыков применения теоретических знаний при выполнении практических заданий. Студент не смог ответить ни на один дополнительный вопрос.
«не допущен»	Курсовая работа не выполнена

Лабораторные работы

Примерные варианты лабораторных работ

№	Наименование	Кол-во часов
1	Методы контроля доступа к файлу	4
2	Методы использования аппаратных средств защиты	4
3	Использование средств ограничения доступа	4
4	Методы защиты программ	4
5	Методы работы с большими числами	4
6	Методы генерации больших простых чисел	4
7	Методы работы с RSA	4
8	Моделирование работы с цифровой подписью	4
	Итого	32

Описание методики оценивания:

Критерии оценки (в баллах):
За отчёт по лабораторной работе
- 7 баллов выставляется студенту, если нет замечаний;
- 5 баллов выставляется студенту, если имеются несущественные замечания;
- 3 баллов выставляется студенту, если в целом получены верные результаты, но имеются существенные замечания.

Приложение № 4

Примеры тестовых заданий

Тест 1
Тема: «Измерение информации»
1. Какое количество информации по Хартли может содержать система, информационная емкость которой определяется десятичным числом 1250.
2. Найти среднее количество информации по Шеннону в системе со следующим вероятностным распределением
p (1/ 2;1/ 4;1/ 4)
.
3. Какое максимальное количество информации по Шеннону содержит система со следующим вероятностным распределением
p (0,2;0,8)

.
Тест 2
Тема: «Модели сигналов. Преобразование сигналов»
1. Выберите наиболее реальную модель сигнала.
Варианты ответов:
a) случайный процесс;
b) детерминированный сигнал;
c) случайный сигнал.
2. Сколько видов модуляции гармонического сигнала существует?

Варианты ответов:
a) два;
b) бесконечно много;
c) три.
3. Какой спектр имеет периодический сигнал?
Варианты ответов:
a) сплошной;
b) линейчатый.
Тест 3
Тема: «Кодирование информации»
1. Что происходит с длиной сообщения при эффективном кодировании?
Варианты ответов:
c) увеличивается;
d) остается прежней;
e) уменьшается.
2. Как изменяется эффективность кода при увеличении длины блока при блоковом кодировании?
Варианты ответов:
a) не убывает;
b) не изменяется;
c) не возрастает.
3. Закодировать сообщение 100110 кодом с проверкой четности.
43
Варианты ответов:
a) 1001100;
b) 10011011;
c) 1001101.
Тест 4
Тема: «Передача информации»
1. Какое устройство системы передачи информации обеспечивает эффективность ее передачи?
Варианты ответов:
a) модулятор;
b) кодер источника;
c) кодер канала.
2. Какое устройство системы передачи информации обеспечивает достоверность ее передачи?
Варианты ответов:
a) кодер канала;
b) кодер источника;
c) модулятор.
3. Что является информационной характеристикой только канала связи?
a) скорость передачи информации;
b) пропускная способность.
Тест 5
Тема: «Классификация и кодирование информации»
Вопрос 1.
Система распределения объектов по классам в соответствии с определенным признаком называется … .
а. Кодирование;
б. Классификация;
в. Классификатор;

г. Реквизит.
Вопрос 2.
Основные методы классификации объектов:
а. Иерархический;
б. Двоичный;
в. Дескрипторный;
г. Фасетный.
Вопрос 3.
Стандарт кодировки, позволяющий закодировать больше символов:
а. КОИ-8;
б. ASCII;
в. ISO;
г. Unicode.
Вопрос 4.
Самая распространённая позиционная система счисления:
а. Римская;
б. Двоичная;
в. Десятичная;
г. Арабская.
Вопрос 5.
Совокупность средств, методов и условий, позволяющих использовать информационные ресурсы, называется …
а. Информационный рынок;
б. Информационный потенциал;
в. Информационная услуга;
г. Информационный продукт.