

Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ
ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ,
ПРОВОДИМОГО РГГМУ САМОСТОЯТЕЛЬНО,
ПО ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ И БЕЗОПАСНОСТИ**

для поступающих
на основные образовательные программы специалитета
в 2025 году

Санкт-Петербург
2025

1. Общие положения

Программа вступительного испытания по информационным технологиям и безопасности предназначена для абитуриентов, поступающих на обучение на программу специалитета федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный гидрометеорологический университет» (далее – РГГМУ) (Приложение).

Целью вступительного испытания по информационным технологиям и безопасности является объективная оценка качества подготовки абитуриентов и проведение конкурсного отбора для поступления в РГГМУ.

Программа составлена в соответствии с требованиями федерального государственного образовательного стандарта среднего профессионального образования.

2. Форма вступительного испытания

Вступительное испытание проводится очно или с применением дистанционных образовательных технологий в форме компьютерного тестирования в соответствии с расписанием, утвержденным председателем приемной комиссии и размещенном на официальном сайте РГГМУ (<http://dovus.rshu.ru/content/priemkom/abit>).

Проведение вступительного испытания с применением дистанционных образовательных технологий регламентируется Положением об организации вступительных испытаний с использованием дистанционных технологий, размещенном на официальном сайте РГГМУ (<http://dovus.rshu.ru/content/priemkom/norm>).

3. Продолжительность вступительного испытания

На выполнение заданий вступительного испытания отводится 60 минут (1 астрономический час).

4. Содержание вступительного испытания

4.1. Системы счисления и представление информации.

Системы счисления для представления данных при использовании компьютерных технологий. Представление информации в системах счисления с разными основаниями. Единицы измерения информации. Основы кодирования.

4.2. Логические основы информационных и компьютерных технологий.

Основы логики. Логические высказывания, логические операции, истинность высказывания. Построение таблиц истинности логических выражений. Основные логические законы.

4.3. Кодирование информации.

Двоичный код. Размещение информации в ОЗУ ЭВМ. Единицы памяти. Байт. Машинное слово. Принципы адресации. Двоичная арифметика. Представление отрицательных целых чисел в двоичном коде. Прямой, обратный и дополнительный код. Двоично - десятичный код. Кодирование символов. Современные кодировки символов. Национальные алфавиты. Кодирование графики. Глубина цвета. Размер графического файла. Графические форматы. Кодирование звука. Частота дискретизации и «глубина» кодирования звуковой волны. Размер звукового файла. Звуковые форматы.

4.4. Основы информационной безопасности.

Основные модели безопасности – модель Харрисона-Рузо-Ульмана, модель Белла-ЛаПадула, ролевая модель безопасности. Классификация шифров. Защита информации в IP-сетях.

4.5. Основные каналы утечки информации.

Акустический канал. Акустоэлектрический канал. Виброакустический канал. Оптический канал. Электрические и электромагнитные каналы.

4.6. Основные конструкции языков программирования.

Элементы языка: алфавит, синтаксис и семантика. Зарезервированные (ключевые)

слова, идентификация данных, константы, переменные. Типы данных, структурированные и неструктурированные данные. Стандартные типы данных. Тождественность и совместимость типов. Понятие выражения, операции, операнда. Присваивание значений переменным. Запись выражений. Структура программы. Операторы: понятие оператора; классификация операторов; простые операторы; структурированные операторы. Ввод-вывод. Представление основных управляющих структур программирования: следование, развилка, циклы.

4.7. Передача и хранение информации.

Понятие источника информации и приемника информации. Каналы связи. Понятие носителя информации. Виды носителей информации.

4.8 Количество информации.

Понятие информации. Свойства информации. Виды информации. Измерение информации. Информационная емкость знаков. Единицы информации.

4.9. Принципы организации компьютерных сетей.

Архитектура компьютеров. Программная и аппаратная организация компьютеров и компьютерных систем. Основные устройства компьютера. Виды программного обеспечения. Операционная система. Компьютерные сети. Принципы организации, основные понятия. Адресация в сети.

4.10. Аутентификация.

Методы аутентификации. Протоколы аутентификации.

5. Структура вступительного испытания

Вступительное испытание включает 20 тестовых заданий, которые различаются формой и уровнем сложности.

Работа содержит 20 заданий с кратким ответом, ответом на которые являются число, последовательность цифр или слово (словосочетание).

Во вступительном испытании представлены следующие разновидности заданий с кратким ответом:

- задания, требующие записать ответ в виде числа;
- задания, требующие записать ответ в виде слова;
- задания на установление правильной последовательности;
- задания на установление соответствия.

б. Примеры заданий вступительного испытания

6.1 Вычитите в дополнительном коде в шестнадцатеричной системе 192 и (-100).

6.2 Переведите в шестнадцатеричную систему (-0,991). С точностью до трёх разрядов после запятой.

6.3 Упростите выражение $\bar{x} \cup y \cap (y \cup) \cap x \cap x \cup \bar{x} \cap (x \cup \bar{x})$.

6.4 Переведите в базис ИЛИ-НЕ выражение $\bar{x} \cup (x \cap y \cup x)$.

6.5 Найдите сумму цветов в GRB. Цвет1 (122.233.098)₁₀, цвет2 (102.200.02)₁₀.

6.6 Зашифруйте с помощью шифра Цезаря с ключом 8 фразу «Информационная безопасность – важнейшее направление человеческой деятельности», пробелы в итоговую фразу не включать.

6.7 Найдите x и y
 $256^y (K) = 64^x (бит)$;
 $2^{2x} (M) = 2^y (байт)$

6.8 Определите сколько хостов содержит сеть 192.168.0.0/28?

7. Критерии оценивания отдельных заданий и работы в целом

№ задания	Критерий оценивания и количество баллов
1-10	полное правильное выполнение задания – 10 баллов; неверное выполнение задания (при указании одной или более ошибочных цифр) – 0 баллов.

Максимальное количество баллов за вступительное испытание – 100.

Минимальное количество баллов, подтверждающее успешность прохождения вступительного испытания, – 44.

8. Список литературы, рекомендуемый для подготовки к вступительному испытанию

1. Макарова Н.В. Информатика и ИКТ. Практикум по программированию. 10–11 классы. Базовый уровень. - СПб.: Питер, 2015. - 16 с.

2. Астафьева Н.Е. Информатика и ИКТ: Практикум для профессий и специальностей технического и социально-экономического профилей. - М.: Academia, 2019. - 384 с.

3. Малясова С.В. Информатика и ИКТ: Пособие для подготовки к ЕГЭ / С.В. Малясова; Под ред. Цветковой М.С.. - М.: Academia, 2024. - 637 с.

4. Плотникова Н.Г. Информатика и информационно-коммуникационные технологии (ИКТ). - М.: Риор, 2018. - 132 с.

5. Зайдельман Я. Н. ЕГЭ 2021 Информатика и ИКТ. Диагностические работы. ФГОС - М.: МЦНМО, 2020 г. - 192 с.

6. Лещинер В. Р. ЕГЭ 2021 Информатика. Готовимся к итоговой аттестации. - М.: Интеллект-Центр, 2023. - 152 с.

7. Цветкова М.С. Информатика и ИКТ: учебник. - М.: Academia, 2017. - 352 с.

8. Медведев В. А. Информационная безопасность. Введение в специальность. М.: Кнорус, 2019. – 144 с.

9. Мельников В.П., Куприянов А.И. Информационная безопасность. — М.: Кнорус, 2018. — 268 с.

10. Нестеров С.А. Информационная безопасность: учебник и практикум для среднего профессионального образования. — М.: Юрайт, 2019.— 321 с.

Приложение
к Программе вступительного испытания,
проводимого РГГМУ самостоятельно,
по информационным технологиям
и безопасности для поступающих
на основные образовательные программы
бакалавриата в 2025 году

Направления подготовки, на которые учитываются результаты вступительного
испытания по информационным технологиям и безопасности

№ п/п	Код	Направление подготовки / направленность (профиль)
1	10.05.02	Информационная безопасность телекоммуникационных систем специализация «Разработка защищенных телекоммуникационных систем»