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
«___» _____ 2017 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

ИНФОРМАЦИОННОЕ КОДИРОВАНИЕ

Перечень сведений о рабочей программе модуля	**Учетные данные**
Модуль ***Информационное кодирование***	**Код модуля** № 1138288 **УП №№ 5433, 6323**
Образовательная программа ***Информационная безопасность телекоммуникационных систем***	**Код ОП** ***10.05.02***
Траектория образовательной программы (ТОП)	***Не предусмотрена***
Направление подготовки ***Информационная безопасность телекоммуникационных систем***	**Код направления и уровня подготовки** 10.05.02/01.01
Уровень подготовки ***Специалитет***	
ФГОС ВО	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: №1426 16 ноября 2016 г

Екатеринбург, 2017

Программа модуля составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Департамент	Подпись
1	Виноградова Нина Сергеевна	-	Старший преподаватель.	Радиоэлектроники и связи	

Руководитель модуля Н.С. Виноградова

Рекомендовано учебно-методическим советом Института радиоэлектроники и информационных технологий – РТФ

Председатель учебно-методического совета В.Г. Коберниченко
Протокол № _____ от _____ г.

Согласовано:

Дирекция образовательных программ Р. Х. Токарева

Руководитель, для которой
реализуется модуль Н.С. Виноградова

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ «ИНФОРМАЦИОННОЕ КОДИРОВАНИЕ»

1.1. Объем модуля, 11 з.е.

1.2. Аннотация содержания модуля

Модуль относится к базовой части образовательной программы и содержит две дисциплины, имеющие исключительное значение для информационной безопасности. На основе прагматических свойств информации изучаются принципы и характеристики модуляции и кодирования. Рассматриваются пять основных видов кодирования: эффективное кодирование, помехоустойчивой кодирование, линейное кодирование потоков данных, скремблирование и криптография. Изучение криптографии и элементов криптоанализа производится в ракурсе основных методов кодирования, обеспечивающих информационное скрытие.

Традиционное внимание уделяется методам перестановки, замены, гаммирования, криптопротоколам, основанным на системах с симметричными и ассиметричными ключами.

2. СТРУКТУРА МОДУЛЯ И РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ ПО ДИСЦИПЛИНАМ

Очная форма обучения

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)** Криптографические методы защиты информации	7	34	-	34	68	76	экз	144	4
2.	**(Б)** Теория информации и кодирования	5,6	68	51	-	119	133	зачет, экз	252	7
			102	**51**	**34**	**187**	**209**		**396**	**11**

Заочная форма обучения не предусмотрена

3. ПОСЛЕДОВАТЕЛЬНОСТЬ ОСВОЕНИЯ ДИСЦИПЛИН В МОДУЛЕ

3.1.	**Пререквизиты и постреквизиты в модуле**	*Дискретная математика и математическая логика* *Векторный анализ* *Теория вероятностей и математическая статистика*
3.2.	**Кореквизиты**	*Безопасность операционных систем* *Аналитические методы в телекоммуникационных системах* *Программно-аппаратные средства защиты информации* *Разработка безопасных веб-приложений* *Безопасность файловых систем*

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**	**Универсальные компетенции (УОК, УОПК,УПК), формируемые при освоении модуля для нескольких ОП**
10.05.02	РО-03 Способность применять в рамках научно-исследовательской деятельности основополагающие принципы и современные достижения физико-математических наук, математического описания и построения технических систем, а также современные информационные технологии в разработке технологических решений с использованием программного кода	ОК-8 способностью к самоорганизации и самообразованию ОПК-1способностью анализировать физические явления и процессы для формализации и решения задач, возникающих в ходе профессиональной деятельности ОПК-2способностью применять соответствующий математический аппарат для решения профессиональных задач ОПК-4способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации ОПК-5способностью	

		применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач ОПК-6способностью применять методы научных исследований в профессиональной деятельности ПК-2 способностью формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование, объектов, явлений и процессов телекоммуникационных систем, включая обработку и оценку достоверности их результатов ПКД-1способность разрабатывать планы и программы проведения научных исследований и технических разработок, подготавливать отдельные задания для исполнителей и контролировать их выполнение	
	РО-07 Способность обеспечить в рамках эксплуатационной деятельности целостность и конфиденциальность информации, в том числе с использованием средств противодействия иностранным техническим разведкам	ОПК-3способностью применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения профессиональных задач ПСК-10.3 способностью оценивать возможности средств технических разведок в отношении к системам связи, управления и объектам информатизации ПСК-10.4 способностью применять наиболее эффективные методы и средства для закрытия	

		возможных каналов перехвата акустической речевой информации ПСК-10.5 способностью проводить оценку уровня защищенности и обеспечивать эффективное применение средств защиты информационных ресурсов компьютерных сетей и систем беспроводной связи	

4.2 Распределение формирования компетенций по дисциплинам модуля

	Дисциплины модуля (РО-03)	ОК-8	ОПК-1	ОПК-2	ОПК-4	ОПК-5	ОПК-6	ПК-2	ПКД-1
1	**(Б)** Криптографические методы защиты информации	*			*		*	*	*
2	**(Б)** Теория информации и кодирования		*	*		*			

	Дисциплины модуля (РО-07)	ОПК-3	ПСК-10.3	ПСК-10.4	ПСК-10.5
1	**(Б)** Криптографические методы защиты информации		*	*	*
2	**(Б)** Теория информации и кодирования	*			

5. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО МОДУЛЮ

5.1. Весовой коэффициент значимости промежуточной аттестации по модулю:
Не предусмотрен

5.2. Форма промежуточной аттестации по модулю:
Не предусмотрена

5.3. Фонд оценочных средств для проведения промежуточной аттестации по модулю (Приложение 1)

ПРИЛОЖЕНИЕ 1
к рабочей программе модуля

5.3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО МОДУЛЮ

5.3.1. ОБЩИЕ КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО МОДУЛЮ

Система критериев оценивания результатов обучения в рамках модуля опирается на три уровня освоения: 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.

5.3.2. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО МОДУЛЮ

5.3.2.1. Перечень примерных вопросов для интегрированного экзамена по модулю
Не предусмотрен
5.3.2.2. Перечень примерных тем итоговых проектов по модулю
Не предусмотрен

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

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Перечень сведений о рабочей программе модуля	**Учетные данные**
Модуль ***Информационное кодирование***	**Код модуля** № 1138288 Учебный планы №№ 5433, **6323**
Образовательная программа ***Информационная безопасность телекоммуникационных систем***	**Код ОП** ***10.05.02***
Траектория образовательной программы (ТОП)	***Не предусмотрена***
Направление подготовки ***Информационная безопасность телекоммуникационных систем***	**Код направления и уровня подготовки** 10.05.02/01.01
Уровень подготовки ***Специалитет***	
ФГОС ВО	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: №1426 16 ноября 2016 г

Екатеринбург, 2017

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Кафедра	Подпись
1	Авдеев Денис Викторович	-	Старший преподаватель.	Департамент радиоэлектроники и связи	

Руководитель модуля Н.С. Виноградова

Рекомендовано учебно-методическим советом Института радиоэлектроники и информационных технологий – РТФ

Председатель учебно-методического совета В.Г. Коберниченко
Протокол № _____ от _____ г.

Согласовано:

Дирекция образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ «КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»

1.1.Аннотация содержания дисциплины

В дисциплине изучаются основы криптографических методов обеспечения информационной безопасности в вычислительных системах и компьютерных сетях. Рассматриваются криптографические протоколы, алгоритмы электронной цифровой подписи, вопросы надежности криптосистем.

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-8 способностью к самоорганизации и самообразованию
- ОПК-4 способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации
- ОПК-6 способностью применять методы научных исследований в профессиональной деятельности
- ПК-2 способностью формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование, объектов, явлений и процессов телекоммуникационных систем, включая обработку и оценку достоверности их результатов
- ПКД-1 способность разрабатывать планы и программы проведения научных исследований и технических разработок, подготавливать отдельные задания для исполнителей и контролировать их выполнение
- ПСК-10.3 способностью оценивать возможности средств технических разведок в отношении к системам связи, управления и объектам информатизации
- ПСК-10.4 способностью применять наиболее эффективные методы и средства для закрытия возможных каналов перехвата акустической речевой информации
- ПСК-10.5 способностью проводить оценку уровня защищенности и обеспечивать эффективное применение средств защиты информационных ресурсов компьютерных сетей и систем беспроводной связи

В результате освоения дисциплины студент должен:

Знать:

- основные понятия криптографии,
- симметричные и асимметричные алгоритмы криптографических преобразований,
- алгоритмы цифровой подписи,
- основные криптографические протоколы,
- отечественные и международные стандарты в области криптографической защиты информации в телекоммуникационных системах.

Уметь:

- использовать стандартные криптографические алгоритмы и протоколы,
- использовать типовые методы криптоанализа,
- разрабатывать модели информационной безопасности телекоммуникационных систем,
- правильно создать ключи для криптографической защиты программных систем и данных от несанкционированного использования (доступа, копирования) или нарушения технологии работы,
- выбрать наиболее удачный криптографический протокол для защиты телекоммуникационной системы от несанкционированного доступа.

Владеть (демонстрировать навыки и опыт деятельности):

— программными и аппаратными средствами криптографической защиты информации и персональных данных,

— навыками оценки и повышения надежности криптографических систем.

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.)*	*6*
1.	**Аудиторные занятия**	68	68	38
2.	Лекции	34	34	34
3.	Практические занятия	0	0	0
4.	Лабораторные работы	34	34	34
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	76	10,20	76
6.	**Промежуточная аттестация**	Э	2,33	Э
7.	**Общий объем по учебному плану, час.**	144	80,53	144
8.	**Общий объем по учебному плану, з.е.**	4		4

Заочная форма обучения не предусмотрена

*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	Общие принципы криптографии	История криптологии. Классификация методов шифрования информации. Шифры замены. Шифры перестановки. Блочные шифры. Шифры гаммирования. Поточные шифры. Модели шифров по К. Шеннону. Математические основы криптографии. Принципы построения и свойства генераторов псевдослучайных последовательностей.
2	Симметричные криптографические системы	Блочные и поточные шифры. Криптосистемы Фейстеля. Американский стандарт шифрования данных DES, основные режимы работы алгоритма. Алгоритм IDEA. Стандарт AES. Стандарт шифрования ГОСТ Р 34.12-2015, режимы работы. Задача криптоанализа. Криптоанализ “полным перебором”. Разностный криптоанализ. Линейный криптоанализ.
3	Асимметричные криптографические системы	Концепция криптосистемы с открытым ключом. Криптосистема шифрования данных RSA. Схема шифрования Эль Гамаля. Проблема аутентификации данных и электронная цифровая подпись. Хеш-функции: SHA, на основе симметричных блочных криптоалгоритмов, ГОСТ. Схемы создания и проверки цифровой подписи с помощью несимметричных схем шифрования. Протоколы электронной цифровой подписи (ЭЦП). Классификация атак на схемы ЭЦП.
4	Управление криптографическими ключами	Криптографические протоколы. Протоколы организации защищенного обмена информацией с подтверждением подлинности участников при наличии прямого защищенного канала без посредника и с использованием посредника. Разрядность ключа. Генерация ключей. Хранение ключей. Схемы распределения ключей. Время жизни ключа. Создание секретного ключа с обменом через незащищенный канал.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

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

Очная форма обучения

Объем модуля (зач.ед.): 11
Объем дисциплины (зач.ед.): 4

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	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 иностр. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
1	Общие принципы криптографии	**29**	**14**	6		8		**4**	2		2		**3**	1																
2	Симметричные криптографические системы	**37**	**18**	10		8		**4**	2		2		**12**	1				1												
3	Асимметричные криптографические системы	**37**	**14**	10		4		**4**	2		2		**3**	1																
4	Управление криптографическими ключами	**41**	**22**	8		14		**6**	2		4		**22**	1					1											
	Всего (час), без учета промежуточной аттестации**:**	**126**	**68**	**34**	**0**	**34**	**58**	**18**	**8**	**0**	**10**	**0**	**40**	**14**	**0**	**0**	**0**	**8**	**18**	**0**	**0**	**0**	**0**	**0**	**0**	**0**				
	Всего по дисциплине (час.):	**144**	**68**				**76**	В т.ч. промежуточная аттестация																			**0**	**18**	**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

Код раздела, темы	Номер работы	Наименование работы	Время на выполнение работы (час.)
1	1	Математические основы криптографии	8
2	2	Настройка протокола IPsec	8
3	3	Применение пакета PGP	4
4	4	Использование цифровых сертификатов	14
		Всего:	**34**

4.2 Практические занятия

Не предусмотрено

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

- *Изучение шифров перестановки, простой и сложной замены;*
- *Алгоритмы RSA, Диффи-Хелмана;*
- *Математические основы и алгоритмы ЭЦП;*
- *Схемы генерации ключей.*

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)

- *Линейные и нелинейные конгруэнтные генераторы*

4.3.6. Примерный перечень тем расчетно-графических работ

- *Шифрование по алгоритму S-DES*

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)
Общие принципы криптографии				*								
Симметричные криптографические системы					*			*				
Асимметричные криптографические системы				*				*				
Управление криптографическими ключами					*			*				

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. Основы криптографии : учеб. пособие для студентов вузов, обучающихся по группе специальностей в обл. информ. безопасности / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин .— 3-е изд., испр. и доп. — М. : Гелиос АРВ, 2005 .— 480 с. 25 экз

2. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях / М.А. Иванов .— М. : КУДИЦ-ОБРАЗ, 2001 .— 368 с.

9.1.2.Дополнительная литература

1. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин; Под ред. В.Ф. Шаньгина .— М. : Радио и связь, 1999 .— 328 с. 24 экз

2. Осипян В.О. Криптография в задачах и упражнениях / В. О. Осипян, К. В. Осипян .— М. : Гелиос АРВ, 2004 .— 144 с. 11 экз

3. Нечаев В.И. Элементы криптографии. (Основы теории защиты информации : Учеб. пособие для вузов / Под ред. В.А. Садовничего .— М. : Высш. шк., 1999 .— 109 с.

4. Молдовян А.А. Криптография / А.А. Молдовян, Н.А. Молдовян, Б.Я. Советов .— СПб. : Лань, 2001 .— 224 с.

5. Баричев С. Г. Основы современной криптографии : Учеб. курс / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов .— 2-е изд., испр. и доп. — М. : Горячая линия-Телеком, 2002 .— 175 с.

9.2. Методические разработки

1. Спиричева Н.Р. Алгоритмы блочной криптографии. ЭОР УрФУ, АПИ, 2013. Метаданные ресурса №13170

9.3. Программное обеспечение

GPG, IPsec, веб-браузер

9.4. Базы данных, информационно-справочные и поисковые системы

http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»
2. http://www.edu.ru/ - Федеральный портал. Российское образование.
3. http://study.ustu.ru –портал информационно-образовательных ресурсов УрФУ
4. http://rtf.ustu.ru - официальный сайт ИРИТ-РтФ

9.5. Электронные образовательные ресурсы

1. Зональная научная библиотека УрФУ — http://lib.urfu.ru
2. Портал информационно-образовательных ресурсов УрФУ — http://study.ustu.ru ;
3. Официальный сайт ИРИТ-РтФ — http://rtf.ustu.ru ;

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Р-402. Персональные компьютеры – 10 шт. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet

Р-411. Персональные компьютеры – 15 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.

Р-125 Персональные компьютеры – 20 Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.

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 не устанавливается.

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: **коэффициент значимости совокупных результатов лекционных занятий – 0,4**		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Домашняя работа №1	*4,1-7*	*25*
Домашняя работа №2	*4,1-7*	*25*
Домашняя работа №3	*4,1-7*	*25*
Домашняя работа №4	*4,1-7*	*25*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – экзамен **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 0		
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 –0,6		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Расчетная работа	*4,8-15*	*20*
Расчетно-графическая работа	*4,8-15*	*20*
Выполнение лабораторных работ	*4,8-15*	*60*
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям – 1,0		
Промежуточная аттестация по лабораторным занятиям – *не предусмотрена* **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям– 0**		

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

Не предусмотрено

8.3.3. Примерные контрольные кейсы

Не предусмотрено

1.3.4. Перечень примерных вопросов для зачета

Не предусмотрено

8.3.5. Перечень примерных вопросов для экзамена

1. Место криптографии в защите информации. Физическая защита. Стеганография. Криптография.
2. Предмет криптографии. Математические основы.
3. История криптографии. Шифр Цезаря. Сцитала. Маршрутная перестановка. Квадрат Полибия.
4. История криптографии. Магический квадрат. Таблица Тритемия. Решетка Кардано.
5. История криптографии. Шифр Виженера. Шифр Плейфера. Принцип Керкгоффса.
6. История криптографии. Лента Вернама. Энигма.
7. Математические основы криптографии. «Теория связи в секретных системах» Шеннона: математическая структура секретных систем.
8. Математические основы криптографии. «Теория связи в секретных системах» Шеннона: теоретическая секретность.
9. Математические основы криптографии. «Теория связи в секретных системах» Шеннона: практическая секретность.
10. Симметричная криптография. Криптоанализ простым перебором. Общая схема симметричной системы. Алгоритм S-DES.
11. Симметричная криптография. Сеть Файстеля. Алгоритм DES.
12. Симметричная криптография. Блочные шифры. Диффузия и конфузия. Проектирование S-блоков.
13. Симметричная криптография. Алгоритмы 3DES, ГОСТ 34.12-2015. Режимы использования блочных шифров.
14. Симметричная криптография. Алгоритм AES.
15. Симметричная криптография. Криптоанализ. Атаки на реализацию. Линейный криптоанализ.
16. Симметричная криптография. Квантовый криптоанализ. Производительность AES.
17. Асимметричная криптография. Проблемы традиционной криптографии. Общая схема асимметричной системы. Возможности и условия применения.
18. Асимметричная криптография. Одностороняя функция с лазейкой. Криптоанализ. Алгоритм RSA.

19. Асимметричная криптография. Протокол Диффи-Хеллмана.
20. Асимметричная криптография. Схема Эль-Гамаля. Эллиптическая криптография.
21. Совместное использование традиционной и асимметричной криптографии. Обеспечение конфиденциальности и целостности. Контроль ошибок.
22. Совместное использование традиционной и асимметричной криптографии. Имитовставка.
23. Функция хэширования. Схемы применения. Требования. Атаки. Способы построения.
24. Цифровая подпись. Назначение. Схемы применения. Атаки. Алгоритм DSA.
25. Распределение ключей. Сравнение особенностей симметричной и асимметричной систем. Иерархия ключей.
26. Распределение ключей. Сеансовые ключи. Сценарии обмена.
27. Распределение ключей. Обмен открытыми ключами. Сценарии.
28. Распределение ключей. Сертификаты открытых ключей. Сценарии обмена.
29. Средства криптографической защиты информации. IPSec.
30. Средства криптографической защиты информации. Организация иерархии удостоверяющих центров.
31. Средства криптографической защиты информации. Kerberos.
32. Распределение ключей. Удостоверяющий центр.
33. Распределение ключей. Взаимодействие УЦ. Жизненный цикл сертификата.
34. Стеганография. Современные подходы. Стегоанализ.

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

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 ИНФОРМАЦИИ И КОДИРОВАНИЯ

Перечень сведений о рабочей программе модуля	**Учетные данные**
Модуль ***Информационное кодирование***	**Код модуля** № 1138288 УП №№ 5433, 6323
Образовательная программа ***Информационная безопасность телекоммуникационных систем***	**Код ОП** ***10.05.02***
Траектория образовательной программы (ТОП)	***Не предусмотрено.***
Направление подготовки ***Информационная безопасность телекоммуникационных систем***	**Код направления и уровня подготовки** 10.05.02/01.01
Уровень подготовки ***Специалитет***	
ФГОС ВО ***10.05.02 Информационная безопасность телекоммуникационных систем***	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: №1426 16 ноября 2016 г

Екатеринбург, 2017

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Кафедра, департамент	Подпись
1	Коберниченко Виктор Григорьевич	К.т.н., доцент	Профессор	Радиоэлектроники и связи	

Руководитель модуля Н.С. Виноградова

Рекомендовано учебно-методическим советом Института радиоэлектроники и информационных технологий – РТФ

Зам Председателя учебно-методического совета Н.В. Папуловская
Протокол № _____ от _____ г.

Согласовано:

Дирекция образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ «ТЕОРИЯ ИНФОРМАЦИИ И КОДИРОВАНИЯ»

1.1.Аннотация содержания дисциплины

Изучение дисциплины нацелено на формирование у студентов знаний, умений и навыков, необходимых для оценки технических возможностей информационных систем общего и специального назначения. Задачей дисциплины является научить принципам информационного подхода к анализу и синтезу систем связи, передачи информации и автоматизированных систем обработки информации.

Первая часть дисциплины - «Основы теории информации», знакомит с количественными закономерностями, связанные с получением, передачей, обработкой и хранением информации. Она посвящена изучению следующих категорий: источник, информационный канал, приемник, кодирование, пропускная способность, производительность источника.

Основное содержание второй части – «Основы теории кодирования» посвящено изучению методов построения и оценки эффективных и помехоустойчивых кодов.

1.2. Язык реализации программы – *русский*

1.3. Планируемые результаты обучения по дисциплине

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

– О П К-1 –способность анализировать физические явления и процессы для формализации и решения задач, возникающих в ходе профессиональной деятельности;

– О П К-2 –способность применять соответствующий математический аппарат для решения профессиональных задач;

– О П К-3 –способность применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения профессиональных задач;

– ОПК-5 – способность применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач.

В результате освоения дисциплины студент должен:

Знать:

- фундаментальные понятия теории информации: энтропия, взаимная информация, источники сообщений, каналы связи, кодирование;
- основные методы оптимального кодирования источников информации;
- основные методы помехоустойчивого кодирования и декодирования информации;
- основные параметры и характеристики помехоустойчивых кодов;
- информационно - математические модели дискретных и непрерывных каналов связи.

Уметь:

- применять знания о кодах, устраняющих избыточность и корректирующих ошибки;
- вычислять теоретико-информационные характеристики источников сообщений и каналов связи.

Владеть (демонстрировать навыки и опыт деятельности):

- навыками применения математического аппарата и прикладного программного обеспечения для решения прикладных теоретико-информационных задач.

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.)*	5	6
1.	**Аудиторные занятия**	119	119	54	65
2.	Лекции	68	68	20	48
3.	Практические занятия	51	51	34	17
4.	Лабораторные работы	-	-	-	-
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	133	12,75	54	79
6.	**Промежуточная аттестация**	З, Э	2,58	З	Э
7.	**Общий объем по учебному плану, час.**	252	134,33	108	144
8.	**Общий объем по учебному плану, з.е.**	7		3	4

Заочная форма обучения не предусмотрена

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела	Раздел дисциплины [наименование]	Содержание*
Р1	Информационные характеристики источников сообщений	Предмет, категории и задачи теории информации. Информация, сообщение, сигнал. Физические источники информации. Способы аналитического описания (математические модели) сообщений и сигналов. Обобщенная структурная схема инфотелекоммуникационной системы. Дискретные и непрерывные ансамбли и источники сообщений. Количественная мера информации. Взаимная, собственная и условная информация дискретных ансамблей. Энтропия и ее свойства. Модель источника дискретных сообщений. Источники без памяти. Эргодические источники. Учет статистических связей между последовательными состояниями дискретного источника. Марковские источники. Энтропия дискретного источника. Производительность источника (поток информации). Избыточность. Энтропия и избыточность текстов. Количество информации в непрерывных сообщениях. Представление непрерывного сообщения многомерным вектором. Дифференциальная энтропия. Взаимная информация для непрерывных ансамблей. Передача непрерывных сообщений с заданным критерием верности. Эпсилон-энтропия. Эпсилон-производительность и избыточность стационарного источника непрерывных сообщений.

Р2	Информационные характеристики каналов	Классификация информационных каналов: дискретные, дискретно-непрерывные и непрерывные каналы. Модели дискретных каналов. Скорость передачи информации и пропускная способность информационного канала. Пропускная способность дискретного канала при отсутствии помех. Скорость передачи информации и пропускная способность дискретного канала с помехами. Скорость передачи информации и пропускная способность непрерывного канала с аддитивным шумом. Основная теорема кодирования для канала без помех и для канала с помехами.
Р3	Кодирование источников сообщений	Задача кодирования источника дискретных сообщений. Теорема оптимального кодирования. Равномерное кодирование. Производительность источника дискретных сообщений при равномерном кодировании. Неравномерное кодирование. Оптимальные статистические коды. Код Шеннона-Фано. Код Хаффмена. Кодирование источника дискретных сообщений при неизвестной статистике. Алгоритмы кодирования, применяемые в архиваторах. Особенности сжатия неподвижных и подвижных изображений. Задача кодирования источника непрерывных сообщений. Регулярная и адаптивная дискретизация. Равномерное и неравномерное квантование, квантование с компадированием. Цифровое кодирование непрерывных сообщений: импульсно-кодовая модуляция. Цифровое кодирование непрерывных сообщений с предсказанием: дифференциальная импульсно-кодовая модуляция и дельта-модуляция. Особенности сжатия речи.
Р4	Принципы помехоустойчивого кодирования	Основная теорема Шеннона для дискретного канала с шумами. Общие принципы использования избыточности. Векторное пространство кодов, кодовое расстояние и вес кодовой комбинации. Связь корректирующей способности кода с кодовым расстоянием. Граница Хэмминга. Скорость и избыточность. Классификация помехоустойчивых кодов. Вероятность ошибки на символ и на бит при использовании помехоустойчивого кодирования. Классификация помехоустойчивых кодов.
Р5	Линейные блочные коды	Основные параметры блочных кодов. Порождающая и проверочная матрицы. Способы задания блочных кодов. Способы кодирования. Способы декодирования. Синдромное декодирование блочных кодов. Коды Хемминга. Модификация кодов Хемминга. Вероятность ошибки на символ и на бит, выигрыш от кодирования при использовании кодов Хемминга.
Р6	Циклические коды	Принципы построения циклических кодов. Порождающий и проверочный многочлены. Способы задания циклических кодов. Задание циклического кода с помощью минимальных многочленов. Наиболее известные цикли-

		ческие коды. Способы кодирования. Аппаратная реализация кодеров. Способы декодирования. Мажоритарное декодирование. Аппаратная реализация декодеров. Метод максимального правдоподобия. Синдромное декодирование циклических кодов. Качество и вычислительная сложность декодирования. Коды БЧХ. Код Голея. Коды Рида-Соломона. Вероятность ошибки на символ и на бит, выигрыш от кодирования при использовании кодов БЧХ, кода Голея и кодов Рида-Соломона.
Р7	Сверточные коды	Основные параметры сверточных кодов. Способы задания сверточных кодов: порождающая матрица, представление связей, полиномиальное представление и импульсный отклик сверточного кодера. Древовидная диаграмма. Диаграмма состояний. Решетчатая диаграмма. Наиболее известные сверточные коды. Способы кодирования. Способы декодирования. Алгоритм максимального правдоподобия. Алгоритм Витерби. Декодирование с «жестким» и «мягким» решением. Последовательное декодирования. Алгоритм Фано. Декодирование с обратной связью. Сравнительная характеристика алгоритмов декодирования. Вероятность ошибки на символ и на бит, выигрыш от кодирования при использовании сверточных кодов.

**Указываются темы или дидактические единицы, или перечень основных вопросов дисциплины.*

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

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

Очная форма обучения

Объем дисциплины (зач.ед.): 7

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	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 иностр. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
1	Информационные характеристики источников сообщений	**48**	**28**	14	14		**20**	**10**	2	8			**10**	2													Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
2	Информационные характеристики каналов	**39**	**20**	6	14		**19**	**10**	2	8			**9**	1																
3	Кодирование источников сообщений	**41**	**24**	16	8		**17**	**5**	2	3			**12**			1														
4	Принципы помехоустойчивого кодирования	**15**	**11**	8	3		**4**	**4**	2	2																				
5	Линейные блочные коды	**17**	**12**	8	4		**5**	**5**	2	3																				
6	Циклические коды	**35**	**12**	8	4		**23**	**5**	2	3			**18**						1											
7	Сверточные коды	**35**	**12**	8	4		**23**	**5**	2	3			**18**						1											
Всего (час), без учета промежуточной аттестации:		**230**	**119**	**68**	**51**	**0**	**111**	**44**	**14**	**30**			**67**	**19**		**12**			**36**											
	Всего по дисциплине (час.):	**252**	**129**				**133**	В т.ч. промежуточная аттестация																			**4**	**18**	**0**	**0**

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1. Лабораторные работы

Не предусмотрено

4.2. Практические занятия

№	Раздел дисциплины	Темы занятий	Объем учебного времени, час.
1	Р1	Информационные характеристики дискретных ансамблей. Условная энтропия и энтропия объединения	6
2	Р1	Информационные характеристики дискретных источников.	4
3	Р1	Дифференциальная энтропия непрерывных распределений	4
4	Р2	Пропускная способность дискретного канала связи.	8
5	Р2	Пропускная способность непрерывных гауссовых каналов	4
6	Р3	Эффективное кодирование. Кодирование источников методами Фано, Шеннона, Хаффмена.	4
7	Р3	Методы упаковки данных.	6
8	Р4	Помехоустойчивое кодирование. Построение групповых кодов. Расчет ошибки декодирования	3
9	Р5	Исследование корректирующей способности блочных кодов	4
10	Р6	Исследование корректирующей способности циклических кодов	4
11	Р7	Исследование корректирующей способности сверточных кодов	4
Всего			**51**

4.3. Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

1. Условная энтропия и энтропия объединения.
2. Передача информации по дискретным каналам.
3. Информационные характеристики непрерывных каналов

4.3.2. Примерный перечень тем графических работ

Не предусмотрено

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

1. Сжатие информации. Основная теорема кодирования при отсутствии помех (доказательство). Алгоритмы Шеннона-Фано и Хаффмена.
2. Сжатие информации. Арифметическое кодирование.

3. Адаптивные алгоритмы сжатия. Адаптивный алгоритм Хаффмена.
4. Сжатие информации. Адаптивное арифметическое кодирование.
5. Словарно-ориентированные алгоритмы сжатия информации. Метод Лемпела-Зива (LZ).
6. Алгоритм сжатия Лемпела-Зива Уэлча (LZW). Кодирование и декодирование.
7. Характеристика программ – архиваторов.
8. Разработка программы архиватора – дезархиватора.
9. Вейвлетные методы сжатия изображений.
10. Сжатие изображений. Метод JPEG. Преобразования и коды.
11. Сжатие изображения. Коды Грея.
12. Сжатие звука. Кодирование в частотной области. Стандарт MPEG-1.
13. Дискретное косинус-преобразование.
14. Дискретное синус-преобразование.
15. Преобразование Уолша-Адамара.
16. Преобразование Хаара.
17. Преобразование Карунена - Лоэва.

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

1. Разработка и анализ структурной схемы декодера циклических кодов.
2. Разработка и анализ структурной схемы декодера сверточных кодов.

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) Практические занятия с ЭНИ	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				*								
Р4				*		*						
Р6	*			*		*						
Р7				*		*						

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. Вернер М. Основы кодирования: Учебник для вузов. – М.: Техносфера, 2004. -288 с.
2. Дмитриев В.И. Прикладная теория информации : Учебник для вузов / В. И. Дмитриев .— М. : Высшая школа, 1989 .— 320 с.

9.1.2. Дополнительная литература

1. Ковалгин Ю.А. Цифровое кодирование звуковых сигналов : учеб. пособие для студентов вузов/ Ю. А. Ковалгин, Э. И. Вологдин .— Санкт-Петербург : КОРОНА-принт, 2004 .— 240 с.
2. Крохин А.Л. Алгебраические основы кодирования и криптографии : учебное пособие / А. Л. Крохин ; науч. ред. Г. Л. Ходак ; Урал. федер. ун-т им. первого Президента России Б. Н. Ельцина .— Екатеринбург : УрФУ, 2011 .— 154 с.
3. Системы передачи данных. Скорости передачи данных и основные параметры помехоустойчивых циклических кодов : ГОСТ 17422-82 : Введ. в действие с 01.01.83 : Взамен ГОСТ 17422-72 : Изд. офиц. / Госстандарт СССР .— М. : Издательство стандартов, 1982 .— 3 с.
4. Липкин И.А. Статистическая радиотехника. Теория информации и кодирования / И. А. Липкин .— М. : Вузовская книга, 2002 .— 216 с.

9.2. Методические разработки

1. Теория информации: рабочая тетрадь/Н.Р. Спиричева. 2-е изд. Екатеринбург: ГОУ ВПО УГТУ-УПИ, 2008. 35 с.

9.3. Программное обеспечение

Программное обеспечение математических вычислений и моделирования Matlab

9.4. Базы данных, информационно-справочные и поисковые системы

Портал информационно-образовательных ресурсов www.http://study.ustu.ru,

Зональная научная библиотека УрФУ - http://lib.urfu.ru,

9.5. Электронные образовательные ресурсы

1. Коберниченко В.Г., Спиричева Н.Р. Теория информации. УМК № 8221. 2008. [Электронный ресурс]. Режим доступа: http://www.study.urfu.ru/Aid/Umk/8221.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Материал дисциплины изучается в специализированных аудиториях Р-411, оснащенной современным компьютером с подключенным к нему мультимедийным проектором.

Р-146. Специализированная лекционная аудитория. Персональный компьютер с подключенным мультимедийным проектором.

Р-402. Лаборатория моделирования и цифровой обработки сигналов. Персональные компьютеры – 10 шт. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.

Р-411. Лаборатория защищенных информационных систем. Персональные компьютеры – 15 шт. Сервер – 1. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.

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 не устанавливается.

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

СЕМЕСТР ОБУЧЕНИЯ V

1.Лекции: **коэффициент значимости совокупных результатов лекционных занятий – 0,8**		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Выполнение домашней работы №1	*5, 10*	*30*
Выполнение домашней работы №2	*5, 12*	*40*
Выполнение домашней работы №3	5, 15	*30*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,6		
Промежуточная аттестация по лекциям – *зачет* **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,4**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0,2		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Посещение практических занятий	*5, 1-16*	*100*
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*		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям – 0		
Промежуточная аттестация по лабораторным занятиям – ***не предусмотрена*** **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям**		

СЕМЕСТР ОБУЧЕНИЯ VI

1.Лекции: **коэффициент значимости совокупных результатов лекционных занятий – 0,7**		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Подготовка и защита реферата	*6, 10*	*100*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – *экзамен* **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0,3		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Выполнение расчетно-графической работы №1	*6, 14*	*50*
Выполнение расчетно-графической работы №2	*6, 14*	*50*
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*		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям – 0		
Промежуточная аттестация по лабораторным занятиям – **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям**		

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

Не предусмотрено

8.3.3. Примерные контрольные кейсы

Не предусмотрено

8.3.4. Перечень примерных вопросов для зачета

1. Доказать, что при заданном количестве дискретных сообщений n энтропия максимальна, когда все сообщения равновероятны.
2. Доказать, что среднее количество информации, доставляемое принятым символом y_i относительно множества всех передаваемых символов X не может быть отрицательным. Когда это количество равно нулю?
3. Доказать, что полная условная энтропия системы H(X/Y) не превосходит её безусловной энтропии.
4. Определить пропускную способность дискретного канала при отсутствии помех, если для передачи сообщений используется код с основанием B. Длительность всех символов кода одинакова и равна τ.
5. Определить пропускную способность двоичного симметричного канала с шумами, при условии, что все символы имеют одинаковую длительность $\tau = 10$ м/сек. Построить зависимость пропускной способности от вероятности искажения символа за счет влияния помех.
6. Определить пропускную способность двоичного канала со стиранием, если входные и выходные символы имеют одинаковую длительность $\tau = 1/F$, где F – частота посылок. Априорные вероятности единицы и нуля равны соответственно p и $1 - p$, вероятность перепутывания каждого символа равна q, а вероятность стирания $P_с$
7. Содержание теоремы Шеннона для дискретных каналов с помехами.
8. Определение пропускной способности непрерывного информационного канала.
9. Основная теорема Шеннона для непрерывного канала с помехами.
10. Что такое «эпсилон - производительность источника»? При каких условиях она достигает максимального значения? Чему оно равно? Что такое «объем сигнала»?
11. Перечислить и доказать свойства взаимной информации.
12. Перечислить и доказать основные свойства энтропии.
13. Определение эпсилон - энтропии.
14. Найти плотность распределения вероятности, при которой дифференциальная энтропия случайной величины максимальна, если задан её второй начальный момент m_2.

15. Определить количество информации, содержащееся в одном замере напряжения x равномерно распределенного в интервале от 200 до 240 В, если погрешность измерения не зависит от x и распределена по нормальному закону со с.к.о. σ_n = 2 В.

8.3.5. Перечень примерных вопросов для экзамена

1. Закодировать по методу Шеннона – Фано алфавит, состоящий из четырех символов A, B, C, D, если вероятности появления каждого символа в сообщении соответственно равны 0,28; 0,14; 0,48; 0,1. Определить экономичность полученного кода.
2. Закодировать методом Хаффмена семь сообщений, имеющих вероятности: p_1=0,35; p_2=p_3=0,15; p_4=0,12; p_5=0,1; p_6=0,05; p_7=p_8=0,04.
3. Сообщение состоит из последовательности двух букв A и B, вероятность появления каждой из которых не зависят от того, какая буква была передана ранее и равны
P(A) = 0,8, P(B) = 0,2.

   Произвести кодирование по методу Шеннона – Фано:
   а/ отдельных букв;
   б/ двухбуквенных сочетаний;
   в/ блоков, состоящих из трехбуквенных сочетаний.
   Сравнить коды по их экономичности и по избыточности.
4. Источник дискретных сообщений задается следующим распределением вероятностей состояний: 7/18, 1/6, 1/6, 1/6, 1/9. Определить энтропию источника и среднюю длину кодового слова при кодировании методом Хаффмена.
5. Составить блочный код Хаффмена (для блоков длины 2) для сообщения ABAAAB, если вероятности независимых состояний источника равны: P(A)=1/3, P(B)=2/3. Определить длину кода сообщения, среднюю длину кодовой комбинации и эффективность кода.
6. Связь корректирующей способности кода с кодовым расстоянием. Определить значность кода, исправляющего все одиночные ошибки при передаче алфавита их пяти символов. Сколько кратных ошибок будет при этом исправляться?
7. Способен ли код исправлять ошибки, если его комбинации имеют вид:
   1001010, 0101110, 1101001, 0011011, 1001010?
8. Построить порождающую матрицу двоичного группового кода, исправляющего однократные ошибки, если количество передаваемых сообщений равно 50.
9. Построить линейный блочный код (5,2), задаваемый производящей матрицей G вида
   1 0 1 0 1
   0 1 1 1 0
   Описать основные характеристики полученного кода: минимальное кодовое расстояние, максимальную кратность обнаруживаемых и исправляемых ошибок, вероятность необнаруживаемой ошибки. Как будут декодированы слова: 10001, 01110, 10101 ?
10. Построить и исследовать линейный блочный код Хэмминга (15,11).
11. Источник передает сообщения при помощи 16 двоичных кодовых слов. Составить информационную, проверочную и полную производящую матрицы группового (n,k)-кода, исправляющего все одиночные ошибки. Исследовать его свойства.
12. Вероятность ошибки декодирования. Имеется линейный блочный код (9,8) с проверкой на четность. Вычислить вероятность необнаруживаемой ошибки, если вероятность ошибки при передаче каждого бита равна 0,01. Определить вероятность ошибочного приема без использования кода.
13. В дискретном симметричном канале без памяти с аддитивным белым гауссовым шумом (АБГШ) применяется код Хэмминга (7,4).При отношении сигнал/шум, равном 6 дБ, в канале обеспечивается скорость передачи информации 16 кбит/сек. Определить вероятность безошибочной передачи кодовой комбинации, вероятность необнаруженной ошибки и эффективную скорость передачи.

14. Синдромное декодирование блочных кодов**.** Найти и исправить однократную ошибку в принятых комбинациях кода Хэмминга:

$$\overline{\alpha}_1 = (1011110\ ) \text{ и } \overline{\alpha}_2 = (1010010\ ), \text{ если } \begin{cases} S_1 = a_1 \oplus a_3 \oplus a_5 \oplus a_7 \\ S_2 = a_2 \oplus a_3 \oplus a_6 \oplus a_7 \\ S_3 = a_4 \oplus a_5 \oplus a_6 \oplus a_7 \end{cases}.$$

15. Дана порождающая матрица кода Хэмминга $G_{(7,4)} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$.

Исправить принятую кодовую комбинацию α=1011001 в случае однократной ошибки. Дать примеры «правильных» комбинаций в случае двукратных ошибок.

16. Представить образующий многочлен $Q(x)=x^5 \oplus x^2 \oplus x \oplus 1$ в виде произведения неприводимых многочленов. Определить максимальную разрядность избыточного циклического кода для исправления однократной ошибки.
17. Определить дополнительные разряды для строк единичной матрицы (k=6), если задан образующий многочлен вида: $g(x)=x^4 \oplus x \oplus 1$.
18. По порождающему многочлену $g(x) = x^7 + x^5 + x + 1$ построить полиномиальные коды для двоичных сообщений 0100, 10001101, 11110.
19. Найти проверочную матрицу циклического кода (7,4) с порождающим многочленом $g(x)= 1+x+ x^3$. Определить кодовое слово, соответствующее передаваемому сообщению 1010. Проанализировать прием этого слова при наличии ошибки в 4 разряде.
20. Определить циклический (7,4)- код в систематической форме при передаче информационного сообщения 1001.
21. Ошибки какой кратности и «пакеты» ошибок какой максимальной длины способен обнаруживать циклический код (7,4)? Приведите обоснование.

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