

**МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ**  
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ**  
**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**  
**«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»**  
**(РУТ (МИИТ))**



Рабочая программа дисциплины (модуля),  
как компонент образовательной программы  
высшего образования - программа бакалавриата  
по направлению подготовки  
10.03.01 Информационная безопасность,  
утвержденной первым проректором ФГАОУ ВО  
РУТ (МИИТ) Тимониным В.С.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Организационное и правовое обеспечение информационной  
безопасности**

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде  
электронного документа выгружена из единой  
корпоративной информационной системы управления  
университетом и соответствует оригиналу

Простая электронная подпись, выданная ФГАОУ ВО РУТ  
(МИИТ)

ID подписи: 4196

Подписал: заведующий кафедрой Желенков Борис  
Владимирович

Дата: 01.09.2026

## 1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины (модуля) является:

- формирование компетенций по основным разделам теоретических и практических основ применения законодательных актов РФ при разработке и эксплуатации систем обеспечения информационной безопасности.

Задачами дисциплины (модуля) являются:

- ознакомление с законодательными актами и нормативно-правовым обеспечением информационной безопасности;
- изучение особенностей практического применения законодательных актов и нормативно-правового обеспечения информационной безопасности;
- изучение технических и организационных методов практического применения законодательных актов и нормативно-правового обеспечения информационной безопасности;
- изучение методов построения систем обеспечения информационной безопасности с учетом законодательных актов и нормативно-правового обеспечения.

## 2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

**ОПК-5** - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности ;

**ОПК-6** - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю ;

**ПК-13** - способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

**Знать:**

- основные законодательные акты и нормативно-правовое обеспечение информационной безопасности на транспорте;

- средства и технологии обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России .

**Уметь:**

- разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;

- организовать работу по созданию, модернизации и сертификации систем, средств и технологий обеспечения информационной безопасности.

**Владеть:**

- навыками разработки и оформления документов, регламентирующих деятельность служб обеспечения информационной безопасности предприятия;

- навыками проектирования политик информационной безопасности предприятия с учетом требований российского законодательства и ведомственных нормативно-правовых актов.

**3. Объем дисциплины (модуля).**

**3.1. Общая трудоемкость дисциплины (модуля).**

Общая трудоемкость дисциплины (модуля) составляет 3 з.е. (108 академических часа(ов)).

**3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:**

| Тип учебных занятий                                       | Количество часов |            |
|-----------------------------------------------------------|------------------|------------|
|                                                           | Всего            | Семестр №7 |
| Контактная работа при проведении учебных занятий (всего): | 48               | 48         |
| В том числе:                                              |                  |            |
| Занятия лекционного типа                                  | 32               | 32         |
| Занятия семинарского типа                                 | 16               | 16         |

**3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации**

образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 60 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

#### 4. Содержание дисциплины (модуля).

##### 4.1. Занятия лекционного типа.

| №<br>п/п | Тематика лекционных занятий / краткое содержание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1        | <b>Информационная безопасность: сущность и содержание</b><br>Рассматриваемые вопросы:<br>-Информация как один из наиболее важных ресурсов современности;<br>- Информационная безопасность в системе национальной безопасности;<br>-Понятие информационной безопасности как состояния защищенности жизненно важных интересов личности, общества и государства в информационной сфере;<br>-Разграничение понятий «информационная безопасность», «компьютерная безопасность» и «защита информации»;<br>-Правовой, организационный и программно-технический уровни обеспечения информационной безопасности;<br>-Проблемы разработки и внедрения методов и средств обеспечения информационной безопасности в государственных организациях и коммерческих предприятиях России. |
| 2        | <b>Государственная политика в сфере обеспечения информационной безопасности</b><br>Рассматриваемые вопросы:<br>-Понятие государственной политики в информационной сфере;<br>-Основные положения государственной политики в сфере информационной безопасности;<br>-Обеспечение равенства участников процесса информационного взаимодействия;<br>-Совершенствование нормативно-правовой базы регулирования информационных отношений;<br>-Контроль за соблюдением законодательства в информационной сфере; -Национальная Программа "Цифровая экономика Российской Федерации";<br>-Национальные проекты в сфере цифровизации.                                                                                                                                                |
| 3        | <b>Основные задачи обеспечения информационной безопасности</b><br>Рассматриваемые вопросы:<br>-Обеспечение информационной безопасности как комплексная задача;<br>-Создание системы органов, ответственных за информационную безопасность;<br>-Разработка теоретико-методологической основы обеспечения безопасности информации;<br>-Создание нормативно-правовой базы, регламентирующей решение всех задач обеспечения информационной безопасности;<br>-Организация подготовки специалистов по защите информации;<br>-Решение проблемы управления защитой информации и ее автоматизация;<br>-Общие задачи обеспечения информационной безопасности;                                                                                                                      |

| №<br>п/п | Тематика лекционных занятий / краткое содержание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | -Режим государственной, коммерческой, личной (семейной) тайны;<br>-Разработка стратегии обеспечения информационной безопасности России.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 4        | <b>Основные законы, регламентирующие организационно-правовую базу в области информационной безопасности</b><br>Рассматриваемые вопросы:<br>• Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и защите информации»<br>• Федеральный закон № 152-ФЗ «О персональных данных»<br>• Доктрина информационной безопасности Российской Федерации<br>• Федеральный закон N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"<br>• Федеральный закон Российской Федерации N 98-ФЗ "О коммерческой тайне"                                                                                                                                                                                                                                                |
| 5        | <b>Основные законы, регламентирующие организационно-правовую базу в области информационной безопасности(продолжение)</b><br>Рассматриваемые вопросы:<br>-Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации;<br>-Обладатель информации, его права и обязанности;<br>-Конфиденциальность персональных данных;<br>-Согласие субъекта персональных данных на обработку его персональных данных;<br>-Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных;<br>-Угрозы развитию отечественной индустрии информации;<br>-Принципы обеспечения безопасности критической информационной инфраструктуры;<br>-Категорирование объектов критической информационной инфраструктуры; |
| 6        | <b>Основные задачи обеспечения информационной безопасности. Организационно-технические, экономические и правовые методы</b><br>Рассматриваемые вопросы:<br>-Этапы обеспечения ИБ на предприятии;<br>-Создание режима охраны информации;<br>-Разработка правил взаимоотношений между сотрудниками; регламентация работы с документами;<br>-Правила использования технических средств в рамках существующего правового поля РФ;<br>-Аналитическая работа по оценке угроз информационной безопасности;<br>-Обязанности руководства организации по обеспечению ИБ (ISO 27001)<br>-Создание нормативно-правовой базы, регламентирующей решение всех задач обеспечения информационной безопасности.                                                                                                            |
| 7        | <b>Угрозы информационной безопасности</b><br>Рассматриваемые вопросы:<br>-Понятие угрозы информационной безопасности;<br>-Виды угроз информационной безопасности;<br>-Внешние и внутренние угрозы информационной безопасности;<br>-Компьютерные сети и информационная безопасность;<br>-Понятие и виды атак на компьютерную систему;<br>-Классификация атак на компьютерную систему;<br>-Вредоносные программы, их виды и направления применения;                                                                                                                                                                                                                                                                                                                                                        |
| 8        | <b>Угрозы информационной безопасности(продолжение)</b><br>Рассматриваемые вопросы:<br>-Понятие угрозы информационной безопасности;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| №<br>п/п | Тематика лекционных занятий / краткое содержание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | -Виды угроз информационной безопасности;<br>-Внешние и внутренние угрозы информационной безопасности;<br>-Компьютерные сети и информационная безопасность;                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 9        | <b>Формирование нормативно-правовой базы обеспечения информационной безопасности</b><br>Рассматриваемые вопросы:<br>-Разработка нормативно-правовых и организационно-методических документов, регламентирующих деятельность органов государственной власти в области информационной безопасности;<br>-Взаимоотношения субъектов информационной деятельности в части обеспечения информационной безопасности;<br>-Государственная регламентация процессов функционирования и развития рынка средств информации, информационных продуктов и услуг;<br>-Разработка концепции информационной безопасности.  |
| 10       | <b>Развитие современных методов обеспечения информационной безопасности</b><br>Рассматриваемые вопросы:<br>-Разработка методов комплексного исследования деятельности персонала информационных систем;<br>-Разработка практических рекомендаций по сохранению и укреплению политической стабильности в обществе, обеспечению прав и свобод граждан, укреплению законности и правопорядка методами информационной безопасности;<br>-Формирование подходов и способов обеспечения органов государственной власти и управления, граждан и их объединений достоверной, полной и своевременной информацией.  |
| 11       | <b>Стандартизация в области информационной безопасности</b><br>Рассматриваемые вопросы:<br>-Проблема стандартизации в области информационной безопасности в международных и национальных стандартах;<br>-ГОСТы серии 27000;<br>-Стандартизация терминологии в ISO/IEC 27000;<br>-Стандартизация базовых требований в ISO/IEC 27001/27002;<br>-Стандартизация порядка внедрения СМИБ в ISO/IEC 27003;                                                                                                                                                                                                    |
| 12       | <b>Стандартизация в области информационной(продолжение)</b><br>Рассматриваемые вопросы:<br>-Стандартизация основных процессов в ISO/IEC 27004/27005/27007/27008;<br>-Стандартизация корпоративного управления СМИБ в ISO/IEC 27014/27016;<br>-Стандартизация кибербезопасности в ISO/IEC 27103.                                                                                                                                                                                                                                                                                                         |
| 13       | <b>Стандартизация и сертификация в области защиты информации</b><br>Рассматриваемые вопросы:<br>-Система ГОСТов в области защиты информации: ГОСТ Р 52069;0-2013;<br>-Общие технические требования к защите от несанкционированного доступа к информации в ГОСТ Р 50739;<br>-Основные требования и определения в ГОСТ Р 50922;<br>-Порядок создания автоматизированных систем в защищенном исполнении в ГОСТ Р 51583;<br>-Стандартизация номенклатуры качества защиты информации в ГОСТ Р 52447;<br>-Стандартизация требований к средствам высоконадежной биометрической аутентификации в ГОСТ Р 52633. |
| 14       | <b>Стандартизация и сертификация в условиях цифровой информации</b><br>Рассматриваемые вопросы:<br>-Национальная Программа "Цифровая экономика Российской Федерации" и ее Федеральные проекты «Цифровое государственное управление», «Цифровые технологии», «Информационная безопасность», «Кадры для цифровой экономики», «Информационная инфраструктура»,                                                                                                                                                                                                                                             |

| №<br>п/п | Тематика лекционных занятий / краткое содержание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | «Нормативное регулирование цифровой среды», «Искусственный интеллект», «Развитие кадрового потенциала ИТ-отрасли», «Обеспечение доступа в Интернет за счет развития спутниковой связи»;<br>-Проблемы стандартизации и сертификации в Федеральных проектах.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 15       | <b>Стандартизация и сертификация систем искусственного интеллекта</b><br>Рассматриваемые вопросы:<br>-Федеральный проект «Искусственный интеллект» и проблемы стандартизации и сертификации;<br>-Стандартизация и унификация представления правовой информации для цифровой платформы «Государственная система правовой информации»;<br>-ПНСТ «Умное производство»;<br>-Двойники цифровые производства» (части 1-4);<br>-ПНСТ «Информационные технологии»;<br>-Умный город;<br>-Функциональная совместимость»;<br>-ПНСТ «Информационные технологии»;<br>-Умный город;<br>-Руководства по обмену и совместному использованию данных»;<br>- ПНСТ «Информационные технологии»;<br>-Интернет вещей;<br>Протокол обмена для высокоскоростных сетей с большим радиусом действия и низким энергопотреблением». |
| 16       | <b>Проблемы повышения эффективности обеспечения информационной безопасности на современном этапе</b><br>Рассматриваемые вопросы:<br>-Обеспечение согласованности решений органов, ответственных за реализацию государственной политики в сфере обеспечения информационной безопасности в рамках единого информационного пространства;<br>-Политика протекционизма, направленная на поддержку деятельности отечественных производителей средств информатизации и защиты информации;<br>-Защита внутреннего рынка от проникновения некачественных средств информатизации и информационных продуктов.                                                                                                                                                                                                      |

#### 4.2. Занятия семинарского типа.

##### Практические занятия

| №<br>п/п | Тематика практических занятий/краткое содержание                                                                                                                                                                               |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1        | <b>Защита персональных данных. ФЗ №152 и ГОСТы РФ</b><br>В результате выполнения практического задания студент получает навыки в применении организационно-правовых методов защиты персональных данных.                        |
| 2        | <b>Способы защиты коммерческой тайны. ФЗ №98 и ГОСТы РФ</b><br>В результате выполнения практического задания студент получает навыки в применении организационно-правовых методов защиты коммерческой тайны.                   |
| 3        | <b>Методы и средства защиты информации. Российские и международные стандарты</b><br>В результате выполнения практического задания студент получает навыки в применении методов и средств защиты информации.                    |
| 4        | <b>Организация службы информационной безопасности на предприятии</b><br>В результате выполнения практического задания студент получает навыки в организации и реорганизации службы информационной безопасности на предприятии. |

| №<br>п/п | Тематика практических занятий/краткое содержание                                                                                                                                                                                                               |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5        | Организационные каналы утечки конфиденциальной информации<br>В результате выполнения практического задания студент получает навыки в определении и классификации организационных каналов утечки конфиденциальной информации.                                   |
| 6        | Оценка угроз безопасности информации<br>В результате выполнения практического задания студент получает навыки в оценке угроз безопасности информации в соответствии с методикой ФСТЭК.                                                                         |
| 7        | Стандартизация и сертификация систем искусственного интеллекта<br>В результате выполнения практического задания студент получает навыки внедрения требований ГОСТов в разрабатываемые или эксплуатируемые системы искусственного интеллекта                    |
| 8        | Стандартизация кибербезопасности вычислительного комплекса<br>В результате выполнения практического задания студент получает навыки разработки методов и средств обеспечения кибербезопасности вычислительного комплекса в соответствии с требованиями ГОСТов. |

#### 4.3. Самостоятельная работа обучающихся.

| №<br>п/п | Вид самостоятельной работы             |
|----------|----------------------------------------|
| 1        | Работа с лекционным материалом         |
| 2        | Подготовка к практическим занятиям     |
| 3        | Подготовка к тестированию              |
| 4        | Подготовка к промежуточной аттестации. |
| 5        | Подготовка к текущему контролю.        |

#### 5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

| №<br>п/п | Библиографическое описание                                                                                                                                          | Место доступа                                                                                                                          |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| 1        | Диогенес Ю., Озкайя Э. Кибербезопасность. Стратегия атак и обороны. Издательство "ДМК Пресс", 2020 - 326с. – ISBN 978-5-97060-709-1                                 | <a href="https://e.lanbook.com/book/131717">https://e.lanbook.com/book/131717</a><br>(дата обращения: 24.02.2024).- Текст электронный. |
| 2        | Ермакова А.Ю. Методы и средства защиты компьютерной информации: учебное пособие. МИРЭА - Российский технологический университет, 2020.- 223с,ISBN 978-5-8114-8034-0 | <a href="https://e.lanbook.com/book/163844">https://e.lanbook.com/book/163844</a> (дата обращения: 24.02.2024).- Текст электронный.    |
| 3        | Мосолов А. С., Акинин Н. И. Компьютерные технологии и методы проектирования в сфере безопасности. Издательство "Лань", 2021 - 444с. – ISBN 978-5-8114-8034-0        | <a href="https://e.lanbook.com/book/183115">https://e.lanbook.com/book/183115</a><br>(дата обращения: 24.02.2024).- Текст электронный  |

|    |                                                                                                                                                                                                           |                                                                                                                                     |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| 4  | Петров А. А. Компьютерная безопасность. Криптографические методы защиты. Издательство "ДМК Пресс", 2008 - 448с. – ISBN 5-89818-064-8                                                                      | <a href="https://e.lanbook.com/book/3027">https://e.lanbook.com/book/3027</a> (дата обращения: 24.02.2024).- Текст электронный.     |
| 5  | Краковский Ю. М. Методы защиты информации. Издательство "Лань", 2021 - 236с. – ISBN 978-5-8114-5632-1                                                                                                     | <a href="https://e.lanbook.com/book/156401">https://e.lanbook.com/book/156401</a> (дата обращения: 24.02.2024).- Текст электронный  |
| 6  | Тумбинская М.В., Петровский М.В. Защита информации на предприятии: учебное пособие. Издательство "Лань", 2020 - 184с. – ISBN 978-5-8114-4291-1                                                            | <a href="https://e.lanbook.com/book/130184">https://e.lanbook.com/book/130184</a> (дата обращения: 24.02.2024).- Текст электронный  |
| 7  | Прохорова О. В. Информационная безопасность и защита информации. Издательство "Лань", 2022 - 124с. – ISBN 978-5-8114-8924-4                                                                               | <a href="https://e.lanbook.com/book/185333">https://e.lanbook.com/book/185333</a> (дата обращения: 24.02.2024).- Текст электронный. |
| 8  | Никифоров С. Н. Методы защиты информации. Защищенные сети, 2021 - 96с. – ISBN 978-5-8114-7907-8                                                                                                           | <a href="https://e.lanbook.com/book/167186">https://e.lanbook.com/book/167186</a> (дата обращения: 24.02.2024).- Текст электронный. |
| 9  | Пугин В. В., Голубничая Е. Ю., Лабада С. А. Защита информации в компьютерных информационных системах: учебное пособие. Поволжский государственный университет телекоммуникаций и информатики, 2018.- 119с | <a href="https://e.lanbook.com/book/182299">https://e.lanbook.com/book/182299</a> (дата обращения: 24.02.2024).- Текст электронный. |
| 10 | Леонтьев А. С. Защита информации: учебное пособие. МИРЭА - Российский технологический университет 2021.-79с                                                                                               | <a href="https://e.lanbook.com/book/182491">https://e.lanbook.com/book/182491</a> (дата обращения: 24.02.2024.- Текст электронный.  |

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

- Официальный сайт РУТ (МИИТ) <https://www.mii.ru/>
- Образовательная платформа «Юрайт» <https://urait.ru/>
- ЭБС ibooks.ru <http://ibooks.ru/>
- ЭБС "Лань" <https://e.lanbook.com/book/>

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

- Microsoft Windows
- Microsoft Office

При организации обучения по дисциплине (модулю) с применением электронного обучения и дистанционных образовательных технологий необходим доступ каждого студента к информационным ресурсам – библиотечному фонду Университета, сетевым ресурсам и информационно-телекоммуникационной сети «Интернет».

В случае проведения занятий с применением электронного обучения и дистанционных образовательных технологий может потребоваться наличие следующего программного обеспечения (или их аналогов): ОС Windows, Microsoft Office, Интернет-браузер, Microsoft Teams и т.д.

В образовательном процессе, при проведении занятий с применением электронного обучения и дистанционных образовательных технологий, могут применяться следующие средства коммуникаций: ЭИОС РУТ(МИИТ), Microsoft Teams, электронная почта, скайп, Zoom, WhatsApp и т.п.

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

- Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций.

Проектор для вывода изображения на экран для студентов, акустическая система, место для преподавателя оснащенное компьютером. Аудитория подключена к интернету МИИТ.

- Учебная аудитория для проведения практических работ.

- персональные компьютеры.

В случае проведения занятий с применением электронного обучения и дистанционных образовательных технологий необходимо наличие компьютерной техники, для организации коллективных и индивидуальных форм общения педагогических работников со студентами, посредством используемых средств коммуникации.

Допускается замена оборудования его виртуальными аналогами.

9. Форма промежуточной аттестации:

Зачет в 7 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

доцент, доцент, к.н. кафедры  
«Вычислительные системы, сети и  
информационная безопасность»

С.В. Малинский

Согласовано:

Заведующий кафедрой ВССиИБ

Б.В. Желенков

Председатель учебно-методической  
комиссии

Н.А. Андриянова