

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования



**Пермский национальный исследовательский
политехнический университет**

УТВЕРЖДАЮ

Проректор по образовательной
деятельности

 А.Б. Петроченков

« 11 » апреля 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Теория и практика кодирования в информационных системах
(наименование)

Форма обучения: очная
(очная/очно-заочная/заочная)

Уровень высшего образования: бакалавриат
(бакалавриат/специалитет/магистратура)

Общая трудоёмкость: 180 (5)
(часы (ЗЕ))

Направление подготовки: 10.03.01 Информационная безопасность
(код и наименование направления)

Направленность: Информационная безопасность (общий профиль, СУОС)
(наименование образовательной программы)

1. Общие положения

1.1. Цели и задачи дисциплины

Формирование заданных компонентов компетенций по применению способов и алгоритмов кодирования в информационных системах.

Задачи:

- сформировать знания методов и алгоритмов криптографического, экономного и помехоустойчивого кодирования;
- сформировать умения расчета параметров и анализа свойств различных кодов;
- сформировать навыки программного и визуального проектирования и моделирования информационных систем с различными видами кодирования.

1.2. Изучаемые объекты дисциплины

- методы и способы криптографического кодирования информации
- алгоритмы и подходы к реализации экономного (эффективного) кодирования;
- методы помехоустойчивого кодирования.

1.3. Входные требования

Цифровая схемотехника
Теория вероятности и математическая статистика
Электроника

2. Планируемые результаты обучения по дисциплине

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
-------------	-------------------	---	--	-----------------

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ОПК-9	ИД-1ОПК-9	Знает методы и алгоритмы кодирования в информационных системах	Знает принципы построения систем и сетей электросвязи; современные виды информационного взаимодействия и обслуживания телекоммуникационных сетей и систем; основные понятия и задачи криптографии, математические модели криптографических систем; основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и криптографические протоколы; национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения; классификацию и количественные характеристики технических каналов утечки информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации;	Экзамен
ОПК-9	ИД-2ОПК-9	Умеет выполнить расчет и анализ основных информационно-технических характеристик	Умеет проводить анализ показателей эффективности сетей и систем телекоммуникаций и качества	Защита лабораторной работы

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
		применяемых способов кодирования.	предоставляемых услуг; применять математические модели для оценки стойкости СКЗИ; использовать СКЗИ в автоматизированных системах; пользоваться нормативными документами в области технической защиты информации; анализировать и оценивать угрозы информационной безопасности объекта информатизации;	
ОПК-9	ИД-3ОПК-9	Владеет навыками применения пакетов прикладных программ для моделирования и исследования выбранных способов кодирования.	Владеет методами и средствами технической защиты информации	Защита лабораторной работы

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		5	
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме:	62	62	
1.1. Контактная аудиторная работа, из них:			
- лекции (Л)	32	32	
- лабораторные работы (ЛР)	28	28	
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	0	0	
- контроль самостоятельной работы (КСР)	2	2	
- контрольная работа			
1.2. Самостоятельная работа студентов (СРС)	82	82	
2. Промежуточная аттестация			
Экзамен	36	36	
Дифференцированный зачет			
Зачет			
Курсовой проект (КП)			
Курсовая работа (КР)	18	18	
Общая трудоемкость дисциплины	180	180	

4. Содержание дисциплины

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
5-й семестр				
Общий подход к кодированию сообщений. Принципы криптографического и экономного кодирования	8	8	0	22
"1. Основные понятия и определения теории передачи сообщений. Математические модели дискретных каналов связи 2. Экономное кодирование (сжатие). Криптографическое кодирование (шифрование)				
Помехоустойчивое кодирование	24	20	0	60
"3. Общие принципы обнаружения и исправления ошибок избыточными кодами 4. Помехоустойчивое кодирование. Комбинаторные коды 5. Помехоустойчивое кодирование. Групповые коды 6. Помехоустойчивое кодирование. Циклические коды 7. Структурные методы повышения помехоустойчивости. Повторение символов/сообщений 8. Структурные методы повышения помехоустойчивости. Обратные связи				
ИТОГО по 5-му семестру	32	28	0	82
ИТОГО по дисциплине	32	28	0	82

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Экономное кодирование. Коды Шеннона-Фано, Хаффмана

Тематика примерных лабораторных работ

№ п.п.	Наименование темы лабораторной работы
1	Экономное кодирование. Коды Шеннона-Фано, Хаффмана
2	Криптографическое кодирование. Шифры Цезаря и Вижинера
3	Помехоустойчивое кодирование. Комбинаторные коды
4	Помехоустойчивое кодирование. Групповые коды. Построение, алгоритмы кодирования, кодирующие устройства

№ п.п.	Наименование темы лабораторной работы
5	Помехоустойчивое кодирование. Групповые коды. Алгоритмы декодирования, декодирующие устройства
6	Помехоустойчивое кодирование. Циклические коды. Задание кода, алгоритмы кодирования, кодирующие устройства
7	Помехоустойчивое кодирование. Циклические коды. Алгоритмы декодирования, декодирующие устройства

Тематика примерных курсовых проектов/работ

№ п.п.	Наименование темы курсовых проектов/работ
1	Построение системы передачи информации, использующей групповой систематический код

5. Организационно-педагогические условия

5.1. Образовательные технологии, используемые для формирования компетенций

<p>Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при котором учащиеся не пассивные слушатели, а активные участники занятия, отвечающие на вопросы преподавателя. Вопросы преподавателя нацелены на активизацию процессов усвоения материала, а также на развитие логического мышления. Преподаватель заранее намечает список вопросов, стимулирующих ассоциативное мышление и установление связей с ранее освоенным материалом.</p> <p>Лабораторные занятия проводятся на основе реализации метода обучения действием: определяются проблемные области, формируются группы. При проведении лабораторных занятий преследуются следующие цели: применение знаний отдельных дисциплин и креативных методов для решения проблем и принятия решений; отработка у обучающихся навыков командной работы, межличностных коммуникаций и развитие лидерских качеств; закрепление основ теоретических знаний.</p> <p>Проведение лабораторных занятий основывается на интерактивном методе обучения, при котором обучающиеся взаимодействуют не только с преподавателем, но и друг с другом. При этом доминирует активность учащихся в процессе обучения. Место преподавателя в интерактивных занятиях сводится к направлению деятельности обучающихся на достижение целей занятия.</p> <p>При проведении учебных занятий используются интерактивные лекции, групповые дискуссии, ролевые игры, тренинги и анализ ситуаций и имитационных моделей.</p>
--

5.2. Методические указания для обучающихся по изучению дисциплины

<p>При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:</p> <ol style="list-style-type: none"> 1. Изучение учебной дисциплины должно вестись систематически. 2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела. 3. Особое внимание следует уделить выполнению отчетов по лабораторным работам и индивидуальным комплексным заданиям на самостоятельную работу. 4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.
--

6. Перечень учебно-методического и информационного обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Печатная учебно-методическая литература

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Количество экземпляров в библиотеке
1. Основная литература		
1	Голиков А. М. Модуляция, кодирование и моделирование в телекоммуникационных системах. Теория и практика : учебное пособие / А. М. Голиков. - Санкт-Петербург [и др.]: Лань, 2018.	1
2	Литвинская О. С. Основы теории передачи информации : учебное пособие / О. С. Литвинская, Н. И. Чернышёв. - Москва: КНОРУС, 2020.	6
3	Матвеев Б. В. Основы корректирующего кодирования: теория и лабораторный практикум : учебное пособие для вузов / Б. В. Матвеев. - Санкт-Петербург [и др.]: Лань, 2014.	1
4	Романьков В. А. Введение в криптографию : курс лекций / В. А. Романьков. - Москва: ФОРУМ, 2012.	2
5	Теория кодирования : сборник трудов : пер. с англ. / Под ред. Э. Л. Блоха. - Москва: Мир, 1964.	1
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Кон Е. Л. Теория электрической связи. Помехоустойчивая передача данных в информационно-управляющих и телекоммуникационных системах: модели, алгоритмы, структуры : учебное пособие / Е. Л. Кон, В. И. Фрейман. - Пермь: Изд-во ПГТУ, 2007.	115
2	Пахомов Г. И. Теория электрической связи. Основные понятия : учебное пособие / Г. И. Пахомов, В. И. Фрейман. - Пермь: Изд-во ПГТУ, 2007.	76
2.2. Периодические издания		
1	Телекоммуникации : научно-технический, информационно-аналитический и учебно-методический журнал. - Москва: , Наука и технологии	1
2.3. Нормативно-технические издания		
	Не используется	
3. Методические указания для студентов по освоению дисциплины		
1	Фрейман В. И. Теория электрической связи. Помехоустойчивое кодирование в телекоммуникационных системах : учебно-методическое пособие / В. И. Фрейман. - Пермь: Изд-во ПНИПУ, 2011.	1
4. Учебно-методическое обеспечение самостоятельной работы студента		
	Не используется	

6.2. Электронная учебно-методическая литература

Вид литературы	Наименование разработки	Ссылка на информационный ресурс	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
Дополнительная литература	Попов И. Ю. Теория информации : учебник / Попов И. Ю., Блинова И. В. - Санкт-Петербург: Лань, 2020.	http://elib.pstu.ru/Record/lanRU-LAN-BOOK-126940	сеть Интернет; авторизованный доступ

6.3. Лицензионное и свободно распространяемое программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Вид ПО	Наименование ПО
Операционные системы	MS Windows 8.1 (подп. Azure Dev Tools for Teaching)
Офисные приложения.	Adobe Acrobat Reader DC. бесплатное ПО просмотра PDF
Прикладное программное обеспечение общего назначения	Dr.Web Enterprise Security Suite, 3000 лиц, ПНИПУ ОЦНИТ 2017
Прикладное программное обеспечение общего назначения	SciLab (лиц. CeCILL https://www.scilab.org/)

6.4. Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Наименование	Ссылка на информационный ресурс
Научная библиотека Пермского национального исследовательского политехнического университета	http://lib.pstu.ru/
Электронно-библиотечная система Лань	https://e.lanbook.com/
Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/
Информационные ресурсы Сети КонсультантПлюс	http://www.consultant.ru/
База данных компании EBSCO	https://www.ebsco.com/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Курсовая работа	Персональный компьютер IBM PC	12
Лабораторная работа	Персональный компьютер IBM PC	12
Лекция	Проектор	1

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Практическое занятие	Персональный компьютер IBM PC	12

8. Фонд оценочных средств дисциплины

Описан в отдельном документе

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
**«Пермский национальный исследовательский политехнический
университет»**

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения промежуточной аттестации обучающихся по дисциплине
«Теория и практика кодирования в информационных системах»
Приложение к рабочей программе дисциплины

Фонд оценочных средств для проведения промежуточной аттестации обучающихся для проведения промежуточной аттестации обучающихся по дисциплине является частью (приложением) к рабочей программе дисциплины. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине разработан в соответствии с общей частью фонда оценочных средств для проведения промежуточной аттестации основной образовательной программы, которая устанавливает систему оценивания результатов промежуточной аттестации и критерии выставления оценок. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине устанавливает формы и процедуры текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине.

1. Перечень контролируемых результатов обучения по дисциплине, объекты оценивания и виды контроля

Согласно РПД, освоение учебного материала дисциплины запланировано в течение одного семестра (5-го семестра учебного плана) и разбито на 2 учебных модуля. В каждом модуле предусмотрены аудиторские лекционные и лабораторные занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируются компоненты компетенций *знать, уметь, владеть*, указанные в РПД, которые выступают в качестве контролируемых результатов обучения по дисциплине (табл. 1.1).

Контроль уровня усвоенных знаний, усвоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала, сдаче отчетов по лабораторным работам и экзамена. Виды контроля сведены в таблицу 1.1.

Таблица 1.1. Перечень контролируемых результатов обучения по дисциплине

Контролируемые результаты обучения по дисциплине (ЗУВы)	Вид контроля					
	Текущий		Рубежный		Итоговый	
	С	ТО	ОЛР	Т/КР		Экзамен
Усвоенные знания						
З.1 знать методы и алгоритмы кодирования в информационных системах		ТО1	ОЛР1 ОЛР2	КР		ТВ
Освоенные умения						
У.1 уметь выполнить расчет и анализ основных информационно-технических характеристик применяемых способов кодирования			ОЛР3	КР		ПЗ
Приобретенные владения						
В.1 владеть навыками применения пакетов прикладных программ для моделирования и исследования выбранных способов кодирования.			ОЛР4 ОЛР5 ОЛР6 ОЛР7	КР		

С – собеседование по теме; *ТО* – коллоквиум (теоретический опрос); *КЗ* – кейс-задача (индивидуальное задание); *ОЛР* – отчет по лабораторной работе; *Т/КР* – рубежное тестирование (контрольная работа, курсовая работа); *ТВ* – теоретический вопрос; *ПЗ* – практическое задание; *КЗ* – комплексное задание экзамена.

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в виде экзамена, проводимая с учетом результатов текущего и рубежного контроля.

2. Виды контроля, типовые контрольные задания и шкалы оценивания результатов обучения

Текущий контроль успеваемости имеет целью обеспечение максимальной эффективности учебного процесса, управление процессом формирования заданных компетенций обучаемых, повышение мотивации к учебе и предусматривает оценивание хода освоения дисциплины. В соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования – программам бакалавриата, специалитета и магистратуры в ПНИПУ предусмотрены следующие виды и периодичность текущего контроля успеваемости обучающихся:

- входной контроль, проверка исходного уровня подготовленности обучаемого и его соответствия предъявляемым требованиям для изучения данной дисциплины;
- текущий контроль усвоения материала (уровня освоения компонента «знать» заданных компетенций) на каждом групповом занятии и контроль посещаемости лекционных занятий;
- промежуточный и рубежный контроль освоения обучаемыми отдельных компонентов «знать», «уметь» заданных компетенций путем компьютерного или бланочного тестирования, контрольных опросов, контрольных работ (индивидуальных домашних заданий), защиты отчетов по лабораторным работам, рефератов, эссе и т.д.

Рубежный контроль по дисциплине проводится на следующей неделе после прохождения модуля дисциплины, а промежуточный – во время каждого контрольного мероприятия внутри модулей дисциплины;

- межсессионная аттестация, единовременное подведение итогов текущей успеваемости не менее одного раза в семестр по всем дисциплинам для каждого направления подготовки (специальности), курса, группы;
- контроль остаточных знаний.

2.1. Текущий контроль усвоения материала

Текущий контроль усвоения материала в форме собеседования или выборочного теоретического опроса студентов проводится по каждой теме. Результаты по 4-балльной шкале оценивания заносятся в книжку преподавателя и учитываются в виде интегральной оценки при проведении промежуточной аттестации.

2.2. Рубежный контроль

Рубежный контроль для комплексного оценивания усвоенных знаний, усвоенных умений и приобретенных владений (табл. 1.1) проводится в форме защиты лабораторных работ (после изучения каждого модуля учебной дисциплины) и курсовой работы (после изучения всех модулей учебной дисциплины).

Всего запланировано 7 лабораторных работ. Типовые темы лабораторных работ приведены в РПД.

Защита лабораторной работы проводится индивидуально каждым студентом. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

Тема курсовой работы приведена в РПД. Курсовая работа содержит расчетную часть и практическое задание – разработать программную модель в указанной среде моделирования.

Защита курсовой работы проводится индивидуально каждым студентом путем собеседования по расчетной части и демонстрации результатов разработки программной модели. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

2.3. Промежуточная аттестация (итоговый контроль)

Допуск к промежуточной аттестации осуществляется по результатам текущего и рубежного контроля. Условиями допуска являются успешная сдача всех лабораторных работ и положительная интегральная оценка по результатам текущего и рубежного контроля.

Промежуточная аттестация, согласно РПД, проводится в виде экзамена по дисциплине устно по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний и практические задания (ПЗ) для проверки освоенных умений всех заявленных компетенций.

Билет формируется таким образом, чтобы в него попали вопросы и практические задания, контролирующие уровень сформированности *всех* заявленных компетенций. Форма билета представлена в общей части ФОС образовательной программы.

2.3.1. Типовые вопросы и задания для экзамена по дисциплине

Типовые вопросы для контроля усвоенных знаний:

1. Мера избыточности кода. Информационная скорость кода.
2. Оценка помехоустойчивости при передаче дискретных сообщений (неизбыточные коды).
3. Оценка помехоустойчивости при передаче дискретных сообщений (коды, обнаруживающие ошибки).
4. Оценка помехоустойчивости при передаче дискретных сообщений (коды, исправляющие ошибки).
5. Оценка помехоустойчивости при передаче дискретных сообщений (коды, обнаруживающие и исправляющие ошибки).
6. Общие принципы обнаружения ошибок избыточными кодами ($d_{\min} = 2$).
7. Общие принципы исправления ошибок избыточными кодами ($d_{\min} = 3$).
8. Общие принципы обнаружения и исправления ошибок избыточными кодами ($d_{\min} = 4$).
9. Связь между кодовым расстоянием Хемминга и максимальной кратностью обнаруживаемых и исправляемых ошибок (теоремы).
10. Верхние и нижние границы избыточных кодов.
11. Оптимальное декодирование с «жестким» и «мягким» принятием решения первой решающей схемой.

Типовые вопросы и практические задания для контроля освоенных умений:

1. Код Шеннона-Фано (для заданной таблицы вероятностей сообщений).
2. Код Хаффмана (для заданной таблицы вероятностей сообщений).
3. Построить кодер БЧХ-кода с предварительным умножением на x^k для кода (9,4,4), $g(x)=1\oplus x\oplus x^4$, промоделировать работу кодера для заданного $u(x)$, сравнить с результатами аналитического расчета.
4. Рассчитать настройку селектора, построить декодер Меггита без предварительного умножения на x^k для кода (7,3,4), $g(x)=1\oplus x^2\oplus x^3$, промоделировать работу декодера для заданного $e(x)$.
5. Построить декодер Меггита с универсальной настройкой селектора для кода (6,2,4), $g(x)=1\oplus x\oplus x^3$, промоделировать работу декодера для заданного $e(x)$.

2.3.2. Шкалы оценивания результатов обучения на экзамене

Оценка результатов обучения по дисциплине в форме уровня сформированности компонентов *знать, уметь, владеть* заявленных компетенций проводится по 4-х балльной шкале оценивания путем выборочного контроля во время экзамена.

Типовые шкала и критерии оценки результатов обучения при сдаче экзамена для компонентов *знать, уметь и владеть* приведены в общей части ФОС образовательной программы.

3. Критерии оценивания уровня сформированности компонентов и компетенций

3.1. Оценка уровня сформированности компонентов компетенций

При оценке уровня сформированности компетенций в рамках выборочного контроля при экзамене считается, что *полученная оценка за компонент проверяемой в билете компетенции обобщается на соответствующий компонент всех компетенций, формируемых в рамках данной учебной дисциплины.*

Типовые критерии и шкалы оценивания уровня сформированности компонентов компетенций приведены в общей части ФОС образовательной программы.

3.2. Оценка уровня сформированности компетенций

Общая оценка уровня сформированности всех компетенций проводится путем агрегирования оценок, полученных студентом за каждый компонент формируемых компетенций, с учетом результатов текущего и рубежного контроля в виде интегральной оценки по 4-х балльной шкале. Все результаты контроля заносятся в оценочный лист и заполняются преподавателем по итогам промежуточной аттестации.

Форма оценочного листа и требования к его заполнению приведены в общей части ФОС образовательной программы.

При формировании итоговой оценки промежуточной аттестации в виде экзамена используются типовые критерии, приведенные в общей части ФОС образовательной программы.