



**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ**  
ФГБОУ ВО «Брянский государственный технический  
университет» (БГТУ)

**Факультет информационных технологий**

*(наименование факультета/института)*

**Кафедра «Системы информационной безопасности»**

*(наименование кафедры, ответственной за реализацию дисциплины)*

**УТВЕРЖДАЮ**

**Первый проректор по учебной  
работе и цифровизации**

**В.А. Шкаберин**

**«20» апреля 2023 г.**

**РАБОЧАЯ ПРОГРАММА**

**учебной дисциплины**

**«Математические основы защиты информации»**

*(наименование дисциплины)*

**10.03.01 Информационная безопасность**

*(код и наименование специальности или направления подготовки)*

**Организация и технологии защиты информации (по отрасли или в сфере  
профессиональной деятельности)**

*(направленность (профиль)/ специализация образовательной программы)*

**высшее образование – бакалавриат**

*(уровень образования)*

**бакалавр**

*(квалификация, присваиваемая по специальности или направлению подготовки)*

**очная**

*(форма обучения)*

**2023**

*(год набора)*

**Брянск 2023**

Рабочая программа учебной дисциплины  
«Математические основы защиты информации»

(наименование дисциплины)

10.03.01 Информационная безопасность

(код и наименование специальности или направления подготовки)

Организация и технологии защиты информации (по отрасли или в сфере  
профессиональной деятельности)

(направленность (профиль)/специализация образовательной программы)

**Разработал(и):**

доцент кафедры «СИБ», к.т.н.

(должность, ученая степень, ученое звание)

(подпись)

С.А. Шпичак

(И.О. Фамилия)

(должность, ученая степень, ученое звание)

(подпись)

(И.О. Фамилия)

Рассмотрена и одобрена на заседании кафедры  
«Системы информационной безопасности»

(наименование кафедры, ответственной за реализацию дисциплины)

от «3» апреля 2023 г., протокол № 9

Заведующий кафедрой

к.т.н., доцент

(ученая степень, ученое звание)

(подпись)

М.Ю. Рытов

(И.О. Фамилия)

**Согласовано:**

Заведующий выпускающей кафедрой

«Системы информационной безопасности»

(наименование выпускающей кафедры)

к.т.н., доцент

(ученая степень, ученое звание)

(подпись)

М.Ю. Рытов

(И.О. Фамилия)

© Шпичак С.А. 2023

© ФГБОУ ВО «Брянский государственный  
технический университет», 2023

## СОДЕРЖАНИЕ

|   |    |
|---|----|
| ПРЕДИСЛОВИЕ.....  | 5  |
| 1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ .....  | 5  |
| 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ<br>ПРОГРАММЫ ФГОС .....   | 5  |
| 3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ .....   | 5  |
| 4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ .....   | 6  |
| 5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ .....  | 7  |
| 5.1. Структура дисциплины.....  | 7  |
| 5.2. Распределение формируемых компетенций по разделам (темам)<br>дисциплины.....   | 8  |
| 5.3. Лекции .....   | 8  |
| 5.4. Лабораторные работы .....  | 9  |
| 5.5. Практические занятия .....   | 10 |
| 5.6. Самостоятельная работа обучающихся .....   | 11 |
| 5.7. Организация текущего контроля успеваемости и промежуточной<br>аттестации обучающихся .....   | 13 |
| 6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ .....   | 14 |
| 7. РЕАЛИЗАЦИЯ ДИСЦИПЛИНЫ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИЙ<br>ЭЛЕКТРОННОГО ОБУЧЕНИЯ И (ИЛИ) ДИСТАНЦИОННЫХ<br>ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ.....   | 14 |
| 8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ<br>ДИСЦИПЛИНЫ .....   | 15 |
| 8.1. Перечень учебно-методического обеспечения для самостоятельной работы<br>обучающихся .....  | 15 |
| 8.2. Перечень основной и дополнительной учебной литературы, необходимой<br>для освоения дисциплины .....  | 16 |
| 8.3. Перечень ресурсов информационно-телекоммуникационной сети<br>«Интернет», используемых при изучении дисциплины .....  | 17 |
| 8.4. Перечень информационных технологий, используемых при осуществлении<br>образовательного процесса по дисциплине, включая перечень программного<br>обеспечения и (или) информационных справочных систем ..... | 17 |
| 9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ .....   | 17 |
| 10. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА<br>ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ<br>ЗДОРОВЬЯ.....   | 18 |

|   |    |
|---|----|
| 11. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ .....  | 19 |
| 11.1. Методические материалы для педагогических работников .....  | 19 |
| 11.2. Методические материалы для обучающихся .....  | 22 |
| 12. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ .....   | 23 |
| 12.1. Виды и средства оценивания результатов освоения дисциплины .....  | 23 |
| 12.2. Шкала оценивания при текущем контроле успеваемости .....  | 23 |
| 12.3. Шкала оценивания при промежуточной аттестации обучающихся .....   | 25 |
| 12.4. Оценивание окончательных результатов обучения по дисциплине .....   | 26 |
| 12.5. Характеристика результатов обучения .....   | 26 |
| 12.6. Контрольно-измерительные материалы для текущего контроля<br>успеваемости и промежуточной аттестации обучающихся ..... | 26 |
| 13. ВОСПИТАТЕЛЬНАЯ РАБОТА .....   | 26 |

## ПРЕДИСЛОВИЕ

Учебная дисциплина «Математические основы защиты информации» (далее – дисциплина) ориентирована на формирование у обучающихся компетенций в рамках основной профессиональной образовательной программы высшего образования (ОПОП ВО) по направлению подготовки 10.03.01 Информационная безопасность, профиль «Организация и технология защиты информации (по отрасли или в сфере профессиональной деятельности)».

### 1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**Цель** освоения дисциплины – повысить уровень математической подготовки студентов в вопросах, связанных с обеспечением информационной безопасности, обучить студентов принципам применения математических методов, подходам к анализу инфраструктуры и решению задач обеспечения информационной безопасности компьютерных систем и сетей.

**Задачи** дисциплины:

- формирование основополагающих знаний о разделах математической науки, связанных с решением задач защиты информации,
- формирование представления об основных подходах к реализации математических методов в области информационной безопасности,
- получение обучаемыми теоретических знаний и практических навыков прикладной и программной реализации математических методов и алгоритмов.

### 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ФГОС

Дисциплина входит в вариативную часть, формируемую участниками образовательных отношений учебного плана образовательной программы и реализуется на 4 курсе(-ах) в 7 семестре(-ах).

Предварительно изучаются дисциплины: *«Перечень дисциплин»*.

Параллельно изучаются дисциплины: *«Перечень дисциплин»*.

Базируются на изучении дисциплины: *«Перечень дисциплин»*.

### 3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Изучение дисциплины направлено на формирование у обучающихся компетенций ПК-4, представленных в таблице 1.

Таблица 1 – Требования к результатам освоения учебной дисциплины

| Код и наименование компетенции | Индикаторы компетенций | В результате изучения учебной дисциплины обучающиеся должны: |       |         |
|--------------------------------|------------------------|--|-------|---------|
|                                |                        | знать  | уметь | владеть |

|   |  |  |   |   |
|---|--|--|---|---|
| ПК-4.<br>Способен<br>проводить<br>работы по<br>установке и<br>техническому<br>обслуживанию<br>защищенных<br>технических<br>средств<br>обработки<br>информации | ПК4.1 Проводить работы по установке, настройке, испытаниям и техническому обслуживанию защищенных технических средств обработки информации<br>ПК4.2 Проводить работы по установке, монтажу, наладке, испытаниям и техническому обслуживанию защищенных программных (программно-технических) средств обработки информации | области применения различных разделов математической науки в защите информации; принципы построения математических моделей различных информационных процессов; | работать со специальной математической литературой в области защиты информации, применять основные математические результаты (определения, теоремы и пр.), операции и алгоритмы; рассматривать и анализировать основные виды математических моделей информационных процессов и угроз; | работать со специальной математической литературой в области защиты информации, применять основные математические результаты (определения, теоремы и пр.), операции и алгоритмы; рассматривать и анализировать основные виды математических моделей информационных процессов и угроз; |
|---|--|--|---|---|

#### 4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины составляет 4 зачетных единиц(ы) (144 академических часа(-ов)). Распределение трудоемкости дисциплины по видам учебной работы и семестрам представлено в таблице 2.

Таблица 2 – Распределение трудоемкости дисциплины по видам учебной работы и семестрам

[illegible]

| Виды учебной работы в соответствии с учебным планом образовательной программы | Трудоемкость, час. |         |   |   |   |   |   |   |   |   |   |   |   |
|---|--------------------|---------|---|---|---|---|---|---|---|---|---|---|---|
|   | Всего              | Семестр |   |   |   |   |   |   |   |   |   |   |   |
|   |                    | 1       | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | А | В | С |
| 3.3. Зачет с оценкой, семестр   |                    | -       |   |   |   |   |   |   |   |   |   |   |   |
| 3.4. Курсовой проект (контроль), семестр                                      |                    | -       |   |   |   |   |   |   |   |   |   |   |   |
| 3.5. Курсовая работа (контроль), семестр                                      |                    | -       |   |   |   |   |   |   |   |   |   |   |   |
| 3.6. Расчетно-графическая работа (контроль), семестр                          |                    | -       |   |   |   |   |   |   |   |   |   |   |   |
| 3.7. Контрольная работа (контроль), семестр                                   |                    | -       |   |   |   |   |   |   |   |   |   |   |   |
| <b>Общая трудоемкость (4 з.е.)</b>  | <b>144</b>         |         |   |   |   |   |   |   |   |   |   |   |   |

## 5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 5.1. Структура дисциплины

Структура дисциплины представлена в виде тематического плана в таблице 3.

Таблица 3 – Тематический план дисциплины

| Наименование раздела (темы) дисциплины   | Трудоемкость, час. |        |                     |                      |                        |
|--|--------------------|--------|---------------------|----------------------|------------------------|
|  | Всего              | Лекции | Лабораторные работы | Практические занятия | Самостоятельная работа |
| Тема 1. Применение методов комбинаторики в вопросах защиты информации.                 | 7                  | 2      | 0                   | 4                    | 1                      |
| Тема 2. Основные алгебраические структуры и их применение в области защиты информации. | 21                 | 2      | 6                   | 12                   | 1                      |
| Тема 3. Арифметические операции над целыми числами и многочленами                      | 9                  | 2      | 6                   | 0                    | 1                      |
| Тема 4. Вопросы теории вероятности и теории информации.                                | 9                  | 4      | 0                   | 4                    | 1                      |
| Тема 5. Элементы теории кодирования.   | 9                  | 4      | 0                   | 4                    | 1                      |
| Тема 6. Структуры данных. Организационный поиск и организация информации.              | 9                  | 4      | 0                   | 4                    | 1                      |
| Тема 7. Построение математических моделей информационных процессов и угроз             | 7                  | 2      | 0                   | 4                    | 1                      |
| Тема 8. Основы теории непрерывных дробей.  | 3                  | 2      | 0                   | 0                    | 1                      |
| Тема 9. Проверка чисел на простоту   | 9                  | 2      | 6                   | 0                    | 1                      |
| Тема 10. Факторизация чисел  | 11                 | 4      | 6                   | 0                    | 1                      |
| Тема 11. Дискретное логарифмирование в конечном поле                                   | 11                 | 2      | 8                   | 0                    | 1                      |
| Тема 12. Элементы теории решеток   | 3                  | 2      | 0                   | 0                    | 1                      |

| Наименование раздела (темы) дисциплины | Трудоемкость, час. |           |                     |                      |                        |
|--|--------------------|-----------|---------------------|----------------------|------------------------|
|  | Всего              | Лекции    | Лабораторные работы | Практические занятия | Самостоятельная работа |
| <b>Итого</b>                           | <b>108</b>         | <b>32</b> | <b>32</b>           | <b>32</b>            | <b>12</b>              |

## 5.2. Распределение формируемых компетенций по разделам (темам) дисциплины

Распределение формируемых компетенций по разделам дисциплины представлено в таблице 4.

Таблица 4 – Формирование компетенций по разделам дисциплины

| Наименование раздела (темы) дисциплины   | Код компетенции |     |     |     |     |     |     |
|--|-----------------|-----|-----|-----|-----|-----|-----|
|  | ПК-4            | ... | ... | ... | ... | ... | ... |
| Тема 1. Применение методов комбинаторики в вопросах защиты информации.                 | +               |     |     |     |     |     |     |
| Тема 2. Основные алгебраические структуры и их применение в области защиты информации. | +               |     |     |     |     |     |     |
| Тема 3. Арифметические операции над целыми числами и многочленами                      | +               |     |     |     |     |     |     |
| Тема 4. Вопросы теории вероятности и теории информации.                                | +               |     |     |     |     |     |     |
| Тема 5. Элементы теории кодирования.   | +               |     |     |     |     |     |     |
| Тема 6. Структуры данных. Организационный поиск и организация информации.              | +               |     |     |     |     |     |     |
| Тема 7. Построение математических моделей информационных процессов и угроз             | +               |     |     |     |     |     |     |
| Тема 8. Основы теории непрерывных дробей.  | +               |     |     |     |     |     |     |
| Тема 9. Проверка чисел на простоту   | +               |     |     |     |     |     |     |
| Тема 10. Факторизация чисел  | +               |     |     |     |     |     |     |
| Тема 11. Дискретное логарифмирование в конечном поле                                   | +               |     |     |     |     |     |     |
| Тема 12. Элементы теории решеток   | +               |     |     |     |     |     |     |

## 5.3. Лекции

Перечень занятий лекционного типа, их содержание и трудоемкость представлены в таблице 5.

Таблица 1 – Тематика и содержание лекций

| Наименование темы дисциплины   | Тема лекции  | Содержание лекции  | Трудоемкость, час. |
|--|--|--|--------------------|
| Тема 1. Применение методов комбинаторики в вопросах защиты информации. | Применение методов комбинаторики в вопросах защиты информации. | Применение методов комбинаторики в вопросах защиты информации. | 2                  |



| Наименование темы дисциплины   | Тема лекции  | Содержание лекции  | Трудоемкость, час. |
|--|--|--|--------------------|
| Тема 2. Основные алгебраические структуры и их применение в области защиты информации. | Основные алгебраические структуры и их применение в области защиты информации. | Основные алгебраические структуры и их применение в области защиты информации. | 2                  |
| Тема 3. Арифметические операции над целыми числами и многочленами                      | Арифметические операции над целыми числами и многочленами                      | Арифметические операции над целыми числами и многочленами                      | 2                  |
| Тема 4. Вопросы теории вероятности и теории информации.                                | Вопросы теории вероятности и теории информации.                                | Вопросы теории вероятности и теории информации.                                | 4                  |
| Тема 5. Элементы теории кодирования.   | Элементы теории кодирования.   | Элементы теории кодирования.   | 4                  |
| Тема 6. Структуры данных. Организационный поиск и организация информации.              | Структуры данных. Организационный поиск и организация информации.              | Структуры данных. Организационный поиск и организация информации.              | 4                  |
| Тема 7. Построение математических моделей информационных процессов и угроз             | Построение математических моделей информационных процессов и угроз             | Построение математических моделей информационных процессов и угроз             | 2                  |
| Тема 8. Основы теории непрерывных дробей.  | Основы теории непрерывных дробей.  | Основы теории непрерывных дробей.  | 2                  |
| Тема 9. Проверка чисел на простоту   | Проверка чисел на простоту   | Проверка чисел на простоту   | 2                  |
| Тема 10. Факторизация чисел  | Факторизация чисел   | Факторизация чисел   | 4                  |
| Тема 11. Дискретное логарифмирование в конечном поле                                   | Дискретное логарифмирование в конечном поле                                    | Дискретное логарифмирование в конечном поле                                    | 2                  |
| Тема 12. Элементы теории решеток   | Элементы теории решеток  | Элементы теории решеток  | 2                  |
| <b>Итого</b>   |  |  | <b>32</b>          |

#### 5.4. Лабораторные работы

Лабораторные работы по дисциплине предусмотрены учебным планом образовательной программы (таблица 6).

Таблица 6 – Тематика лабораторных работ

| Наименование<br>темы дисциплины | Тема лабораторной работы   | Трудоемкость,<br>час. |
|---------------------------------|--|-----------------------|
| Тема 2                          | Вычисление наибольшего общего делителя                                       | 6                     |
| Тема 3                          | Арифметические алгоритмы многократной точности для целых чисел и многочленов | 6                     |
| Тема 9                          | Вероятностные алгоритмы проверки чисел на простоту                           | 6                     |
| Тема 10                         | Разложение чисел на множители  | 6                     |
| Тема 11                         | Дискретное логарифмирование в конечном поле.                                 | 8                     |
| <b>Итого</b>                    | –  | 32                    |

### 5.5. Практические занятия

Практические занятия по дисциплине предусмотрены учебным планом образовательной программы.

Перечень практических занятий, их содержание и трудоемкость представлены в таблице 7.

Таблица 7 – Тематика и содержание практических занятий

| Наименование темы<br>дисциплины | Тема практического<br>занятия  | Содержание<br>практического занятия  | Трудоемкость,<br>час. |
|---------------------------------|--|--|-----------------------|
| 1                               | Подсчет количества ключей различных шифров методами комбинаторики.   | Подсчет количества ключей различных шифров методами комбинаторики.   | 4                     |
| 2                               | Арифметические действия в кольце вычетов. Применение унарных и бинарных операций для шифрования и дешифрования.            | Арифметические действия в кольце вычетов. Применение унарных и бинарных операций для шифрования и дешифрования.            | 4                     |
| 2                               | Операции с матрицами над кольцом.  | Операции с матрицами над кольцом.  | 4                     |
| 2                               | Применение аффинных функций в поточных и блочных шифрах простой замены. Дешифрование аффинных шифров                       | Применение аффинных функций в поточных и блочных шифрах простой замены. Дешифрование аффинных шифров                       | 4                     |
| 4                               | Определение статистических характеристик различных открытых текстов. Генерация открытых сообщений на основе статистических | Определение статистических характеристик различных открытых текстов. Генерация открытых сообщений на основе статистических | 4                     |

| Наименование темы дисциплины | Тема практического занятия   | Содержание практического занятия   | Трудоемкость, час. |
|------------------------------|--|--|--------------------|
|                              | характеристик.   |  |                    |
| 5                            | Применение методов оптимального и помехоустойчивого кодирования.   | Применение методов оптимального и помехоустойчивого кодирования.   | 4                  |
| 6                            | Представление данных различной структуры. Алгоритмы поиска и сортировки данных. Оценка эффективности алгоритмов. | Представление данных различной структуры. Алгоритмы поиска и сортировки данных. Оценка эффективности алгоритмов. | 4                  |
| 7                            | Построение алгебраических, вероятностных и автоматных моделей информационных процессов.                          | Построение алгебраических, вероятностных и автоматных моделей информационных процессов.                          | 4                  |
| <b>Итого</b>                 | –  | ...  | <b>32</b>          |

## 5.6. Самостоятельная работа обучающихся

Вопросы, выносимые на самостоятельное изучение, представлены в таблице 8.

Таблица 2 – Вопросы для самостоятельного изучения дисциплины

| Наименование темы дисциплины   | Вопросы для самостоятельного изучения темы |
|--|--|
| Тема 1. Применение методов комбинаторики в вопросах защиты информации.                 | Изучение дополнительной литературы         |
| Тема 2. Основные алгебраические структуры и их применение в области защиты информации. | Подготовка к лабораторным работам          |
| Тема 3. Арифметические операции над целыми числами и многочленами                      | Подготовка к экзамену                      |
| Тема 4. Вопросы теории вероятности и теории информации.                                | Изучение дополнительной литературы         |
| Тема 5. Элементы теории кодирования.   | Подготовка к лабораторным работам          |
| Тема 6. Структуры данных. Организационный поиск и организация информации.              | Подготовка к экзамену                      |
| Тема 7. Построение математических моделей информационных процессов и угроз             | Изучение дополнительной литературы         |
| Тема 8. Основы теории непрерывных дробей.  | Подготовка к лабораторным работам          |
| Тема 9. Проверка чисел на простоту   | Подготовка к экзамену                      |

| Наименование темы дисциплины                         | Вопросы для самостоятельного изучения темы |
|--|--|
| Тема 10. Факторизация чисел                          | Изучение дополнительной литературы         |
| Тема 11. Дискретное логарифмирование в конечном поле | Подготовка к лабораторным работам          |
| Тема 12. Элементы теории решеток                     | Подготовка к экзамену                      |

Примерные темы рефератов/расчетно-графических работ/курсовых работ/курсовых проектов В процессе самостоятельной работы обучающиеся должны принимать решение по рассматриваемой проблеме с минимальным участием педагогического работника. Для решения поставленных задач может использоваться дополнительная литература и источники в информационно-коммуникационной сети «Интернет». Для закрепления пройденного материала педагогическим работником могут выдаваться домашние задания.

В таблице 9 указаны виды самостоятельной работы, выполняемые обучающимися при изучении соответствующих тем дисциплины.

Таблица 3 – Виды самостоятельной работы

| Наименование темы дисциплины   | Виды самостоятельной работы <i>(выбрать нужное)</i>  |
|--|--|
| Тема 1. Применение методов комбинаторики в вопросах защиты информации.                 | Изучение дополнительной литературы<br>Подготовка к экзамену  |
| Тема 2. Основные алгебраические структуры и их применение в области защиты информации. | Изучение дополнительной литературы<br>Подготовка к лабораторным/практическим работам.<br>Подготовка к экзамену |
| Тема 3. Арифметические операции над целыми числами и многочленами                      | Изучение дополнительной литературы<br>Подготовка к лабораторным/практическим работам.<br>Подготовка к экзамену |
| Тема 4. Вопросы теории вероятности и теории информации.                                | Изучение дополнительной литературы<br>Подготовка к лабораторным/практическим работам.<br>Подготовка к экзамену |
| Тема 5. Элементы теории кодирования.   | Изучение дополнительной литературы<br>Подготовка к лабораторным/практическим работам.<br>Подготовка к экзамену |
| Тема 6. Структуры данных. Организационный поиск и организация информации.              | Изучение дополнительной литературы<br>Подготовка к лабораторным/практическим работам.<br>Подготовка к экзамену |
| Тема 7. Построение математических моделей информационных процессов и угроз             | Изучение дополнительной литературы<br>Подготовка к лабораторным/практическим работам.<br>Подготовка к экзамену |
| Тема 8. Основы теории непрерывных дробей.  | Изучение дополнительной литературы<br>Подготовка к лабораторным/практическим работам.<br>Подготовка к экзамену |
| Тема 9. Проверка чисел на простоту   | Изучение дополнительной литературы   |

| Наименование темы дисциплины                         | Виды самостоятельной работы (выбрать нужное)   |
|--|--|
|  | Подготовка к лабораторным/практическим работам.<br>Подготовка к экзамену                                       |
| Тема 10. Факторизация чисел                          | Изучение дополнительной литературы<br>Подготовка к лабораторным/практическим работам.<br>Подготовка к экзамену |
| Тема 11. Дискретное логарифмирование в конечном поле | Изучение дополнительной литературы<br>Подготовка к лабораторным/практическим работам.<br>Подготовка к экзамену |
| Тема 12. Элементы теории решеток                     | Изучение дополнительной литературы<br>Подготовка к лабораторным/практическим работам.<br>Подготовка к экзамену |

Учебным планом в рамках дисциплины не предусмотрено выполнение расчетно-графической работы (РГР)/курсовое проектирование.

### 5.7. Организация текущего контроля успеваемости и промежуточной аттестации обучающихся

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины. Формы контрольно-оценочных мероприятий, проводимых в рамках текущего контроля успеваемости, представлены в таблице 10.

Таблица 10 – Формы и периодичность текущего контроля успеваемости

| Вид учебной работы                         | Форма текущего контроля успеваемости   | Периодичность осуществления |
|--|--|-----------------------------|
| Практические занятия / Лабораторные работы | Устный экспресс-опрос, экспресс-тестирование.  | На каждом занятии           |
| Самостоятельная работа обучающихся         | - устная (устный опрос, защита письменной работы, доклада по результатам самостоятельной работы, рефератов и т.д.);<br>- письменная (письменный опрос, выполнение конспектов, глоссариев, расчетно-графической работы / курсового проекта / курсовой работы и т.д.);<br>- тестовая (бланочное или компьютерное тестирование) | В течение семестра          |

Оценивание промежуточных и окончательных результатов обучения по дисциплине (промежуточная аттестация обучающихся) осуществляется в форме экзамена, проводимого в устной / письменной форме. Аттестационное испытание может включать в себя прохождение теста с использованием технологии компьютерного тестирования. Для уточнения оценки экзаменатор может проводить короткий опрос-собеседование с обучающимся и (или) выдавать ему дополнительные задания.

## 6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе освоения дисциплины применяются следующие образовательные технологии: личностно-ориентированные, активизации деятельности обучающихся, интеллектуальной направленности, проблемного обучения, диалоговые и профессионально-ориентированные (таблица 11).

Таблица 11 – Образовательные технологии, применяемые в ходе преподавания дисциплины

| Вид учебной работы                            | Применяемые образовательные технологии   |
|---|--|
| Лекции  | Проблемная лекция.<br>Лекция-визуализация.<br>Лекция-беседа.<br>Лекция-дискуссия.  |
| Практические занятия /<br>Лабораторные работы | Групповые дискуссии.<br>Решение практических задач.<br>Тестирование.<br>Деловая игра.  |
| Самостоятельная работа обучающихся            | Проработка лекционного материала.<br>Изучение рекомендуемой литературы.<br>Подготовка к дискуссии.<br>Выполнение практического задания / лабораторной работы.<br>Подготовка докладов, рефератов<br>Подготовка к лекциям.<br>Подготовка к практическим занятиям.<br>Изучение дополнительной литературы и самостоятельное формирование конспекта.<br>Подготовка к экзамену |
| Консультации                                  | Концентрация внимания на отдельных вопросах.<br>Личностно-ориентированный подход.<br>Диалог.   |
| Промежуточная аттестация обучающихся          | экзамен (в устной или письменной форме).   |

## 7. РЕАЛИЗАЦИЯ ДИСЦИПЛИНЫ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИЙ ЭЛЕКТРОННОГО ОБУЧЕНИЯ И (ИЛИ) ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

В электронной информационно-образовательной среде БГТУ размещается электронный курс дисциплины, включающий в себя:

- сведения об авторе курса;
- краткое описание курса;
- рабочую программу дисциплины;
- полный перечень тем дисциплины;
- презентационные материалы для проведения занятий лекционного типа;
- лекции/краткий конспект лекций по каждой теме;

– методические указания по выполнению каждого практического задания;

– материалы и тестовые задания для текущего контроля успеваемости и промежуточной аттестации обучающихся.

Наименование электронного курса в электронной информационно-образовательной среде БГТУ — «Математические основы защиты информации – автор Шпичак С.А. РПД для обучающихся по направлению подготовки 10.03.01 Информационная безопасность, профиль «Организация и технология защиты информации (по отрасли или в сфере профессиональной деятельности)», форма обучения – очная.

Электронный курс предназначен для обеспечения обучающихся всеми необходимыми учебно-методическими материалами, а также проведения контрольно-оценочных мероприятий в процессе обучения. При необходимости осуществляется файловый обмен отчетами о выполнении обучающимися самостоятельной работы.

## **8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

### **8.1. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся**

1. Шпичак С.А. Математические основы защиты информации. Вычисление наибольшего общего делителя [Текст] + [Электронный ресурс]: Методические указания к выполнению лабораторной работы для студентов очной формы обучения по специальности 10.05.03 – «Информационная безопасность автоматизированных систем» и направлению подготовки 10.03.01 – «Информационная безопасность». –Брянск: БГТУ, 2020. –13с.
2. Шпичак С.А. Математические основы защиты информации. Арифметические алгоритмы многократной точности для целых чисел и многочленов [Текст] + [Электронный ресурс]: Методические указания к выполнению лабораторной работы для студентов очной формы обучения по специальности 10.05.03 – «Информационная безопасность автоматизированных систем» и направлению подготовки 10.03.01 – «Информационная безопасность». –Брянск: БГТУ, 2020. –13с.
3. Шпичак С.А. Математические основы защиты информации. Вероятностные алгоритмы проверки чисел на простоту [Текст] + [Электронный ресурс]: Методические указания к выполнению лабораторной работы для студентов очной формы обучения по специальности 10.05.03 – «Информационная безопасность автоматизированных систем» и направлению подготовки 10.03.01 – «Информационная безопасность». –Брянск: БГТУ, 2020. –13с.
4. Шпичак С.А. Математические основы защиты информации. Разложение чисел на множители [Текст] + [Электронный ресурс]: Методические указания к выполнению лабораторной работы для студентов очной формы обучения по специальности 10.05.03 – «Информационная безопасность

автоматизированных систем» и направлению подготовки 10.03.01 – «Информационная безопасность». –Брянск: БГТУ, 2020. –13с.

5. Шпичак С.А. Математические основы защиты информации. Дискретное логарифмирование в конечном поле [Текст] + [Электронный ресурс]: Методические указания к выполнению лабораторной работы для студентов очной формы обучения по специальности 10.05.03 – «Информационная безопасность автоматизированных систем» и направлению подготовки 10.03.01 – «Информационная безопасность». –Брянск: БГТУ, 2020. –13с.

## **8.2. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины**

### ***а) основная литература***

1. Рытов, М.Ю. Математические основы криптологии: Задачник [Текст] + [Электронный ресурс]/ М.Ю. Рытов, И.Е. Грабежов, С.А. Шпичак. – Брянск: БГТУ, 2019. – 60 с. – (Серия «Организация и технология защиты информации»)
2. Аверченков В.И. Криптографические методы защиты информации [Текст] + [Электронный ресурс]: учебное пособие/ В.И. Аверченков, М.Ю. Рытов, С.А. Шпичак. – Брянск: БГТУ, 2017. – 216 с. – (Серия «Организация и технология защиты информации»)
3. Маховенко Е. Б. Теоретико-числовые методы в криптографии. Учебное пособие. – М.: Гелиос-АРВ, 2017. – 320 с.
4. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. – М.: КомКнига, 2017. – 328 с.
5. Глухов, М. М. Алгебра : учебник / М. М. Глухов, В.П. Елизаров, А. А. Нечаев. – СПб.: Издательство «Лань», 2020. – 608 с.
6. Глухов, М. М. Введение в теоретико-числовые методы криптографии: учебное пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. – СПб.: Издательство «Лань», 2021. – 400 с.

### ***б) дополнительная литература***

1. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии – М.: МЦНМО, 2003. – 328 с.
2. Фомичев В. М. Дискретная математика и криптология. – М.: ДИАЛОГ-МИФИ, 2003. – 400 с.
3. Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии. – Мн.: Новое знание, 2003. – 382 с.
4. Коблиц Н. Курс теории чисел и криптографии. Пер. с англ. М.: ТВП, 2001. – 254 с.
5. Кнут, Д. Искусство программирования. / Д. Кнут. – 3-е изд. – М.: Вильямс, 2000. – Т.2: Получисленные алгоритмы. – 832 с.



### **8.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», используемых при изучении дисциплины**

1. Официальный сайт ФСТЭК России [Электронный ресурс]. –Режим доступа: [www.fstec.ru](http://www.fstec.ru).
2. Официальный сайт ФСБ России [Электронный ресурс]. –Режим доступа: [www.fsb.ru](http://www.fsb.ru).
3. Исследовательский центр Агентура.ru [Электронный ресурс]. –Режим доступа: <http://www.agentura.ru/dossier/>.
4. Российский портал по безопасности. –Режим доступа: [www.secur.ru](http://www.secur.ru).
5. Электронная газета по безопасности. –Режим доступа: [www.ohrana.ru/](http://www.ohrana.ru/).

### **8.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и (или) информационных справочных систем**

Операционная система MS Windows.

1. Программы для открытия файлов форматов PDF, DJVU
2. Архиватор WinRar или аналогичный.
3. Интернет-браузер – любой.
4. MS Visual Studio 2012
5. Пакет LibreOffice.
6. Panda Free Antivirus – бесплатный антивирус.

## **9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

Для обеспечения обучения необходима следующая материально-техническая база:

- аудитория для проведения лекционных занятий и организации защиты курсовых работ/курсовых проектов, оборудованная персональными компьютерами, мультимедийным компьютерным проектором, средства звуковоспроизведения (по возможности), проекционным экраном, наличием доступа в информационно-коммуникационную сеть Интернет;
- компьютерный класс для проведения лабораторных работ с установленным комплектом программного обеспечения и доступом в информационно-коммуникационную сеть интернет, оборудованный мультимедийным компьютерным проектором, средства звуковоспроизведения (по возможности), проекционным экраном / лаборатория со специализированным оборудованием для проведения лабораторных работ;
- учебная аудитория, оснащенная комплектом мебели и доской, для проведения консультаций, зачета, зачета с оценкой, экзамена;
- компьютерные классы с постоянным доступом к информационно-телекоммуникационной сети «Интернет», а также читальные залы

научной библиотеки БГТУ для самостоятельной работы обучающихся.

## **10. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ**

Изучение дисциплины инвалидами и лицами с ограниченными возможностями здоровья организуется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

При проведении учебных занятий обеспечивается соблюдение следующих требований:

- учебные занятия проводятся для инвалидов и лиц с ограниченными возможностями здоровья в одной аудитории совместно с обучающимися, не имеющими ограниченных возможностей здоровья, если это не создает трудностей для обучающихся в ходе учебных занятий;
- присутствие ассистента из числа работников БГТУ или привлеченных лиц, оказывающего обучающимся необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочесть и оформить задание, общаться с педагогическим работником и т. п.);
- обучающиеся с учетом их индивидуальных особенностей могут пользоваться необходимыми им техническими средствами;
- материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов, лифтов, при отсутствии лифтов аудитория должна располагаться на первом этаже; наличие специальных кресел и других приспособлений).

Университетом созданы специальные условия для получения высшего образования обучающимися с ОВЗ:

- 1) для лиц с ограниченными возможностями здоровья по зрению:
  - наличие альтернативной версии официального сайта организации в сети "Интернет" для слабовидящих;
  - размещение в доступных для обучающихся, являющихся слепыми или слабовидящими, местах и в адаптированной форме (с учетом их особых потребностей) справочной информации о расписании учебных занятий (информация должна быть выполнена крупным рельефно-контрастным шрифтом (на белом или желтом фоне) и продублирована шрифтом Брайля);
  - присутствие ассистента, оказывающего обучающемуся необходимую помощь;
  - обеспечение выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);
  - обеспечение доступа обучающегося, являющегося слепым и

использующего собаку-проводника, к зданию организации;

2) для лиц с ограниченными возможностями здоровья по слуху:

- дублирование звуковой справочной информации о расписании учебных занятий визуальной (установка мониторов с возможностью трансляции субтитров (мониторы, их размеры и количество необходимо определять с учетом размеров помещения);
- обеспечение надлежащими звуковыми средствами воспроизведения информации;

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения Университета, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов, лифтов, локальное понижение стоек-барьеров; наличие специальных кресел и других приспособлений).

## 11. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

### 11.1. Методические материалы для педагогических работников

Основными формами организации обучения по дисциплине являются лекции, практические занятия и самостоятельная работа обучающихся.

**Организация теоретического обучения** предполагает использование инновационных технологий проведения занятий лекционного типа, к которым, в частности, относятся: проблемная лекция, лекция-визуализация, лекция-беседа, лекция-дискуссия, лекция-исследование.

1. *Проблемная лекция* предполагает преимущественно всесторонний анализ исторических и социокультурных, образовательных явлений, научный поиск истины. Проблемная лекция опирается на логику последовательно моделируемых проблемных ситуаций путем постановки проблемных вопросов или предъявления проблемных задач.

2. *Лекция-визуализация* реализует принцип наглядности и учит обучающихся преобразовывать устную и письменную информацию в визуальную форму, что формирует у них профессиональное мышление за счет систематизации и выделения наиболее значимых, существенных элементов содержания обучения.

3. *Лекция-беседа* является наиболее распространенной и сравнительно простой формой активного вовлечения обучающихся в учебный процесс. Такая лекция предполагает непосредственный контакт (диалог) педагогического работника с аудиторией.

4. *Лекция-дискуссия*, в которой в отличие от лекции-беседы педагогический работник при изложении лекционного материала не только

использует ответы обучающихся на свои вопросы, но и организует свободный обмен мнениями в интервалах между логическими разделами.

**Организация практических занятий по дисциплине** направлена на углубление научно-теоретических знаний обучающихся, формирование практических умений и овладение определенными методами самостоятельной работы.

Практические занятия представляют собой занятия по решению различных прикладных задач, образцы которых были даны на лекциях.

Задачи практических занятий:

- помочь обучающимся систематизировать, закрепить и углубить знания теоретического характера;
- научить обучающихся приемам решения задач из предметной области дисциплины;
- способствовать овладению навыками и умениями, входящих в структуру формируемых компетенций в результате освоения дисциплины;
- научить их работать с информацией, книгой, пользоваться справочной и научной и методической литературой;
- формировать умение учиться самостоятельно, т.е. овладевать методами, способами и приемами самообучения, саморазвития и самоконтроля.

Содержание практических работ составляют:

- устные экспресс-опросы;
- групповые дискуссии;
- выполнение практических заданий;
- письменное или компьютерное экспресс-тестирование и др.

Цели практических занятий наилучшим образом достигаются в том случае, если студент предварительно проработал тематику практического занятия. Поэтому преподаватель должен информировать студентов о теме следующего практического занятия, чтобы они могли целенаправленно самостоятельно заниматься в домашних условиях.

**Организация лабораторных занятий по дисциплине** направлена на следующие цели и задачи:

- углубление и закрепление знания теоретического курса путем практического изучения в лабораторных условиях изложенных в лекциях законов и положений;
- приобретение навыков в научном экспериментировании, анализе полученных результатов;
- формирование первичных навыков организации, планирования и проведения научных исследований.

Порядок подготовки лабораторного занятия:

- изучение требований программы дисциплины;
- формулировка цели и задач лабораторного занятия;
- разработка плана проведения лабораторного занятия;
- подбор содержания лабораторного занятия;
- разработка необходимых для лабораторного занятия инструкционных

карт;

- моделирование лабораторного занятия;
- проверка специализированной лаборатории на соответствие санитарно-гигиеническим нормам, требованиям по безопасности и технической эстетике;
- проверка количества лабораторных мест, необходимых и достаточных для достижения поставленных целей обучения;
- проверка материально-технического обеспечения лабораторных занятий на соответствие требованиям программы дисциплины.

Формы проведения лабораторных занятий:

- фронтальная;
- по циклам;
- индивидуальная;
- смешанная (комбинированная).

При проведении лабораторных работ используют три подхода к их выполнению:

- на основе рецептурных действий обучающихся, когда они проявляют умение работать преимущественно в стандартных условиях, отраженных в руководстве по лабораторному практикуму;
- на основе частично поисковых действий, когда обучающиеся могут действовать достаточно самостоятельно, решать несложные творческие задачи при подсказке или непосредственном руководстве преподавателя;
- на основе активных творческих действий обучающихся, когда они проявляют способность действовать в условиях, близких к реальным, используя запас приобретенных знаний.

***Самостоятельная работа обучающихся*** предполагает аудиторную и внеаудиторную формы организации.

Основными видами самостоятельной работы обучающихся без участия педагогического работника являются: формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.); подготовка к занятиям; составление аннотированного списка статей из соответствующих журналов по отраслям знаний и т.п.; текущий самоконтроль, выполнение расчетно-графической работы/курсового проекта/курсовой работы.

Выполнение РГР/курсового проекта/курсовой работы по дисциплине предусматривает информирование студентов о ее целях, структуре, выдачу методических указаний и задания, разъяснения по выбору варианта, ознакомление с порядком и сроками сдачи готовых материалов, проведение индивидуальных консультаций и разъяснение отдельных вопросов при необходимости.

Основными видами самостоятельной работы обучающихся с участием педагогического работника являются: текущие консультации, прием и разбор домашних заданий и др.

При подготовке к экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую литературу, консультации преподавателя и др.

## 11.2. Методические материалы для обучающихся

Обучающимся, изучающим дисциплину, необходимо знать требования, предъявляемые к их различным видам учебных занятий, в том числе лекционным, практическим, индивидуальным и др. (таблица 12).

Таблица 12 – Методические рекомендации обучающимся по освоению дисциплины

| <b>Вид учебной работы</b>   | <b>Организация деятельности обучающегося</b>  |
|---|---|
| Лекции  | Изучение дисциплины следует начинать с прослушивания и конспектирования лекций, перечитывать конспект перед выполнением домашних заданий и практическими занятиями. Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; пометать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать педагогическому работнику на консультации, на практическом занятии. Над конспектами лекций надо работать систематически: первый просмотр рекомендуется сделать вечером того же дня, когда была прочитана лекция, затем просмотреть через 3-4 дня, и сделать это еще раз накануне практического занятия. |
| Практические занятия  | Ознакомление с целью и задачами занятия. Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом. Прослушивание аудио- и видеозаписей по заданной теме. Выполнение (решение) практических заданий и задач по алгоритму, на основе частично поисковой и или исследовательской деятельности и др.   |
| Изучение дополнительной литературы и самостоятельное формирование конспекта | Ознакомление с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующих для запоминания и являющихся основополагающими в конкретной теме. Составление аннотаций к прочитанным источникам и др. Рефлексия собственных достижений  |
| Подготовка к экзамену   | При подготовке к зачету/зачету с оценкой/экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую литературу, шкалу оценивания и др.  |

## 12. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

### 12.1. Виды и средства оценивания результатов освоения дисциплины

Виды и средства оценивания результатов освоения дисциплины представлены в таблице 13.

Таблица 13 – Виды и средства оценивания результатов освоения дисциплины

| Код индикатора достижения компетенции | Оценочные средства текущего контроля успеваемости  | Оценочные средства промежуточной аттестации обучающихся |
|---------------------------------------|--|---|
| ПК-3.1.                               | 1. Устные экспресс-опросы (представлены в ФОС по дисциплине)<br>2. Экспресс-тестирование (комплекты тестов по темам представлены в ФОС по дисциплине). | Вопросы к экзамену представлены в ФОС по дисциплине     |
| ПК-3.2                                | 1. Устные экспресс-опросы (представлены в ФОС по дисциплине)<br>2. Экспресс-тестирование (комплекты тестов по темам представлены в ФОС по дисциплине). | Вопросы к экзамену представлены в ФОС по дисциплине     |
| ПК-3.3                                | 1. Устные экспресс-опросы (представлены в ФОС по дисциплине)<br>2. Экспресс-тестирование (комплекты тестов по темам представлены в ФОС по дисциплине). | Вопросы к экзамену представлены в ФОС по дисциплине     |

### 12.2. Шкала оценивания при текущем контроле успеваемости

Оценивание отдельных видов работ в процессе изучения дисциплины рекомендуется осуществлять с использованием следующей шкалы:

– обучающийся ответил правильно на более, чем 90 % заданных вопросов или вопросов-тестов, выполнил и успешно защитил практические работы, показал отличное владение навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала и т.д. – «отлично» (максимальный уровень освоения компетенций);

– обучающийся ответил правильно на 75-89% заданных вопросов или вопросов-тестов, выполнил и защитил практические работы с незначительными замечаниями, показал хорошее владение навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала и т.д. – «хорошо» (средний уровень освоения компетенций);

– обучающийся ответил правильно на 60-74% заданных вопросов или вопросов-тестов, выполнил и защитил практические работы со значительными замечаниями, показал удовлетворительное владение навыками применения полученных знаний и умений при решении профессиональных задач в рамках

усвоенного учебного материала и т.д. – «удовлетворительно» (минимальный уровень освоения компетенций);

– обучающийся ответил правильно на менее, чем 60% заданных вопросов или вопросов-тестов, не выполнил все или выполнил часть практических работ, не защитил или защитил их со значительными замечаниями, при выполнении задания обучающийся не продемонстрировал уровень самостоятельного владения умениями и навыками при решении профессиональных задач в рамках усвоенного учебного материала и т.д. – «неудовлетворительно» (минимальный уровень освоения компетенций не достигнут).

Критерии и шкала оценки доклада (реферата), его презентации (выбрать необходимое) по дисциплине представлены в таблице 14.

Таблица 14 – Критерии и шкала оценки доклада (реферата), его презентации (выбрать необходимое) по дисциплине

| Оценка                | Оцениваемые параметры  |
|-----------------------|--|
| «отлично»             | Теоретический вопрос раскрыт полностью без смысловых и логических ошибок. Задание решено верно. На защите ответ обучающегося полный и правильный. Обучающийся способен изложить решение задания, сделать собственные выводы, проанализировать основные показатели. В полном объеме представлен соответствующий графический материал.   |
| «хорошо»              | Теоретический вопрос раскрыт на достаточно высоком уровне без смысловых и логических ошибок. Задание решено верно. Имеются незначительные недочеты в определении единиц измерения, точности вычислений и т.п. На защите ответ обучающегося в целом полный и правильный. Обучающийся способен изложить решение задания, сделать собственные выводы, проанализировать основные показатели. В полном объеме представлен соответствующий графический материал.   |
| «удовлетворительно»   | Теоретический вопрос раскрыт на достаточном уровне, без существенных смысловых и логических ошибок. Задание решено верно, но имеются значительные недочеты в его решении, связанные с неполнотой ответа, с правильным исчислением одних данных и неверным – других и пр. На защите ответ неполный. Обучающийся способен четко изложить решение задания, но допускает неточности в формулировке собственных выводов и анализе основных показателей. В неполном объеме представлен графический материал. |
| «неудовлетворительно» | Теоретический вопрос не раскрыт или раскрыт не полностью при наличии разного рода неточностей и ошибок. Задание решено со значительными недочетами, с неполными ответами, с неправильным исчислением данных. На защите ответ обучающегося неполный. Обучающийся не способен четко изложить решение задания, допускает неточности в формулировке собственных выводов, не способен проанализировать основные показатели. Графический материал не представлен или представлен не в полном объеме.         |

В процесс преподавания дисциплины педагогическим работником



формируется оценка, характеризующая текущую успеваемость обучающегося.

### 12.3. Шкала оценивания при промежуточной аттестации обучающихся

При проведении промежуточной аттестации обучающихся в форме экзамена используется шкала оценивания, представленная в таблице 15.

Таблица 45 – Шкала оценивания при промежуточной аттестации обучающихся

| Уровень освоения<br>(оценка)    | Планируемые результаты освоения дисциплины  |
|---------------------------------|---|
| Высокий ( «отлично»)            | Обучающийся глубоко и прочно усвоил теоретический и практический материал, уверенно это демонстрирует в ходе промежуточной аттестации. Исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе.   |
| Повышенный ( «хорошо»)          | Обучающийся знает теоретический и практический материал, грамотно и по существу излагает его в ходе промежуточной аттестации, не допуская существенных неточностей. Правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе.   |
| Базовый ( «удовлетворительно»)  | Обучающийся знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. |
| Низкий ( «неудовлетворительно») | Обучающийся не знает на пороговом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине.            |

## 12.4. Оценивание окончательных результатов обучения по дисциплине

Итоговая оценка по дисциплине определяется с учетом результатов промежуточной аттестации обучающегося (экзамена) и оценок, полученных обучающимся в ходе текущего контроля успеваемости в семестре.

## 12.5. Характеристика результатов обучения

Характеристики результатов обучения по дисциплине в зависимости от полученной обучающимся оценки приведены в таблице 16.

Таблица 16 – Характеристика результатов обучения по дисциплине

| Оценка   | Характеристика результатов обучения   |
|--|---|
| «Отлично» (высокий уровень освоения всех индикаторов достижения компетенций в дисциплине)            | Содержание дисциплины освоено полностью, все цели достигнуты, все предусмотренные программой обучения учебные задания выполнены   |
| «Хорошо» (повышенный уровень освоения всех индикаторов достижения компетенций в дисциплине)          | Содержание дисциплины освоено полностью, все предусмотренные программой обучения учебные задания выполнены с незначительными замечаниями  |
| «Удовлетворительно» (базовый уровень освоения всех индикаторов достижения компетенций в дисциплине)  | Содержание дисциплины освоено частично, большинство предусмотренных программой обучения учебных заданий выполнено, в них имеются ошибки   |
| «Неудовлетворительно» (низкий уровень освоения всех индикаторов достижения компетенций в дисциплине) | Содержание дисциплины не освоено, большинство предусмотренных программой обучения учебных заданий либо не выполнены, либо содержат грубые ошибки; дополнительная самостоятельная работа над материалом не привела к какому-либо значительному повышению качества выполнения учебных заданий |

## 12.6. Контрольно-измерительные материалы для текущего контроля успеваемости и промежуточной аттестации обучающихся

Контрольно-измерительные материалы для текущего контроля успеваемости и промежуточной аттестации обучающихся представлены в электронном курсе «Математические основы защиты информации», размещенном в системе электронной поддержки учебных курсов на базе программного обеспечения Moodle со встроенной подсистемой тестирования (edu.tu-bryansk.ru), входящей в состав электронной информационно-образовательной среды БГТУ (<http://edu.tu-bryansk.ru>) и «Фонд оценочных средств по дисциплине «Математические основы защиты информации».

## 13. ВОСПИТАТЕЛЬНАЯ РАБОТА

В соответствии с Федеральным законом «Об образовании в Российской Федерации» воспитание - «деятельность, направленная на развитие личности, создание условий для самоопределения и социализации обучающихся на

основе социокультурных, духовно-нравственных ценностей и принятых в российском обществе правил и норм поведения в интересах человека, семьи, общества и государства, формирование у обучающихся чувства патриотизма, гражданственности, уважения к памяти защитников Отечества и подвигам Героев Отечества, закону и правопорядку, человеку труда и старшему поколению, взаимного уважения, бережного отношения к культурному наследию и традициям многонационального народа Российской Федерации, природе и окружающей среде».

В учебном процессе воспитательная работа с обучающимися реализуется средствами учебных дисциплин.

Воспитательная деятельность в ходе преподавания дисциплины направлена на формирование у обучающегося системы убеждений, нравственных норм и общекультурных качеств, на оказание им помощи в жизненном самоопределении, нравственном, гражданском и профессиональном становлении, на создание условий для самореализации личности. Воспитательная работа также ориентирует обучающихся на будущую профессиональную деятельность, формируя не только личностные, но и профессионально значимые качества.

Воспитательные задачи во время учебных занятий выполняются в скрытой (контекстной) и открытой (целенаправленной) формах. Скрытая форма воспитательной работы представляет собой воздействие всего хода педагогического процесса на становление личностных качеств обучающихся. Например, соблюдение педагогическим работником трудовой дисциплины, демонстрация преданности науке, заинтересованность в успехе обучающихся, правильная речь, хорошие манеры и т.п. имеют положительное воспитательное значение и формируют у обучающихся добросовестность, исполнительность, трудолюбие, ответственность и другие положительные качества. Обучающиеся неосознанно перенимают данные черты у педагогического работника.

Воспитание в открытой форме – это целенаправленное воздействие содержанием учебной дисциплины на становление личности обучающегося. Например, решение проблем и исследовательская работа формируют у обучающихся умение аргументировать, самостоятельно мыслить, стремление к научному поиску, развивают творчество, профессиональные умения.