

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Баламирзоев Назим Лиодинович  
Должность: Ректор  
Дата подписания: 07.11.2025 09:35:38  
Уникальный программный ключ:  
5cf0d6f89e80f49a334f6a4ba58e91f3326b9926

Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение  
высшего образования

«Дагестанский государственный технический университет»

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина Методы и средства криптографической защиты информации  
наименование дисциплины по ОПОП

для направления 10.03.01 Информационная безопасность  
код и полное наименование специальности

по профилю Безопасность автоматизированных систем

факультет Компьютерных технологий, вычислительной техники и энергетики  
наименование факультета, где ведется дисциплина

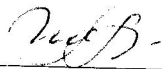
кафедра Информационная безопасность  
наименование кафедры, за которой закреплена дисциплина

Форма обучения очная, очно-заочная курс 4 семестр (ы) 7  
очная, очно-заочная, заочная

г. Махачкала 2021

Программа составлена в соответствии с требованиями ФГОС ВО по направлению 10.03.01 Информационная безопасность с учетом рекомендаций и ОПОП ВО по направления 10.03.01 Информационная безопасность и профилю Безопасность автоматизированных систем.

Разработчик



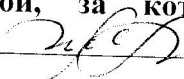
подпись

Качаева Г.И., к.э.н.

(ФИО уч. степень, уч. звание)

« 18 » 09 2021 г.

Зав. кафедрой, за которой закреплена дисциплина (модуль)



подпись

Качаева Г.И., к.э.н.

(ФИО уч. степень, уч. звание)

«20» сентября 2021 г.

Программа одобрена на заседании выпускающей кафедры Информационная безопасность от 20 сентября 2021 года, протокол № 2.

Зав. выпускающей кафедрой по данному направлению (специальности, профилю)



подпись

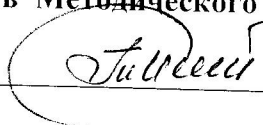
Качаева Г.И., к.э.н.

(ФИО уч. степень, уч. звание)

«20» сентября 2021 г.

Программа одобрена на заседании Методического совета факультета Компьютерных технологий, вычислительной техники и энергетики от «18» октября 2021 г., протокол № 2

Председатель Методического совета факультета КТВТиЭ



подпись

Исабекова Т.И., к.ф-м.н., доцент

(ФИО уч. степень, уч. звание)

от «18» октября 2021 г.

Декан факультета



подпись

Юсуфов Ш.А.

ФИО

Начальник УО

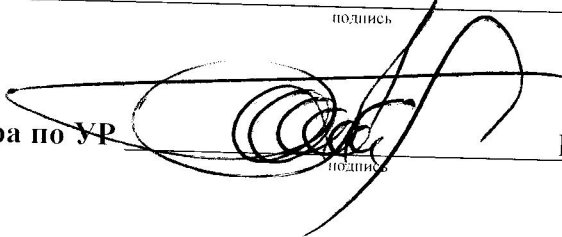


подпись

Магомаева Э.В.

ФИО

И.о проректора по УР



подпись

Баламирзоев Н.А.

ФИО

### **1. Цели и задачи освоения дисциплины.**

Целями освоения дисциплины (модуля) «Методы и средства криптографической защиты информации» является формирование у студентов общих представлений о криптографических методах защиты информации, о применении криптографических методов защиты информации для решения отдельных задач обеспечения информационной безопасности и об основных принципах, лежащих в основе функционирования криптографических средств защиты информации.

### **2. Место дисциплины в структуре ОПОП**

Дисциплина «Методы и средства криптографической защиты информации» относится к блоку I (Обязательная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Алгебра и геометрия, Дискретная математика, Информатика, Основы информационной безопасности, Математическая логика и теория алгоритма.

Последующими дисциплинами являются: Управление информационной безопасностью, Защита программ и данных, Обеспечение ИБ в интеллектуальных системах.

### **3. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)**

В результате освоения дисциплины «Методы и средства криптографической защиты информации» студент должен овладеть следующими компетенциями:

| <b>Код компетенции</b> | <b>Наименование компетенции</b>                                                                                               | <b>Наименование показателя оценивания (показатели достижения заданного уровня освоения компетенций)</b>                                                                                                                                     |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ОПК-9                  | Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности | ОПК-9.1.1 - знает основные понятия и задачи криптографии, математические модели криптографических систем                                                                                                                                    |
|                        |                                                                                                                               | ОПК-9.1.2 - знает основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и криптографические протоколы |
|                        |                                                                                                                               | ОПК-9.1.3- знает национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения                                                                                                            |

#### 4. Объем и содержание дисциплины (модуля)

| Форма обучения                                                                                                                    | очная                   | очно-<br>заочная        | заочная |
|-----------------------------------------------------------------------------------------------------------------------------------|-------------------------|-------------------------|---------|
| Общая трудоемкость по дисциплине (ЗЕТ/ в часах)                                                                                   | 4/144                   | 4/144                   |         |
| Семестр                                                                                                                           | 7                       | 8                       |         |
| Лекции, час                                                                                                                       | 34                      | 17                      |         |
| Практические занятия, час                                                                                                         | -                       |                         |         |
| Лабораторные занятия, час                                                                                                         | 51                      | 26                      |         |
| Самостоятельная работа, час                                                                                                       | 23                      | 65                      |         |
| Курсовой проект (работа), РГР, семестр                                                                                            | 7                       | 8                       |         |
| Зачет (при заочной форме <b>4 часа</b> отводится на контроль)                                                                     | -                       |                         |         |
| Часы на экзамен (при очной, очно-заочной формах <b>1 ЗЕТ – 36 часов</b> , при заочной форме <b>9 часов</b> отводится на контроль) | <b>1 ЗЕТ – 36 часов</b> | <b>1 ЗЕТ – 36 часов</b> |         |



#### 4.1.Содержание дисциплины (модуля) «Методы и средства криптографической защиты информации»

| дисциплины, тема лекции и вопросы                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Очная форма |    |    |    | Очно-заочная форма |    |    |    | Заочная форма |    |    |    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|----|----|----|--------------------|----|----|----|---------------|----|----|----|
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | ЛК          | ПЗ | ЛБ | СР | ЛК                 | ПЗ | ЛБ | СР | ЛК            | ПЗ | ЛБ | СР |
| Задания и угрозы в компьютерных системах». Анализ развития подходов к разработке криптографической защиты информации. Понятия ее «источники и носители». Информация и ограниченного доступа. Категории информации. Основные понятия и определения, информационной безопасности: атаки, политика безопасности. механизмы и сервисы. Оценивается классификация атак. Моделиности и безопасности информации. Задача криптографической защиты информации. Методы и средства защиты информации в системах. Анализ угроз информационной классификация угроз. | 2           | -  | 2  | 1  | 1                  | -  | 1  | 4  |               |    |    |    |
| Задания в криптологии. Основные цели и задачи криптографии и криптоанализа. Развитие криптографии и криптоанализа. Виды криптографии и криптоанализа. Виды криптографии и их защита. Способы криптографической защиты информации (СКЗИ). Преобразование информации. Шифрование информации. Взлом криптоалгоритмов. Криптографические протоколы. Причины безопасности информации при ее обработке                                                                                                                                                       | 2           | -  | 2  | 1  | 1                  | -  | 1  | 4  |               |    |    |    |
| Классическая криптография» Модель шифра. Классические шифры: перестановочный, шифр Хилла, шифры                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2           | -  | 2  | 1  | 1                  | -  | 1  | 4  |               |    |    |    |

|   |   |   |   |   |   |  |  |  |  |
|---|---|---|---|---|---|--|--|--|--|
| 2 | 1 | 1 | - | 1 | 4 |  |  |  |  |
| 4 | 2 | 1 | - | 1 | 4 |  |  |  |  |
| 4 | 1 | 1 | - | 1 | 4 |  |  |  |  |
| 4 | 1 | 1 | - | 1 | 4 |  |  |  |  |

|  |  |  |  |
|--|--|--|--|
|  |  |  |  |
|  |  |  |  |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |   |   |   |   |   |   |   |   |  |  |  |  |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|---|---|---|---|---|--|--|--|--|
| 12 | Тема №12: «Криптография с открытым ключом». Процедуры шифрования и расшифрования в шифрсистеме Эль-Гамала. Процедура генерации ключей шифрсистемы Эль-Гамала. Работа в режиме подписи. Криптостойкость алгоритма. Преимущества и недостатки систем асимметричного шифрования. Взлом криптосистем с открытым ключом.                                                                                                                                                                                                                                                                                                                                                                                                   | 2 | - | 2 | 1 | 1 | - | 2 | 4 |  |  |  |  |
| 13 | Тема №13: «Идентификация и аутентификация». Функции хэширования. Классификация. Функции хэширования без ключа (MDC) и с ключом (MAC). Принципы построения. Функции хэширования Ривеста: MD2, MD4, MD5. Американский стандарт функции хэширования (SHS) и его изменения. Российский стандарт функции хэширования (ГОСТ Р 34.11-94).                                                                                                                                                                                                                                                                                                                                                                                    | 2 | - | 4 | 2 | 1 | - | 2 | 4 |  |  |  |  |
| 14 | Тема №14: «Идентификация и аутентификация». Применение функции хэширования в схемах цифровой подписи и при построении криптосистем. Сильные хэш-функции SHA-1, SHA-2. Основные понятия, относящиеся к обеспечению целостности сообщений и вычислению MAC с помощью алгоритмов симметричного шифрования, хэш-функций и алгоритма HMAC. Контроль целостности данных. Идентификация и аутентификация. Использование для аутентификации открытых и шифрованных сообщений режимов шифрования, распространяющихся в шифртексте искажения открытого текста. Шифрование, создание и проверка цифровой подписи. Использование открытых ключей. Схемы подписи RSA и Рабина. Схема цифровой подписи Эль Гамала и ее модификации. | 2 | - | 2 | 1 | 1 | - | 2 | 2 |  |  |  |  |
| 15 | Тема №15: «Хеширование» Криптографические хеш-функции. ГОСТ Р 34.11-2012. DES. AES.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 2 | - | 4 | 2 | 1 | - | 2 | 4 |  |  |  |  |

|                                                                                |                                                                                                                                                                                                                                                                                                           |                                                                                                   |          |           |                                            |           |          |           |           |  |  |  |  |  |  |
|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|----------|-----------|--------------------------------------------|-----------|----------|-----------|-----------|--|--|--|--|--|--|
| 16                                                                             | Тема №16: «Стойкость шифра».<br>Определение теоретической стойкости алгоритма. Шифр Вернама для 8-битных символов. Побитный «одноразовый блокнот». Виды атак. Понятие о и практической стойкости шифра. Защита от угроз нарушения целостности информации на уровне содержания. Временная стойкость шифра. | 2                                                                                                 | -        | 2         | 1                                          | 1         | -        | 2         | 4         |  |  |  |  |  |  |
| 17                                                                             | Тема №17: «Электронная подпись»<br>Коды аутентичности сообщений. Электронная подпись. ГОСТ Р 34.10- 2012. DSS. Инфраструктура открытого ключа.                                                                                                                                                            | 2                                                                                                 | -        | 3         | 2                                          | 1         | -        | 2         | 3         |  |  |  |  |  |  |
| Форма текущего контроля успеваемости (по срокам текущих аттестаций в семестре) |                                                                                                                                                                                                                                                                                                           | Входная конт.работа<br>1 аттестация 1-5 тема<br>2 аттестация 6-10 тема<br>3 аттестация 11-15 тема |          |           | Входная конт.работа;<br>Контрольная работа |           |          |           |           |  |  |  |  |  |  |
| Форма промежуточной аттестации (по семестрам)                                  |                                                                                                                                                                                                                                                                                                           | Экзамен                                                                                           |          |           | Зачет/ зачет с оценкой/<br>экзамен         |           |          |           |           |  |  |  |  |  |  |
| <b>Итого</b>                                                                   |                                                                                                                                                                                                                                                                                                           | <b>34</b>                                                                                         | <b>-</b> | <b>51</b> | <b>23</b>                                  | <b>17</b> | <b>-</b> | <b>26</b> | <b>65</b> |  |  |  |  |  |  |

К видам учебной работы в вузе относятся: лекции, консультации, семинары, практические занятия, лабораторные работы, контрольные работы, коллоквиумы, самостоятельные работы, научно- исследовательская работа, практики, курсовое проектирование (курсовая работа). Вуз может устанавливать другие виды учебных занятий.

\* - Разделы, тематику и вопросы по дисциплине следует разделить на три текущие аттестации в соответствии со сроками проведения текущих аттестаций. По материалу программы, пройденному студентом после завершения 3-ей аттестации до конца семестра (2-3 недели), контроль успеваемости осуществляется при сдаче зачета или экзамена.

#### 4.2. Содержание лабораторных (практических) занятий

| № п/п | № лекции из рабочей программы | Наименование лабораторного (практического, семинарского) занятия | Количество часов |             |        | Рекомендуемая литература и методические разработки (№ источника из списка литературы) |
|-------|-------------------------------|------------------------------------------------------------------|------------------|-------------|--------|---------------------------------------------------------------------------------------|
|       |                               |                                                                  | Очно             | Очно-заочно | Заочно |                                                                                       |
| 1     | 2                             | 3                                                                | 4                | 5           | 6      | 7                                                                                     |
| 1     | №1                            | Нападения и угрозы в компьютерных системах.                      | 2                | 1           |        | №№ 1-8                                                                                |
| 2     | №2                            | Введение в криптологию. Основные цели и задачи криптографии.     | 2                | 1           |        | №№ 1-8                                                                                |

|              |     |                                                        |  |           |           |        |
|--------------|-----|--------------------------------------------------------|--|-----------|-----------|--------|
| 3            | №3  | Историческая криптография.                             |  | 2         | 1         | №№ 1-8 |
| 4            | №4  | Математические основы криптографии.                    |  | 2         | 1         | №№ 1-8 |
| 5            | №5  | Симметричное шифрование. Симметричные криптоалгоритмы. |  | 4         | 1         | №№ 1-8 |
| 6            | № 6 | Симметричное шифрование. Симметричные криптоалгоритмы. |  | 4         | 1         | №№ 1-8 |
| 7            | №7  | Симметричное шифрование. Симметричные криптоалгоритмы. |  | 4         | 1         | №№ 1-8 |
| 8            | №8  | Симметричное шифрование. Симметричные криптоалгоритмы. |  | 4         | 1         | №№ 1-8 |
| 9            | №9  | Алгоритмические проблемы теории чисел.                 |  | 4         | 2         | №№ 1-8 |
| 10           | №10 | Криптография с открытым ключом.                        |  | 2         | 2         | №№ 1-8 |
| 11           | №11 | Криптография с открытым ключом.                        |  | 4         | 2         | №№ 1-8 |
| 12           | №12 | Криптография с открытым ключом.                        |  | 2         | 2         | №№ 1-8 |
| 13           | №13 | Идентификация и аутентификация.                        |  | 4         | 2         | №№ 1-8 |
| 14           | №14 | Идентификация и аутентификация.                        |  | 2         | 2         | №№ 1-8 |
| 15           | №15 | Хеширование.                                           |  | 4         | 2         | №№ 1-8 |
| 16           | №16 | Стойкость шифра.                                       |  | 2         | 2         | №№ 1-8 |
| 17           | №17 | Электронная подпись.                                   |  | 3         | 2         | №№ 1-8 |
| <b>ИТОГО</b> |     |                                                        |  | <b>51</b> | <b>26</b> |        |

#### 4.3. Тематика для самостоятельной работы студента

| №<br>п/п | Тематика по содержанию дисциплины,<br>выделенная для самостоятельного изучения | Количество часов из содержания дисциплины |             |        | Рекомендуемая литература и источники информации | Формы контроля СРС     |
|----------|--------------------------------------------------------------------------------|-------------------------------------------|-------------|--------|-------------------------------------------------|------------------------|
|          |                                                                                | Очно                                      | Очно-заочно | Заочно |                                                 |                        |
| 1        | 2                                                                              | 1                                         | 4           | 5      | 6                                               | 7                      |
| 1        | Нападения и угрозы в компьютерных системах.                                    | 1                                         | 4           |        | №№ 1-8                                          | Опрос, реферат, статья |
| 2        | Введение в криптологию. Основные цели и задачи криптографии.                   | 1                                         | 4           |        | №№ 1-8                                          | Опрос, реферат, статья |

|                  |           |           |        |                        |
|------------------|-----------|-----------|--------|------------------------|
| фия.             | 1         | 4         | №№ 1-8 | Опрос, реферат, статья |
| криптографии.    | 2         | 4         | №№ 1-8 | Опрос, реферат, статья |
| ние.             | 1         | 4         | №№ 1-8 | Опрос, реферат, статья |
| торитмы.         | 1         | 4         | №№ 1-8 | Опрос, реферат, статья |
| ие.              | 2         | 4         | №№ 1-8 | Опрос, реферат, статья |
| торитмы.         | 1         | 4         | №№ 1-8 | Опрос, реферат, статья |
| ие.              | 2         | 4         | №№ 1-8 | Опрос, реферат, статья |
| торитмы.         | 1         | 4         | №№ 1-8 | Опрос, реферат, статья |
| мы теории чисел. | 2         | 4         | №№ 1-8 | Опрос, реферат, статья |
| и ключом.        | 1         | 4         | №№ 1-8 | Опрос, реферат, статья |
| и ключом.        | 1         | 4         | №№ 1-8 | Опрос, реферат, статья |
| и ключом.        | 2         | 4         | №№ 1-8 | Опрос, реферат, статья |
| фикация.         | 1         | 4         | №№ 1-8 | Опрос, реферат, статья |
| фикация.         | 2         | 2         | №№ 1-8 | Опрос, реферат, статья |
|                  | 1         | 4         | №№ 1-8 | Опрос, реферат, статья |
|                  | 2         | 4         | №№ 1-8 | Опрос, реферат, статья |
|                  | 1         | 3         | №№ 1-8 | Опрос, реферат, статья |
|                  | <b>23</b> | <b>65</b> |        |                        |

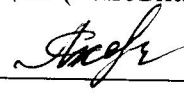
## 5. Образовательные тех



# 7. Учебно-методическое и информационное обеспечение дисциплины

## Рекомендуемая литература и источники информации (основная и дополнительная)

Зав. библиотекой



Алиева Ж.А.

| п/п            | Виды занятий               | Необходимая учебная, учебно-методическая (основная и дополнительная) литература, программное обеспечение и Интернет-ресурсы                                                                                                                                           | Количество изданий                                                                        |            |
|----------------|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|------------|
|                |                            |                                                                                                                                                                                                                                                                       | В библиотек<br>е                                                                          | На кафедре |
| Основная       |                            |                                                                                                                                                                                                                                                                       |                                                                                           |            |
| 1.             | лк, пз, курс. проект., срс | Борисова, С. Н. Криптографические методы защиты информации: классическая криптография : учебное пособие / С. Н. Борисова. — Пенза : ПГУ, 2018. — 186 с. — ISBN 978-5-907102-51-4. — Текст : электронный // Лань : электронно-библиотечная система. —                  | URL:<br><a href="https://e.lanbook.com/book/162235">https://e.lanbook.com/book/162235</a> |            |
| 2.             | лк, пз, курс. проект., срс | Овчинников, А. А. Криптографические методы защиты информации : учебное пособие / А. А. Овчинников. — Санкт-Петербург : ГУАП, 2021. — 133 с. — ISBN 978-5-8088-1591-9. — Текст : электронный // Лань : электронно-библиотечная система. —                              | URL:<br><a href="https://e.lanbook.com/book/216491">https://e.lanbook.com/book/216491</a> |            |
| 3.             | лк, пз, курс. проект., срс | Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2021. — 172 с. — Текст : электронный // Лань : электронно-библиотечная система. —                                                    | URL:<br><a href="https://e.lanbook.com/book/176563">https://e.lanbook.com/book/176563</a> |            |
| Дополнительная |                            |                                                                                                                                                                                                                                                                       |                                                                                           |            |
| 4.             | лк, пз, курс. проект., срс | Котов, Ю. А. Криптографические методы защиты информации. Стандартные шифры. Шифры с открытым ключом : учебное пособие / Ю. А. Котов. — Новосибирск : НГТУ, 2017. — 67 с. — ISBN 978-5-7782-3411-6. — Текст : электронный // Лань : электронно-библиотечная система. — | URL:<br><a href="https://e.lanbook.com/book/118230">https://e.lanbook.com/book/118230</a> |            |
| 5.             | лк, пз, курс. проект., срс | Исследование методов кодирования и шифрования : учебное пособие / А. П. Алексеев, М. И. Макаров, О. В. Сирант, С. С. Яковлева ; под редакцией А. П.                                                                                                                   | URL:<br><a href="https://e.lanbook.com/book/182252">https://e.lanbook.com/book/182252</a> |            |

|    |                                     |                                                                                                                                                                                                                  |                                                                                           |
|----|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
|    |                                     | Алексеева. — Самара : ПГУТИ, 2018. — 102 с. — Текст : электронный // Лань : электронно-библиотечная система. —                                                                                                   |                                                                                           |
| 6. | лк, пз,<br>курс.<br>проект.,<br>срс | Криптографические методы защиты информации : учебное пособие / составители И. А. Калмыков [и др.]. — Ставрополь : СКФУ, 2015. — 109 с. — Текст : электронный // Лань : электронно-библиотечная система. —        | URL:<br><a href="https://e.lanbook.com/book/155280">https://e.lanbook.com/book/155280</a> |
| 7. | лк, пз,<br>курс.<br>проект.,<br>срс | Каширская, Е. Н. Криптографический анализ и методы защиты информации : учебное пособие / Е. Н. Каширская. — Москва : РТУ МИРЭА, 2020. — 91 с. — Текст : электронный // Лань : электронно-библиотечная система. — | URL:<br><a href="https://e.lanbook.com/book/163861">https://e.lanbook.com/book/163861</a> |
| 8. | лк, пз,<br>курс.<br>проект.,<br>срс | Стеганографические и криптографические методы защиты информации : учебное пособие. — Уфа : БГПУ имени М. Акмуллы, 2016. — 112 с. — Текст : электронный // Лань : электронно-библиотечная система. —              | URL:<br><a href="https://e.lanbook.com/book/90963">https://e.lanbook.com/book/90963</a>   |

## **7. Материально-техническое обеспечение дисциплины (модуля) «Методы и средства криптографической защиты информации»**

Материально-техническое обеспечение дисциплины включает:

- библиотечный фонд (учебная, учебно-методическая, справочная экономическая литература, экономическая научная и деловая периодика);
- компьютеризированные рабочие места для обучаемых с доступом в сеть Интернет (лаборатории по автоматизированным информационным системам, оснащенные современной электронно-вычислительной техникой с соответствующим программным обеспечением);
- аудитории, оборудованные проекционной техникой.

Для проведения практических занятий используются компьютерные классы кафедры ИБ, оборудованные современными персональными компьютерами, характеристики которых не ниже:

Pentium 4, DDR 1 Gb, HDD – 150 GB, Video Card – 126 MB, CD/DVD, USB -2.

Все персональные компьютеры подключены к сети университета и имеют выход в глобальную сеть Интернет.

На компьютере предустанавливается ОС Windows XP/Vista/7 и программное обеспечение MS Office 2010, Borland C++ , Borland C++ Builder 6 и др. Приложение командной строки dumpasn1 Питера Гутмана (Peter Gutmann) для просмотра файлов формата ASN.1 BER/DER: dumpasn1.rar (Windows, x86).

КриптоПро OCSPCOM (версия 1.05.0726).

КриптоПро TSPCOM (версия 1.05.0972).

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

При проведении лекционных и практических (семинарских) занятий предусматривается использование систем мультимедиа, программного обеспечения и информационных справочных систем:

Microsoft Office (Word, Excel, PowerPoint, Access)

ЭБС <http://library.mirea.ru/>.

Дистрибутив КриптоПро WinLogon и КриптоПро EAP-TLS;

Дистрибутив КриптоПро JCP и КриптоПро JTLS

### **Специальные условия инвалидам и лицам с ограниченными возможностями здоровья (ОВЗ)**

Специальные условия обучения и направления работы с инвалидами и лицами с ОВЗ определены на основании:

- Федерального закона от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»;
- Федерального закона от 24.11.1995 № 181-ФЗ «О социальной защите инвалидов в Российской Федерации»;
- приказа Минобрнауки России от 05.04.2017 № 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»;
- методических рекомендаций по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащённости образовательного процесса, утвержденных Минобрнауки России 08.04.2014 № АК-44/05вн).

Под специальными условиями для получения образования обучающихся с ОВЗ понимаются условия обучения, воспитания и развития, включающие в себя использование при необходимости адаптированных образовательных программ и методов обучения и воспитания, специальных учебников, учебных пособий и дидактических материалов.

специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего необходимую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания ДГТУ и другие условия, без которых невозможно или затруднено освоение ОПОП обучающихся с ОВЗ.

Обучение в рамках учебной дисциплины обучающихся с ОВЗ осуществляется ДГТУ с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Обучение по учебной дисциплине обучающихся с ОВЗ может быть организовано как совместно с другими обучающимися, так и в отдельных группах.

В целях доступности обучения по дисциплине обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

- наличие альтернативной версии официального сайта ДГТУ в сети «Интернет» для слабовидящих;

- весь необходимый для изучения материал, согласно учебному плану (в том числе, для обучающихся по индивидуальным учебным планам) предоставляется в электронном виде на диске.

- индивидуальное равномерное освещение не менее 300 люкс;

- присутствие ассистента, оказывающего обучающемуся необходимую помощь;

- обеспечение возможности выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

- обеспечение доступа обучающегося, являющегося слепым и использующего собаку-проводника, к зданию ДГТУ.

2) для лиц с ОВЗ по слуху:

- наличие микрофонов и звукоусиливающей аппаратуры коллективного пользования (аудиоколонки);

3) для лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата, материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов и других приспособлений).

Перед началом обучения могут проводиться консультативные занятия, позволяющие студентам с ОВЗ адаптироваться к учебному процессу.

Р. \_\_\_\_\_

