

УТВЕРЖДАЮ  
 Декан факультета

\_\_\_\_\_ Матвеев П.В.

« \_\_\_\_ » \_\_\_\_\_ 20\_\_

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

*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: 2025

Программу составил:

Кафедра О7 Информационные системы и программная инженерия  
Бескин Дмитрий Александрович, д.т.н., профессор

\_\_\_\_\_

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**

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:

ПК-2.2 — Способен 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:

### **ПК-2.2**

*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
- 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

### 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		ПК-2.2
3	5	<b>Раздел 1. Элементы теории информации и информационной техники.</b> 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.	24	13	10	3	11	20
3	5	<b>Раздел 2. Кодирование данных.</b> 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.	20	9	6	3	11	20
3	5	<b>Раздел 3. Сжатие данных.</b> 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.	21	10	6	4	11	20
3	5	<b>Раздел 4. Элементы криптографии.</b> 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.	23	12	8	4	11	20
3	5	<b>Раздел 5. Перспективные разработки.</b> 5.1 Общие направления развития информационной техники. Возникающие проблемы и возможные пути их решения. Перспективные разработки.	20	7	4	3	13	20
<b>Всего за 5 семестр</b>			108	51	34	17	57	100
<b>Всего по дисциплине</b>			108	51	34	17	57	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	4

		потерями. Алгоритм дискретно-косинусного преобразования. Вейвлет- алгоритм сжатия.	
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
<b>Всего за 5 семестр</b>			<b>17</b>

### 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.	11
2	Раздел 2. Кодирование данных.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям.	11
3	Раздел 3. Сжатие данных.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям.	11
4	Раздел 4. Элементы криптографии.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям.	11
5	Раздел 5. Перспективные разработки.	Оформление практических работ	3
6		Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям.	10
Всего за 5 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
5				Отч. по ПЗ		ДР	Отч. по ПЗ		Отч. по ПЗ	ДР			Отч. по ПЗ		Отч. по ПЗ	ДР	диф. зач.

Условные обозначения:

- ДР – диагностическая работа;
- Отч. по ПЗ – отчет по практическому заданию;
- диф. зач. – дифференцированный зачет.

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

- диагностическая работа;
- отчет по практическому заданию.

**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. Санкт-Петербург: Лань, 2022, 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. Рыгов, 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. <https://urait.ru/> — Образовательная платформа «Юрайт». Для вузов и ссузов.;;;
3. <http://library.voenmeh.ru/> — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.

### 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](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 Естественнотехнический БГТУ "ВОЕНМЕХ"* им. Д.Ф. Устинова кафедрой *О7 Информационные системы и программная инженерия*.

Дисциплина нацелена на формирование *компетенций*:

ПК-2.2 Способен 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;
- отчет по практическому заданию.

**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.
<b>Раздел 1. Элементы теории информации и информационной техники.</b>		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям.	М. Вернер. . Основы кодирования: М.: Техносфера, 2004 (1) А. В. Черёмушкин. . Криптографические протоколы. Основные свойства и уязвимости: М.: Академия, 2009 (1) А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (1-2) 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) С. А. Курицын. . Телекоммуникационные технологии и системы: М.: Академия, 2008 (1) Г. Г. Раннев. . Измерительные информационные системы: М.: Академия, 2010 (1)	11
Итого по разделу 1		11
<b>Раздел 2. Кодирование данных.</b>		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям.	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) Л. К. Бабенко, Е. А. Ищукова. . Криптографическая защита информации: симметричное шифрование: Москва: Юрайт, 2020 (1-3) А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (2)	11
Итого по разделу 2		11
<b>Раздел 3. Сжатие данных.</b>		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям.	А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (2-3) Е. Ф. Берёзкин. . Основы теории	11

	<p>информации и кодирования: Санкт-Петербург: Лань, 2022 (1-3)</p> <p>А. В. Черёмушкин. . Криптографические протоколы. Основные свойства и уязвимости: М.: Академия, 2009 (2-3)</p> <p>С. Б. Гашков, Э. А. Применко, М. А. Черепнев. . Криптографические методы защиты информации: М.: Академия, 2010 (1-3)</p> <p>М. Ю. Рытов, М. Л. Гулак, А. П. Горлов. . Криптографические методы защиты информации: Старый Оскол: ТНТ, 2021 (1-3)</p> <p>М. Вернер. . Основы кодирования: М.: Техносфера, 2004 (2)</p>	
Итого по разделу 3		11
<b>Раздел 4. Элементы криптографии.</b>		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям.	<p>Е. Ф. Берёзкин. . Основы теории информации и кодирования: Санкт-Петербург: Лань, 2022 (3-5)</p> <p>С. А. Курицын. . Телекоммуникационные технологии и системы: М.: Академия, 2008 (2)</p> <p>М. Вернер. . Основы кодирования: М.: Техносфера, 2004 (3)</p> <p>А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (2-4)</p> <p>А. В. Черёмушкин. . Криптографические протоколы. Основные свойства и уязвимости: М.: Академия, 2009 (4-6)</p> <p>С. Б. Гашков, Э. А. Применко, М. А. Черепнев. . Криптографические методы защиты информации: М.: Академия, 2010 (2-5)</p>	11
Итого по разделу 4		11
<b>Раздел 5. Перспективные разработки.</b>		
Оформление практических работ	С. А. Курицын. . Телекоммуникационные технологии и системы: М.: Академия, 2008 (5-6)	3
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям.	С. Б. Макаров, Н. В. Певцов, Е. А. Попов. . Телекоммуникационные технологии. Введение в технологию GSM: М.: Академия, 2008 (4)	10
Итого по разделу 5		13

## ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

- диагностическая работа
- отчет по практическому заданию;
- 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.

#### Отчет по практическому заданию

Задание представлено в срок, не представлен чужой отчет.

Выполненные практические задания представляются в электронной форме в виде подготовленной электронной версии пояснительной записки, оформленной в соответствии с ГОСТ

Выполненные практические задания представляются в электронной форме в виде подготовленных к сборке исходных текстов и полностью готовой к выполнению программы для тестирования преподавателем и электронной версии отчета, оформленной в соответствии с ГОСТ. При успешном тестировании программы и проверке соответствия отчета требованиям ГОСТ и требованиям задания студент допускается к защите задания.

Работа допускается к защите при следующих условиях:

- предъявляемые к защите решения являются корректными;
- работа выполнена в соответствии с заданием;
- электронная и/или печатная версии отчета соответствуют установленным требованиям.

Количество баллов и критерии регламентируется технологической картой дисциплины.

#### Дифференцированный зачет

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 «зачтено-удовлетворительно» на основании успешных ответов на дополнительные вопросы. При неуспешной сдаче 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		ПК-2.2	
3	5	Раздел 1. Элементы теории информации и информационной техники.	24	13	10	3	11	20	Отчет по практическому заданию
3	5	Раздел 2. Кодирование данных.	20	9	6	3	11	20	Отчет по практическому заданию
3	5	Раздел 3. Сжатие данных.	21	10	6	4	11	20	Отчет по практическому заданию
3	5	Раздел 4. Элементы криптографии.	23	12	8	4	11	20	Отчет по практическому заданию
3	5	Раздел 5. Перспективные разработки.	20	7	4	3	13	20	Отчет по практическому заданию
Всего за 5 семестр			108	51	34	17	57	100	
Всего по дисциплине			108	51	34	17	57	100	

## Оценочные материалы по дисциплине КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

**ПК-2.2 - Способен 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**

№ 1 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Какой алгоритм асимметричного шифрования основан на факторизации?

A. ElGamal

B. RSA

C. ECC

D. Blum–Goldwasser

№ 2 Прочитайте текст и запишите развернутый обоснованный ответ

Объясните принципы формирования циклических кодов и их свойства.

№ 3 Прочитайте текст и запишите развернутый обоснованный ответ

Опишите методы статистического сжатия данных и отличие их от словарных.

№ 4 Прочитайте текст и установите соответствие

Соотнесите тип компрессии с алгоритмом:

A	Потерянное	1 JPEG
Б	Без потерь	2 Deflate
В	Словарное	3 LZ77
		4 LP74

№ 5 Прочитайте текст и установите соответствие

Соотнесите классификацию каналов связи и пример:

A	Без помех	Оптический 1 канал в оптоволокне Радиоканал
Б	С помехами	2 <sup>с</sup> гауссовским шумом Канал с коррекцией
В	Устойчивый к помехам	3 ошибок на уровне канала Канал без коррекции 4 ошибок на уровне канала

№ 6 Прочитайте текст и установите последовательность

Укажите правильную последовательность этапов передачи информации по каналу с помехами:

1. Кодирование
2. Модуляция
3. Декодирование
4. Демодуляция

- № 7 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов  
Какие алгоритмы относятся к блочным симметричным шифрам?
- A. DES
  - B. AES
  - C. RC4
  - D. Blowfish
- № 8 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов  
Какие меры защищают от атак по боковым каналам питания?
- A. Маскирование
  - B. Рандомизация
  - C. Укреплённая фарадеева клетка
  - D. Применение одноразовых ключей
- № 9 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов  
Какие методы повышают помехоустойчивость канала передачи?
- A. Избыточное кодирование
  - B. Модуляция QAM
  - C. Шумоподавление
  - D. Сжатие данных
- № 10 Прочитайте текст и установите последовательность  
Установите правильную последовательность этапов криптоанализа RSA методом факторизации:
- 1. Сбор открытых ключей
  - 2. Факторизация  $n$
  - 3. Вычисление  $\phi(n)$
  - 4. Нахождение  $d$
- № 11 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа  
Какой код исправляет одиночные и двойные ошибки на основе многочленов?
- A. Хэмминга
  - B. Рида–Соломона
  - C. Циклический код
  - D. Прямоугольный код
- № 12 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа  
Какое преобразование используется в JPEG для сжатия с потерями?
- A. Быстрое преобразование Фурье
  - B. Дискретное косинусное преобразование
  - C. Вейвлет-преобразование
  - D. Z-преобразование