

УТВЕРЖДАЮ
Декан факультета

(подпись) Страхов С. Ю.
ФИО
«___» _____ 20__

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ОСНОВЫ ТЕОРИИ КОДИРОВАНИЯ, КРИПТОГРАФИИ И ПЕРЕДАЧИ ИНФОРМАЦИИ

Направление/специальность подготовки	11.04.01 Радиотехника
Специализация/профиль/программа подготовки	Системы и устройства передачи, приема и обработки сигналов
Уровень высшего образования	Магистратура
Форма обучения	Заочная
Факультет	И Информационных и управляющих систем
Выпускающая кафедра	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	
2	3	3	108	6	4	0	2	102	0	0	102	диф. зач.

ЛИСТ СОГЛАСОВАНИЯ

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

11.04.01 Радиотехника

год набора группы: 2023

Программу составил:

Кафедра И4 РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ
Стукалова Анна Сергеевна, старший преподаватель

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 выпускающей кафедры

И4 РАДИОЭЛЕКТРОННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОСНОВЫ ТЕОРИИ КОДИРОВАНИЯ, КРИПТОГРАФИИ И ПЕРЕДАЧИ ИНФОРМАЦИИ

Разделы рабочей программы

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО
3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ
4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ
5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ
6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приложения к рабочей программе дисциплины

- Приложение 1. Аннотация рабочей программы
- Приложение 2. Технологии и формы обучения
- Приложение 3. Фонды оценочных средств

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование следующих компетенций:

ПСК-1.1 — способность самостоятельно осуществлять постановку задачи исследования, формирование плана его реализации, выбор методов исследования и обработку результатов
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:

ПСК-1.1

знания:

знать основы передачи информации, включая современные беспроводные методы, понимать принцип действия алгоритмов кодирования и криптографии, включая алгоритмы квантовой криптографии и технологии блокчейн;

умения:

уметь определять круг задач, решаемых с помощью исследуемых методов и алгоритмов;

уметь применять физико-математический аппарат для решения задач кодирования и криптографии;

уметь собирать и анализировать информацию для формирования исходных данных при проектировании линий и каналов связи;

уметь использовать научно-техническую информацию, отечественный и зарубежный опыт для выполнения работ по заданной тематике;

навыки:

владеть методами анализа, трансформации, визуализации исследуемой информации и применять знания и умения для получения требуемого результата.

ПСК-1.3

знания:

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

знать существующие виды модуляции и методы доступа, используемые в современных системах связи;

знать методы оценки и устранения влияния канала связи на передаваемый сигнал, существующие методы помехоустойчивого кодирования, в том числе применяемые в системах связи 4-го поколения;

умения:

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

уметь применять способы и методы моделирования различных систем связи и алгоритмов эффективного и помехоустойчивого кодирования;

навыки:

иметь навык моделирования работы алгоритмов кодирования;

иметь навык моделирования криптографических систем на ЯВУ;

иметь навык моделирования поведения тракта системы беспроводной связи с расчетом скорости передачи информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **ОСНОВЫ ТЕОРИИ КОДИРОВАНИЯ, КРИПТОГРАФИИ И ПЕРЕДАЧИ ИНФОРМАЦИИ** является дисциплиной **части, формируемой участниками образовательных отношений блока 1**, программы подготовки по направлению *11.04.01 Радиотехника*.

Содержание дисциплины является логическим продолжением дисциплин: **РАДИОСИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ, РАДИОНАВИГАЦИОННЫЕ СИСТЕМЫ (РНС)**.

Содержание дисциплины является основой для освоения дисциплин: **ПОДГОТОВКА К ПРОЦЕДУРЕ ЗАЩИТЫ И ЗАЩИТА ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ**.

Предварительные компетенции, сформированные у обучающегося до начала изучения дисциплины:

- ПСК-1.1 — Способен самостоятельно осуществлять постановку задачи исследования, формирование плана его реализации, выбор методов исследования и обработку результатов
- ПСК-1.2 — Способен 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 — Способен разрабатывать и обеспечивать программную реализацию эффективных алгоритмов решения сформулированных задач с использованием современных языков программирования
- ПСК-1.4 — Способен к организации и проведению экспериментальных исследований с применением современных средств и методов
- ПСК-1.6 — Способен анализировать состояние научно-технической проблемы путем подбора, изучения и анализа литературных и патентных источников
- ПСК-1.7 — Способен определять цели, осуществлять постановку задач проектирования, подготавливать технические задания на выполнение проектных работ
- ПСК-1.8 — Способен проектировать радиотехнические устройства, приборы, системы и комплексы с учетом заданных требований

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		ПСК-1.1	ПСК-1.3
2	3	Раздел 1. Элементы теории информации и информационной техники. Раздел 1. Элементы теории информации и информационной техники. 1.1 Теоретические основы информации и информационной техники. Измерение информации. Меры информации. Понятие энтропии. Дискретизация информации. Этапы обращения информации в автоматизированных системах.1.2 Общие сведения о датчиках и сенсорах. Физические принципы функционирования. Датчики на ПАВ. MEMS. RFID. 1.3 Передача информации по каналам связи. Режимы передачи. Виды каналов и линий связи. Разделение каналов. Электрические, акустические, электромагнитные, оптические линии связи. Беспроводная связь. UWB, CDMA, расширенный спектр с перестройкой частоты. Технология Li-Fi. Спутниковые линии связи. Основные радиointерфейсы: Wi-Fi, Wi MAX, Zig Bee, Bluetooth, Wireless USB, WHDI, Wireless HD. Теоретические основы передачи сообщений без помех и с помехами. Повышение достоверности передачи и приема.	25	1	1	0	24	10	10
2	3	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	2	1	1	24	30	30
2	3	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. Метод Хаффмана. Метод арифметического кодирования. 3.3 Алгоритмы сжатия с потерями. Принципы дискретно-косинусного преобразования. Вейвлет-алгоритм. Область применения и особенности.	26	2	1	1	24	30	30
2	3	Раздел 4. Элементы криптографии. 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 симметричным ключом. Математические основы. Технические средства. Область применения и особенности. 4.3 Алгоритмы криптографии с открытым ключом. Математические основы. Технические средства. Область применения и особенности. Квантовая криптография. Алгоритм BB84. 4.4 Алгоритмы электронной подписи. Математические основы. Технические средства. Область применения и особенности. 4.5 Прочие криптографические протоколы: аутентификации, целостности, анонимности. Хеширование, алгоритм Фейге-Фиата-Шамира, Kerberos, биометрические технологии идентификации.	31	1	1	0	30	30	30
Всего за 3 семестр			108	6	4	2	102	100	100
Всего по дисциплине			108	6	4	2	102	100	100

3.2. Аудиторный практикум

№ п/п	Номер и наименование раздела дисциплины	Тема практического занятия	Объем, ауд. часов
1	Раздел 2. Кодирование данных.	Повторение принципов построения блочных кодов. Код Хэмминга для исправления однократных ошибок. Повторение кода Хэмминга для исправления двукратных ошибок.	1
2	Раздел 3. Сжатие данных.	Сжатие последовательности методом Хаффмана. Работа в малых группах. Реализация алгоритма Хаффмана по заданному варианту с использованием пакета прикладных программ, построение дерева решений при помощи инструментов визуализации, расчет эффективности алгоритма для заданного случая, сдача отчета в электронном виде. Арифметическое кодирование. Реализация алгоритма в среде программирования либо в MS Excel, расчет эффективности алгоритма для заданного случая, сдача отчета в электронном виде	1
Всего за 3 семестр			2

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 техники. Элементы теории информации и информационной техники. Измерение информации. Меры информации. Понятие энтропии. Дискретизация информации. Этапы обращения информации в автоматизированных системах. Общие сведения о датчиках и сенсорах. Физические принципы функционирования. Датчики на ПАВ. MEMS. RFID. 1.3 Передача информации по каналам связи. Режимы передачи. Виды каналов и линий связи. Разделение каналов. Электрические, акустические, электромагнитные, оптические линии связи. Беспроводная связь. UWB, CDMA, расширенный спектр с перестройкой частоты. Технология Li-Fi. Спутниковые линии связи. Основные радиоинтерфейсы: Wi-Fi, Wi MAX, Zig Bee, Bluetooth, Wireless USB, WHDI, Wireless HD. Теоретические основы передачи сообщений без помех и с помехами. Повышение достоверности передачи и приема.	24
2	Раздел 2. Кодирование данных.	Повторение и осмысление информации о прямоугольных и циклических кодах, блочных кодах и способах их реализации. Исследование реализации сверточного кода с использованием пакета специализированного ПО.	24
3	Раздел 3. Сжатие данных.	Повторение и осмысление сведений о принципах построения алгоритмов сжатия данных. Исследование вариантов реализации алгоритмов Хаффмана, арифметического кодирования, RLE, LZ78 с применением средств программирования. Исследование алгоритма JPEG.	24
4	Раздел 4. Элементы криптографии.	Повторение и осмысление сведений о криптографии, ее назначении, способах реализации, алгоритмах различной сложности. Исследование разных типов алгоритмов хеширования. Обзор в виде таблицы сравнения.	30
Всего за 3 семестр			102

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
3			ИПЗ		ИПЗ	ДР	ИПЗ		ИПЗ	ДР	ИПЗ		ИПЗ			ДР	Тест, диф. зач.

Условные обозначения:

- ДР – диагностическая работа;
- ИПЗ – индивидуальное практическое задание;
- Тест – тест;
- диф. зач. – дифференцированный зачет.

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

- диагностическая работа;
- индивидуальное практическое задание;
- тест.

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. М. Голиков. . Кодирование и шифрование информации в системах связи. Томск: ТУСУР, 2016, эл. рес.
3. В. Д. Вавилов, С. П. Тимошенко, А. С. Тимошенко. . Микросистемные датчики физических величин. М.: Техносфера, 2018, 40 экз.
4. В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации. СПб.: Питер, 2007, эл. рес.
5. Е. Г. Лебедько. . Теоретические основы передачи информации. Санкт-Петербург: Лань, 2022, эл. рес.
6. Е. Ф. Берёзкин. . Основы теории информации и кодирования. СПб.: Лань, 2019, 9 экз.
7. И. В. Черпаков. . Теоретические основы информатики. Москва: Юрайт, 2017, эл. рес.
8. Л. К. Бабенко, Е. А. Ищукова. . Криптографическая защита информации: симметричное шифрование. Москва: Юрайт, 2020, эл. рес.
9. М. Вернер. . Основы кодирования. М.: Техносфера, 2004, 50 экз.
10. М. Ю. Рыгов, М. Л. Гулак, А. П. Горлов. . Криптографические методы защиты информации. Старый Оскол: ТНТ, 2021, эл. рес.
11. С. А. Курицын. . Телекоммуникационные технологии и системы. М.: Академия, 2008, 6 экз.
12. С. А. Ляшева, М. П. Шлеймович, З. Т. Яхина. . Теория информации и кодирования. Казань: КНИТУ-КАИ, 2020, эл. рес.

5.2. Дополнительная литература по дисциплине:

1. Д. Сэломон. . Сжатие данных, изображений и звука. М.: Техносфера, 2004, 3 экз.
2. С. Бернет, С. Пэйн. Криптография. Официальное руководство RSA Security. М.: БИНОМ, 2007, 3 экз.

5.3. Периодические издания:

1. Информационно-измерительные и управляющие системы;
2. Моделирование и анализ информационных систем;
3. 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..

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. NI Multisim - академическая версия.

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. NI Multisim - академическая версия.

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 **части, формируемой участниками образовательных отношений 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*:

ПСК-1.1 способность самостоятельно осуществлять постановку задачи исследования, формирование плана его реализации, выбор методов исследования и обработку результатов;

ПСК-1.3 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**:

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

- диагностическая работа;
- индивидуальное практическое задание;
- тест.

Промежуточная аттестация проводится в формах:

- дифференцированный зачет.

Общая трудоемкость освоения дисциплины составляет **3 з.е., 108 ч**. Программой дисциплины предусмотрены лекционные занятия (**4 ч.**), практические занятия (**2 ч.**), самостоятельная работа студента (**102 ч**).

ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 108 ч., из них 6 ч. аудиторных занятий, и 102 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 техники. Элементы теории информации и информационной техники. Измерение информации. Меры информации. Понятие энтропии. Дискретизация информации. Этапы обращения информации в автоматизированных системах. Общие сведения о датчиках и сенсорах. Физические принципы функционирования. Датчики на ПАВ. MEMS. RFID. 1.3 Передача информации по каналам связи. Режимы передачи. Виды каналов и линий связи. Разделение каналов. Электрические, акустические, электромагнитные, оптические линии связи. Беспроводная связь. UWB, CDMA, расширенный спектр с перестройкой частоты. Технология Li-Fi. Спутниковые линии связи. Основные радиointерфейсы: Wi-Fi, Wi MAX, Zig Bee, Bluetooth, Wireless USB, WHDI, Wireless HD. Теоретические основы передачи сообщений без помех и с помехами. Повышение достоверности передачи и приема.	С. А. Курицын. . Телекоммуникационные технологии и системы: М.: Академия, 2008 (2, 3) В. Д. Вавилов, С. П. Тимошенко, А. С. Тимошенко. . Микросистемные датчики физических величин: М.: Техносфера, 2018 (все) Е. Г. Лебедько. . Теоретические основы передачи информации: Санкт-Петербург: Лань, 2022 (все) В. Л. Бройдо, О. П. Ильина. . Вычислительные системы, сети и телекоммуникации: СПб.: Питер, 2007 (1, 2, 3) И. В. Черпаков. . Теоретические основы информатики: Москва: Юрайт, 2017 (1-3)	24
Итого по разделу 1		24
Раздел 2. Кодирование данных.		
Повторение и осмысление информации о прямоугольных и циклических кодах, блочных кодах и способах их реализации. Исследование реализации сверточного кода с использованием пакета специализированного ПО.	А. М. Голиков. . Кодирование и шифрование информации в системах связи: Томск: ТУСУР, 2016 (все) М. Вернер. . Основы кодирования: М.: Техносфера, 2004 (1, 2, 3)	24

Итого по разделу 2		24
Раздел 3. Сжатие данных.		
Повторение и осмысление сведений о принципах построения алгоритмов сжатия данных. Исследование вариантов реализации алгоритмов Хаффмана, арифметического кодирования, RLE, LZ78 с применением средств программирования. Исследование алгоритма JPEG.	<p>Е. Ф. Берёзкин. . Основы теории информации и кодирования: СПб.: Лань, 2019 (все)</p> <p>С. А. Ляшева, М. П. Шлеймович, З. Т. Яхина. . Теория информации и кодирования: Казань: КНИТУ-КАИ, 2020 (все)</p> <p>Д. Сэломон. . Сжатие данных, изображений и звука: М.: Техносфера, 2004 (все)</p>	24
Итого по разделу 3		24
Раздел 4. Элементы криптографии.		
Повторение и осмысление сведений о криптографии, ее назначении, способах реализации, алгоритмах различной сложности. Исследование разных типов алгоритмов хеширования. Обзор в виде таблицы сравнения.	<p>С. Бернет, С. Пэйн. Криптография. Официальное руководство RSA Security: М.: БИНОМ, 2007 (все)</p> <p>Л. К. Бабенко, Е. А. Ищукова. . Криптографическая защита информации: симметричное шифрование: Москва: Юрайт, 2020 (все)</p> <p>М. Ю. Рытов, М. Л. Гулак, А. П. Горлов. . Криптографические методы защиты информации: Старый Оскол: ТНТ, 2021 (3-8)</p> <p>А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (все)</p> <p>Л. К. Бабенко, Е. А. Ищукова. . Криптографическая защита информации: симметричное шифрование: Москва: Юрайт, 2020 (все)</p>	30
Итого по разделу 4		30

ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

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

- диагностическая работа
- тест;
- индивидуальное практическое задание;
- 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.

Тест

Тест включает в себя 10 вопросов. Требуется выбирать один правильный ответ из предложенных. Время выполнения 20 минут. Успешное прохождение теста регистрируется при условии получения не менее 6 правильных ответов. 7-8 правильных ответов - хорошо, 9-10 - отлично. Примеры представлены в УМК в дисциплины.

Индивидуальное практическое задание

Отчет по индивидуальному заданию должен содержать полное решение согласованной с преподавателем задачи. Примеры заданий и типовые задачи представлены в УМК в дисциплины.

Дифференцированный зачет

Итоговый контроль по дисциплине проходит в форме дифференцированного зачета, который выставляется на 17 неделе семестра

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		ПСК-1.1	ПСК-1.3	
2	3	Раздел 1. Элементы теории информации и информационной техники.	25	1	1	0	24	10	10	Тест, Индивидуальное практическое задание
2	3	Раздел 2. Кодирование данных.	26	2	1	1	24	30	30	Индивидуальное практическое задание, Тест
2	3	Раздел 3. Сжатие данных.	26	2	1	1	24	30	30	Индивидуальное практическое задание, Тест
2	3	Раздел 4. Элементы криптографии.	31	1	1	0	30	30	30	Индивидуальное практическое задание, Тест
Всего за 3 семестр			108	6	4	2	102	100	100	
Всего по дисциплине			108	6	4	2	102	100	100	