

Минобрнауки России

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ  
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»  
(ФГБОУ ВО «ВГУ»)**



**УТВЕРЖДАЮ**  
Заведующий кафедрой  
Борисов Дмитрий Николаевич  
Кафедра информационных систем  
05.03.2025

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ**

Б1.О.31 Информатика

**1. Код и наименование направления подготовки/специальности:**

10.05.01 Компьютерная безопасность

**2. Профиль подготовки/специализация:**

Анализ безопасности компьютерных систем, Разработка защищенного программного обеспечения

**3. Квалификация (степень) выпускника:**

Специалитет

**4. Форма обучения:**

Очная

**5. Кафедра, отвечающая за реализацию дисциплины:**

Кафедра информационных систем

**6. Составители программы:**

ФИО Сычев Александр Васильевич

Ученая степень кандидат физико-математических наук

Ученое звание доцент

E-mail: sav@cs.vsu.ru

Факультет: компьютерных наук

Кафедра: информационных систем

**7. Рекомендована:** НМС ФКН, протокол № 5 от 05.03.2025

**8. Учебный год:**

2025-2026

**9. Цели и задачи учебной дисциплины:**

Целью учебной дисциплины является введение студентов первого курса в круг основных фактов, концепций, принципов и теоретических проблем, а также практических задач и приложений, основных методов и технологий, относящихся к сфере информатики.

Задачи учебной дисциплины:

- знакомство студентов с понятием информации, формами ее представления, способами измерения ее количества, качественные характеристики информации, принципами кодирования, передачи, защиты и обработки информации, особенностями ее восприятия человеком;
- владение методами перевода чисел между различными системами счисления;

- умение рассчитывать степень избыточности кода и оценивать возможности его сжатия;
- владение методами построения префиксных кодов для оптимального кодирования данных.

#### 10. Место учебной дисциплины в структуре ООП:

#### 11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников) и индикаторами их достижения:

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.1 Знает общие принципы построения современных компьютеров, формы и способы представления данных в персональном компьютере;	Знает: <ul style="list-style-type: none"> <li>• формы и способы представления данных в ЭВМ;</li> <li>• особенности машинного представления целых чисел со знаком и без знака, вещественных чисел;</li> <li>• особенности машинной арифметики для целых и вещественных чисел.</li> </ul>
ОПК-2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.5 Умеет применять типовые программные средства сервисного назначения, информационного поиска и обмена данными в сети Интернет;	Умеет: <ul style="list-style-type: none"> <li>• применять типовые программные средства сервисного назначения и информационного поиска при работа на компьютере.</li> </ul>
ОПК-2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.6 Умеет составлять документы, используя прикладные программы офисного назначения	Умеет: <ul style="list-style-type: none"> <li>• работать с документами в программах Word и Excel.</li> </ul>
ОПК-2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.7 Владеет средствами управления пользовательскими интерфейсами операционных систем	Имеет навыки: <ul style="list-style-type: none"> <li>• настройки пользовательского интерфейса при работе с ОС Windows.</li> </ul>

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности;	ОПК-3.20 Знает различные подходы к определению понятия алгоритма, методы доказательства алгоритмической неразрешимости и методы построения эффективных алгоритмов	Знает: <ul style="list-style-type: none"> <li>• различные подходы к определению понятия алгоритма;</li> <li>• понятия алгоритмической сходимости и алгоритмической сложности.</li> </ul>
ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	ОПК-10.21 Знает фундаментальные понятия теории информации (энтропия, взаимная информация, источники сообщений, каналы связи, коды), свойства энтропии и взаимной информации	Знает понятия: энтропии, источника сообщений, канала связи, кодов и кодирования.
<p>ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;</p> <p>ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;</p>	<p>ОПК-10.23 Знает основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи (коды - линейные, циклические, Хемминга)</p> <p>ОПК-10.22 Знает основные результаты о кодировании дискретных источников сообщений при наличии и отсутствии шума</p>	<p>Знает:</p> <ul style="list-style-type: none"> <li>• основы оптимального кодирования источников информации (префиксные коды Шеннона-Фано и Хаффмана) информации;</li> <li>• основы помехоустойчивого кодирования каналов связи (код Хэмминга, расстояние Хэмминга)</li> </ul> <p>Знает:</p> <ul style="list-style-type: none"> <li>• понятие пропускной способности канала связи</li> <li>• теорему Шеннона о кодировании каналов связи с шумом</li> </ul>

## 12. Объем дисциплины в зачетных единицах/час:

4/144

## Форма промежуточной аттестации:

Экзамен

### 13. Трудоемкость по видам учебной работы

Вид учебной работы	Семестр 1	Всего
Аудиторные занятия	68	68
Лекционные занятия	34	34
Практические занятия	34	34
Лабораторные занятия		0
Самостоятельная работа	40	40
Курсовая работа		0
Промежуточная аттестация	36	36
Часы на контроль	36	36
Всего	144	144

#### 13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1	Введение в информатику	Введение в информатику. Информатика и компьютерные науки. Канал передачи информации. Требования, предъявляемые к специалистам в области информационных технологий, основные сферы практических приложений информатики	<a href="https://edu.vsu.ru/course/view.php?id=2628">https://edu.vsu.ru/course/view.php?id=2628</a>
2	Машинное представление целых и вещественных чисел	Машинное представление чисел без знака. Арифметическое переполнение. Особенности машинной арифметики. Машинное представление чисел со знаком. Двоично-дополнительный код. Арифметическое переполнение. Машинное представление вещественных чисел. Особенности машинной арифметики для чисел с плавающей запятой	<a href="https://edu.vsu.ru/course/view.php?id=2628">https://edu.vsu.ru/course/view.php?id=2628</a>

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
3	Данные и знания. Системы классификации данных	Данные и знания. Экстенционал и интенционал понятия. Системы классификации данных: иерархическая, фасетная и дескрипторная. Информационный поиск	<a href="https://edu.vsu.ru/course/view.php?id=2628">https://edu.vsu.ru/course/view.php?id=2628</a>
4	Дискретные сообщения. Кодирование информации. Оптимальное и помехоустойчивое кодирование	Дискретные сообщения. Кодирование информации. Системы кодирования: регистрационная, порядковая и серийно-порядковая. Избыточность. Префиксные коды. Оптимальное кодирование. Алгоритмы Шеннона-Фано и Хаффмана. Расширение кода. Теорема Шеннона о кодировании без шума. Способы обеспечения помехоустойчивой передачи информации. Корректирующие коды и расстояние Хэмминга.	<a href="https://edu.vsu.ru/course/view.php?id=2628">https://edu.vsu.ru/course/view.php?id=2628</a>
5	Цифровые и аналоговые сигналы. ЦАП и АЦП	Аналоговые и цифровые сигналы. Спектр сигнала. Модуляция сигнала. Цифро-аналоговое преобразование. Дискретизация, квантование. Теорема Котельникова-Найквиста. Форматы кодирования цифровых сигналов.	<a href="https://edu.vsu.ru/course/view.php?id=2628">https://edu.vsu.ru/course/view.php?id=2628</a>

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
6	Передача информации. Каналы передачи информации	Измерение количества информации. Три подхода к определению количества информации (по Колмогорову): вероятностный, комбинаторный и алгоритмический. Понятие канала связи. Пропускная способность канала связи. Способы передачи информации. Локальные и глобальные компьютерные сети.	<a href="https://edu.vsu.ru/course/view.php?id=2628">https://edu.vsu.ru/course/view.php?id=2628</a>
7	Восприятие информации человеком	Органы чувств человека и их характеристики. Порог восприятия и разрешающая способность рецептора. Особенности зрительного восприятия. Структура алгоритма JPEG. Особенности слухового восприятия. Психоакустическое маскирование.	<a href="https://edu.vsu.ru/course/view.php?id=2628">https://edu.vsu.ru/course/view.php?id=2628</a>

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
8	<p>Обработка информации.</p> <p>Введение в теорию алгоритмов.</p> <p>Алгоритмические модели и понятие о сложности алгоритма</p>	<p>Обработка сообщений.</p> <p>Классификация способов обработки. Понятие об алгоритме. Структура алгоритма.</p> <p>Характеристики алгоритмов.</p> <p>Универсальные алгоритмические модели: машина Тьюринга, частично-рекурсивные функции и нормальный алгоритм Маркова. Их свойства и применение.</p> <p>Понятие сложности алгоритма. Функция временной сложности.</p> <p>Полиномиальные и экспоненциальные алгоритмы. Понятие о NP-полноте.</p>	<p><a href="https://edu.vsu.ru/course/view.php?id=2628">https://edu.vsu.ru/course/view.php?id=2628</a></p>
9	<p>Защита информации.</p> <p>Симметричные и асимметричные криптосистемы</p>	<p>Криптосистемы с открытым ключом.</p> <p>Цифровая электронная подпись. Односторонние функции. Асимметричные криптосистемы. Структура алгоритма RSA.</p> <p>Электронная подпись.</p> <p>Протоколы криптосистем с открытым ключом.</p> <p>Технические и программные средства защиты информации в компьютерных системах.</p> <p>Антивирусная защита.</p>	<p><a href="https://edu.vsu.ru/course/view.php?id=2628">https://edu.vsu.ru/course/view.php?id=2628</a></p>

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
10	Введение в системы искусственного интеллекта	Искусственный интеллект (ИИ). Тест Тьюринга. Основные подходы к моделированию ИИ. Программные средства для систем искусственного интеллекта.	<a href="https://edu.vsu.ru/course/view.php?id=2628">https://edu.vsu.ru/course/view.php?id=2628</a>

### 13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
1	Введение в информатику	2	2	0	3	7
2	Машинное представление целых и вещественных чисел	5	5	0	6	16
3	Данные и знания. Системы классификации. Информационный поиск. данных	3	2	0	3	8
4	Дискретные сообщения. Кодирование информации. Оптимальное и помехоустойчивое кодирование	4	5	0	4	13
5	Цифровые и аналоговые сигналы. ЦАП и АЦП	2	4	0	3	9
6	Передача информации. Каналы передачи информации	4	4	0	4	12

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
7	Восприятие информации человеком	2	2	0	4	8
8	Обработка информации. Введение в теорию алгоритмов. Алгоритмические модели и понятие о сложности алгоритма	4	2	0	4	10
9	Защита информации. Симметричные и асимметричные криптосистемы. Криптосистемы с открытым ключом. Цифровая электронная подпись	4	6	0	5	15
10	Введение в системы искусственного интеллекта	4	2	0	4	10
		34	34	0	40	108

#### **14. Методические указания для обучающихся по освоению дисциплины**

1) При изучении дисциплины рекомендуется использовать следующие средства:

- рекомендуемую основную и дополнительную литературу;
- методические указания и пособия;
- контрольные задания для закрепления теоретического материала;
- электронные версии учебников.

2) Для лучшего усвоения дисциплины рекомендуется проведение письменного опроса (тестирование, выполнение заданий) студентов по материалам лекций и лабораторных работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала.

3) При проведении лабораторных занятий обеспечивается практическая демонстрация материалов лекционных занятий и осуществляется экспериментальная проверка методов, алгоритмов и технологий, излагаемых в рамках лекций.

4) При переходе на дистанционный режим обучения для создания электронных курсов, чтения лекций онлайн и проведения лабораторно- практических занятий используются информационные ресурсы из образовательного портала "Электронный университет ВГУ, базирующегося на системе дистанционного обучения Moodle, развернутой в университете: (<https://edu.vsu.ru/course/view.php?id=2628>)

**15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины**

№ п/п	Источник
1	Грошев, А. С. Информатика [Электронный ресурс] / Грошев А. С., Закляков П. В. — 3-е .— Москва : ДМК Пресс, 2015 .— 588 с. <URL: <a href="http://e.lanbook.com/books/element.php?pl1_id=69958">http://e.lanbook.com/books/element.php?pl1_id=69958</a> >
2	Львович, И. Я. Основы информатики : учебное пособие / И. Я. Львович, Ю. П. Преображенский, В. В. Ермолова. — Воронеж : ВИБТ, 2019. — 253 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/157487">https://e.lanbook.com/book/157487</a>

б) дополнительная литература:

№ п/п	Источник
1	Щапова, И. Н. Информатика : учебное пособие / И. Н. Щапова, В. А. Щапов. — Пермь : ПНИПУ, 2016. — 154 с. — ISBN 978-5-398-01556-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/160821">https://e.lanbook.com/book/160821</a>
2	Маркс, Р. Введение в эволюционную информатику : руководство / Р. Маркс, У. Дембски, У. Эверт ; перевод с английского В. С. Яценкова. — Москва : ДМК Пресс, 2020. — 276 с. — ISBN 978-5-97060-725-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/140583">https://e.lanbook.com/book/140583</a>
3	Петрищев, И. О. Теоретические основы информатики : учебно-методическое пособие / И. О. Петрищев, Е. А. Фёдорова. — Ульяновск : УлГПУ им. И.Н. Ульянова, 2017. — 70 с. — ISBN 978-5-86045-933-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/112083">https://e.lanbook.com/book/112083</a>
4	Губарев, В. В. Введение в теоретическую информатику : учебное пособие / В. В. Губарев. — Новосибирск : НГТУ, [б. г.]. — Часть 2 — 2015. — 472 с. — ISBN 978-5-7782-2778-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/118223">https://e.lanbook.com/book/118223</a>

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
1	Онлайн курс на <a href="https://edu.vsu.ru">edu.vsu.ru</a> : <a href="https://edu.vsu.ru/course/view.php?id=2628">https://edu.vsu.ru/course/view.php?id=2628</a>

№ п/п	Источник
2	Электронная библиотека "Лань": <a href="https://e.lanbook.com/">https://e.lanbook.com/</a>
3	<a href="http://www.lib.vsu.ru">www.lib.vsu.ru</a> - ЗНБ ВГУ

#### 16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Сычев А.В. Информатика / А.В. Сычев. – Воронеж : Издательский дом ВГУ, 2017. – 126 с.
2	Информатика. Практикум : учебно-методическое пособие. Ч. 1 / составители: А. В. Сычев, Л. О. Подоприхина, А. А. Борисова. Воронеж : Издательский дом ВГУ, 2024. - 50 с.

#### 17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

Пакет прикладных программ MATLAB.

Для проведения занятий используется смешанное обучение с использованием онлайн курса на [edu.vsu.ru](http://edu.vsu.ru): <https://edu.vsu.ru/course/view.php?id=2628>

#### 18. Материально-техническое обеспечение дисциплины:

Компьютерная лаборатория с локальной сетью из 15 персональных компьютеров с установленным системным и прикладным программным обеспечением и выходом в Интернет.

#### 19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	2	ОПК-2	ОПК-2.1	Практическое задание, письменный тест
2	4,5,9	ОПК-2	ОПК-2.5	Практическое задание
3	9	ОПК-2	ОПК-2.6	Практическое задание
4	4,5,9	ОПК-2	ОПК-2.7	Практическое задание
5	6,8	ОПК-3	ОПК-3.20	Письменный тест
6	4	ОПК-10	ОПК-10.21	Письменный тест
7	4	ОПК-10	ОПК-10.23	Практическое задание, письменный тест
	6	ОПК-10	ОПК-10.22	Письменный тест

Промежуточная аттестация

Форма контроля - Экзамен

Оценочные средства для промежуточной аттестации

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в форме(ах): *письменных работ (лабораторные работы); тестирования.*

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Контрольно-измерительные материалы промежуточной аттестации включают в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и практические задания, позволяющие оценить степень сформированности умений и навыков.

При оценивании используется следующая шкала:

5 баллов ставится, если обучающийся демонстрирует полное соответствие знаний, умений, навыков приведенным в таблицах показателям, свободно оперирует приобретенными знаниями, умениями, применяет их при решении практических задач;

4 балла ставится, если обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач;

3 балла ставится, если обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач;

2 балла ставится, если обучающийся демонстрирует явное несоответствие знаний, умений, навыков приведенным в таблицах показателям.

*При сдаче экзамена*

оценка «отлично» - 5 баллов

оценка «хорошо» - 4 балла

оценка «удовлетворительно» - 3 балла

оценка «неудовлетворительно» - 2 балла

## **20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания**

### **20.1 Текущий контроль успеваемости**

Тестовые задания - 1 балл за каждый правильный тест (максимум).

Компетенция ОПК-2

1. Для десятичного числа 4511 выберите ответы, которые соответствуют представлению данного числа в других системах счисления (двоичной, восьмеричной, шестнадцатеричной):

a) 0001000110011111

b) 010110011010101

c) 101000110101

d) 10637

e) 119F

f) 2342543

- g) 3164
- h) 3a32
- i) c211

2. В результате сложения со знаком двух двоичных 11-разрядных чисел

11101101000

11111010101

имели место следующие переносы относительно старшего разряда:

- a) Больше двух переносов
- b) Входящий и исходящий вместе
- c) Не было переносов вообще
- d) Только входящий
- e) Только исходящий

Компетенция ОПК-3

3. Выберите утверждения, которые отражают необходимые требования к алгоритмам:

- a) Алгоритм - это компактное описание последовательности действий, нацеленных на получение необходимого результата.
- b) Алгоритм должен останавливаться после конечного числа шагов (зависящего от данных) с указанием того, что считать результатом.
- c) Алгоритм и компьютерная программа - это, по-сути, одно и то же.
- d) Алгоритм применяется к исходным данным и выдает результаты. Кроме того, в ходе работы алгоритма появляются промежуточные результаты, которые используются в дальнейшем.
- e) Алгоритм состоит из отдельных элементарных шагов, или действий, причем множество различных шагов, из которых составлен алгоритм, конечно.
- f) Данные для своего размещения требуют памяти. Память обычно считается однородной и дискретной, т. е. состоит из одинаковых ячеек, причем каждая ячейка может содержать один символ алфавита данных.
- g) Количество шагов в алгоритме должно быть минимальным.
- h) Последовательность шагов алгоритма детерминирована, т. е. после каждого шага либо указывается, какой шаг делать дальше, либо дается команда остановки, после чего работа алгоритма считается законченной.

4. Выберите верные утверждения, относящиеся к функции временной сложности алгоритма:

- a) Это функция, которая каждой входной длине  $n$  ставит в соответствие максимальное (по всем индивидуальным задачам длины  $n$ ) время, затрачиваемое алгоритмом на решение индивидуальных задач этой длины.
- b) Это функция, которая каждому набору значений входных данных алгоритма ставит в соответствие максимальное время, затрачиваемое алгоритмом на решение индивидуальной задачи с этими входными данными.
- c) Измеряется в количестве операций (тактов), которые должен выполнить исполнитель для решения задачи на основе выбранного алгоритма
- d) Измеряется физическим временем, которое требуется для решения задачи на основе выбранного алгоритма.
- e) Не зависит от выбора исполнительного устройства для реализации алгоритма
- f) Зависит от исполнительного устройства, выбранного для реализации алгоритма.

5. Как изменится размер задач  $N'$ , решаемой за один час машинного времени, и имеющей функцию временной сложности  $f(n) = (10n \cdot a + b)$ , если благодаря совершенствованию технологии быстродействие ЭВМ возрастет в 150 раз по сравнению с современными вычислительными машинами?

- a)  $N'$  станет равным  $\log_{10} [(10 N * a + b) * 150 - b] / a$
  - b) Увеличится в 150 раз
  - c)  $N'$  станет равным  $(10 N' * a + b) * 150$
  - d)  $N'$  станет равным  $150 * \sqrt{10 [10 N * a + b]}$
  - e)  $N'$  станет равным  $\log_{10} [(10 N * a + b) * 150] / a$
6. Выберите правильные утверждения относительно полиномиального алгоритма:
- a) Полиномиальным алгоритмом называется алгоритм, у которого временная сложность равна  $O(p(n))$ , где  $p(n)$  - некоторая полиномиальная функция, а  $n$  — входная длина.
  - b) К полиномиальным алгоритмам относятся только такие алгоритмы, у которых временная сложность является полиномиальной функцией от входной длины задачи.
  - c) Более предпочтительными являются экспоненциальные алгоритмы, нежели полиномиальные.
  - d) С помощью полиномиальных алгоритмов решаются только труднорешаемые задачи.
  - e) Как правило, экспоненциальные алгоритмы являются более эффективными при решении задач, нежели полиномиальные.
7. Выберите правильные утверждения, относящиеся к асимметричным криптосистемам:
- a) Асимметричные криптосистемы реализуются с помощью функций, для которых вычисление обратной функции является труднорешаемой задачей, если неизвестно секретное число.
  - b) В асимметричной криптосистеме допустимо использование публичного ключа.
  - c) В асимметричной криптосистеме как и в любой криптосистеме все ключи должны быть секретными.
  - d) Шифр Цезаря является асимметричной криптосистемой.
  - e) Асимметричные криптосистемы - это криптосистемы открытого шифрования.
  - f) Криптосистема RSA не является асимметричной криптосистемой.
8. Выберите неверные утверждения, относящиеся к электронной цифровой подписи (ЭЦП):
- a) В ЭЦП значение сообщения отправителя шифруется с помощью публичного ключа получателя.
  - b) В ЭЦП значение хеш-функции от сообщения отправителя шифруется с помощью секретного ключа отправителя.
  - c) Для реализации ЭЦП используются только секретные ключи отправителя и получателя.
  - d) Для реализации ЭЦП хеш-функция может не использоваться.

#### Компетенция ОПК-10

9. Выберите правильное соответствие:
- a) Элемент некоторого конечного множества отличимых друг от друга «вещей» или «сущностей».
  - b) Набор знаков, в котором определён линейный порядок следования.
  - c) Правило, описывающее отображение одного набора знаков в другой набор знаков (или слов).
  - d) Конечная последовательность знаков.
  - e) Способ отображения, при котором каждый образ является отдельным знаком.
- a) Алфавит
  - b) Знак
  - c) Код
  - d) Слово
  - e) Шифр
10. Выберите правильное соответствие:
- a) Каждый из объектов множества кодируется с помощью текущего номера по порядку. При этом обеспечивается простота добавления новых объектов и компактность кода, однако такой код не несет информации о самом объекте.
  - b) Кодами служат числа натурального ряда с предварительным выделением групп объектов классификации с одинаковыми признаками.
  - c) В кодовом обозначении знаки на каждой ступени деления зависят от результатов разбиения на

предыдущих ступенях. В результате кодовое обозначение группировки дает информацию о наборе признаков, характеризующих эту группировку. Для выделения группировок используется иерархический метод классификации.

d) Признаки классификации кодируются независимо друг от друга определенными разрядами или группой разрядов кодового обозначения. Данный способ кодирования чаще всего используется при фасетной классификации.

- a) Параллельный метод кодирования
- b) Порядковый метод кодирования
- c) Последовательный метод кодирования
- d) Серийно-порядковый метод кодирования

11. Выберите правильное соответствие для методов классификации:

a) Метод классификации, при котором язык описания информационных объектов приближается к естественному языку. Предполагает предварительный отбор совокупности ключевых слов или словосочетаний, описывающих определенную предметную область или совокупность однородных объектов. Выбранные ключевые слова и словосочетания подвергаются нормализации, т.е. из совокупности синонимов выбирается один или несколько наиболее употребимых.

b) Основным преимуществом метода классификации является гибкость структуры ее построения. Изменения в любом из наборов значений признака не оказывают существенного влияния на все остальные. Большая гибкость обуславливает хорошую адаптируемость построенной системы классификации к характеру решаемых задач. Имеется возможность агрегации объектов и осуществления информационного поиска по любому сочетанию фасетов. Недостатками метода классификации являются неполное использование емкости, нетрадиционность и возможная сложность применения.

c) Основными преимуществами метода являются большая информационная емкость, традиционность и привычность применения. Значительным недостатком метода классификации является слабая гибкость структуры, обусловленная фиксированным основанием деления и заранее установленным порядком следования, не допускающим включение новых объектов и классификационных группировок. Таким образом, при изменении состава объектов классификации и характеристик с помощью классификационных задач, требуется коренная перестройка всей классификационной схемы.

- a) Deskрипторный метод классификации
- b) Иерархический метод классификации
- c) Фасетный метод классификации

12. Выберите правильное соответствие:

a) Цифровой сигнал представляется последовательностью двоично-закодированных отсчетов исходного аналогового сигнала.

b) В двоичном виде кодируется только разность между предсказанным значением (на основе предшествующих отсчетов) и фактически измеренным значением отсчета аналогового сигнала.

c) Шаг квантования выбирается в зависимости от скорости изменения формы аналогового сигнала.

d) В цифровом виде представляется разность величин последовательных отсчетов сигнала, частота дискретизации выбирается значительно выше минимально необходимой (по т. Котельникова-Найквиста).

- a) адаптивная дифференциальная импульсно-кодовая модуляция
- b) дельта-модуляция
- c) дифференциальная импульсно-кодовая модуляция
- d) импульсно-кодовая модуляция

13. Выберите из приведенного ниже списка неверные утверждения относительно процесса

дискретизации сигнала:

- a) Частота дискретизации сигнала определяется по теореме Котельникова-Найквиста.
- b) Частота дискретизации сигнала выбирается равной удвоенной минимальной частоте в спектре сигнала.
- c) Частота дискретизации сигнала выбирается равной удвоенной максимальной частоте в спектре сигнала.
- d) Дискретизация применяется к аналоговым сигналам.
- e) В результате дискретизации формируется аналоговый сигнал.
- f) В результате дискретизации формируется конечная последовательность отсчетов аналогового сигнала.

14. Помехоустойчивое кодирование сообщений в канале связи с шумом:

- a) Увеличивает избыточность кода.
- b) Уменьшает избыточность кода.
- c) Не влияет на избыточность кода.
- d) Непредсказуемо влияет на избыточность кода.

15. Что такое префиксный код?

- a) Это код фиксированной длины.
- b) Это код, в котором никакое кодовое слово не совпадает с начальной частью какого-то другого кодового слова.
- c) Это код, в котором никакое кодовое слово не совпадает с завершением какого-то другого кодового слова.

16. Для чего он необходим префиксный код?

- a) Он позволяет любое слово, составленное из кодовых слов переменной длины, декодировать только единственным способом.
- b) Он позволяет уменьшить среднюю длину кода, необходимого для кодирования сообщений источника.
- c) Он упрощает процесс кодирования сообщений источника.

17. Какой из кодовых наборов обладает свойством префиксности?

- a) 101010; 101; 10001; 1100
- b) 101110; 1010; 10001; 1100
- c) 10; 101; 10001; 1100
- d) 10111; 1010; 100; 1101

18. Какой алгоритм используется для построения префиксного кода?

- a) Хэмминга.
- b) Хаффмана.
- c) Шеннона-Фано.
- d) Тьюринга.

19. Каким образом количество проверочных разрядов корректирующего кода Хэмминга (для исправления однократных ошибок), зависит от числа информационных разрядов?

- a) Линейно.
- b) Логарифмически.
- c) Полиномиально.
- d) Выбирается произвольно.
- e) Обрато пропорционально.

20. В каких единицах измеряется пропускная способность аналоговых каналов передачи информации?

- a) Гц.

- b) Бит/с.
- c) Является безразмерной величиной.
- d) Байт.

21. Выберите правильное значение расстояния Хэмминга для следующего двоичного кодового набора:

0101100000010001101  
0010011110110101000  
1110010010001010011  
1001111101001110100

- a) 12
- b) 11
- c) 10
- d) 13
- e) 14

22. Выберите правильные утверждения, относящиеся к спектральному представлению сигналов в канале передачи информации:

- a) Спектр — это коэффициенты разложения сигнала в базисе ортогональных функций.
- b) Спектр - это разноцветная полоса, получающаяся при прохождении светового излучения через стеклянную призму или диффракционную решетку.
- c) Спектр отображает частотный состав сигнала.
- d) Спектральное представление сигнала отображает зависимость амплитуды сигнала от времени
- e) Спектральное представление сигнала отображает зависимость частоты сигнала от времени.

23. Выберите правильные утверждения, которые относятся к теореме Котельникова-Найквиста:

- a) Теорема доказывает принципиальную необратимость преобразования сигнала при его дискретизации.
- b) Теорема утверждает о возможности точного восстановления аналогового сигнала из его дискретных отсчетов.
- c) В теореме не приводятся указания на то, каким именно образом по дискретным отсчетам можно получить исходный аналоговый сигнал.
- d) В теореме вообще не рассматривается представление сигнала в частотной области.
- e) В теореме указывается, как рассчитывать частоту дискретизации сигнала.

24. В соответствии с теоремой Котельникова-Найквиста:

- a) Частота дискретизации не может быть определена, исходя из спектрального состава сигнала.
- b) Частота дискретизации должна быть как минимум в два раза выше максимальной частоты в спектре сигнала.
- c) Частота дискретизации выбирается по усмотрению пользователя.
- d) Частота дискретизации должна быть как минимум в два раза ниже максимальной частоты в спектре сигнала.
- e) Частота дискретизации должна быть такой же, как частота сигнала.

25. Выберите правильные утверждения, относящиеся к первой теореме Шеннона:

- a) В теореме рассматривается передача сообщений в канале без шума.
- b) В теореме рассматривается передача сообщений в канале с шумом.
- c) В теореме определяется формула для оценки пропускной способности канала.
- d) В теореме определяется соотношение между средней длиной кода и энтропией.
- e) В теореме, по-сути, предлагается подход к уменьшению избыточности кодирования сообщений источника (вплоть до нуля).

26. Выберите неправильные утверждения относительно второй теоремы Шеннона:

- a) В теореме рассматривается передача сообщений в канале без шума.

- b) В теореме рассматривается передача сообщений в канале с шумом.
  - c) В теореме определяется формула для оценки пропускной способности канала.
  - d) Теорема определяет условие, при котором сообщения источника будут передаваться через канал связи сколь угодно высокой точностью.
  - e) В теореме, по-сути, предлагается подход к уменьшению избыточности кодирования сообщений источника (вплоть до нуля).
27. Согласно второй теореме Шеннона пропускная способность канала связи зависит от:
- a) Избыточности кода передаваемых сообщений.
  - b) Отношения сигнал-шум.
  - c) Размера алфавита источника.
  - d) Скорости передачи данных источником.
  - e) Ширины полосы пропускания канала связи.
28. Расположите форматы кодирования цифровых сигналов в порядке убывания разрядности кодирования отсчетов:
- a) АДИКМ
  - b) Дельта-модуляция
  - c) ДИКМ
  - d) ИКМ
29. Выберите правильное соответствие:
- a) Отображает формально-структурные характеристики информации и не затрагивает ее смыслового содержания.
  - b) Способствует восприятию внешних структурных характеристик сообщений.
  - c) Определяет степень соответствия образа объекта и самого объекта.
  - d) Предполагает учет смыслового содержания информации.
  - e) Отражает отношение информации и ее потребителя.
  - f) Непосредственно связана с практическим использованием информации, с соответствием ее целевой функции деятельности системы.
- a) Прагматическая адекватность
  - b) Прагматическая адекватность
  - c) Семантическая адекватность
  - d) Семантическая адекватность
  - e) Синтаксическая адекватность
  - f) Синтаксическая адекватность
30. Выберите правильное соответствие:
- a) Измеряется значением единицы младшего разряда числа.
  - b) Определяется значением единицы последнего разряда числа, верность которого гарантируется.
  - c) Определяется функциональным назначением информационного показателя.
- a) Необходимая точность
  - b) Реальная точность
  - c) Формальная точность
31. Выберите правильное соответствие:
- a) Необработанный материал, предоставляемый поставщиками и используемый потребителями для формирования полезных сведений на их основе.
  - b) Любые, неизвестные ранее сведения о каком-либо событии, сущности, процессе и т.п., являющиеся объектом некоторых операций, для которых существует содержательная интерпретация.
  - c) Совокупность фактов, закономерностей и эвристических правил, с помощью которых решается

поставленная задача.

- a) Данные
- b) Знания
- c) Информация

32. Выберите правильное соответствие:

- a) Связана с правильностью ее отбора и формирования в целях адекватного отражения свойств объекта.
- b) Отражает семантическую емкость, равную отношению количества семантической информации в сообщении к объему обрабатываемых данных.
- c) Означает, что она содержит минимальный, но достаточный для принятия правильного решения состав (набор показателей).
- d) Достигается путем согласования семантической формы информации с тезаурусом пользователя.
- e) Означает ее поступление не позже заранее назначенного момента времени, согласованного с временем решения поставленной задачи.
- f) Определяется степенью близости получаемой информации к реальному состоянию объекта, процесса, явления и т.п.
- g) Определяется свойством информации отражать реально существующие объекты с необходимой точностью.
- h) Отражает способность информации реагировать на изменения исходных данных без нарушения необходимой точности.
- i) Определяется степенью сохранения ценности информации для управления в момент ее использования

- a) Актуальность информации
- b) Достаточность информации
- c) Достоверность информации
- d) Доступность информации
- e) Репрезентативность информации
- f) Своевременность информации
- g) Содержательность информации
- h) Точность информации
- i) Устойчивость информации

33. Выберите правильное соответствие для методов классификации:

- a) Метод классификации, при котором язык описания информационных объектов приближается к естественному языку. Предполагает предварительный отбор совокупности ключевых слов или словосочетаний, описывающих определенную предметную область или совокупность однородных объектов. Выбранные ключевые слова и словосочетания подвергаются нормализации, т.е. из совокупности синонимов выбирается один или несколько наиболее употребимых.
- b) Основным преимуществом метода классификации является гибкость структуры ее построения. Изменения в любом из наборов значений признака не оказывают существенного влияния на все остальные. Большая гибкость обуславливает хорошую адаптируемость построенной системы классификации к характеру решаемых задач. Имеется возможность агрегации объектов и осуществления информационного поиска по любому сочетанию фасетов. Недостатками метода классификации являются неполное использование емкости, нетрадиционность и возможная сложность применения.
- c) Основными преимуществами метода являются большая информационная емкость, традиционность и привычность применения. Значительным недостатком методы классификации является слабая гибкость структуры, обусловленная фиксированным основанием деления и заранее установленным порядком следования, не допускающим включение новых объектов и

классификационных группировок. Таким образом, при изменении состава объектов классификации и характеристик с помощью классификационных задач, требуется коренная перестройка всей классификационной схемы.

- a) Deskрипторный метод классификации
- b) Иерархический метод классификации
- c) Фасетный метод классификации

34. Какие задачи относятся к интеллектуальным?

- a) Решение системы линейных алгебраических уравнений.
- b) Численное интегрирование.
- c) Распознавание образов.
- d) Доказательство теорем.
- e) Автоматический перевод естественно-языковых сообщений.

35. Выберите варианты, которые соответствуют определению понятия через интенционал:

- a) Бинобль - это оптический прибор.
- b) Телевизор - это электронный прибор для отображения аудио-визуальной информации, принимаемой в виде телевизионного сигнала.
- c) Велосипед имеет 2-3 колеса, педали, руль. Предназначен для передвижения по твердой поверхности.
- d) Вертолет - это транспортное средство.
- e) Холодильник - устройство, поддерживающее низкую температуру в теплоизолированной камере.
- f) Микрофон — это электроакустический прибор.
- g) Нож используется как колющий (рубящий, режущий) инструмент. Рабочей частью ножа является клинок с лезвием на одной или нескольких сторонах. В конструкции ножа можно выделить клинок и рукоять.
- h) Смартфон - это HTC Wildfire, Huawei P Smart, Samsung Galaxy, LG V60, Philips Xenium, Apple iPhone.
- i) Автомобиль - это седан, лимузин, фургон, микроавтобус, грузовик, автобус.
- j) Стиральная машина имеет вращающийся вал с лопастями или диск, обеспечивающий перемешивание при стирке. Основа конструкции стиральной машины является емкость из нержавеющей стали или пластмассы. По способу загрузки бывают вертикальные и фронтальные.
- k) Фонарь — переносной или стационарный искусственный источник света, предназначенный для освещения отдельных участков пространства в темное время суток.

36. Выберите варианты, которые соответствуют определению понятия через экстенционал:

- a) Танк — бронированная боевая машина, чаще всего на гусеничном ходу, как правило с пушечным и дополнительным пулемётным вооружением, обычно во вращающейся полноповоротной башне, предназначенной в основном для стрельбы прямой наводкой.
- b) Будильник — часы, подающие звуковой, световой и т.п. сигнал в заранее установленный момент времени.
- c) Самолет - тяжелее воздуха, но может летать в атмосфере, имеет неподвижные крылья и двигатель. Самолеты бывают военные, пассажирские, транспортные, почтовые, спортивные, учебно-тренировочные и др.
- d) Сказка — один из жанров фольклора, либо литературы.
- e) Тигр — вид хищных млекопитающих семейства кошачьих, один из пяти представителей рода пантера, который относится к подсемейству больших кошек.
- f) Колонка — устройство для воспроизведения звука.
- g) Вилка состоит из рукояти и нескольких узких зубцов (обычно от двух до четырёх) на одном конце. По правилам этикета, при приеме пищи вилку обычно держат левой рукой.
- h) Фотоаппарат - это CANON EOS, Sony Alpha, NIKON D5600, Fujifilm X-T200.

- i) Автомобиль - это седан, лимузин, фургон, микроавтобус, грузовик, автобус.
- j) Стиральная машина имеет вращающийся вал с лопастями или диск, обеспечивающий перемешивание при стирке. Основа конструкции стиральной машины является емкость из нержавеющей стали или пластмассы. По способу загрузки бывают вертикальные и фронтальные.
- k) Фонарь — переносной или стационарный искусственный источник света, предназначенный для освещения отдельных участков пространства в темное время суток.
- l) Микроволновка — это электроприбор, позволяющий совершать разогрев водосодержащих веществ благодаря электромагнитному излучению дециметрового диапазона.

37. Выберите утверждения, описывающие направления в моделировании ИИ:

- a) Целью является воспроизведение интеллектуальной деятельности с помощью вычислительных машин.
- b) Объектом являются структура и механизмы работы мозга человека, а конечная цель заключается в раскрытии тайн мышления.
- c) Ориентируется на создание смешанных человеко-машинных, или интерактивных интеллектуальных систем, на симбиоз возможностей естественного и искусственного интеллекта.
- d) Попытка построения ИИ путем моделирования структуры человеческого мозга.
- e) Основное внимание уделяется построению начальной модели, и правилам, по которым она может изменяться (эволюционировать).
- f) В центре находится понятие "черного ящика" — устройства, т.е. программного модуля или набора данных, информация о внутренней структуре и содержании которых отсутствуют полностью, но известны спецификации входных и выходных данных. Не важно, что у него внутри и как он функционирует, главное, чтобы модель в аналогичных ситуациях вела себя точно так же.

Вопросы с кратким (вычисляемым) ответом - 1 балл за каждый правильный тест (максимум)

Компетенция ОПК-2

1. Запишите в десятичном виде результате сложения двух двоичных 9-разрядных целых чисел со знаком:

101110111

110010010

Компетенция ОПК-10

2. Вычислите пропускную способность канала связи, если  $f_m = 11000$  Гц, а  $N_s/N_r = 28$ .

3. Оцените количество уровней шкалы восприятия, если безразмерная величина  $k = 0.003$ , а  $S_{max}/S_{min} = 104$ . Результат привести с точностью до 2 знаков после запятой.

Вопросы с развернутым ответом

Критерии оценивания развернутого ответа:

В зависимости от степени полноты ответа на вопрос максимально можно получить за развернутый ответ на вопрос 3 балла.

Компетенция ОПК-3

1) Объясните разницу между симметричными и асимметричными криптосистемами. На чем основана криптостойкость таких систем?

2) Какими параметрами описываются алгоритмы? Какие показатели используются для оценки эффективности алгоритмов?

3) В чем заключается разница между полиномиальными и экспоненциальными алгоритмами? Какой практический смысл имеет это различие?

4) Дайте определение функции временной сложности алгоритма. Какое практическое значение имеет функция временной сложности? В каких единицах измеряются значения данной функции?

Компетенция ОПК-10

5) Опишите алгоритм Хаффмана по шагам. Какую задачу решает данный алгоритм и что является

его результатом?

- 6) Опишите процесс аналогово-цифрового преобразования (АЦП) сигналов. Что представляет собой результат АЦП?
- 7) Какие принципиальные проблемы компьютерных технологий решает аналогово-цифровое преобразование?
- 8) Опишите процесс дискретизации аналоговых сигналов. От чего зависит выбор интервала дискретизации?
- 9) Какую роль играет избыточность в задачах сжатия, помехоустойчивого кодирования и шифрации данных?
- 10) Опишите процесс квантования аналоговых сигналов. На что влияет выбор шага квантования?
- 11) Сформулируйте теорему Котельникова-Найквиста. Какой практический смысл имеет данная теорема?
- 12) Сформулируйте теорему Шеннона для канала передачи сообщений без шума. Какой практический смысл имеет данная теорема?
- 13) Сформулируйте теорему Шеннона для канала передачи сообщений с шумом. Какой практический смысл имеет данная теорема?
- 14) Приведите описание структуры системы передачи информации. Опишите назначение компонентов этой системы.
- 15) Опишите содержание теста Тьюринга. Какой практический смысл имеет этот тест?

## 20.2 Промежуточная аттестация

### Форма контрольно-измерительного материала

УТВЕРЖДАЮ

Заведующий кафедрой информационных систем

\_\_\_\_\_  
\_\_\_. \_\_. 20\_\_

Направление подготовки / специальность 10.05.01 Компьютерная безопасность

Дисциплина Информатика

Форма обучения очное

Вид контроля экзамен

Вид аттестации промежуточная

### Контрольно-измерительный материал №1

1. Данные и знания. Экстенционал и интенционал понятия.
2. Алгоритмы Хаффмана и Шеннона.
3. Три обобщенные модели алгоритма. Тезисы Черча и Тьюринга, принцип нормализации Маркова.

Преподаватель \_\_\_\_\_ А.В. Сычев

