



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

**Факультет информационных технологий**

*(наименование факультета/института)*

**Кафедра «Информатика и программное обеспечение»**

*(наименование кафедры, ответственной за реализацию дисциплины)*

**УТВЕРЖДАЮ**

**Первый проректор по учебной  
работе и цифровизации**

**В.А. Шкаберин**

**«22» апреля 2022 г.**

**РАБОЧАЯ ПРОГРАММА**

**учебной дисциплины**

**«Защита информации»**

*(наименование дисциплины)*

**02.03.03 Математическое обеспечение и администрирование  
информационных систем**

*(код и наименование специальности или направления подготовки)*

**Технология программирования**

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

**высшее образование – бакалавриат**

*(уровень образования)*

**бакалавр**

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

**очная**

*(форма обучения)*

**2021**

*(год набора)*

**Брянск 2022**

Рабочая программа учебной дисциплины  
«Защита информации»

(наименование дисциплины)

02.03.03 Математическое обеспечение и администрирование  
информационных систем

(код и наименование специальности или направления подготовки)

Технология программирования

(направленность (профиль)/специализация образовательной программы)

**Разработал(и):**

Доцент, к.т.н., доцент

(должность, ученая степень, ученое звание)

(подпись)

К.В. Дергачев

(И.О. Фамилия)

(должность, ученая степень, ученое звание)

(подпись)

(И.О. Фамилия)

Рассмотрена и одобрена на заседании кафедры  
«Информатика и программное обеспечение»

(наименование кафедры, ответственной за реализацию дисциплины)

«15» марта 2022 г., протокол № 7

**Заведующий кафедрой**

Доцент, к.т.н., доцент

(ученая степень, ученое звание)

(подпись)

Д.И. Копелиович

(И.О. Фамилия)

**Согласовано:**

**Заведующий выпускающей кафедрой**

«Информатика и программное обеспечение»

(наименование выпускающей кафедры)

к.т.н., доцент

(ученая степень, ученое звание)

(подпись)

Д.И. Копелиович

(И.О. Фамилия)

© К.В. Дергачев, 2022

© ФГБОУ ВО «Брянский государственный  
технический университет», 2022

## 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 .....   | 9  |
| 5.4. Лабораторные работы .....  | 13 |
| 5.5. Практические занятия .....   | 14 |
| 5.6. Самостоятельная работа обучающихся .....   | 14 |
| 5.7. Организация текущего контроля успеваемости и промежуточной<br>аттестации обучающихся .....   | 16 |
| 6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ .....   | 16 |
| 7. РЕАЛИЗАЦИЯ ДИСЦИПЛИНЫ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИЙ<br>ЭЛЕКТРОННОГО ОБУЧЕНИЯ И (ИЛИ) ДИСТАНЦИОННЫХ<br>ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ.....   | 17 |
| 8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ<br>ДИСЦИПЛИНЫ .....   | 18 |
| 8.1. Перечень учебно-методического обеспечения для самостоятельной работы<br>обучающихся .....  | 18 |
| 8.2. Перечень основной и дополнительной учебной литературы, необходимой<br>для освоения дисциплины .....  | 19 |
| 8.3. Перечень ресурсов информационно-телекоммуникационной сети<br>«Интернет», используемых при изучении дисциплины .....  | 19 |
| 8.4. Перечень информационных технологий, используемых при осуществлении<br>образовательного процесса по дисциплине, включая перечень программного<br>обеспечения и (или) информационных справочных систем ..... | 21 |
| 9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ .....   | 21 |
| 10. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА<br>ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ<br>ЗДОРОВЬЯ.....   | 22 |

|   |    |
|---|----|
| 11. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ .....  | 23 |
| 11.1. Методические материалы для педагогических работников .....  | 23 |
| 11.2. Методические материалы для обучающихся .....  | 25 |
| 12. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ .....   | 26 |
| 12.1. Виды и средства оценивания результатов освоения дисциплины .....  | 26 |
| 12.2. Шкала оценивания при текущем контроле успеваемости .....  | 27 |
| 12.3. Шкала оценивания при промежуточной аттестации обучающихся .....   | 28 |
| 12.4. Оценивание окончательных результатов обучения по дисциплине.....  | 31 |
| 12.5. Характеристика результатов обучения .....   | 31 |
| 12.6. Контрольно-измерительные материалы для текущего контроля<br>успеваемости и промежуточной аттестации обучающихся ..... | 32 |
| 13. ВОСПИТАТЕЛЬНАЯ РАБОТА .....   | 32 |

## ПРЕДИСЛОВИЕ

Учебная дисциплина «Защита информации» (далее – дисциплина) ориентирована на формирование у обучающихся компетенций в рамках основной профессиональной образовательной программы высшего образования (ОПОП ВО) по направлению подготовки 02.03.03 Математическое обеспечение и администрирование информационных систем, профиль «Технология программирования».

### 1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**Цель** освоения дисциплины – формирование у обучающихся знаний о методах и средствах защиты компьютерной информации (программ и данных) для повышения надежности и безопасности разрабатываемого программного обеспечения, научить разрабатывать собственные эффективные программные средства защиты информации.

**Задачи** дисциплины:

- формирование знаний, умений и навыков, достаточных при рассмотрении объектов, технологий, процессов, методов в области защиты информации;
- формирование умений, связанных с использованием защиты информации в интересах профессиональной культуры;
- формирование стиля мышления в категориях и терминах защиты информации.

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

Дисциплина входит в обязательную часть учебного плана образовательной программы, и реализуется на 4 курсе в 7 семестре.

Предварительно изучаются дисциплины: «Программирование, Объектно-ориентированное программирование», «Структуры и алгоритмы обработки данных».

Параллельно изучаются дисциплины: «Проектирование информационных систем».

### 3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Изучение дисциплины направлено на формирование у обучающихся компетенций ОПК-1, ОПК-6, 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 |

|  |  |  |   |  |
|--|--|--|---|--|
| ОПК-1. Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности | ОПК-1.2. Умеет использовать их в профессиональной деятельности.  | -  | Решать задачи криптографической защиты информации | -  |
|  | ОПК-1.3. Имеет навыки выбора методов решения задач профессиональной деятельности на основе теоретических знаний. | -  | -   | Навыками выбора способов и средств защиты информации |
| ОПК-6. Способен использовать в педагогической деятельности научные основы знаний в сфере информационно-коммуникационных технологий                                 | ОПК-6.1. Знает основные языки программирования, сетевые технологии, области применения веб-технологий            | Основные языки программирования, сетевые технологии, области применения веб-технологий | -   | -  |

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

Общая трудоемкость дисциплины составляет 5 зачетных единиц(ы) (180 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 |
| в том числе в форме практической подготовки  |                    |         |   |   |   |   |   |    |   |   |   |   |   |
| <b>2. Самостоятельная работа обучающихся, час.</b>   | <b>71</b>          | -       | - | - | - | - | - | 71 | - | - | - | - | - |
| <b>3. Текущий контроль успеваемости и промежуточная аттестация обучающихся, в том числе:</b> | <b>45</b>          |         |   |   |   |   |   |    |   |   |   |   |   |
| 3.1. Экзамен, семестр  |                    | 7       |   |   |   |   |   |    |   |   |   |   |   |
| 3.2. Зачет, семестр  |                    | -       |   |   |   |   |   |    |   |   |   |   |   |
| 3.3. Зачет с оценкой, семестр  |                    | -       |   |   |   |   |   |    |   |   |   |   |   |
| 3.4. Курсовой проект (контроль), семестр   |                    | -       |   |   |   |   |   |    |   |   |   |   |   |
| 3.5. Курсовая работа (контроль), семестр   |                    | 7       |   |   |   |   |   |    |   |   |   |   |   |
| 3.6. Расчетно-графическая работа (контроль), семестр   |                    | -       |   |   |   |   |   |    |   |   |   |   |   |
| 3.7. Контрольная работа (контроль), семестр  |                    | -       |   |   |   |   |   |    |   |   |   |   |   |
| <b>Общая трудоемкость (5 з.е.)</b>   | <b>180</b>         | 180     |   |   |   |   |   |    |   |   |   |   |   |

## 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 |
| <b>Раздел 1. Основы защиты информации</b>            |                    |        |                     |                      |                        |
| Тема 1. Основы информационной безопасности           | <b>12</b>          | 4      | 0                   | -                    | 8                      |
| Тема 2. Основы криптографической защиты информации   | <b>8</b>           | 2      | 0                   | -                    | 6                      |
| <b>Раздел 2. Криптографическая защита информации</b> |                    |        |                     |                      |                        |
| Тема 3. Симметричные криптографические алгоритмы     | <b>32</b>          | 6      | 14                  | -                    | 12                     |
| Тема 4. Асимметричные алгоритмы шифрования           | <b>24</b>          | 4      | 8                   | -                    | 12                     |

| Наименование раздела (темы) дисциплины                     | Трудоемкость, час. |           |                     |                      |                        |
|--|--------------------|-----------|---------------------|----------------------|------------------------|
|  | Всего              | Лекции    | Лабораторные работы | Практические занятия | Самостоятельная работа |
| Тема 5. Аутентификация. Электронная цифровая подпись       | 22                 | 6         | 6                   | -                    | 10                     |
| Тема 6. Управление криптографическими ключами              | 17                 | 4         | 4                   | -                    | 9                      |
| <b>Раздел 3. Защита информации в компьютерных сетях</b>    |                    |           |                     |                      |                        |
| Тема 7. Защита информации в компьютерных сетях             | 12                 | 4         | 0                   | -                    | 8                      |
| <b>Раздел 4. Законодательный уровень защиты информации</b> |                    |           |                     |                      |                        |
| Тема 8. Законодательный уровень защиты информации          | 8                  | 2         | 0                   | -                    | 6                      |
| <b>Итого</b>   | <b>135</b>         | <b>32</b> | <b>32</b>           | <b>-</b>             | <b>71</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 |      |
|--|-----------------|------|
|  | ОПК1            | ОПК6 |
| Тема 1. Основы информационной безопасности           | +               |      |
| Тема 2. Основы криптографической защиты информации   | +               |      |
| Тема 3. Симметричные криптографические алгоритмы     | +               | +    |
| Тема 4. Асимметричные алгоритмы шифрования           | +               | +    |
| Тема 5. Аутентификация. Электронная цифровая подпись | +               | +    |
| Тема 6. Управление криптографическими ключами        | +               | +    |
| Тема 7. Защита информации в компьютерных сетях       | +               | +    |
| Тема 8. Законодательный уровень защиты информации    | +               |      |



### 5.3. Лекции

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

Таблица 5 – Тематика и содержание лекций

| Наименование темы дисциплины               | Тема лекции   | Содержание лекции   | Трудоемкость, час. |
|--|---|---|--------------------|
| Тема 1. Основы информационной безопасности | История защиты информации, основные понятия и определения | История развития проблемы защиты информации. Актуальность и важность проблемы обеспечения защиты информации. Современная ситуация в области информационной безопасности. Категории информационной безопасности и информационных систем. Модели защиты информации. Автоматизированные системы обработки данных (АСОД). Основные понятия информационной безопасности: безопасность АСОД, несанкционированный доступ (НСД), разграничение доступа, субъекты и объекты доступа, конфиденциальность и целостность информации, угроза безопасности, уязвимость, атака, комплекс средств защиты, политика безопасности. Информация как объект защиты: важность и уровень секретности. Основные угрозы безопасности АСОД. Классификация и анализ возможных угроз безопасности. Природные и технические угрозы. Угрозы созданные людьми. Случайные угрозы. Преднамеренные угрозы. Модель нарушителя. Пути реализации угроз безопасности. Каналы и способы НСД к конфиденциальной информации. | 2                  |

| Наименование темы дисциплины                       | Тема лекции  | Содержание лекции  | Трудоемкость, час. |
|--|--|--|--------------------|
| Тема 1. Основы информационной безопасности         | Противодействие угрозам. Политика безопасности               | Противодействие угрозам. Принципы разработки систем защиты информации. Этапы построения системы защиты. Виды и уровни защиты информации. Оценка рисков и безопасности АСОД. Подходы к проблеме обеспечения безопасности АСОД. Этапы создания и компоненты политики безопасности. Избира- тельная и полномочная политики безопасности.  | 2                  |
| Тема 2. Основы криптографической защиты информации | Основы криптографической защиты информации                   | Основные понятия криптологии. Принципы криптографической защиты информации. Краткий обзор и классификация методов шифрования информации. Схемы симметричной и асимметричной криптосистем. Классификация криптографических алгоритмов. Фундаментальное правило криптоанализа. Криптоанализ и виды криптоаналитических атак. Шифры перестановки. Шифры простой замены. Шифры сложной замены. Одноразовая система шифрования. | 2                  |
| Тема 3. Симметричные криптографические алгоритмы   | Современные блочные симметричные криптографические алгоритмы | Принципы построения современных симметричных криптосистем по К.Шеннону. Составные блочные шифры. Криптоалгоритмы DES, IDEA, ГОСТ 28147-89, AES. Режимы работы и области применения современных блочных алгоритмов шифрования. Комбинирование блочных алгоритмов.   | 4                  |

| Наименование темы дисциплины                         | Тема лекции  | Содержание лекции  | Трудоемкость, час. |
|--|--|--|--------------------|
| Тема 3. Симметричные криптографические алгоритмы     | Гаммирование и сравнительный анализ блочных и поточных методов шифрования. | Основные понятия гаммирования. Методы генерации псевдослучайных последовательностей чисел. Сравнительный анализ блочных и поточных методов шифрования.   | 2                  |
| Тема 4. Асимметричные алгоритмы шифрования           | Асимметричные алгоритмы шифрования   | Концепция асимметричных криптосистем с открытым ключом. Однонаправленные функции. Асимметричные криптоалгоритмы: RSA, Полига-Хеллмана, Эль Гамаля. Оценка их безопасности и скорости.  | 2                  |
| Тема 4. Асимметричные алгоритмы шифрования           | Комбинированный метод шифрования данных                                    | Сравнительный анализ симметричных и асимметричных криптосистем. Комбинированный метод шифрования данных. Оптимальные длины ключей симметричной и асимметричной криптосистем.   | 2                  |
| Тема 5. Аутентификация. Электронная цифровая подпись | Электронная цифровая подпись (ЭЦП). Однонаправленные хэш-функции.          | Цель и задачи аутентификации данных. Электронная цифровая подпись (ЭЦП). Схема формирования и проверки ЭЦП. Однонаправленные хэш-функции. Требования, предъявляемые к хэш-функциям. Хэш-функции на основе симметричных блочных алгоритмов. Безопасные схемы хеширования. | 2                  |
| Тема 5. Аутентификация. Электронная цифровая подпись | Алгоритмы ЭЦП и хеширования  | Алгоритм хеширования SHA. Стандарт хэш-функции ГОСТ Р 34.11-94. Алгоритмы и стандарты ЭЦП (RSA, EGSA, DSA, ГОСТ Р 34.10-94).   | 2                  |
| Тема 5. Аутентификация. Электронная цифровая подпись | Аутентификация и взаимная проверка подлинности                             | Основные понятия и концепции идентификации и проверки подлинности. Механизмы аутентификации. Механизмы взаимной проверки подлинности.  | 2                  |

| Наименование темы дисциплины                      | Тема лекции                                      | Содержание лекции  | Трудоемкость, час. |
|---|--|--|--------------------|
|   |  | Алгоритмы идентификации с нулевой передачей знаний.  |                    |
| Тема 6. Управление криптографическими ключами     | Управление ключами. Генерация и хранение ключей. | Основные понятия и концепции управления ключами. Механизмы генерации надежных криптографических ключей. Хранение ключей.   | 2                  |
| Тема 6. Управление криптографическими ключами     | Методы распространения ключей                    | Методы распространения ключей. Сертификаты. Метод Диффи-Хеллмана.  | 2                  |
| Тема 7. Защита информации в компьютерных сетях    | Основы безопасности компьютерных сетей           | Проблемы безопасности сетей. Уровни безопасности сетевых систем. Источники угроз в сетях. Виды сетевых угроз и противодействие им. Принципы построения системы защиты информации в вычислительных сетях. Удаленные атаки через сеть Internet. Уязвимости протоколов и служб Internet. Объекты защиты. Политика сетевой безопасности.                             | 2                  |
| Тема 7. Защита информации в компьютерных сетях    | Межсетевые экраны                                | Межсетевые экраны (МЭ). Компоненты МЭ. Основные схемы защиты на базе МЭ. Модули МЭ. Программные методы защиты, реализуемые МЭ.   | 2                  |
| Тема 8. Законодательный уровень защиты информации | Законодательный уровень защиты информации        | Реализация законодательного уровня защиты информации в РФ. Конституция. Закон об информатизации. Закон об электронной цифровой подписи. Уголовный кодекс РФ о незаконном использовании объектов авторского права и смежных прав. Международные и отечественные требования по защите информации и их стандартизация. Уровни безопасности информации. Требования к | 2                  |

| Наименование темы дисциплины | Тема лекции | Содержание лекции                        | Трудоемкость, час. |
|------------------------------|-------------|--|--------------------|
|                              |             | криптографическим алгоритмам и системам. |                    |
| <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 темы дисциплины                     | Тема лабораторной работы                                 | Трудоемкость, час. |
|--|--|--------------------|
| Тема 3. Симметричные криптографические алгоритмы | Методы простых замен. Шифрование.                        | 2                  |
| Тема 3. Симметричные криптографические алгоритмы | Методы простых замен. Дешифрация.                        | 2                  |
| Тема 3. Симметричные криптографические алгоритмы | Методы перестановок. Шифрование.                         | 2                  |
| Тема 3. Симметричные криптографические алгоритмы | Методы перестановок. Дешифрация.                         | 2                  |
| Тема 3. Симметричные криптографические алгоритмы | Криптоанализ шифров замен. Шифрование.                   | 2                  |
| Тема 3. Симметричные криптографические алгоритмы | Криптоанализ шифров замен. Расшифрование и криптоанализ. | 2                  |
| Тема 3. Симметричные криптографические алгоритмы | Методы сложных замен. Шифрование.                        | 2                  |
| Тема 3. Симметричные криптографические алгоритмы | Методы сложных замен. Дешифрация.                        | 2                  |

|  |   |           |
|--|---|-----------|
| Тема 3. Симметричные криптографические алгоритмы     | Методы генерации псевдослучайных последовательностей чисел. Реализация первой ступени генератора.               | 2         |
| Тема 3. Симметричные криптографические алгоритмы     | Методы генерации псевдослучайных последовательностей чисел. Реализация второй ступени генератора. Гаммирование. | 2         |
| Тема 6. Управление криптографическими ключами        | Современные симметричные криптосистемы. Генерация раундовых ключей.   | 2         |
| Тема 3. Симметричные криптографические алгоритмы     | Современные симметричные криптосистемы. Программная реализация криптоалгоритма.                                 | 4         |
| Тема 4. Асимметричные алгоритмы шифрования           | Программная реализация фрагментов асимметричных криптосистем.   | 2         |
| Тема 5. Аутентификация. Электронная цифровая подпись | Программная реализация алгоритмов электронной цифровой подписи.   | 4         |
| <b>Итого</b>   | —   | <b>32</b> |

### 5.5. Практические занятия

Практические занятия по дисциплине не 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 дисциплины | Тема практического занятия | Содержание практического занятия | Трудоемкость, час. |
|------------------------------|----------------------------|----------------------------------|--------------------|
| <b>Итого</b>                 | -                          | -                                | -                  |

### 5.6. Самостоятельная работа обучающихся

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

Таблица 8 – Вопросы для самостоятельного изучения дисциплины

| Наименование темы дисциплины                     | Вопросы для самостоятельного изучения темы   |
|--|--|
| Тема 3. Симметричные криптографические алгоритмы | 1. Основы криптографического алгоритма BlowFish<br>2. Основы криптографического алгоритма MARS<br>3. Основы криптографического алгоритма RC6 |
| Тема 4. Асимметричные алгоритмы шифрования       | 1. Асимметричные алгоритмы шифрования на эллиптических кривых  |

| Наименование темы дисциплины                         | Вопросы для самостоятельного изучения темы  |
|--|---|
| Тема 5. Аутентификация. Электронная цифровая подпись | 1. Основы метода хеширования MD5<br>2. Сравнительный анализ группы методов хеширования SHA<br>3. Сравнительный анализ методов ЭЦП |
| Тема 8. Законодательный уровень защиты информации    | 1. Требования ГОСТ к системам защиты информации   |

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 9 – Виды самостоятельной работы

| Наименование темы дисциплины                         | Виды самостоятельной работы  |
|--|--|
| Тема 1. Основы информационной безопасности           | Написание конспекта.<br>Проработка и повторение лекционного материала.<br>Изучение рекомендуемой литературы  |
| Тема 2. Основы криптографической защиты информации   | Написание конспекта.<br>Составление глоссария по теме.<br>Проработка и повторение лекционного материала.<br>Изучение рекомендуемой литературы<br>Выполнение курсовой работы  |
| Тема 3. Симметричные криптографические алгоритмы     | Самостоятельное изучение вопросов темы.<br>Написание конспекта.<br>Проработка и повторение лекционного материала.<br>Изучение рекомендуемой литературы<br>Выполнение лабораторной работы<br>Выполнение курсовой работы |
| Тема 4. Асимметричные алгоритмы шифрования           | Самостоятельное изучение вопросов темы.<br>Написание конспекта.<br>Проработка и повторение лекционного материала.<br>Изучение рекомендуемой литературы<br>Выполнение лабораторной работы<br>Выполнение курсовой работы |
| Тема 5. Аутентификация. Электронная цифровая подпись | Самостоятельное изучение вопросов темы.<br>Написание конспекта.<br>Проработка и повторение лекционного материала.<br>Изучение рекомендуемой литературы<br>Выполнение лабораторной работы<br>Выполнение курсовой работы |
| Тема 6. Управление криптографическими ключами        | Написание конспекта.<br>Проработка и повторение лекционного материала.<br>Изучение рекомендуемой литературы<br>Выполнение лабораторной работы  |

| Наименование темы дисциплины                      | Виды самостоятельной работы  |
|---|--|
|   | Выполнение курсовой работы   |
| Тема 7. Защита информации в компьютерных сетях    | Написание конспекта.<br>Проработка и повторение лекционного материала.<br>Изучение рекомендуемой литературы  |
| Тема 8. Законодательный уровень защиты информации | Самостоятельное изучение вопросов темы.<br>Написание конспекта.<br>Проработка и повторение лекционного материала.<br>Изучение рекомендуемой литературы |

Учебным планом в рамках дисциплины предусмотрено курсовое проектирование.

Курсовое проектирование осуществляется в соответствии с методическими указаниями, содержащимися в соответствующем разделе электронного курса «Защита информации» информационно-образовательной среды БГТУ (<http://edu.tu-bryansk.ru>).

### 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 |
|------------------------------------|--|-----------------------------|
| Лабораторные работы                | Устный экспресс-опрос, защита лабораторных работ.  | На каждом занятии           |
| Самостоятельная работа обучающихся | - устная (устный опрос, защита курсовой работы);<br>- письменная (письменный опрос, выполнение конспектов, курсовой работы);<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.   |
| Лабораторные работы                  | Групповые дискуссии.<br>Решение практических задач.<br>Тестирование.  |
| Самостоятельная работа обучающихся   | Проработка лекционного материала.<br>Изучение рекомендуемой литературы.<br>Подготовка к дискуссии.<br>Выполнение лабораторной работы.<br>Выполнение курсовой работы<br>Подготовка к лекциям.<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;
- методические указания для выполнения курсовой работы;
- материалы и тестовые задания для текущего контроля успеваемости и промежуточной аттестации обучающихся.

Наименование электронного курса в электронной информационно-образовательной среде БГТУ — «Защита информации» – автор Дергачев К.В. – для обучающихся по направлению подготовки 02.03.03 Математическое обеспечение и администрирование информационных систем, профиль «Технология программирования», 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. Дергачев, К.В. Защита информации. Методы простых замен. Шифрование: методические указания к выполнению лабораторной работы №1 / К.В. Дергачев. – Брянск: БГТУ, 2022. – 16 с.
2. Дергачев, К.В. Защита информации. Методы простых замен. Дешифрация: методические указания к выполнению лабораторной работы №2 / К.В. Дергачев. – Брянск: БГТУ, 2022. – 12 с.
3. Дергачев, К.В. Защита информации. Методы перестановок. Шифрование: методические указания к выполнению лабораторной работы №3 / К.В. Дергачев. – Брянск: БГТУ, 2022. – 12 с.
4. Дергачев, К.В. Защита информации. Методы перестановок. Дешифрация: методические указания к выполнению лабораторной работы №4 / К.В. Дергачев. – Брянск: БГТУ, 2022. – 8 с.
5. Дергачев, К.В. Защита информации. Криптоанализ шифров замен. Шифрование: методические указания к выполнению лабораторной работы №5 / К.В. Дергачев. – Брянск: БГТУ, 2022. – 20 с.
6. Дергачев, К.В. Защита информации. Криптоанализ шифров замен. Расшифрование и криптоанализ: методические указания к выполнению лабораторной работы №6 / К.В. Дергачев. – Брянск: БГТУ, 2022. – 12 с.
7. Дергачев, К.В. Защита информации. Методы сложных замен. Шифрование: методические указания к выполнению лабораторной работы №7 / К.В. Дергачев. – Брянск: БГТУ, 2022. – 8 с.
8. Дергачев, К.В. Защита информации. Методы сложных замен. Дешифрация: методические указания к выполнению лабораторной работы №8 / К.В. Дергачев. – Брянск: БГТУ, 2022. – 16 с.
9. Дергачев, К.В. Защита информации. Методы генерации псевдослучайных последовательностей чисел. Реализация первой ступени генератора: методические указания к выполнению лабораторной работы №9 / К.В. Дергачев. – Брянск: БГТУ, 2022. – 15 с.
10. Дергачев, К.В. Защита информации. Методы генерации псевдослучайных последовательностей чисел. Реализация второй ступени генератора. Гаммирование: методические указания к выполнению лабораторной работы №10 / К.В. Дергачев. – Брянск: БГТУ, 2022. – 12 с.

11. Дергачев, К.В. Защита информации. Современные симметричные криптосистемы. Генерация раундовых ключей: методические указания к выполнению лабораторной работы №11 / К.В. Дергачев. – Брянск: БГТУ, 2022. – 11 с.

12. Дергачев, К.В. Защита информации. Современные симметричные криптосистемы. Программная реализация криптоалгоритма: методические указания к выполнению лабораторной работы №12 / К.В. Дергачев. – Брянск: БГТУ, 2022. – 15 с.

13. Дергачев, К.В. Защита информации. Программная реализация фрагментов асимметричных криптосистем: методические указания к выполнению лабораторной работы №13 / К.В. Дергачев. – Брянск: БГТУ, 2022. – 16 с.

14. Дергачев, К.В. Защита информации. Программная реализация алгоритмов электронной цифровой подписи: методические указания к выполнению лабораторной работы №14 / К.В. Дергачев. – Брянск: БГТУ, 2022.

15. Дергачев, К.В. Защита информации. Методические указания к выполнению курсовой работы / К.В. Дергачев. – Брянск: БГТУ, 2022. – 12 с.

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

### ***а) основная литература***

1. Басалова, Г. В. Основы криптографии : учебное пособие / Г. В. Басалова. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 282 с. — ISBN 978-5-4497-0340-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/89455.html>.

2. Дергачев, К.В. Защита информации: лабораторный практикум: учеб. пособие/ К.В. Дергачев, Д.В. Титарев. М: Русайнс, – 2021. – 156 с.

3. Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие / Б. А. Фороузан ; под редакцией А. Н. Берлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 776 с. — ISBN 978-5-4497-0946-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/102017.html>.

4. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/87995.html>.

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

1. Ожиганов, А.А. Криптография [Электронный ресурс] : учебное пособие / А.А. Ожиганов. – Электрон. текстовые данные. – СПб.: Университет

ИТМО, 2016. – 142 с. – Режим доступа: <http://www.iprbookshop.ru/67231.html>. – ЭБС «IPRbooks».

2. Майстренко, Н. В. Основы теории информации и криптографии : учебное пособие / Н. В. Майстренко, А. В. Майстренко. — Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2018. — 81 с. — ISBN 978-5-8265-1950-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/94362.html>

3. Петров, А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. — 2-е изд. — Саратов : Профобразование, 2019. — 446 с. — ISBN 978-5-4488-0091-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/87998.html>

#### ***в) справочная литература***

1. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – Взамен ГОСТ Р 34.10-94 ; введ. 01.07.2002. – М.: Изд-во стандартов, 2001. – 11 с.

2. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – Взамен ГОСТ Р 34.10-2001; введ. 01.01.2013. – М.: Стандартиформ, 2013.

3. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хеширования. – Взамен ГОСТ Р 34.11-94; введ. 01.01.2013. – М.: Стандартиформ, 2013. – 34 с.

4. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – введ. 02.06.89 – М.: Изд-во стандартов, 1996.

5. Савельев А.И. Комментарий к Федеральному закону от 27 июля 2006 г. №149- ФЗ «Об информации, информационных технологиях и защите информации» (постатейный) [Электронный ресурс] / А.И. Савельев. — Электрон. текстовые данные. – М. : Статут, 2015. – 320 с. – Режим доступа: <http://www.iprbookshop.ru/49072.html>. – ЭБС «IPRbooks».

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

1. Сайт научной библиотеки БГТУ (<https://libri.tu-bryansk.ru>)
2. Электронно-библиотечная система «Лань» (<https://e.lanbook.com>).

3. Электронно-библиотечная система «IPRbooks»  
(<http://www.iprbookshop.ru>).
4. Электронно-библиотечная система ИД «Гребенников»  
(<https://grebennikon.ru>).
5. Единое окно доступа к информационным ресурсам  
(<http://window.edu.ru>).
6. Национальная электронная библиотека (<http://www.elibrary.ru>).

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

1. Операционная система класса MS Windows или Linux.
2. Любая среда разработки программного обеспечения (рекомендуется MS Visual Studio).
3. Пакет офисных прикладных программ OpenOffice или Microsoft Office.
4. Справочная правовая система «КонсультантПлюс»

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

Для обеспечения обучения необходима следующая материально-техническая база:

- аудитория для проведения лекционных занятий и организации защиты курсовых работ, 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;
- учебная аудитория, оснащенная комплектом мебели и доской, для проведения консультаций, 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, прочитывать 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 субтит-

ров (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 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 положений;

- приобретение навыков в 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 курсовой работы.

Выполнение курсовой работы по дисциплине предусматривает информи-



рование 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

| Вид учебной работы  | Организация деятельности обучающегося   |
|---|---|
| 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 лабораторного занятия. |
| Лабораторные работы   | Подготовка к выполнению работы (ознакомление с целью и задачами, ходом лабораторной работы, работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, построение алгоритма, выполнение работы (написание программы), оформление результатов лабораторной работы и др.). Анализ полученных результатов. Защита лабораторной работы (программы).  |
| 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  |

| <b>Вид учебной работы</b>  | <b>Организация деятельности обучающегося</b>  |
|----------------------------|---|
| Выполнение курсовой работы | При выполнении курсовой работы, обучающемуся следует придерживаться методических указаний. Предусмотрен следующий алгоритм действий: выбор варианта темы курсовой работы, подбор и систематизация теоретического материала, являющегося основой для написания теоретического раздела/решения практических задач, выполнение работы по заданному варианту (написание программы и документации на нее) и анализ полученных значений, формулирование выводов по полученным результатам. Выполненная работа передается преподавателю на проверку. При необходимости осуществляется доработка отдельных частей работы с учетом требований и замечаний преподавателя. |
| Подготовка к экзамену      | При подготовке к 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

| <b>Код индикатора достижения компетенции</b> | <b>Оценочные средства текущего контроля успеваемости</b>   | <b>Оценочные средства промежуточной аттестации обучающихся</b> |
|--|--|--|
| ОПК-1.2.                                     | 1. Устные экспресс-опросы. (темы 1-2).<br>2. Защита лабораторных работ (темы 3-6)<br>3. Экспресс-тестирование (комплекты тестов по темам 1-8).<br>4. Курсовая работа (темы 3-6). | Вопросы к экзамену представлены в ФОС по дисциплине.           |
| ОПК-1.3.                                     | 1. Защита лабораторных работ (темы 3-6)<br>2. Курсовая работа (темы 3-6).  | Вопросы к экзамену представлены в ФОС по дисциплине.           |
| ОПК-6.1.                                     | 1. Защита лабораторных работ (темы 3-6)<br>2. Экспресс-тестирование (комплекты тестов по темам 3-7).<br>Курсовая работа (темы 3-6).  | 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 презентации доклада по дисциплине представлены в таблице 14.

Таблица 14 – Критерии и шкала оценки презентации доклада 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 |

| Оценка                | Оцениваемые параметры  |
|-----------------------|--|
|                       | 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 15 – Шкала оценивания при промежуточной аттестации обучающихся

| Уровень освоения (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.   |

| Уровень освоения<br>(оценка)   | Планируемые результаты освоения дисциплины   |
|--------------------------------|--|
| Базовый («удовлетворительно»)  | Обучающийся знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении в ходе промежуточной аттестации.<br>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.               |

Уровень знаний, умений и навыков обучающегося при выполнении и защите курсовой работы оценивается по пятибалльной системе. Шкала оценивания представлена в таблице 16.

Таблица 16 – Шкала оценивания, применяемая при выполнении и защите курсовой работы

| Уровень освоения<br>(оценка) | Планируемые результаты освоения дисциплины   |
|------------------------------|--|
| «отлично»                    | <p><b>а) Содержание работы:</b></p> <ul style="list-style-type: none"> <li>– работа полностью соответствует теме исследования;</li> <li>– грамотно обоснована актуальность работы;</li> <li>– обучающийся показывает глубокую общетеоретическую подготовку;</li> <li>– обучающийся корректно использует терминологический аппарат;</li> <li>– в работе используются актуальные источники, нормативные документы, законодательные акты;</li> <li>– обучающийся демонстрирует умение работать с различными видами источников информации, в том числе с данными, полученными экспериментальным путем и с электронными библиотечными системами вуза;</li> <li>– обучающийся проявляет умение обобщать, систематизировать и научно классифицировать материал;</li> <li>– исследование завершается научно-значимыми выводами и/или практическими рекомендациями.</li> </ul> <p><b>б) Владение навыками научного исследования:</b></p> <ul style="list-style-type: none"> <li>– обучающийся владеет методологическими подходами к изучению предмета исследования и конкретными методиками;</li> <li>– обучающийся умеет грамотно составить программу исследования (определить научную проблему, объект, предмет, цели, задачи,</li> </ul> |

| Уровень освоения<br>(оценка) | Планируемые результаты освоения дисциплины  |
|------------------------------|---|
|                              | <p>подобрать методы исследования), обосновать научную новизну и/или практическую значимость данного исследования;</p> <ul style="list-style-type: none"> <li>– обучающийся умеет делать аргументированные выводы, соответствующие поставленным целям и задачам;</li> <li>– обучающийся умеет предложить варианты использования результатов исследования в профессиональной деятельности.</li> </ul> <p><b>в) Оформление курсовой работы (проекта):</b></p> <ul style="list-style-type: none"> <li>– работа оформлена в соответствии с локальными актами.</li> </ul> <p><b>г) Защита курсовой работы (проекта):</b></p> <ul style="list-style-type: none"> <li>– обучающийся в устном выступлении на защите адекватно представляет результаты исследования;</li> <li>– обучающийся аргументированно отвечает на вопросы и ведет научную дискуссию;</li> <li>– обучающийся владеет научным стилем изложения;</li> <li>– обучающийся владеет понятийным аппаратом.</li> </ul>  |
| «хорошо»                     | <p><b>а) Содержание работы:</b></p> <ul style="list-style-type: none"> <li>– полностью соответствует теме исследования;</li> <li>– актуальность работы обоснована недостаточно аргументированно;</li> <li>– обучающийся показывает достаточную общетеоретическую подготовку, допуская погрешности в использовании терминологического аппарата;</li> <li>– обзор теоретических и практических наработок по проблеме имеет описательный, а не аналитический характер;</li> <li>– источниковая база исследования недостаточно широкая;</li> <li>– обучающийся демонстрирует умение работать с различными видами источников, в том числе с данными, полученными экспериментальным путем;</li> <li>– обучающийся проявляет способности обобщать, систематизировать и научно классифицировать материал;</li> <li>– в работе отсутствуют научно-значимые выводы и/или практические результаты.</li> </ul> <p><b>б) Владение навыками научного исследования:</b></p> <ul style="list-style-type: none"> <li>– не обоснована научная новизна и практическая значимость данного исследования;</li> <li>– присутствуют отдельные недочеты в программе исследования (недостаточно аргументированно определена научная проблема, неверно сформулированы объект, предмет, цели, задачи, методы исследования подобраны не вполне корректно);</li> <li>– выводы исследования недостаточно аргументированны, не соответствуют поставленным целям и задачам.</li> </ul> <p><b>в) Оформление курсовой работы (проекта):</b></p> <ul style="list-style-type: none"> <li>– работа оформлена в соответствии с локальными актами.</li> </ul> <p><b>г) Защита курсовой работы (проекта):</b></p> <ul style="list-style-type: none"> <li>– обучающийся в устном выступлении на защите адекватно представляет результаты исследования;</li> <li>– обучающийся владеет научным стилем изложения;</li> <li>– обучающийся владеет понятийным аппаратом;</li> </ul> |

| Уровень освоения<br>(оценка) | Планируемые результаты освоения дисциплины  |
|------------------------------|---|
|                              | – обучающийся во время защиты не смог ответить на ряд вопросов по предмету исследования.  |
| «удовлетворительно»          | <p><b>а) Содержание работы:</b></p> <ul style="list-style-type: none"> <li>– частично соответствует теме исследования;</li> <li>– не обоснована актуальность работы;</li> <li>– обучающийся обнаружил удовлетворительные знания по предмету;</li> <li>– в работе отсутствует обзор теоретических и практических наработок по проблеме;</li> <li>– источниковая база исследования недостаточно широка, обучающийся использует лишь данные научной литературы;</li> <li>– обучающийся не сумел продемонстрировать умение работать с различными видами источников;</li> <li>– в работе отсутствуют научно-значимые выводы или практические результаты.</li> </ul> <p><b>б) Оформление курсовой работы (проекта):</b></p> <ul style="list-style-type: none"> <li>– работа оформлена в соответствии с локальными актами.</li> </ul> <p><b>в) Защита курсовой работы (проекта):</b></p> <ul style="list-style-type: none"> <li>– в устном выступлении на защите обучающийся не может адекватно представить результаты исследования;</li> <li>– обучающийся отступает от научного стиля изложения;</li> <li>– обучающийся затрудняется в аргументации, отвечая на вопросы по теме работы.</li> </ul> |
| «неудовлетворительно»        | <ul style="list-style-type: none"> <li>– имеются принципиальные замечания по пяти и более параметрам курсовой работы (проекта);</li> <li>– обучающийся допустил грубые теоретические ошибки, не владеет навыками исследования.</li> </ul>   |

#### 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 18.

Таблица 18 – 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 |

| Оценка   | Характеристика результатов обучения   |
|--|---|
| «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 «Защита 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 «Защита 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.