МИНОБРНАУКИ РОССИИ

БАЛТИЙСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ «ВОЕНМЕХ» ИМ. Д.Ф. УСТИНОВА

УТВЕРЖДАЮ
Первый проректор - проректор по образовательной деятельности
_____ Бородавкин В.А.
«31» 01 2021
м.п.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ОСНОВЫ ТЕОРИИ КОДИРОВАНИЯ, КРИПТОГРАФИИ И ПЕРЕДАЧИ ИНФОРМАЦИИ

Направление/специальность подготовки — **09.04.04 Программная инженерия**
11.04.01 Радиотехника

Специализация/профиль/ программа подготовки — **Процессы и методы разработки программного обеспечения**
Системы и устройства передачи, приема и обработки сигналов

Уровень высшего образования — **Магистратура**

Форма обучения — **Очная**

Факультет — **О Естественнонаучный**
И Информационных и управляющих систем

Выпускающая кафедра — **О7 Информационные системы и программная инженерия**
И4 РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ

Кафедра-разработчик рабочей программы — **И4 РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ**

КУРС	СЕМЕСТР	ОБЩАЯ ТРУДОЁМКОСТЬ (ЗАЧЕТНЫХ ЕДИНИЦ)	ЧАСЫ (по наличию видов занятий)									ВИД ПРОМЕЖУТОЧНОГО КОНТРОЛЯ
			ОБЩАЯ ТРУДОЁМКОСТЬ	АУДИТОРНЫЕ ЗАНЯТИЯ				САМОСТОЯТЕЛЬНАЯ РАБОТА				
				ВСЕГО	ЛЕКЦИИ	ЛАБОРАТОРНЫЙ ПРАКТИКУМ	ПРАКТИЧЕСКИЕ ЗАНЯТИЯ	ВСЕГО	КУРСОВОЙ ПРОЕКТ	КУРСОВАЯ РАБОТА	ДРУГИЕ ВИДЫ САМОСТ. РАБОТЫ	
5	10	3	108	51	34	0	17	57	0	0	57	диф. зач.

Начальник отдела основных образовательных программ
_____ /Русина А.А./

Санкт-Петербург
2021 г.

2013

ЛИСТ СОГЛАСОВАНИЯ

РАБОЧАЯ ПРОГРАММА СОСТАВЛЕНА В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ВЫСШЕГО ОБРАЗОВАНИЯ (ФГОС ВО)

09.04.04 Программная инженерия
11.04.01 Радиотехника

2021

Программу составил:

Кафедра И4 РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ
Стукалова Анна Сергеевна, старший преподаватель

Эксперт:

Эрлих А.Г., вед. науч. сотр АО «Радиоавионика»

Программа рассмотрена
на заседании кафедры-разработчика
рабочей программы **И4 РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ**

Заведующий кафедрой Страхов С.Ю., д.т.н., проф.

Программа рассмотрена
на заседании выпускающих кафедр рабочей программы

О7 Информационные системы и программная инженерия

Заведующий кафедрой Скулябина О.В., к.т.н., доц.

И4 РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ

Заведующий кафедрой Страхов С.Ю., д.т.н., проф.

ФАКУЛЬТЕТ "И" ИНФОРМАЦИОННЫХ И УПРАВЛЯЮЩИХ СИСТЕМ

Декан Страхов С.Ю., д.т.н., проф.

ФАКУЛЬТЕТ "О" ЕСТЕСТВЕННОНАУЧНЫЙ

и.о. декана Зиновьев Н.А., к.пед.н., доц.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ОСНОВЫ ТЕОРИИ КОДИРОВАНИЯ, КРИПТОГРАФИИ И ПЕРЕДАЧИ ИНФОРМАЦИИ

Разделы рабочей программы

Приложения к рабочей программе дисциплины

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование следующих компетенций:

09.04.04 (О7)	ОПК-5 — способность разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем
09.04.04 (О7)	ПСК-1.05 — Владение навыками создания программного обеспечения для анализа, распознавания и обработки информации
09.04.04 (О7)	ПСК-1.07 — Владение навыками создания программного обеспечения для систем цифровой обработки сигналов
11.04.01 (И4)	ПСК-1.2 — способность выполнять моделирование объектов и процессов с целью анализа и оптимизации их параметров с использованием имеющихся средств исследований, включая стандартные пакеты прикладных программ
11.04.01 (И4)	ПСК-1.3 — способность разрабатывать и обеспечивать программную реализацию эффективных алгоритмов решения сформулированных задач с использованием современных языков программирования

Формированию компетенций служит достижение следующих результатов образования:

ОПК-5 (09.04.04, О7)

знания:

знать программное и аппаратное обеспечение информационных и автоматизированных систем;;

умения:

уметь разрабатывать модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем с учетом алгоритмов криптографии;;

ПСК-1.05 (09.04.04, О7)

знания:

знать принципы обработки информации;;

умения:

уметь создавать программное обеспечение для исследования принципов передачи информации с использованием алгоритмов кодирования;;

навыки:

иметь навык исследования алгоритмов кодирования и криптографии с помощью разработанного программного обеспечения.

ПСК-1.07 (09.04.04, О7)

знания:

знать основы цифровой обработки сигналов;

умения:

уметь создавать программное обеспечение для систем цифровой обработки сигналов;

ПСК-1.2 (11.04.01, И4)

знания:

знать современные информационные технологии и основные подходы к защите информации при передаче по каналам связи;;

умения:

уметь оценивать защищенность информации при передаче по каналам связи при использовании различных алгоритмов кодирования и криптографии;

навыки:

иметь навык моделирования работы алгоритмов кодирования с использованием САПР.

ПСК-1.3 (11.04.01, И4)

знания:

знать современные языки программирования;

умения:

меть использовать современные языки программирования для программной реализации алгоритмов кодирования и криптографии;

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **ОСНОВЫ ТЕОРИИ КОДИРОВАНИЯ, КРИПТОГРАФИИ И ПЕРЕДАЧИ ИНФОРМАЦИИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.04.04 Программная инженерия* и **вариативной части по выбору студента блока 1** программы подготовки по направлению *11.04.01 Радиотехника*.

Содержание дисциплины является логическим продолжением дисциплин: **ТЕХНОЛОГИИ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, МЕТОДОЛОГИЯ ПРОГРАММНОЙ ИНЖЕНЕРИИ**.

Содержание дисциплины является основой для освоения дисциплин: **ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ**.

Предварительные компетенции, сформированные у обучающегося до начала изучения дисциплины:

- ОПК-1 — Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте
- ОПК-2 — Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач
- ОПК-3 — Способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями
- ОПК-5 — Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем
- ПСК-1.01 — Способность выполнить постановку новых задач анализа и синтеза новых проектных решений
- ПСК-1.05 — Владение навыками создания программного обеспечения для анализа, распознавания и обработки информации

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч.

3.1. Содержание (дидактика) дисциплины

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме			Самостоятельная работа студентов	Формируемая компетенция, %				
				ВСЕГО	Лекции	Практические занятия		ОПК-5 (09.04.04)	ПСК-1.05 (09.04.04)	ПСК-1.07 (09.04.04)	ПСК-1.2 (11.04.01)	ПСК-1.3 (11.04.01)
5	10	**Раздел 1. Элементы теории информации и информационной техники.** 1.1 Теоретические основы информации и информационной техники. Измерение информации. Меры информации. Понятие энтропии. Дискретизация информации. 1.2 Передача информации по каналам связи. Виды каналов передачи. Разделение каналов. Теоретические основы передачи сообщений без помех и с помехами. Повышение помехоустойчивости передачи и приема.	20	8	4	4	12	20	20	20	20	20
5	10	**Раздел 2. Кодирование данных.** 2.1 Общие понятия и определения. Цели кодирования. Принципы помехоустойчивого кодирования. 2.2 Блочные коды. Простейшее кодирование, прямоугольные коды, код Хэмминга. Технические средства кодирования и декодирования. 2.3 Циклические коды. Математические основы и принципы формирования. Технические средства кодирования и декодирования.	26	14	10	4	12	20	20	20	20	20
5	10	**Раздел 3. Сжатие данных.** 3.1 Общие понятия и определения. Цели сжатия данных. Принципы построения алгоритмов сжатия данных. 3.2 Алгоритмы сжатия без потерь. Кодирование длин серий. Сжатие со словарем. Статистические методы сжатия. Область применения и особенности. 3.3 Алгоритмы сжатия с потерями. Принципы дискретно-косинусного преобразования. Вэйвлет- алгоритм. Область применения и особенности.	24	12	10	2	12	20	20	20	20	20
5	10	**Раздел 4. Элементы криптографии.** 4.1 Общие понятия и определения. Цели криптографии. Принципы построения алгоритмов криптографии. Обзор существующих методов криптографии. 4.2 Алгоритмы криптографии с открытым ключом. Математические основы. Технические средства. Область применения и особенности. 4.3 Алгоритмы криптографии с закрытым ключом. Математические основы. Технические средства. Область применения и особенности. 4.4 Алгоритмы электронной подписи. Математические основы. Технические средства. Область применения и особенности.	24	12	8	4	12	20	20	20	20	20
5	10	**Раздел 5. Перспективные разработки.** 5.1 Общие направления развития информационной техники. Возникающие проблемы и возможные пути их решения. Перспективные разработки.	14	5	2	3	9	20	20	20	20	20
Всего за 10 семестр			108	51	34	17	57	100	100	100	100	100
Всего по дисциплине			108	51	34	17	57	100	100	100	100	100

3.2. Аудиторный практикум

№ п/п	Номер и наименование раздела дисциплины	Тема практического занятия	Объем, ауд. часов
1	Раздел 1. Элементы теории информации и информационной техники.	Повторение сведений о геометрической, комбинаторной и аддитивной мере информации и связи с системами счисления.	2
2		Повторение сведений о пропускной способности канала. Повторение формул Найквиста и Шеннона.	2
3	Раздел 2. Кодирование данных.	Повторение принципов построения блочных кодов. Код Хэмминга для исправления однократных ошибок	2
4		Повторение кода Хэмминга для исправления двукратных ошибок	2

5	Раздел 3. Сжатие данных.	Повторение принципов построения блочных кодов. Код Хэмминга для исправления однократных ошибок	1
6		Повторение кода Хэмминга для исправления двукратных ошибок	1
7	Раздел 4. Элементы криптографии.	Повторение алгоритмов криптографии с открытым ключом	2
8		Повторение алгоритмов криптографии с закрытым ключом	2
9	Раздел 5. Перспективные разработки.	Поиск современных криптографических систем и алгоритмов по Интернету	3
Всего за 10 семестр			17

3.3. Самостоятельная работа студента (СРС)

№ п/п	Номер и наименование раздела дисциплины	Содержание учебного задания	Объем, часов
1	Раздел 1. Элементы теории информации и информационной техники.	Повторение и осмысление сведений об основных элементах теории информации и информационной технике	12
2	Раздел 2. Кодирование данных.	Повторение и осмысление информации о прямоугольных и циклических кодах, блочных кодах и способах их реализации	12
3	Раздел 3. Сжатие данных.	Повторение и осмысление сведений о принципах построения алгоритмов сжатия данных.	12
4	Раздел 4. Элементы криптографии.	Повторение и осмысление сведений о криптографии, ее назначении, способах реализации, алгоритмах различной сложности	12
5	Раздел 5. Перспективные разработки.	Осмысление и поиск новых перспективных разработок в области кодировании, криптографии и передачи информации	9
Всего за 10 семестр			57

4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

СЕМЕСТР	НЕДЕЛИ СЕМЕСТРА																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
10			Контр.Р.				Контр.Р.				Контр.Р.			Контр.Р.			Контр.Р., диф. зач.

Условные обозначения:

- Контр.Р. – контрольная работа;
- диф. зач. – дифференцированный зачет.

Текущая аттестация студентов проводится в дискретные временные интервалы в следующих формах:

- контрольная работа.

Рубежная аттестация студентов производится по итогам половины семестра в следующих формах:

- контрольная работа.

Промежуточная аттестация проводится в формах:

- дифференцированный зачет.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература по дисциплине:

1. А. В. Бабаш, Е. К. Баранова. Криптографические методы защиты информации. М.: КноРус, 2018, 70 экз.
2. В. Л. Бройдо, О. П. Ильина. Вычислительные системы, сети и телекоммуникации. СПб.: Питер, 2007, эл. рес.
3. Г. Г. Раннев. Измерительные информационные системы. М.: Академия, 2010, 22 экз.
4. Л. К. Бабенко, Е. А. Ищукова. Криптографическая защита информации: симметричное шифрование. Москва: Юрайт, 2020, эл. рес.
5. М. Вернер. Основы кодирования. М.: Техносфера, 2004, 50 экз.
6. С. А. Курицын. Телекоммуникационные технологии и системы. М.: Академия, 2008, 6 экз.

5.2. Дополнительная литература по дисциплине:

не требуется.

5.3. Периодические издания:

1. Радиотехника – XXI век.

5.4. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины, электронные библиотечные системы:

1. http://library.voenmeh.ru — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова;
2. http://e.lanbook.com — ЭБС Лань;
3. http://urait.ru — Образовательная платформа «Юрайт». Для вузов и ссузов..

5.5. Программное обеспечение:

1. Mathcad Education - University Edition Term.

5.6. Информационные технологии:

взаимодействие с обучающимися посредством ЭИОС Moodle БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Лекционные занятия:

специализированные требования по оборудованию отсутствуют; аудитория с посадочными местами по количеству студентов; доска.

6.2. Практические занятия:

1. Проектор;
2. Mathcad Education - University Edition Term.

6.3. Прочее:

1. рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
2. рабочие места студентов, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде.

Аннотация рабочей программы

Дисциплина **ОСНОВЫ ТЕОРИИ КОДИРОВАНИЯ, КРИПТОГРАФИИ И ПЕРЕДАЧИ ИНФОРМАЦИИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.04.04 Программная инженерия* и **вариативной части по выбору студента блока 1** программы подготовки по направлению *11.04.01 Радиотехника*. Дисциплина реализуется на факультете *И* Информационных и управляющих систем БГТУ "ВОЕНМЕХ" им. Д.Ф. Устинова кафедрой И4 РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ.

Дисциплина нацелена на формирование *компетенций*:
ОПК-5 (09.04.04)способность разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем;
ПСК-1.05 (09.04.04)Владение навыками создания программного обеспечения для анализа, распознавания и обработки информации;
ПСК-1.07 (09.04.04)Владение навыками создания программного обеспечения для систем цифровой обработки сигналов;
ПСК-1.2 (11.04.01)способность выполнять моделирование объектов и процессов с целью анализа и оптимизации их параметров с использованием имеющихся средств исследований, включая стандартные пакеты прикладных программ;
ПСК-1.3 (11.04.01)способность разрабатывать и обеспечивать программную реализацию эффективных алгоритмов решения сформулированных задач с использованием современных языков программирования.

Содержание дисциплины охватывает круг вопросов, связанных с основами кодирования, криптографии и передачи информации.

Программой дисциплины предусмотрены следующие **виды контроля**:

Текущая аттестация студентов проводится в дискретные временные интервалы в следующих формах:
- контрольная работа.

Рубежная аттестация студентов производится по итогам половины семестра в следующих формах:
- контрольная работа.

Промежуточная аттестация проводится в формах:
- дифференцированный зачет.

Общая трудоемкость освоения дисциплины составляет **3** з.е., **108** ч. Программой дисциплины предусмотрены лекционные занятия **(34 ч.)**, практические занятия **(17 ч.)**, самостоятельная работа студента **(57 ч)**.

ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 108 ч., из них 51 ч. аудиторных занятий, и 57 ч., отведенных на самостоятельную работу студента.

Рекомендации по распределению учебного времени по видам самостоятельной работы и разделам дисциплины приведены в таблице.

Контроль освоения дисциплины производится в соответствии с Положением о текущем, рубежном контроле успеваемости и промежуточной аттестации обучающихся.

Формы контроля и критерии оценивания приведены в приложении 3 к Рабочей программе.

Наименование работы	Рекомендуемая литература	Трудоемкость, час.
Раздел 1. Элементы теории информации и информационной техники.		
Повторение и осмысление сведений об основных элементах теории информации и информационной технике	В. Л. Бройдо, О. П. Ильина. Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2007 (1, 2, 3) С. А. Курицын. Телекоммуникационные технологии и системы: М.: Академия, 2008 (2, 3)	12
Итого по разделу 1		12
Раздел 2. Кодирование данных.		
Повторение и осмысление информации о прямоугольных и циклических кодах, блочных кодах и способах их реализации	М. Вернер. Основы кодирования: М.: Техносфера, 2004 (1, 2, 3)	12
Итого по разделу 2		12
Раздел 3. Сжатие данных.		
Повторение и осмысление сведений о принципах построения алгоритмов сжатия данных.	А. В. Бабаш, Е. К. Баранова. Криптографические методы защиты информации: М.: КноРус, 2018 (4)	12
Итого по разделу 3		12
Раздел 4. Элементы криптографии.		
Повторение и осмысление сведений о криптографии, ее назначении, способах реализации, алгоритмах различной сложности	В. Л. Бройдо, О. П. Ильина. Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2007 (20) Л. К. Бабенко, Е. А. Ищукова. Криптографическая защита информации: симметричное шифрование: Москва: Юрайт, 2020 (все) М. Вернер. Основы кодирования: М.: Техносфера, 2004 (3.3 - 3.6)	12
Итого по разделу 4		12
Раздел 5. Перспективные разработки.		
Осмысление и поиск новых перспективных разработок в области кодировании, криптографии и передачи информации	Г. Г. Раннев. Измерительные информационные системы: М.: Академия, 2010 (6, 7)	9
Итого по разделу 5		9

ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

Фонды оценочных средств, позволяющие оценить результаты обучения по данной дисциплине, включают в себя:

- контрольная работа;
- дифференцированный зачет.

Критерии оценивания

Контрольная работа

Результаты выполнения каждой контрольной работы оцениваются по четырехбалльной шкале («отлично», «хорошо», «удовлетворительно» и «неудовлетворительно»).
Контрольная работа проводится в виде теста, на котором студенту предлагается 10 вопросов. Если студент верно ответил на 6-7 вопросов – ему выставляется оценка «удовлетворительно», если студент верно ответил на 8-9 вопросов – ему выставляется оценка «хорошо», если студент верно ответил на 10 вопросов – ему выставляется оценка «отлично».

Дифференцированный зачет

Итоговый контроль по дисциплине проходит в форме дифференцированного зачета, который выставляется на 17 неделе семестра. Оценка выставляется как среднее арифметическое оценок за пять контрольных работ.

Паспорт фонда оценочных средств

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме			Самостоятельная работа студентов	Формируемая компетенция, %					НАИМЕНОВАНИЕ ОЦЕНОЧНОГО СРЕДСТВА
				ВСЕГО	Лекции	Практические занятия		ОПК-5 (09.04.04)	ПСК-1.05 (09.04.04)	ПСК-1.07 (09.04.04)	ПСК-1.2 (11.04.01)	ПСК-1.3 (11.04.01)	
5	10	**Раздел 1. Элементы теории информации и информационной техники.**	20	8	4	4	12	20	20	20	20	20	Контрольная работа
5	10	**Раздел 2. Кодирование данных.**	26	14	10	4	12	20	20	20	20	20	Контрольная работа
5	10	**Раздел 3. Сжатие данных.**	24	12	10	2	12	20	20	20	20	20	Контрольная работа
5	10	**Раздел 4. Элементы криптографии.**	24	12	8	4	12	20	20	20	20	20	Контрольная работа
5	10	**Раздел 5. Перспективные разработки.**	14	5	2	3	9	20	20	20	20	20	Контрольная работа
Всего за 10 семестр			108	51	34	17	57	100	100	100	100	100	
Всего по дисциплине			108	51	34	17	57	100	100	100	100	100	