ФГБОУ ВО «УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»
БИРСКИЙ ФИЛИАЛ УУНиТ
ФАКУЛЬТЕТ ФИЗИКИ И МАТЕМАТИКИ

Утверждено:
на заседании кафедры информатики и экономики
протокол № 4 от 24.11.2022 г.
Зав. кафедрой *подписано ЭЦП* /Мухаметшина Г.С.

Согласовано:
Председатель УМК
факультета физики и математики
подписано ЭЦП /Бигаева Л.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
для очной формы обучения

Теоретические основы информатики
Обязательная часть

программа бакалавриата

Направление подготовки (специальность)
44.03.05 *Педагогическое образование (с двумя профилями подготовки)*

Направленность (профиль) подготовки
Информатика, физика

Квалификация
Бакалавр

Разработчик (составитель) Старший преподаватель (должность, ученая степень, ученое звание)	*подписано ЭЦП* /Садыкова О.С. (подпись, Фамилия И.О.)

Для приема: 2020,2021 г.

Бирск 2022 г.

Составитель / составители: Садыкова О.С. ____________________

Рабочая программа дисциплины утверждена на заседании кафедры информатики и экономики протокол № ___ от «___» _________ 20__ г.

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» ____________ 20 _ г.

Заведующий кафедрой ___________________/ _____________Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» ____________ 20 _ г.

Заведующий кафедрой ___________________/ _____________Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» ____________ 20 _ г.

Заведующий кафедрой ___________________/ _____________Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» ____________ 20 _ г.

Заведующий кафедрой ___________________/ _____________Ф.И.О/

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

По итогам освоения дисциплины обучающийся должен достичь следующих результатов обучения:

Категория (группа) компетенций (при наличии ОПК)	Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
Научные основы педагогической деятельности	Способен осуществлять педагогическую деятельность на основе специальных научных знаний (ОПК-8);	ОПК-8.1. Знать научные основы педагогической деятельности, предметную область базовых дисциплин и (или) дисциплин, актуальных для освоения основных дисциплин профиля	Знать научные основы педагогической деятельности, предметную область базовых дисциплин и (или) дисциплин, актуальных для освоения основных дисциплин профиля
		ОПК-8.2. Уметь использовать специальные научные знания для осуществления педагогической деятельности	Уметь использовать специальные научные знания для осуществления педагогической деятельности
		ОПК-8.3. Владеть опытом и навыками осуществления педагогической деятельности на основе специальных научных знаний	Владеть опытом и навыками осуществления педагогической деятельности на основе специальных научных знаний
Разработка основных и дополнительных образовательных программ	Способен участвовать в разработке основных и дополнительных образовательных программ, разрабатывать отдельные их компоненты (в том числе с использованием информационно-коммуникационных технологий) (ОПК-2);	ОПК-2.1. Знать требования федеральных государственных образовательных стандартов к структуре и содержанию основной образовательной программы, нормативно-правовую базу, определяющую содержание и структуру дополнительной	Знать требования федеральных государственных образовательных стандартов к структуре и содержанию основной образовательной программы, нормативно-правовую базу, определяющую содержание и структуру дополнительной образовательной

		образовательной программы, возможности и области применения информационно-коммуникационных технологии; знать предметную область дисциплин, необходимых для освоения основных дисциплин профиля	программы, возможности и области применения информационно-коммуникационных технологии; знать предметную область дисциплин, необходимых для освоения основных дисциплин профиля
		ОПК-2.2. Уметь разрабатывать компоненты основных и дополнительных образовательных программ, использовать возможности информационно-коммуникационных технологий для разработки основных и дополнительных образовательных программ, использовать знания предметной области дисциплин для разработки компонентов образовательных программ	Уметь разрабатывать компоненты основных и дополнительных образовательных программ, использовать возможности информационно-коммуникационных технологий для разработки основных и дополнительных образовательных программ, использовать знания предметной области дисциплин для разработки компонентов образовательных программ
		ОПК-2.3. Владеть навыками разработки компонентов основных и дополнительных образовательных программ, использования информационно-коммуникационных технологий для разработки основных и дополнительных образовательных программ	Владеть навыками разработки компонентов основных и дополнительных образовательных программ, использования информационно-коммуникационных технологий для разработки основных и дополнительных образовательных программ
Системное и критическое мышление	Способен осуществлять поиск, критический анализ и	УК-1.1. Знать основы поиска информации в библиографических	Знать основы поиска информации в библиографических

	синтез информации, применять системный подход для решения поставленных задач (УК-1);	источниках и в сети Интернет; основы критического анализа и синтеза информации; основы системного подхода при решении поставленных задач	источниках и в сети Интернет; основы критического анализа и синтеза информации; основы системного подхода при решении поставленных задач
		УК-1.2. Уметь осуществлять поиск информации в библиографических источниках и в сети Интернет; анализировать и синтезировать информацию; применять системный подход для решения поставленных задач	Уметь осуществлять поиск информации в библиографических источниках и в сети Интернет; анализировать и синтезировать информацию; применять системный подход для решения поставленных задач
		УК-1.3. Владеть навыками поиска информации; критического анализа и синтеза информации; применения системного подхода для решения поставленных задач	Владеть навыками поиска информации; критического анализа и синтеза информации; применения системного подхода для решения поставленных задач

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Теоретические основы информатики» относится к обязательной части.

Дисциплина изучается на __2__ курсе в ___4___ семестре.

Цель изучения дисциплины: формирование знаний, умений и навыков в области теоретических основ информатики, необходимых для использования естественнонаучных и математических знаний для ориентирования в современном информационном пространстве и реализации образовательных программы по учебным предметам в соответствии с требованиями образовательных стандартов.

3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)

ФГБОУ ВО «УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»
БИРСКИЙ ФИЛИАЛ УУНиТ
ФАКУЛЬТЕТ ФИЗИКИ И МАТЕМАТИКИ

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины «Теоретические основы информатики» на 4 семестр
очная
форма обучения

Вид работы	**Объем дисциплины**
Общая трудоемкость дисциплины (ЗЕТ / часов)	3/108
Учебных часов на контактную работу с преподавателем:	36.2
лекций	18
практических/ семинарских	18
лабораторных	0
контроль самостоятельной работы (КСР)	0
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) ФКР	0.2
Учебных часов на самостоятельную работу обучающихся (СРС)	71.8
Учебных часов на подготовку к зачету (Контроль)	0

Форма контроля:
Зачет 4 семестр

№ п/п	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Основная и дополнительная литература, рекомендуемая студентам (номера из списка)	Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		Лек	П	Зч	СРС			
2 курс / 4 семестр								
1	Теория информации							
1.1	Исходные понятия информатики. Теория Шеннона. Кодирование символьной информации. Использование естественнонаучных и математических знаний для ориентирования в современном информационном пространстве. Начальные определения. Формы представления информации. Преобразование сообщений. Понятие энтропии. Энтропия и информация. Информация и алфавит. Постановка задачи первичного кодирования. Первая теорема	4	2		12	Осн. лит-ра №№ 1,2 Доп. лит-ра № 1	Доклад	Групповой опрос, Практические работы

	Шеннона. Способы построения двоичных кодов. Использование естественнонаучных и математических знаний для ориентирования в современном информационном пространстве.							
1.2	Представление и обработка чисел в компьютере. Передача информации. Системы счисления. Представление чисел в различных системах счисления. Кодирование чисел в компьютере и действия над ними. Общая схема передачи информации по линии связи. Характеристики дискретного канала связи. Влияние шумов на пропускную способность дискретного канала связи. Передача информации по непрерывному каналу. Способы передачи информации в компьютерных линиях связи.	2	4		12	Осн. лит-ра №№ 1,2 Доп. лит-ра № 1	Домашняя контрольная работа	Практические работы, Групповой опрос
1.3	Обеспечение надежности передачи и хранения информации. Элементы криптографии. Хранение информации. Общие подходы. Принципы построения (n; k)-кодов. Систематический помехоустойчивый код. Код Хемминга. Матричные коды. Основные понятия криптографии. Симметричное шифрование. Шифрование с открытым ключом. Электронная подпись. Классификация данных. Проблемы представления данных. Представление элементарных данных в ОЗУ. Структуры данных и их представление в ОЗУ.	2	2		12	Осн. лит-ра №№ 1,2 Доп. лит-ра № 1	Тестирование	Групповой опрос, Практические работы

	Представление данных на внешних носителях.							
2	Алгоритмы. Модели. Системы							
2.1	Элементы теории алгоритмов. Нестрогое определение алгоритма. Рекурсивные функции. Алгоритм как абстрактная машина. Алгоритмическая машина Поста. Алгоритмическая машина Тьюринга. Нормальные алгоритмы Маркова. Сопоставление алгоритмических моделей. Проблема алгоритмической разрешимости. Сложность алгоритма	4	4		12	Осн. лит-ра №№ 1,2 Доп. лит-ра № 1	Решение задач	Групповой опрос, Практические работы
2.2	Формализация понятия алгоритм. Представления о конечном автомате. Формальные языки. Способы представления алгоритмов. Структурная теорема. Общие подходы к описанию устройств, предназначенных для автоматической обработки дискретной информации. Комбинационные схемы. Конечные автоматы	4	4		12	Осн. лит-ра №№ 1,2 Доп. лит-ра № 1	Решение задач	Групповой опрос, Практические работы
2.3	Модели и системы. Понятие модели. Общая идея моделирования. Классификация моделей. Понятие математической модели. Понятие системы. Определение объекта. Определение системы. Формальная система. Значение формализации. Этапы	2	2		11.8	Доп. лит-ра № 1	Решение задач	Практические работы, Групповой опрос

	решения задачи посредством компьютера. Об объектном подходе в прикладной информатике							
3	Зачет			1	0.2			
Итого по 2 курсу 4 семестру		18	18	1	72			
Итого по дисциплине		18	18	1	72			

4. Фонд оценочных средств по дисциплине

4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине.

Код и формулировка компетенции: Способен участвовать в разработке основных и дополнительных образовательных программ, разрабатывать отдельные их компоненты (в том числе с использованием информационно-коммуникационных технологий) (ОПК-2);

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения (Зачет)	
		Незачтено	Зачтено
ОПК-2.1. Знать требования федеральных государственных образовательных стандартов к структуре и содержанию основной образовательной программы, нормативно-правовую базу, определяющую содержание и структуру дополнительной образовательной программы, возможности и области применения информационно-коммуникационных технологии; знать предметную область дисциплин, необходимых для освоения основных	Знать требования федеральных государственных образовательных стандартов к структуре и содержанию основной образовательной программы, нормативно-правовую базу, определяющую содержание и структуру дополнительной образовательной программы, возможности и области применения информационно-коммуникационных технологии; знать предметную область дисциплин, необходимых для освоения основных	Знания не сформированы	Знания полностью сформированы

дисциплин профиля	дисциплин профиля		
ОПК-2.2. Уметь разрабатывать компоненты основных и дополнительных образовательных программ, использовать возможности информационно-коммуникационных технологий для разработки основных и дополнительных образовательных программ, использовать знания предметной области дисциплин для разработки компонентов образовательных программ	Уметь разрабатывать компоненты основных и дополнительных образовательных программ, использовать возможности информационно-коммуникационных технологий для разработки основных и дополнительных образовательных программ, использовать знания предметной области дисциплин для разработки компонентов образовательных программ	Умения не сформированы	Умения в основном сформированы
ОПК-2.3. Владеть навыками разработки компонентов основных и дополнительных образовательных программ, использования информационно-коммуникационных технологий для разработки основных и	Владеть навыками разработки компонентов основных и дополнительных образовательных программ, использования информационно-коммуникационных технологий для разработки основных и дополнительны	Владение навыками не сформировано	Владение навыками в основном сформировано

дополнительных образовательных программ	х образовательных программ		

Код и формулировка компетенции: Способен осуществлять педагогическую деятельность на основе специальных научных знаний (ОПК-8);

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения (Зачет)	
		Незачтено	Зачтено
ОПК-8.1. Знать научные основы педагогической деятельности, предметную область базовых дисциплин и (или) дисциплин, актуальных для освоения основных дисциплин профиля	Знать научные основы педагогической деятельности, предметную область базовых дисциплин и (или) дисциплин, актуальных для освоения основных дисциплин профиля	Знания не сформированы	Знания полностью сформированы
ОПК-8.2. Уметь использовать специальные научные знания для осуществления педагогической деятельности	Уметь использовать специальные научные знания для осуществления педагогической деятельности	Умения не сформированы	Умения в основном сформированы
ОПК-8.3. Владеть опытом и навыками осуществления педагогической деятельности на основе специальных научных знаний	Владеть опытом и навыками осуществления педагогической деятельности на основе специальных научных знаний	Владение навыками не сформировано	Владение навыками в основном сформировано

Код и формулировка компетенции: Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач (УК-1);

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения (Зачет)	
		Незачтено	Зачтено
УК-1.1. Знать основы поиска информации в библиографических источниках и в сети Интернет; основы критического анализа и синтеза информации; основы системного подхода при решении поставленных задач	Знать основы поиска информации в библиографических источниках и в сети Интернет; основы критического анализа и синтеза информации; основы системного подхода при решении поставленных задач	Знания не сформированы	Знания полностью сформированы
УК-1.2. Уметь осуществлять поиск информации в библиографических источниках и в сети Интернет; анализировать и синтезировать информацию; применять системный подход для решения поставленных задач	Уметь осуществлять поиск информации в библиографических источниках и в сети Интернет; анализировать и синтезировать информацию; применять системный подход для решения поставленных задач	Умения не сформированы	Умения в основном сформированы
УК-1.3. Владеть навыками поиска информации; критического анализа и	Владеть навыками поиска информации; критического анализа и синтеза	Владение навыками не сформировано	Владение навыками в основном сформировано

синтеза информации; применения системного подхода для решения поставленных задач	информации; применения системного подхода для решения поставленных задач		

Критериями оценивания являются баллы, которые выставляются за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины. Баллы, выставляемые за конкретные виды деятельности представлены ниже.

4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине.

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ОПК-2.1. Знать требования федеральных государственных образовательных стандартов к структуре и содержанию основной образовательной программы, нормативно-правовую базу, определяющую содержание и структуру дополнительной образовательной программы, возможности и области применения информационно-коммуникационных технологии; знать предметную область дисциплин, необходимых для освоения основных дисциплин профиля	Знать требования федеральных государственных образовательных стандартов к структуре и содержанию основной образовательной программы, нормативно-правовую базу, определяющую содержание и структуру дополнительной образовательной программы, возможности и области применения информационно-коммуникационных технологии; знать предметную область дисциплин, необходимых для освоения основных дисциплин профиля	Групповой опрос, Тестирование, Практические работы, Доклад
ОПК-2.2. Уметь разрабатывать компоненты основных и дополнительных образовательных программ, использовать возможности информационно-коммуникационных технологий для разработки основных и дополнительных образовательных программ, использовать знания предметной области дисциплин	Уметь разрабатывать компоненты основных и дополнительных образовательных программ, использовать возможности информационно-коммуникационных технологий для разработки основных и дополнительных образовательных программ, использовать знания предметной области дисциплин	Практические работы, Тестирование, Решение задач

для разработки компонентов образовательных программ	для разработки компонентов образовательных программ	
ОПК-2.3. Владеть навыками разработки компонентов основных и дополнительных образовательных программ, использования информационно-коммуникационных технологий для разработки основных и дополнительных образовательных программ	Владеть навыками разработки компонентов основных и дополнительных образовательных программ, использования информационно-коммуникационных технологий для разработки основных и дополнительных образовательных программ	Решение задач, Практические работы
ОПК-8.1. Знать научные основы педагогической деятельности, предметную область базовых дисциплин и (или) дисциплин, актуальных для освоения основных дисциплин профиля	Знать научные основы педагогической деятельности, предметную область базовых дисциплин и (или) дисциплин, актуальных для освоения основных дисциплин профиля	Практические работы, Групповой опрос, Тестирование
ОПК-8.2. Уметь использовать специальные научные знания для осуществления педагогической деятельности	Уметь использовать специальные научные знания для осуществления педагогической деятельности	Решение задач, Практические работы
ОПК-8.3. Владеть опытом и навыками осуществления педагогической деятельности на основе специальных научных знаний	Владеть опытом и навыками осуществления педагогической деятельности на основе специальных научных знаний	Практические работы, Решение задач
УК-1.1. Знать основы поиска информации в библиографических источниках и в сети Интернет; основы критического анализа и синтеза информации; основы системного подхода при решении поставленных задач	Знать основы поиска информации в библиографических источниках и в сети Интернет; основы критического анализа и синтеза информации; основы системного подхода при решении поставленных задач	Доклад, Практические работы, Групповой опрос, Тестирование
УК-1.2. Уметь осуществлять поиск информации в библиографических источниках и в сети Интернет; анализировать и синтезировать информацию; применять системный подход для решения поставленных задач	Уметь осуществлять поиск информации в библиографических источниках и в сети Интернет; анализировать и синтезировать информацию; применять системный подход для решения поставленных задач	Домашняя контрольная работа, Доклад, Тестирование, Решение задач, Практические работы
УК-1.3. Владеть навыками поиска информации; критического анализа и синтеза информации; применения системного подхода для	Владеть навыками поиска информации; критического анализа и синтеза информации; применения системного подхода для решения	Решение задач, Практические работы, Домашняя контрольная работа

решения поставленных задач	поставленных задач	

Критериями оценивания при модульно-рейтинговой системе являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины

для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

для зачета:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),

не зачтено – от 0 до 59 рейтинговых баллов.

Тестовые задания

Описание тестовых заданий: тестовые задания включают тесты закрытого типа (с одним правильным ответом), тесты на установлении последовательности и на установление соответствия. Оценка за выполнение тестовых заданий выставляется на основании процента заданий, выполненных студентами в процессе прохождения промежуточного и рубежного контроля знаний

Тестирование проводиться для получения сведений об усвоенности материала.

1. Кем была предложена первая практическая реализация криптографии с открытым ключом?

А) Уитфилдом Диффи (Whitfield Diffie) и Мартином Хеллманом (Martin Hellman) и Ральфом Мерклем (Ralf Merkle);

Б) Рональдом Райвистом (Ronald Rivest), Ади Шамиром (Adi Shamir) и Леонардом Адлеманом (Leonard Adleman);

В) Шафи Гольдвассером (Shafi Goldwasser) и Сильвио Микэли (Silvio Micali).

2. Как называются используемые в криптографии модели открытого текста, учитывающие зависимость букв текста от предыдущих букв?

А) позначные модели открытого текста;

Б) вероятностные модели k -го приближения;

В) Марковские модели открытых текстов.

3. В чем состоит принципиальное отличие нового стандарта ГОСТ Р 34.10–2001 на алгоритм формирования и проверки ЭЦП от старого ГОСТ Р 34.10–94?

А) все специфицированные в ГОСТ Р 34.10–2001 вычисления исполняются в группе элементов конечного поля Fp;

Б) все специфицированные в ГОСТ Р 34.10–2001 вычисления исполняются в группе точек эллиптической кривой, определенной над конечным полем Fp;

В) оба ответа верны.

4. В чем состоит основной принцип Керкгоффса?

А) компрометация системы не должна причинять неудобств корреспондентам;

Б) необходимо, чтобы криптосистема была простой в использовании, и её применение не требовало соблюдения длинного списка правил;

В) у корреспондентов должна быть возможность по собственной воле менять ключ.

5. Что понимается под криптографическим протоколом?

А) алгоритм шифрования данных перед передачей по общедоступному каналу связи;

Б) распределенный алгоритм решения двумя или более участниками некоторой криптографической задачи;

В) набор правил шифрования и расшифрования криптосистемы.

6. В чем состоит криптографическая задача обеспечения целостности?

А) гарантирование невозможности внесения случайных ошибок в процессе передачи по каналам связи;

Б) гарантирование невозможности несанкционированного изменения информации;
В) оба ответа верны.
7. Какие методы разрабатываются с целью обеспечения аутентификации?
А) методы подтверждения подлинности сторон и самой информации в процессе информационного взаимодействия;
Б) методы присвоения уникального идентификатора взаимодействующим сторонам и самой информации в процессе информационного взаимодействия;
В) оба ответа верны.
9. Какой механизм используется для обеспечения невозможности отказа от авторства или приписывания авторства?
А) механизм симметричного шифрования с привлечением арбитра;
Б) механизм цифровой подписи;
В) оба ответа верны.
9. С чем связана активная атака на зашифрованную информацию?
А) с прослушиванием, анализом трафика, перехватом, записью передаваемых шифрованных сообщений;
Б) с дешифрованием, т. е. попытками "взломать" защиту с целью овладения информацией;
В) с прерыванием процесса передачи сообщений, созданием поддельных сообщений, модификацией передаваемых сообщений.
11. От чего зависит выбор способа шифрования?
А) от особенностей передаваемой информации (ее ценности, объема, способа представления, необходимой скорости передачи;
Б) от возможностей владельцев по защите своей информации (стоимость применяемых технических устройств, удобство использования, надежность функционирования;
В) оба ответа верны.
12. Для обнаружения целенаправленного навязывания противником ложной информации
А) в передаваемой информации стирается избыточность;
Б) в передаваемую информацию вносится избыточность;
В) используется код четности.
13. Как называется числовая комбинация, используемая для проверки целостности?
А) имитовставка;
Б) код аутентификации сообщения;
В) оба ответа верны.
14. Какие требования предъявляются к ключевым хэш-функциям hk(M)=S?
А) невозможность вычисления значения hk(M) = Sдля заданного сообщения Мбез знания ключа k;
Б) невозможность подбора для заданного сообщения M с известным значением hk (M) = Sдругого сообщения M1, с известным значением hk (M1) = S1 без знания ключak;
В) оба ответа верны.
15. Какое требование направлено против создания поддельных (сфабрикованных) сообщений при атаках типа имитация?
А) невозможность вычисления значения hk(M) = Sдля заданного сообщения M без знания ключа k;
Б) невозможность подбора для заданного сообщения M с известным значением hk (M) = Sдругого сообщения M1, с известным значением hk (M1) = S1 без знания ключak;
В) оба ответа верны.
16. Какое требование направлено против модификации передаваемых сообщений при атаках типа подмена?
А) невозможность вычисления значения hk(M) = Sдля заданного сообщения Мбез знания ключа k;
Б) невозможность подбора для заданного сообщения M с известным значением hk (M) = Sдругого сообщения M1, с известным значением hk (M1) = S1 без знания ключak;
Тест с ответами: “Криптография”
1. Что такое шифрование?

а) способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого+
б) совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств
в) удобная среда для вычисления конечного пользователя

2. Что такое кодирование?
а) преобразование обычного, понятного текста в код+
б) преобразование
в) написание программы

3. Для восстановления защитного текста требуется:
а) ключ
б) матрица
в) вектор

4. Сколько лет назад появилось шифрование?
а) четыре тысячи лет назад+
б) две тысячи лет назад
в) пять тысяч лет назад

5. Первое известное применение шифра:
а) египетский текст+
б) русский
в) нет правильного ответа

6. Секретная информация, которая хранится вWindows:
а) пароли для доступа к сетевым ресурсам+
б) пароли для доступа в Интернет+
в) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере+

7. Что такое алфавит?
а) конечное множество используемых для кодирования информации знаков+
б) буквы текста
в) нет правильного ответа

8. Что такое текст?
а) упорядоченный набор из элементов алфавита+
б) конечное множество используемых для кодирования информации знаков
в) все правильные

9. Выберите примеры алфавитов:
а) Z256 – символы, входящие в стандартные коды ASCII и КОИ-8+
б) восьмеричный и шестнадцатеричный алфавиты+
в) AEE

10. Что такое шифрование?
а) преобразовательный процесс исходного текста в зашифрованный+
б) упорядоченный набор из элементов алфавита
в) нет правильного ответа

11. Что такое дешифрование?

а) на основе ключа шифрованный текст преобразуется в исходный+
б) пароли для доступа к сетевым ресурсам
в) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере

12. Что представляет собой криптографическая система?
а) семейство T преобразований открытого текста, члены его семейства индексируются символом k+
б) программу
в) систему

13. Что такое пространство ключей k?
а) набор возможных значений ключа+
б) длина ключа
в) нет правильного ответа

14. На какие виды подразделяют криптосистемы?
а) симметричные+
б) ассиметричные+
в) с открытым ключом+

15. Количество используемых ключей в симметричных криптосистемах для шифрования и дешифрования:
а) 1+
б) 2
в) 3

16. Количество используемых ключей в системах с открытым ключом:
а) 2+
б) 3
в) 1

17. Ключи, используемые в системах с открытым ключом:
а) открытый+
б) закрытый+
в) нет правильного ответа

18. Выберите то, как связаны ключи друг с другом в системе с открытым ключом:
а) математически+
б) логически
в) алгоритмически

19. Что принято называть электронной подписью?
а) присоединяемое к тексту его криптографическое преобразование+
б) текст
в) зашифрованный текст

20. Что такое криптостойкость?
а) характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа+
б) свойство гаммы
в) все ответы верны

21. Выберите то, что относится к показателям криптостойкости:

а) количество всех возможных ключей+
б) среднее время, необходимое для криптоанализа+
в) количество символов в ключе

Еще: Обязанности ТСЖ перед жильцами дома
22. Требования, предъявляемые к современным криптографическим системам защиты информации:
а) знание алгоритма шифрования не должно влиять на надежность защиты+
б) структурные элементы алгоритма шифрования должны быть неизменными+
в) не должно быть простых и легко устанавливаемых зависимостью между ключами +последовательно используемыми в процессе шифрования+

23. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:
а) длина шифрованного текста должна быть равной лине исходного текста+
б) зашифрованное сообщение должно поддаваться чтению только при наличии ключа+
в) нет правильного ответа

24. Основными современными методами шифрования являются:
а) алгоритм гаммирования+
б) алгоритмы сложных математических преобразований+
в) алгоритм перестановки+

25. Чем являются символы исходного текста, складывающиеся с символами некой случайной последовательности?
а) алгоритмом гаммирования+
б) алгоритмом перестановки
в) алгоритмом аналитических преобразований

26. Чем являются символы оригинального текста, меняющиеся местами по определенному принципу, которые являются секретным ключом?
а) алгоритм перестановки+
б) алгоритм подстановки
в) алгоритм гаммирования

27. Самая простая разновидность подстановки:
а) простая замена+
б) перестановка
в) простая перестановка

28. Количество последовательностей, из которых состоит расшифровка текста по таблице Вижинера:
а) 3+
б) 4
в) 5

29. Таблицы Вижинера, применяемые для повышения стойкости шифрования:
а) во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке+
б) в качестве ключа используется случайность последовательных чисел+
в) нет правильного ответа

30. Суть метода перестановки:

а) символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов+
б) замена алфавита
в) все правильные

31. Цель криптоанализа:
а) Определение стойкости алгоритма+
б) Увеличение количества функций замещения в криптографическом алгоритме
в) Уменьшение количества функций подстановок в криптографическом алгоритме
г) Определение использованных перестановок

32. По какой причине произойдет рост частоты применения брутфорс-атак?
а) Возросло используемое в алгоритмах количество перестановок и замещений
б) Алгоритмы по мере повышения стойкости становились менее сложными и более подверженными атакам
в) Мощность и скорость работы процессоров возросла+
г) Длина ключа со временем уменьшилась

33. Не будет являться свойством или характеристикой односторонней функции хэширования:
а) Она преобразует сообщение произвольной длины в значение фиксированной длины
б) Имея значение дайджеста сообщения, невозможно получить само сообщение
в) Получение одинакового дайджеста из двух различных сообщений невозможно, либо случается крайне редко
г) Она преобразует сообщение фиксированной длины в значение переменной длины+

34. Выберите то, что указывает на изменение сообщения:
а) Изменился открытый ключ
б) Изменился закрытый ключ
в) Изменился дайджест сообщения+
г) Сообщение было правильно зашифровано

35. Алгоритм американского правительства, который предназначен для создания безопасных дайджестов сообщений:
а) Data Encryption Algorithm
б) Digital Signature Standard
в) Secure Hash Algorithm+
г) Data Signature Algorithm

36. Выберите то, что лучшеописывает отличия между HMAC и CBC-MAC?
а) HMAC создает дайджест сообщения и применяется для контроля целостности; CBC-MAC используется для шифрования блоков данных с целью обеспечения конфиденциальности
б) HMAC использует симметричный ключ и алгоритм хэширования; CBC-MAC использует первый блок в качестве контрольной суммы
в) HMAC обеспечивает контроль целостности и аутентификацию источника данных; CBC-MAC использует блочный шифр в процессе создания MAC+
г) HMAC зашифровывает сообщение на симметричном ключе, а затем передает результат в алгоритм хэширования; CBC-MAC зашифровывает все сообщение целиком

37. Определите преимущество RSA над DSA?
а) Он может обеспечить функциональность цифровой подписи и шифрования+
б) Он использует меньше ресурсов и выполняет шифрование быстрее, поскольку использует симметричные ключи

в) Это блочный шифр и он лучше поточного
г) Он использует одноразовые шифровальные блокноты

38. С какой целью многими странами происходит ограничение использования и экспорта криптографических систем?
а) Без ограничений может возникнуть большое число проблем совместимости при попытке использовать различные алгоритмы в различных программах
б) Эти системы могут использоваться некоторыми странами против их местного населения
в) Криминальные элементы могут использовать шифрование, чтобы избежать обнаружения и преследования+
г) Законодательство сильно отстает, а создание новых типов шифрования еще больше усиливает эту проблему

39. Выберите то, что используют для создания цифровой подписи:
а) Закрытый ключ получателя
б) Открытый ключ отправителя
в) Закрытый ключ отправителя+
г) Открытый ключ получателя

40. Выберите то, что лучше всего описывает цифровую подпись:
а) Это метод переноса собственноручной подписи на электронный документ
б) Это метод шифрования конфиденциальной информации
в) Это метод, обеспечивающий электронную подпись и шифрование
г) Это метод, позволяющий получателю сообщения проверить его источник и убедиться в целостности сообщения+

Методические материалы, определяющие процедуру оценивания выполнения тестовых заданий

Описание методики оценивания выполнения тестовых заданий: оценка за выполнение тестовых заданий ставится на основании подсчета процента правильно выполненных тестовых заданий.
Критерии оценки (в баллах)*:*
- **9-10** баллов выставляется студенту, если процент правильно выполненных тестовых заданий составляет 81 – 100 %;
- **7-8** баллов выставляется студенту, если процент правильно выполненных тестовых заданий составляет 61 – 80 %;
- **4-6** баллов выставляется студенту, если процент правильно выполненных тестовых заданий составляет 41 – 60 %;
- **до 4** баллов выставляется студенту, если процент правильно выполненных тестовых заданий составляет 40 %;

Решение задач

Решение задач способствует формированию умений и навыков относящихся к конкретной сфере деятельности
Примерные задачи по теме "Машина Поста"
Задача No1
Дано N массивов меток. После последнего массива на расстоянии более трёх пустых ячеек находится одна метка. Массивы разделены тремя пустыми ячейками. Количество меток в массиве >=2. Если количество меток в массиве кратно трём, то стереть метки в этом массиве через одну, в противном случае стереть весь массив. Каретка находится над крайней левой меткой первого массива.
Задача No2

Дан массив меток. Каретка располагается где - то над массивом, но не над крайними метками. Стереть все метки, кроме крайних, и поставить каретку в исходное положение.

Задача No3

Составить программу нахождения разности двух целых неотрицательных чисел a и b. Если a меньше b, то перед разностью через одну пустую ячейку поставить метку. Каретка находится над крайней левой меткой левого числа.

Задача No4

Произвести умножение двух чисел. Каретка располагается над пустой ячейкой, которая разделяет данные массивы.

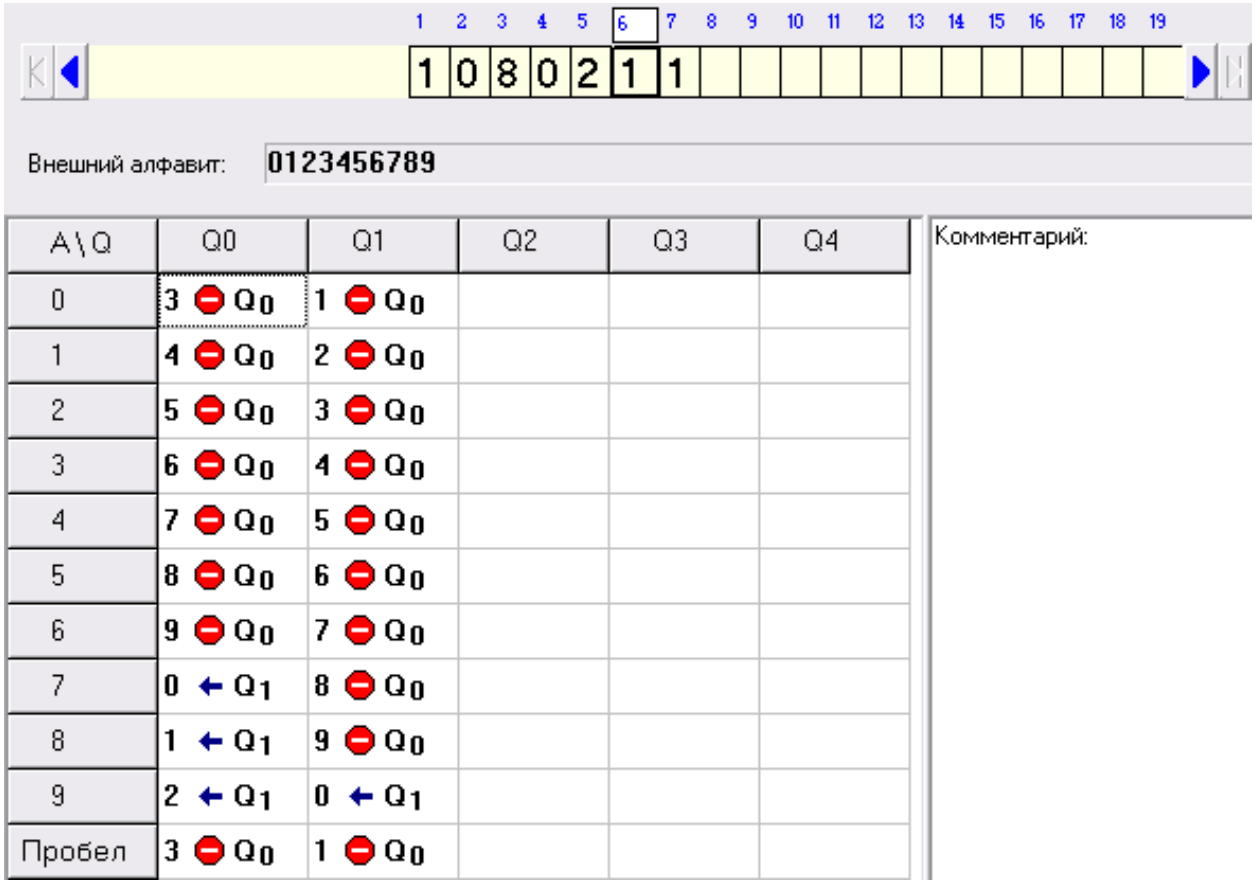
Задача No5

Дан массив из N Меток. Сделать из него массив, в котором будет 2N+1 меток. Если полученный массив делится нацело на 3, то справа от него, через одну пустую ячейку, поставить две метки; если нет -то три метки. Каретка находится над крайней левой меткой.

Примерные задачи по тема "Машина Тьюринга"

Написать программу на машине Тьюринга, прибавляющую число 2 к введенному числу.

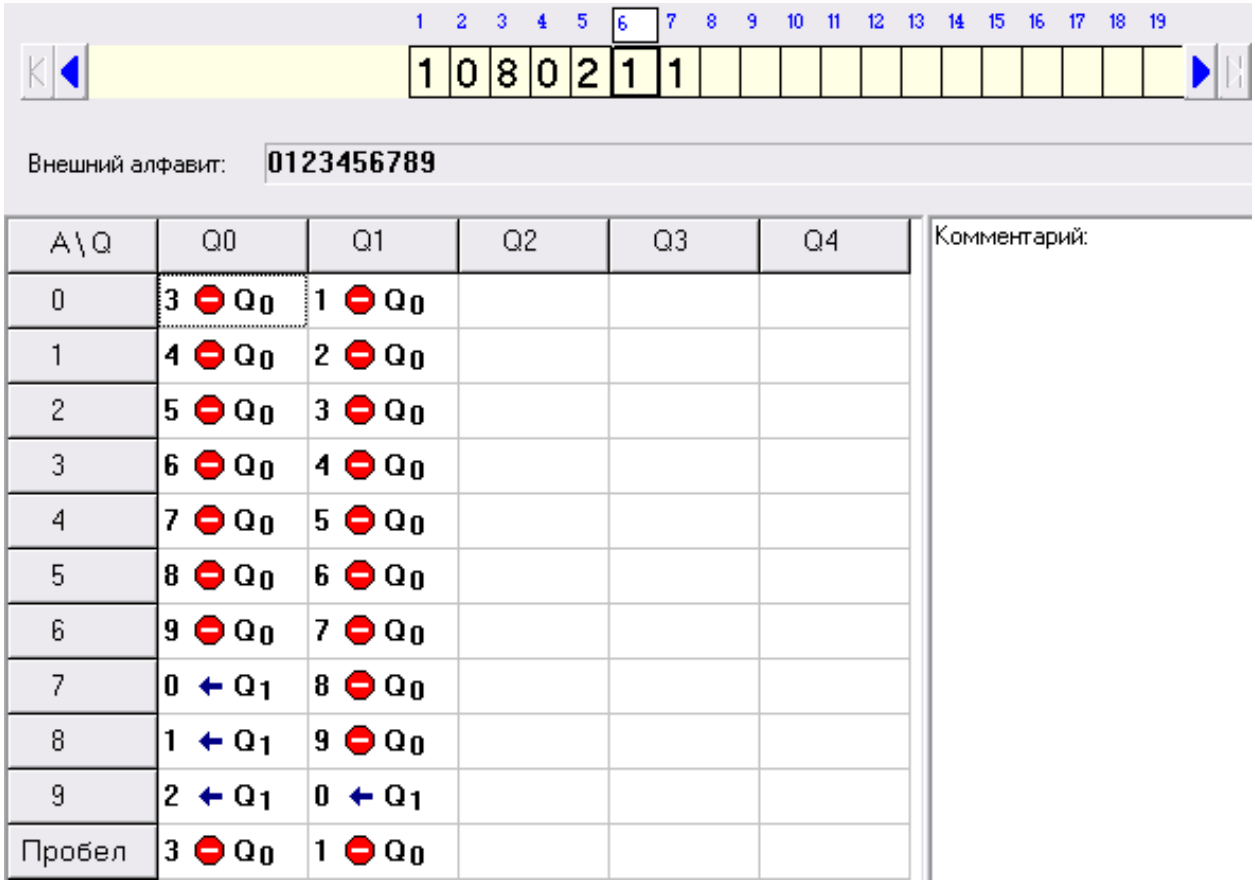
Решение



Задание 2

Написать на машине Тьюринга программу, прибавляющую 3 к введенному числу.

Решение



Методические материалы, определяющие процедуру оценивания выполнения Решение задач

Оценка «отлично»
Составлен правильный алгоритм решения задачи, в логическом рассуждении, в выборе формул и решении нет ошибок, получен верный ответ, задача решена рациональным способом.
Оценка «хорошо»
Составлен правильный алгоритм решения задачи, в логическом рассуждении и решении нет существенных ошибок; правильно сделан выбор формул для решения; есть объяснение решения, но задача решена нерациональным способом или допущено не более двух несущественных ошибок, получен верный ответ.
Оценка «удовлетворительно»
Допущены существенные ошибки в выборе формул или в расчетах; задача решена не полностью или в общем виде.
Оценка «неудовлетворительно» Задача решена неправильно. Объяснение дано неполное, непоследовательное, с грубыми ошибками, без теоретического обоснования.

Практические работы

Практические работы, являются важным источником познания нового материала, способствуют формированию и совершенствованию практических умений и навыков обучающихся.

Вариант практической работы

Шифр Цезаря.

Шифр Цезаря, также известный как шифр сдвига, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования.
Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.
Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера, и всё ещё имеет современное приложение в системе ROT13. Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет почти никакого применения на практике.
В данной работе представлено 28 фраз, которые закодированы с помощью шифра Цезаря. Ученик должен расшифровать и указать на сколько сделан сдвиг. Ниже указаны исходные фразы.
Задания:

1. ЗГ, ЪИОСЕИН ФПИУХИР, РС АХС ДЮОС ДЮ ИЬИ ТСОДИЗЮ. ТОСШС ХС, ЪХС СР ЛРСЖЗГ ЕРИКГТРС ФПИУХИР, ЕСХ Е ЪИП ЧСНЦФ!
2. СМОТЗИД М СМЫЙЗТ СЙ УФТХМЦЙ! СМОТЗИД М СМЫЙЗТ, М Ж ТХТЕЙССТХЦМ Ч ЦЙЩ, ОЦТ ХМПАСЙЙ ЖДХ. ХДРМ УФЙИПТКДЦ М ХДРМ ЖХЙ ИДИЧЦ!
3. ЗМХУЦРАК ТНПУИЙЕ ТНЬКИУ ТК ФУТНСЕГЧ ЦЕСН, Е ЙРД ЙКЧКО УЬКТБ ШЧУСНЧКРБТУ ЖКМ ПУТЫЕ НС ЗЦК УЖЯДЦТДЧБ Н ХЕЦЧУРПУЗАЗЕЧБ.

Ответы

1. Да, человек смертен, но это было бы еще полбеды. Плохо то, что он иногда внезапно смертен, вот в чем фокус!
2. Никогда и ничего не просите! Никогда и ничего, и в особенности у тех, кто сильнее вас. Сами предложат и сами всё дадут!
3. Взрослые никогда ничего не понимают сами, а для детей очень утомительно без конца им всё объяснять и растолковывать.

Методические материалы, определяющие процедуру оценивания выполнения практических работ

Описание методики оценивания выполнения практических работ: оценка за выполнение тестовых заданий ставится на основании знания теоретического материала по теме практической работы, умений и навыков применения знаний на практике, работы с оборудованием, анализировать результаты практической работы.
Критерии оценки (в баллах*):*
- **5** баллов выставляется студенту, если демонстрируются знания темы, цели и задач практической работы, хода работы, применяемых методик исследования; демонстрируется полное знание теоретического материала по теме практической работы (в процессе обсуждения, при ответе на контрольные вопросы); демонстрируются умения и навыки работы с оборудованием, применения знания на практике, анализа результатов практической работы и формулирование выводов, владение навыками прикладной деятельности;
- **4** балла выставляется студенту, если демонстрируются знания темы, цели и задач практической работы, хода работы, имеются пробелы в знании применяемых методик исследования; демонстрируется неполное знание фактического материала по теме практической работы (в процессе обсуждения, при ответе на контрольные вопросы); демонстрируются некоторые недостатки умения работать с оборудованием, применять знания на практике, недостатки владения навыками прикладной деятельности и способности анализировать результаты практической работы, формулировать выводы, прослеживать причинно-следственные связи;
- **3** балла выставляется студенту, если демонстрируются неполные знания цели и задач практической работы, хода работы, применяемых методик исследования; демонстрируется неполное, несистемное знание теоретического материала по теме практической работы (в процессе обсуждения, при ответе на контрольные вопросы); демонстрируются заметные недостатки в умении работать с оборудованием, применять знания на практике, недостаточно владеет навыками прикладной деятельности, способностью анализировать результаты практической работы и формулировать выводы, прослеживать причинно-следственные связи;
- **0-2** балла выставляется студенту, если демонстрируются полное или почти полное отсутствие знания цели и задач практической работы, хода работы, применяемых методик исследования;

демонстрируется полное или почти полное отсутствие знания теоретического материала по теме практической работы (в процессе обсуждения, при ответе на контрольные вопросы); демонстрируются значительные недостатки умения работать с оборудованием, применять знания на практике, владения навыками прикладной деятельности, способности анализировать результаты практической работы и формулировать выводы, прослеживать причинно-следственные связи.

Домашняя контрольная работа

Образцы вариантов контрольной работы

Задания к работе

1. Перевести данное число из десятичной системы счисления в двоичную, восьмеричную и шестнадцатеричную системы счисления.
2. Перевести данное число в десятичную систему счисления.
3. Сложить числа.
4. Выполнить вычитание.
5. Выполнить умножение.
6. Выполнить деление.

Примечание. В заданиях 3–6 проверять правильность вычислений переводом исходных данных и результатов в десятичную систему счисления. В задании 1д получить пять знаков после запятой в двоичном представлении.

Вариант 1

1. а) $666_{(10)}$; б) $305_{(10)}$; в) $153{,}25_{(10)}$; г) $162{,}25_{(10)}$; д) $248{,}46_{(10)}$
2. а) $1100111011_{(2)}$; б) $10000000111_{(2)}$; в) $10110101{,}1_{(2)}$; г) $100000110{,}10101_{(2)}$; д) $671{,}24_{(8)}$; е) $41A{,}6_{(16)}$.
3. а) $10000011_{(2)}+1000011_{(2)}$; б) $1010010000_{(2)}+1101111011_{(2)}$; в) $110010{,}101_{(2)}+1011010011{,}01_{(2)}$; г) $356{,}5_{(8)}+1757{,}04_{(8)}$; д) $293{,}8_{(16)}+3CC{,}98_{(16)}$.
4. а) $100111001_{(2)}-110110_{(2)}$; б) $1111001110_{(2)}-111011010_{(2)}$; в) $1101111011{,}01_{(2)}-101000010{,}0111_{(2)}$; г) $2025{,}2_{(8)}-131{,}2_{(8)}$; д) $2D8{,}4_{(16)}-A3{,}B_{(16)}$.
5. а) $1100110_{(2)}\acute{}\ 1011010_{(2)}$; б) $2001{,}6_{(8)}\acute{}\ 125{,}2_{(8)}$; в) $2C{,}4_{(16)}\acute{}\ 12{,}98_{(16)}$.
6. а) $110011000_{(2)} : 10001_{(2)}$; б) $2410_{(8)} : 27_{(8)}$; в) $D4A_{(16)} : 1B_{(16)}$;

Задания к работе

1. Перевести данное число из десятичной системы счисления в двоичную, восьмеричную и шестнадцатеричную системы счисления.
2. Перевести данное число в десятичную систему счисления.
3. Сложить числа.
4. Выполнить вычитание.
5. Выполнить умножение.
6. Выполнить деление.

Примечание. В заданиях 3–6 проверять правильность вычислений переводом исходных данных и результатов в десятичную систему счисления. В задании 1д получить пять знаков после запятой в двоичном представлении.

Вариант 2

1. а) $164_{(10)}$; б) $255_{(10)}$; в) $712{,}25_{(10)}$; г) $670{,}25_{(10)}$; д) $11{,}89_{(10)}$
2. а) $1001110011_{(2)}$; б) $1001000_{(2)}$; в) $1111100111{,}01_{(2)}$; г) $1010001100{,}101101_{(2)}$; д) $413{,}41_{(8)}$; е) $118{,}8C_{(16)}$.

3. а) $1100001100_{(2)}$+$1100011001_{(2)}$; б) $110010001_{(2)}$+$1001101_{(2)}$; в) $111111111,001_{(2)}$+$1111111110,0101_{(2)}$; г) $1443,1_{(8)}$+$242,44_{(8)}$; д) $2B4,C_{(16)}$+$EA,4_{(16)}$.
4. а) $1001101100_{(2)}$-$1000010111_{(2)}$; б) $1010001000_{(2)}$-$1000110001_{(2)}$; в) $1101100110,01_{(2)}$-$111000010,1011_{(2)}$; г) $1567,3_{(8)}$-$1125,5_{(8)}$; д) $416,3_{(16)}$-$255,3_{(16)}$.
5. а) $100001_{(2)}$´ $1001010_{(2)}$; б) $1723,2_{(8)}$´ $15,2_{(8)}$; в) $54,3_{(16)}$´ $9,6_{(16)}$.
6. а) $10010100100_{(2)}$: $1100_{(2)}$; б) $2760_{(8)}$: $23_{(8)}$; в) $4AC_{(16)}$: $17_{(16)}$;

Задачи по теме"Позиционные системы счисления. Арифметические операции"

Задания к работе

1. Перевести данное число из десятичной системы счисления в двоичную, восьмеричную и шестнадцатеричную системы счисления.
2. Перевести данное число в десятичную систему счисления.
3. Сложить числа.
4. Выполнить вычитание.
5. Выполнить умножение.
6. Выполнить деление.

Примечание. В заданиях 3–6 проверять правильность вычислений переводом исходных данных и результатов в десятичную систему счисления. В задании 1д получить пять знаков после запятой в двоичном представлении.

Вариант3

1. а) $273_{(10)}$; б) $661_{(10)}$; в) $156,25_{(10)}$; г) $797,5_{(10)}$; д) $53,74_{(10)}$
2. а) $1100000000_{(2)}$; б) $1101011111_{(2)}$; в) $1011001101,00011_{(2)}$; г) $1011110100,011_{(2)}$; д) $1017,2_{(8)}$; е) $111,B_{(16)}$.
3. а) $1110001000_{(2)}$+$110100100_{(2)}$; б) $1001001101_{(2)}$+$1111000_{(2)}$; в) $111100010,0101_{(2)}$+$1111111,01_{(2)}$; г) $573,04_{(8)}$+$1577,2_{(8)}$; д) $108,8_{(16)}$+$21B,9_{(16)}$.
4. а) $1010111001_{(2)}$-$1010001011_{(2)}$; б) $1110101011_{(2)}$-$100111000_{(2)}$; в) $1110111000,011_{(2)}$-$111001101,001_{(2)}$; г) $1300,3_{(8)}$-$464,2_{(8)}$; д) $37C,4_{(16)}$-$1D0,2_{(16)}$.
5. а) $1011010_{(2)}$´ $1000010_{(2)}$; б) $632,2_{(8)}$´ $141,34_{(8)}$; в) $2A,7_{(16)}$´ $18,8_{(16)}$.
6. а) $111010110_{(2)}$: $1010_{(2)}$; б) $4120_{(8)}$: $23_{(8)}$; в) $4F8_{(16)}$: $18_{(16)}$;

Задания к работе

1. Перевести данное число из десятичной системы счисления в двоичную, восьмеричную и шестнадцатеричную системы счисления.
2. Перевести данное число в десятичную систему счисления.
3. Сложить числа.
4. Выполнить вычитание.
5. Выполнить умножение.
6. Выполнить деление.

Примечание. В заданиях 3–6 проверять правильность вычислений переводом исходных данных и результатов в десятичную систему счисления. В задании 1д получить пять знаков после запятой в двоичном представлении.

Методические материалы, определяющие процедуру оценивания выполнения Домашней контрольной работы

Домашняя контрольная работа оценивается по 4-х бальной шкале:

1. Оценка «**отлично»** выставляется при условии, что студент полностью выполнил задание контрольной и проявил отличные знания учебного материала. При этом работа оформлена в соответствии с требованиями, к ней можно предъявить минимум замечаний.
2. **«Хорошо»** ставится тогда, когда студент выполнил все задания, показал хорошие знания по пройденному материалу, но не сумел обосновать предложенные решения задач, когда есть недочеты в оформлении контрольной работы и общие небольшие замечания, не влияющие на ее качество.
3. Оценку «**удовлетворительно»** студент получает за полностью выполненное задание контрольной при наличии в ней существенных неточностей и недочетов, не умении студента верно применить полученные знания, в оформлении работы есть нарушения, не аргументированные ответы, неактуальные или ненадежные источники информации.
4. **«Неудовлетворительно»** студент получает в том случае, когда он не полностью выполнил задание проявил недостаточный уровень знаний, не смог объяснить полученные результаты. Такая контрольная работа не отвечает требованиям, содержит противоречивые сведения, задачи в ней решены неверно.

Групповой опрос

Групповой опрос реализуется во время лекционных и практических занятий.
Примерный перечень вопросов для группового опроса по Теме 1:

1. Основные черты информационного общества.
2. Информационные революции в обществе.
3. Информатика - понятие, объекты приложения, предмет изучения, составные части, место среди других наук.

4.Основные понятия информатики - информация, материальный носитель, сигнал, сообщение, информационный процесс, источник сообщения, получатель сообщения, виды сигналов.
5. Основные понятия информатики - объект: виды, признаки, характеристики, поведение.
6. Основные понятия информатики - система: компоненты, свойства, понятие информационной системы.
7. Основные понятия информатики - моделирование и формализация.
8.Вероятностный и объемный поход к измерению количества информации.
9. Понятие энтропии.

Методические материалы, определяющие процедуру оценивания группового опроса

Критерии оценки
5 баллов выставляется студенту, если: в ответе качественно раскрыто содержание темы. Ответ хорошо структурирован. Прекрасно освоен понятийный аппарат. Продемонстрирован высокий уровень понимания материала. Превосходное умение формулировать свои мысли, обсуждать дискуссионные положения.

4 балла выставляется студенту, если: основные вопросы темы раскрыты. Структура ответа в целом адекватна теме. Хорошо освоен понятийный аппарат. Продемонстрирован хороший уровень понимания материала.
Хорошее умение формулировать свои мысли, обсуждать дискуссионные положения.
3 балла выставляется студенту, если: тема частично раскрыта. Ответ слабо структурирован. Понятийный аппарат освоен частично. Понимание отдельных положений из материала по теме. Удовлетворительное

умение формулировать свои мысли, обсуждать дискуссионные положения.
0-2 балла выставляется студенту, если: тема не раскрыта. Понятийный аппарат освоен неудовлетворительно. Понимание материала фрагментарное или отсутствует. Неумение формулировать свои мысли, обсуждать дискуссионные положения.

Доклад

Варианты тематики докладов:

1. Понятие энтропии.
2. Энтропия и информация.
3. Информация и алфавит.
4. Постановка задачи первичного кодирования.
5. Первая теорема Шеннона.
6. Способы построения двоичных кодов
7. Использование естественнонаучных и математических знаний для ориентирования в современном

Методические материалы, определяющие процедуру оценивания выполнения Доклада

Оценка **Отлично** - Соответствие целям и задачам дисциплины, актуальность темы и рассматриваемых проблем, соответствие содержания заявленной теме, заявленная тема полностью раскрыта, рассмотрение дискуссионных вопросов по проблеме, сопоставлены различные точки зрения по рассматриваемому вопросу, научность языка изложения, логичность и последовательность в изложении материала, количество исследованной литературы, в том числе новейших источников по проблеме, четкость выводов, оформление работы соответствует предъявляемым требованиям.
Оценка **Хорошо** - Соответствие целям и задачам дисциплины, актуальность темы и рассматриваемых проблем, соответствие содержания заявленной теме, научность языка изложения, заявленная тема раскрыта недостаточно полно, отсутствуют новейшие литературные источники по проблеме, при оформлении работы имеются недочеты.
Оценка **Удовлетворительно** - Соответствие целям и задачам дисциплины, содержание работы не в полной мере соответствует заявленной теме, заявленная тема раскрыта недостаточно полно, использовано небольшое количество научных источников, нарушена логичность и последовательность в изложении материала, при оформлении работы имеются недочеты.
Оценка **Неудовлетворительно** - Работа не соответствует целям и задачам дисциплины, содержание работы не соответствует заявленной теме, содержание работы изложено не научным стилем.

Зачет

Зачет является оценочным средством для всех этапов освоения компетенций.

Примерные вопросы к зачету, 2 курс / 4 семестр

1. Исходные понятия информатики: сообщение, информация, источник и приемник информации.
2. Сигнал и его информационные параметры.
3. Виды информации (непрерывная, дискретная).
4. Преобразование форм представления информации
5. Универсальность дискретного представления информации.
6. Понятие энтропии. Свойства энтропии.
7. Энтропия и информация. Статистическое определение информации.
8. Информация и алфавит. Формула Шеннона.
9. Математическая постановка задачи кодирования.

10. Неравномерное алфавитное кодирование с разделителем кодов.
11. Оптимальные коды (Хаффмана, Шеннона-Фано).
12. Равномерное двоичное кодирование. Байт. Стандарты компьютерных кодов.
13. Системы счисления. Позиционные системы счисления.
14. Перевод целых и дробных чисел в различные системы счисления.
15. Системы счисления, используемые в компьютере. Перевод целых и дробных чисел между системами счисления с основанием 2 – 8 – 16.
16. Представление целых чисел в компьютере. Сложение и умножение целых чисел.
17. Дополнительный код двоичного числа. Вычитание двоичных целых чисел.
18. Нормализованная форма вещественного числа. Представление вещественных чисел в компьютере.
19. Сложение и умножение нормализованных двоичных чисел. Влияние ограниченной разрядности чисел на точность вычислений. Понятие переполнения и машинного нуля.
20. Понятие канала и линии связи. Характеристики канала связи: ширина пропускания, пропускная способность, скорость передачи.
21. Влияние шумов на пропускную способность канала. 16
22. Параллельная передача данных в компьютерных линиях.
23. Последовательная передача. Модемная связь.
24. Постановка задачи хранения информации. Хранение элементарных данных в памяти компьютера. Идентификаторы.
25. Структуры данных. Классификация и примеры структур данных. Размещение структур данных в ОЗУ: последовательные и связанные списки.
26. Размещение данных на внешних носителях. Понятия физической записи, файла, каталога (папки), структур каталогов. Блок, кластер.
27. Понятие автомата. Описание автомата. Автоматные функции.
28. Дискретные устройства без памяти. Построение комбинационной схемы по логической функции (или наоборот).
29. Решение алгоритмических задач с помощью машин Поста и Тьюринга.
30. Конечные автоматы. Способы описания конечных автоматов (табличный, с помощью диаграмм).
31. Виды элементов памяти конечных автоматов; их диаграммы.
32. Построение конечного автомата по системе уравнений, таблице значений, диаграмме или для заданной схемы автомата построение его описания.
33. Понятие модели. Классификация моделей. Особенности информационных моделей.
34. Понятие объекта. Понятие системы. Классификация систем.
35. Значение формализации. Порядок решения задач с применением компьютера.
36. Информация и управление. Схемы управления (разомкнутая, с обратной связью).
37. Управление и регулирование. Автоматическое регулирование.
38. Автомат. Коллективное поведение автоматов.
39. Нейрокибернетика. Персептрон. Нейрокомпьютер. Нейронные сети.

Методические материалы, определяющие процедуру оценивания зачета

Зачет выставляется по рейтингу, в зависимости от эффективности работы в процессе изучения дисциплины, что определяется количеством набранных баллов за все виды заданий текущего и рубежного контроля
зачтено – от 60 до 110 баллов
не зачтено – от 0 до 59 баллов.

1.3. Рейтинг-план дисциплины

Таблица перевода баллов текущего контроля в баллы рейтинга

	5	**5**	**5**	**5**	**5**	**5**	**5**	**5**	**5**	**5**

0	0	0	0	0	0	0	0	0	0	0
1	5	3	2	2	1	1	1	1	1	1
2		5	4	3	2	2	2	2	2	1
3			5	4	3	3	3	2	2	2
4				5	4	4	3	3	3	2
5					5	5	4	4	3	3
6						5	5	4	4	3
7							5	5	4	4
8								5	5	4
9									5	5
10										5

Рейтинг-план дисциплины представлен в Приложении 1.

2. Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература

1. Волкова, В.Н. Теоретические основы информатики: Учебное пособие по дисциплине «Теоретические основы информатики» : учебное пособие / В.Н. Волкова, А.В. Логинова ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - Санкт-Петербург : Издательство Политехнического университета, 2011. - 160 с. : схем., табл., ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=363069 (30.08.2018)
2. Стариченко, Б.Е. Теоретические основы информатики : учебное пособие для вузов / Б.Е. Стариченко. - 3-е изд. перераб. и доп. - Москва : Горячая линия - Телеком, 2016. - 400 с. URL: http://biblioclub.ru/index.php?page=book&id=441381

Дополнительная литература

1. Теоретические основы информатики : учебник / Р.Ю. Царев, А.Н. Пупков, В.В. Самарин и др. ; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск : Сибирский федеральный университет, 2015. - 176 с. - URL: http://biblioclub.ru/index.php?page=book&id=435850

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины

1. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс]. – Режим доступа: https://elibrary.ru/.
2. Электронная библиотечная система «Лань» [Электронный ресурс]. – Режим доступа: https://e.lanbook.com/.
3. Университетская библиотека онлайн biblioclub.ru [Электронный ресурс]. – Режим доступа: http://biblioclub.ru/.
4. Электронная библиотека УУНиТ [Электронный ресурс]. – Режим доступа: https://elib.bashedu.ru/.
5. Российская государственная библиотека [Электронный ресурс]. – Режим доступа: https://www.rsl.ru/.
6. Национальная электронная библиотека [Электронный ресурс]. – Режим доступа: https://xn--90ax2c.xn--p1ai/viewers/.

7. Национальная платформа открытого образования npoed.ru [Электронный ресурс]. – Режим доступа: http://npoed.ru/.
8. Электронное образование Республики Башкортостан [Электронный ресурс]. – Режим доступа: https://edu.bashkortostan.ru/.
9. Информационно-правовой портал Гарант.ру [Электронный ресурс]. – Режим доступа: http://www.garant.ru/.

Программное обеспечение

1. Браузер Google Chrome - Бесплатная лицензия https://www.google.com/intl/ru_ALL/chrome/privacy/eula_text.html
2. Office Professional Plus - Договор №0301100003620000022 от 29.06.2020, Договор № 2159-ПО/2021 от 15.06.2021, Договор №32110448500 от 30.07.2021
3. Windows - Договор №0301100003620000022 от 29.06.2020, Договор № 2159- ПО/2021 от 15.06.2021, Договор №32110448500 от 30.07.2021
4. Pascalabc, PascalABC.NET - Бесплатная лицензия https://pascal-abc.ru, http://pascalabc.net

6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
Аудитория 301 Читальный зал (электронный каталог)(ФМ)	Для самостоятельной работы	Компьютеры в сборе, учебная мебель. Программное обеспечение 1. Браузер Google Chrome 2. Office Professional Plus
Аудитория 311(ФМ)	Лекционная, Семинарская, Для консультаций, Для контроля и аттестации	Учебная мебель, компьютеры в сборе, мультимедийный проектор vivitek d862, экран настенный dinon manual 160x160 mw, доска маркерная. Программное обеспечение 1. Pascalabc, PascalABC.NET 2. Windows 3. Office Professional Plus
Аудитория 313 а(ФМ)	Для хранения оборудования	Оверхед-проектор "reflex" с кейсом, проектор infocds in 2104dlp.
Аудитория 420(ФМ)	Для самостоятельной работы	Компьютеры в сборе, учебная мебель. Программное обеспечение 1. Office Professional Plus 2. Windows 3. Браузер Google Chrome