МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова»
(БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова)

УТВЕРЖДАЮ
Декан факультета
_____ Матвеев П.В.
(подпись) ФИО
«31» 05 2022

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Направление/специальность подготовки — 09.03.02 Информационные системы и технологии

Специализация/профиль/программа подготовки — Информационная безопасность

Уровень высшего образования — Бакалавриат

Форма обучения — Очная

Факультет — О Естественнонаучный

Выпускающая кафедра — О7 Информационные системы и программная инженерия

Кафедра-разработчик рабочей программы — О7 Информационные системы и программная инженерия

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	
3	5	5	180	51	34	0	17	129	0	18	111	диф. зач.

Санкт-Петербург
2022 г.

ЛИСТ СОГЛАСОВАНИЯ

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

09.03.02 Информационные системы и технологии

год набора группы: 2022

Программу составил:

Кафедра О7 Информационные системы и программная инженерия
Бармина Анастасия Александровна, старший преподаватель

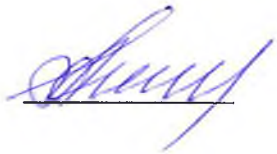
Программа рассмотрена
на заседании кафедры-разработчика
рабочей программы **О7 Информационные системы и программная инженерия**

Заведующий кафедрой Семенова Е.Г., д.т.н., проф.

Программа рассмотрена
на заседании выпускающей кафедры

О7 Информационные системы и программная инженерия

Заведующий кафедрой Семенова Е.Г., д.т.н., проф.



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Разделы рабочей программы

Приложения к рабочей программе дисциплины

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-1 — способность применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности
ПСК-2.1 — Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности, принимать участие в проведении экспериментальных исследований системы защиты информации.
ПСК-2.12 — Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

Формированию компетенций служит достижение следующих результатов образования:

ОПК-1

знания:

представление проблем, возникающих при обработке информации и передачи данных по каналам связи и путей их решения;

представление о путях развития информационной техники;

умения:

анализ принципов функционирования информационной техники;

использования нового математического аппарата кодирования и криптографии;

навыки:

разработки и обслуживания отдельных блоков систем обработки данных.

ПСК-2.1

знания:

иметь базовые знания для дальнейшего углубленного изучения материала;

понимание подходов к обработке и передаче данных;

умения:

расчет характеристик канала связи;

расчет и разработка помехоустойчивых кодов;

навыки:

разработки и обслуживания отдельных блоков систем обработки данных.

ПСК-2.12

знания:

представление проблем, возникающих при обработке информации и передачи данных по каналам связи и путей их решения;

математического аппарата кодирования и криптографии;

умения:

расчет и разработка алгоритмов сжатия данных;

расчет и разработка помехоустойчивых кодов;

навыки:

разработки и обслуживания отдельных блоков систем обработки данных.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.02 Информационные системы и технологии*.

Содержание дисциплины является логическим продолжением дисциплин: **СТРУКТУРЫ И ОРГАНИЗАЦИЯ ДАННЫХ, ВВЕДЕНИЕ В ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ**.

Содержание дисциплины является основой для освоения дисциплин: **ВЫПОЛНЕНИЕ И ЗАЩИТА ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ**.

Предварительные компетенции, сформированные у обучающегося до начала изучения дисциплины:

- ОПК-3 — Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
- ОПК-6 — Способен разрабатывать алгоритмы и программы, пригодные для практического применения в области информационных систем и технологий
- ОПК-7 — Способен осуществлять выбор платформ и инструментальных программно-аппаратных средств для реализации информационных систем
- ПК-94 — способен к управлению информацией и данными, поиску источников информации и данных, восприятию, анализу, запоминанию и передаче информации с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач
- ПСК-2.4 — Владение навыками использования различных технологий разработки программного обеспечения
- ПСК-2.5 — Способность оценивать качество программного обеспечения, в том числе с точки зрения информационной безопасности, проведение тестирования и исследование результатов

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 5 з.е., 180 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-1	ПСК-2.1	ПСК-2.12
3	5	**Раздел 1. Элементы теории информации и информационной техники.** 1.1 Теоретические основы информации и информационной техники. 1.2 Измерение информации. Меры информации. Понятие энтропии. Дискретизация информации. 1.3 Передача информации по каналам связи. Виды каналов передачи. Разделение каналов. 1.4 Теоретические основы передачи сообщений без помех и с помехами. 1.5 Повышение помехоустойчивости передачи и приема.	43	13	10	3	30	20	15	10
3	5	**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.	31	9	6	3	22	20	25	20
3	5	**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.	34	10	6	4	24	20	25	30
3	5	**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.	35	12	8	4	23	20	15	20
3	5	**Раздел 5. Перспективные разработки.** 5.1 Общие направления развития информационной техники. Возникающие проблемы и возможные пути их решения. Перспективные разработки.	37	7	4	3	30	20	20	20
Всего за 5 семестр			180	51	34	17	129	100	100	100
Всего по дисциплине			180	51	34	17	129	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.	Рассмотрение основных теоретических основ информации и информационной техники. Геометрическая, комбинаторная и аддитивная мера информации. Примеры. Связь с системами счисления. Статистическая мера информации. Понятие энтропии, свойства энтропии. Примеры вычисления и использования энтропии	2
2		Информационные подходы к передаче данных по каналам связи. Виды каналов связи и принципы их разделения. Соотношение характеристик сигнала и канала. Дискретные каналы без помех и с помехами. Непрерывные каналы с помехами. Пропускная способность канала. Формулы Найквиста и Шеннона. Повышение помехоустойчивости.	1
3	Раздел 2. Кодирование данных.	Математические основы помехоустойчивого кодирования. Проверка на четность. Прямоугольный код. Примеры и задачи. Принципы построения блочных кодов. Код Хэмминга для исправления однократных ошибок. Решение задач.	2
4		Код Хэмминга для исправления двукратных ошибок. Технические средства кодирования и декодирования. Задачи. Математические основы циклических кодов. Обнаружение и исправление ошибок с помощью циклических кодов. Решение задач.	1

5	Раздел 3. Сжатие данных.	Общие понятия, определения и принципы сжатия данных. Алгоритм кодирования длин серий. Алгоритм сжатия со словарем. Статистический алгоритм сжатия. Пример. Задачи. Сжатие с потерями. Алгоритм дискретно-косинусного преобразования. Вейвлет- алгоритм сжатия.	4
6	Раздел 4. Элементы криптографии.	Общие понятия, определения и цели криптографии. Принципы построения алгоритмов криптографии. Обзор существующих методов криптографии. Алгоритмы с открытым ключом. Алгоритмы криптографии с закрытым ключом. Примеры.	2
7		Электронная цифровая подпись. Примеры.	2
8	Раздел 5. Перспективные разработки.	Общие направления развития информационной техники. Возникающие проблемы и возможные пути их решения. Перспективные разработки.	3
Всего за 5 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.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям.	30
2	Раздел 2. Кодирование данных.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям.	18
3		Выполнение 1-го этапа курсовой работы.	4
4	Раздел 3. Сжатие данных.	Выполнение 2-го этапа курсовой работы	4
5		Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям.	20
6	Раздел 4. Элементы криптографии.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям.	19
7		Выполнение 3-го этапа курсовой работы.	4
8	Раздел 5. Перспективные разработки.	Оформление курсовой работы	3
9		Подготовка к защите курсовой работы	3
10		Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям.	24
Всего за 5 семестр			129

3.4. Курсовая работа

СОДЕРЖАНИЕ ЭТАПА	ПЕРИОД ИСПОЛНЕНИЯ (недели семестра)	ПЛАНИРУЕМОЕ ВРЕМЯ (час)
Этап 1. Выполнение 1-го этапа курсовой работы: выбор темы, обоснование актуальности темы	4 - 6	4
Этап 2. Выполнение 2-го этапа курсовой работы: выбор криптографических алгоритмов	8 - 13	4
Этап 3. Выполнение 3-го этапа курсовой работы: обоснование решений, принятых при создании программного обеспечения	13 - 15	4
Этап 4. Оформление курсовой работы	15 - 15	3
Этап 5. Подготовка к защите курсовой работы	16 - 17	3
Всего за 5 семестр		18

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
5						ДР		КР		ДР		КР		КР		ДР	диф. зач.

Условные обозначения:

- ДР – диагностическая работа;
- КР – курсовая работа;
- диф. зач. – дифференцированный зачет.

Текущий контроль успеваемости студентов проводится в дискретные временные интервалы в следующих формах:

- диагностическая работа;
- курсовая 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. А. В. Черёмушкин. . Криптографические протоколы. Основные свойства и уязвимости. М.: Академия, 2009, 9 экз.
3. Г. Г. Раннев. . Измерительные информационные системы. М.: Академия, 2010, 22 экз.
4. Е. К. Александров, Р. И. Грушвицкий, М. С. Куприянов. . Микропроцессорные системы. СПб.: Политехника, 2002, 31 экз.
5. Е. Ф. Берёзкин. . Основы теории информации и кодирования. СПб.: Лань, 2019, эл. рес.
6. Л. К. Бабенко, Е. А. Ищукова. . Криптографическая защита информации: симметричное шифрование. Москва: Юрайт, 2020, эл. рес.
7. М. Вернер. . Основы кодирования. М.: Техносфера, 2004, 50 экз.
8. М. Ю. Рытов, М. Л. Гулак, А. П. Горлов. . Криптографические методы защиты информации. Старый Оскол: ТНТ, 2021, эл. рес.
9. С. А. Курицын. . Телекоммуникационные технологии и системы. М.: Академия, 2008, 6 экз.
10. С. Б. Гашков, Э. А. Применко, М. А. Черепнев. . Криптографические методы защиты информации. М.: Академия, 2010, 22 экз.
11. С. Б. Макаров, Н. В. Певцов, Е. А. Попов. . Телекоммуникационные технологии. Введение в технологию GSM. М.: Академия, 2008, 26 экз.

5.2. Дополнительная литература по дисциплине:

1. А. Б. Сергиенко. . Цифровая обработка сигналов. М.: Питер, 2006, 3 экз.

5.3. Периодические издания:

не требуются.

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

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

Современные профессиональные базы данных:

1. https://rusneb.ru – Национальная электронная библиотека (НЭБ);
2. https://cyberleninka.ru/ - Научная электронная библиотека «Киберленинка»; http://www.rfbr.ru/rffi/ru/library - Полнотекстовая электронная библиотека Российского фонда фундаментальных исследований.

Информационные справочные системы:

1. Техэксперт – Информационный портал технического регулирования: Нормы, правила, стандарты РФ;
2. http://library.voenmeh.ru/jirbis2/index.php?option=com_irbis&view=irbis&Itemid=457 - БД ГОСТов собственной генерации БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова;
3. http://www.consultant.ru/- КонсультантПлюс- информационный портал правовой информации.

5.5. Программное обеспечение:

1. LibreOffice;
2. Linux.

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. LibreOffice;
3. Linux.

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 **КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ** является дисциплиной **обязательной части блока 1** программы подготовки по направлению *09.03.02 Информационные системы и технологии*. Дисциплина реализуется на факультете *О* Естественнонаучный БГТУ "ВОЕНМЕХ" им. Д.Ф. Устинова кафедрой О7 Информационные системы и программная инженерия.

Дисциплина нацелена на формирование *компетенций*:
ОПК-1 способность применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности;
ПСК-2.1 Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности, принимать участие в проведении экспериментальных исследований системы защиты информации.;
ПСК-2.12 Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.

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

Программой дисциплины предусмотрены следующие **виды контроля**:

Текущий контроль успеваемости студентов проводится в дискретные временные интервалы в следующих формах:
- диагностическая работа;
- курсовая работа.

Промежуточная аттестация проводится в формах:
- дифференцированный зачет.

Общая трудоемкость освоения дисциплины составляет **5** з.е., **180** ч. Программой дисциплины предусмотрены лекционные занятия **(34 ч.)**, практические занятия **(17 ч.)**, самостоятельная работа студента **(129 ч)**.

ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 180 ч., из них 51 ч. аудиторных занятий, и 129 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.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям.	М. Вернер. . Основы кодирования: М.: Техносфера, 2004 (1) Г. Г. Раннев. . Измерительные информационные системы: М.: Академия, 2010 (1) А. В. Черёмушкин. . Криптографические протоколы. Основные свойства и уязвимости: М.: Академия, 2009 (1) С. Б. Гашков, Э. А. Применко, М. А. Черепнев. . Криптографические методы защиты информации: М.: Академия, 2010 (1) А. Б. Сергиенко. . Цифровая обработка сигналов: М.: Питер, 2006 (1) А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (1-2) С. А. Курицын. . Телекоммуникационные технологии и системы: М.: Академия, 2008 (1)	30
Итого по разделу 1		30
Раздел 2. Кодирование данных.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям.	Л. К. Бабенко, Е. А. Ищукова. . Криптографическая защита информации: симметричное шифрование: Москва: Юрайт, 2020 (1-3) М. Вернер. . Основы кодирования: М.: Техносфера, 2004 (2-3) Е. К. Александров, Р. И. Грушвицкий, М. С. Куприянов. . Микропроцессорные системы: СПб.: Политехника, 2002 (1-3) А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (2)	18
Выполнение 1-го этапа курсовой работы.		4
Итого по разделу 2		22
Раздел 3. Сжатие данных.		
Выполнение 2-го этапа курсовой работы	М. Вернер. . Основы кодирования: М.: Техносфера, 2004 (2) Е. Ф. Берёзкин. . Основы теории информации и кодирования: СПб.: Лань,	4
Изучение предусмотренных программой дидактических единиц по рекомендуемой		20

литературе. Подготовка к практическим занятиям.	2019 (1-3) А. В. Черёмушкин. . Криптографические протоколы. Основные свойства и уязвимости: М.: Академия, 2009 (2-3) С. Б. Гашков, Э. А. Применко, М. А. Черепнев. . Криптографические методы защиты информации: М.: Академия, 2010 (1-3) А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (2-3) М. Ю. Рытов, М. Л. Гулак, А. П. Горлов. . Криптографические методы защиты информации: Старый Оскол: ТНТ, 2021 (1-3)	
Итого по разделу 3		24
Раздел 4. Элементы криптографии.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям.	М. Вернер. . Основы кодирования: М.: Техносфера, 2004 (3) С. А. Курицын. . Телекоммуникационные технологии и системы: М.: Академия, 2008 (2) А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (2-4) Е. Ф. Берёзкин. . Основы теории информации и кодирования: СПб.: Лань, 2019 (3-5) А. В. Черёмушкин. . Криптографические протоколы. Основные свойства и уязвимости: М.: Академия, 2009 (4-6)	19
Выполнение 3-го этапа курсовой работы.	С. Б. Гашков, Э. А. Применко, М. А. Черепнев. . Криптографические методы защиты информации: М.: Академия, 2010 (2-5)	4
Итого по разделу 4		23
Раздел 5. Перспективные разработки.		
Оформление курсовой работы	С. А. Курицын. . Телекоммуникационные технологии и системы: М.: Академия, 2008 (5-6) С. Б. Макаров, Н. В. Певцов, Е. А. Попов. . Телекоммуникационные технологии. Введение в технологию GSM: М.: Академия, 2008 (4)	3
Подготовка к защите курсовой работы		3
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям.		24
Итого по разделу 5		30

ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

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

- диагностическая работа
- курсовая работа;
- дифференцированный зачет.

Критерии оценивания

Диагностическая работа
Диагностическая работа проводится в форме теста в ЭИОС Moodle:

- при правильном ответе менее чем на 60% вопросов - не аттестация;
- при правильном ответе на 60% вопросов и более - аттестация.

Курсовая работа
Список примерных тем курсовых работ содержится в УМК дисциплины.
Выполненные курсовые работы представляются в электронной форме в виде подготовленной электронной версии пояснительной записки, оформленной в соответствии с Положением по содержанию, оформлению, организации выполнения и защиты курсовых проектов и курсовых работ БГТУ.
При проверке соответствия пояснительной записки требованиям Положения и требованиям задания на данную курсовую работу, дается разрешение на ее печать. При наличии распечатанной пояснительной записки студент допускается к защите КР.
Критерии оценивания:
Курсовая работа допускается к защите при следующих условиях:
- предъявляемые к защите решения являются корректными;
- работа выполнена соответствии с заданием;
- электронная и печатная версии пояснительной записки соответствуют установленным требованиям.
Выполненные курсовые работы представляются в электронной форме в виде подготовленных к сборке исходных текстов и полностью готовой к выполнению программы для тестирования преподавателем и электронной версии пояснительной записки, оформленной в соответствии с Положением по содержанию, оформлению, организации выполнения и защиты курсовых проектов и курсовых работ БГТУ. СМК-П-4.2-12 – электронный ресурс – http://voenmeh.ru/files/0/Polozhenie_KRKP_2.0.pdf. При успешном тестировании программы и проверке соответствия пояснительной записки требованиям Положения и требованиям задания на данную курсовую работу, дается разрешение на ее печать без исходных текстов программ (они заменяются на «приложение в электронной форме»). При наличии распечатанной пояснительной записки студент допускается к защите КрР.
Критерии оценивания:
Курсовая работа допускается к защите при следующих условиях:
- предъявляемая программа работоспособна;
- программа выполнена соответствии с заданием;
- электронная и печатная версии пояснительной записки соответствуют установленным требованиям.

Оценка написанной КР:
- Работа выполнена, но не соответствует теме либо не использованы требуемые технологии, либо не реализованы все заявленные требования – 3 балла
- Работа выполнена в соответствие с темой реализована большая часть возможностей, но не все, не исправлены технические ошибки - 6 баллов
- Работа выполнена реализованы все заявленные возможности, однако имеются незначительные технические ошибки, не влияющие на корректность основного алгоритма- 9 баллов
- Работа выполнена реализованы все возможности, огрехов в работе не выявлено - 10 баллов
Оценка содержания пояснительной записки к курсовой работе:
- Содержание пояснительной записки имеет признаки чрезмерного заимствования слабо описана структура программы недостаточно описано произведенное тестирование – 2 балла
- Содержание пояснительной записки имеет незначительные признаки заимствования структура программы описана исключительно текстом и недостаточно полно тестирование слабо раскрыто в тексте ПЗ – 3 балла

- Структура программы описана полностью, описан базовый процесс тестирования, записка имеет четкую структуру в виде выделенных разделов и подразделов – 4 балла
- Структура программы описана полностью, полностью описан процесс тестирования, записка имеет четкую структуру в виде выделенных разделов и подразделов - 5 баллов
Оценка оформления, стиля пояснительной записки
- Пояснительная записка оформлена с нарушениями, язык работы не соответствует научному стилю, некорректно оформленные заимствования, некорректно оформлен список источников – 2 балла
- Пояснительная записка оформлена с нарушениями, язык работы не соответствует научному стилю, есть замечания к оформлению списка источников – 3 балла
- Есть отдельные замечания к оформлению и стилю изложения, оформлению списка источников – 4 балла
- Нет замечаний к оформлению и стилю изложения, оформлению списка источников – 5 баллов
Максимальное количество баллов – 20
Оценка «отлично» - 17-20 баллов
Оценка «хорошо» - 13-16 баллов
Оценка «удовлетворительно» - 10-12 баллов
Оценка «не защитил» - меньше 10 или работа не была предъявлена

Дифференцированный зачет

Обучающийся имеет право на получение минимальной положительной оценки при условии успешного прохождения текущего контроля успеваемости в форме диагностической работы в соответствии с графиком раздела 4.
Перечень теоретических вопросов к диф.зачету, представленный в УМК дисциплины, предоставляется преподавателем. Задачи соответствуют программе практических занятий. При подготовке ответов на теоретические вопросы рекомендуется помимо текстов лекций использовать источники основной и дополнительной литературы. Особое внимание следует уделить подготовке практических примеров к теоретическим экзаменационным вопросам.

На зачете студенту предлагается два теоретических вопроса. При успешном ответе на оба вопроса выставляется оценка «зачтено-отлично». При ответе на один из двух предложенных вопросов преподавателем может быть выставлена оценка «зачтено-хорошо». При отсутствии успешных ответов зачет может быть оформлен с оценкой «удовлетворительно» на основании успешного выполнения курсовой работы. При неуспешной сдачи экзамена выставляется оценка «не зачтено».

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-1	ПСК-2.1	ПСК-2.12	
3	5	**Раздел 1. Элементы теории информации и информационной техники.**	43	13	10	3	30	20	15	10	Курсовая работа
3	5	**Раздел 2. Кодирование данных.**	31	9	6	3	22	20	25	20	Курсовая работа
3	5	**Раздел 3. Сжатие данных.**	34	10	6	4	24	20	25	30	Курсовая работа
3	5	**Раздел 4. Элементы криптографии.**	35	12	8	4	23	20	15	20	Курсовая работа
3	5	**Раздел 5. Перспективные разработки.**	37	7	4	3	30	20	20	20	Курсовая работа
Всего за 5 семестр			180	51	34	17	129	100	100	100	
Всего по дисциплине			180	51	34	17	129	100	100	100	