**МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»**
**(РУТ (МИИТ)**

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
базового высшего образования
по направлению подготовки
02.03.02 Фундаментальная информатика и
информационные технологии,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

## Криптографическая защита информации

Направление подготовки: 02.03.02 Фундаментальная информатика и информационные технологии

Направленность (профиль): Квантовые вычислительные системы и сети

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины «Криптографическая защита информации» является формирование профессиональных компетенций по основным разделам дисциплины.

Задачами дисциплины являются:

- изучение основных методов и средств криптографической защиты информации, стандартов в этой области;
- получение представления о математических методах криптографической защиты информации;
- студенты должны научиться применять современные методы и средства криптографической защиты информации на практике.

2. Планируемые результаты обучения по дисциплине (модулю).

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

**ПК-8** - Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты и принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации.

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

**Знать:**

- математические методы и основополагающие документы в области криптографической защищенности компьютерных систем (КС) и сетей;
- международные и национальные стандарты по оценке безопасности в области информационных технологий;
- политики информационной безопасности.

**Уметь:**

- применять фундаментальные знания, полученные в области математически для работы с криптографическими протоколами;
- применять комплексный подход к обеспечению информационной безопасности объекта защиты;
- применять стандарты и другие нормативные документы по информационной безопасности для оценки защищенности объекта защиты.

**Владеть:**

- навыками применения математические методов при работе с криптографическими средствами защиты информации;

- реализации политики информационной безопасности на объекте информатизации с помощью криптографических средств защиты информации;

- навыками организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации в рамках использования криптографических средств защиты информац

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 8 з.е. (288 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 | |
| | | №5 | №6 |
| Контактная работа при проведении учебных занятий (всего): | 128 | 64 | 64 |
| В том числе: | | | |
| Занятия лекционного типа | 64 | 32 | 32 |
| Занятия семинарского типа | 64 | 32 | 32 |

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 160 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.

| № п/п | Тематика лекционных занятий / краткое содержание |
|---|---|
| 1 | СЕМЕСТР 5 ЗАЩИТА ИНФОРМАЦИИ<br>Рассматриваемые вопросы:<br>- требования ФСТЭК по защите информации;<br>- рекомендации по технической защите данных;<br>- классы средств защиты данных. |
| 2 | ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ<br>Рассматриваемые вопросы:<br>- меры по обеспечению информационной безопасности;<br>- документы ФСТЭК по ИБ;<br>- сертифицированные средства ИБ ФСТЭК |
| 3 | ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ<br>Рассматриваемые вопросы:<br>- порядок обеспечения информационной безопасности;<br>- криптографическая защита информации. |
| 4 | КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ<br>Рассматриваемые вопросы:<br>- методы защиты виды, классификация;<br>- шифрование, стенография, кодирование, сжатие и др.. |
| 5 | КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ<br>Рассматриваемые вопросы:<br>- средства криптографической защиты информации (СКЗИ);<br>- сертифицированные криптографические средства защиты информации в России. |
| 6 | ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ<br>Рассматриваемые вопросы:<br>- алгоритм Евклида, соотношение Безу;<br>- Диофантовы линейные уравнения;<br>- теорема Ферма, функция и теорема Эйлера;<br>- квадратичные вычеты, символы Лежандра и Якоби. |
| 7 | ТЕСТИРОВАНИЕ ЧИСЕЛ НА ПРОСТОТУ И ПОСТРОЕНИЕ<br>Рассматриваемые вопросы:<br>- элементарные методы проверки простоты чисел;<br>- алгоритмы Конягина-Померанса, Миллера;<br>- вероятностные тесты на простоту и детерминированный полиномиальный алгоритм проверки простоты чисел. |
| 8 | ФАКТОРИЗАЦИЯ ЦЕЛЫХ ЧИСЕЛ С ЭКСПОНЕНЦИАЛЬНОЙ<br>Рассматриваемые вопросы:<br>- методы Ферма, Полларда, Шермана-Лемана,<br>- алгоритмы Ленстры и Полларда-Штрассена;<br>- (P +1)-метод Уильямса и его обобщения. |
| 9 | ФАКТОРИЗАЦИЯ ЦЕЛЫХ ЧИСЕЛ С СУБЭКСПОНЕНЦИАЛЬНОЙ СЛОЖНОСТЬЮ |

| № п/п | Тематика лекционных занятий / краткое содержание |
|---|---|
| | Рассматриваемые вопросы:<br>- методы Диксона, Шнорра-Ленстры, Ленстры-Померанса;<br>- алгоритм Бриллхарта-Моррисона;<br>- алгоритмы решета числового поля. |
| 10 | АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ: ГРУППЫ, КОЛЬЦА, ПОЛЯ<br>Рассматриваемые вопросы:<br>- группы, морфизмы групп, кольца, поля;<br>- поля Галуа или конечные поля;<br>- задача дискретного логарифмирования в конечных полях;<br>- кольцо многочленов. |
| 11 | ПРИМЕНЕНИЕ КРИВЫХ ДЛЯ ПРОВЕРКИ ПРОСТОТЫ И ФАКТОРИЗАЦИИ<br>Рассматриваемые вопросы:<br>- эллиптические кривые и их свойства;<br>- алгоритм Ленстры для факторизации целых чисел с помощью эллиптических кривых;<br>- вычисление порядка группы точек эллиптической кривой над конечным полем;<br>- тестирование чисел на простоту с помощью эллиптических кривых. |
| 12 | АЛГОРИТМЫ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ<br>Рассматриваемые вопросы:<br>- детерминированные методы;<br>- дискретное логарифмирование в простых полях, в полях Галуа; решето числового поля;<br>- частное Ферма и дискретное логарифмирование по составному модулю. |
| 13 | ФАКТОРИЗАЦИЯ МНОГОЧЛЕНОВ НАД КОНЕЧНЫМИ ПОЛЯМИ<br>Рассматриваемые вопросы:<br>- вероятностный алгоритм решения алгебраических уравнений в конечных полях;<br>- решение квадратных уравнений;<br>- вероятностный алгоритм проверки неприводимости многочленов над конечными полями. |
| 14 | ПРИВЕДЕННЫЕ БАЗИСЫ РЕШЕТОК И ИХ ПРИЛОЖЕНИЯ<br>Рассматриваемые вопросы:<br>- решетки и базисы;<br>- LLL-приведенный базис и его свойства;<br>- алгоритм Фергюсона-Форкейда. |
| 15 | ФАКТОРИЗАЦИЯ МНОГОЧЛЕНОВ НАД ПОЛЕМ РАЦИОНАЛЬНЫХ ЧИСЕЛ<br>Рассматриваемые вопросы:<br>- LLL-алгоритм факторизации;<br>- факторизация многочленов с использованием приближенных вычислений. |
| 16 | ДИСКРЕТНОЕ ПРЕОБРАЗОВАНИЕ ФУРЬЕ<br>Рассматриваемые вопросы:<br>- вычисление дискретного преобразования Фурье;<br>- применение дискретного преобразования Фурье в алгоритме Полларда-Штрассена. |
| 17 | СЕМЕСТР 6 ЦЕЛОЧИСЛЕННАЯ АРИФМЕТИКА МНОГОКРАТНОЙ ТОЧНОСТИ<br>Рассматриваемые вопросы:<br>- основные операции;<br>- алгоритмы модулярной арифметики. |
| 18 | СИСТЕМЫ ЛИНЕЙНЫХ УРАВНЕНИЙ НАД КОНЕЧНЫМИ ПОЛЯМИ<br>Рассматриваемые вопросы:<br>- решение систем линейных уравнений в целых числах; |

| № п/п | Тематика лекционных занятий / краткое содержание |
|---|---|
| | - гауссово и структурированное гауссово исключение;<br>- алгоритмы Ланцоша и Видемана. |
| 19 | ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ<br>Рассматриваемые вопросы:<br>- понятие эллиптической кривой над полем;<br>- порядок эллиптической кривой;<br>- применение эллиптических кривых в криптографии. |
| 20 | КРИПТОГРАФИЧЕСКИЕ КЛЮЧИ<br>Рассматриваемые вопросы:<br>- управление криптографическими ключами;<br>- генерация ключей;<br>- хранение ключей;<br>- распределение ключей. |
| 21 | КРИПТОГРАФИЧЕСКИЕ ПРИМИТИВЫ<br>Рассматриваемые вопросы:<br>- свойства примитивов, основные примитивы, объединение примитивов;<br>- свойства безопасности. |
| 22 | КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ<br>Рассматриваемые вопросы:<br>- отличия протоколов от криптосистем;<br>- виды атак на криптографические протоколы;<br>- базовые протоколы;<br>- стандартные протоколы. |
| 23 | КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ<br>Рассматриваемые вопросы:<br>- электронная подпись;<br>- протоколы электронных платежей, другие виды протоколов. |
| 24 | СИММЕТРИЧНЫЕ И АССИМЕТРИЧНЫЕ КРИПТОСИСТЕМЫ 1<br>Рассматриваемые вопросы:<br>- стандарты шифрования данных (алгоритм шифрования данных DES, Triple DES, AES, алгоритм Ривеста);<br>- Российский стандарт крипто- и имитозащиты сообщений. |
| 25 | СИММЕТРИЧНЫЕ И АССИМЕТРИЧНЫЕ КРИПТОСИСТЕМЫ 2<br>Рассматриваемые вопросы:<br>- концепция криптосистемы с открытым ключом;<br>- криптосистема шифрования данных RSA, схемы шифрования Полига-Хеллмана, Эль Гамаля, комбинированный метод шифрования. |
| 26 | ХЭШ-ФУНКЦИИ<br>Рассматриваемые вопросы:<br>- виды;<br>- хэш-функции - использование в ЭП, стандарты хэш-функций. |
| 27 | ЭЛЕКТРОННАЯ ПОДПИСЬ<br>Рассматриваемые вопросы: |

| № п/п | Тематика лекционных занятий / краткое содержание |
|---|---|
| | - проблема аутентификации данных;<br>- подписи с дополнительными функциональными свойствами. |
| 28 | АЛГОРИТМЫ ЭП<br>Рассматриваемые вопросы:<br>- алгоритмы электронной подписи (назначение и виды, классификация, подделка ЭП);<br>- слепая ЭП, быстрая, неоспоримая. |
| 29 | БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ<br>Рассматриваемые вопросы:<br>- формальные методы доказательства правильности программ и их спецификаций;<br>- методы и средства анализа безопасности ПО;<br>- контрольно-испытательные и логико-аналитические методы. |
| 30 | БЕЗОПАСНОСТЬ ТЕХНИЧЕСКИХ СРЕДСТВ КОМПЬЮТЕРНЫХ СИСТЕМ<br>Рассматриваемые вопросы:<br>- требования к техническим средствам;<br>- анализ безопасности технических средств КС;<br>- подходы к оценке информационной безопасности. |
| 31 | ОСНОВНЫЕ МЕТОДЫ ДЛЯ РЕШЕНИЯ ПРОБЛЕМЫ ОПРЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ КС<br>Рассматриваемые вопросы:<br>- структура критериев оценки соответствия уровня защищенности;<br>- показатели уязвимости;<br>- использование эмпирического, теоретического и теоретико-эмпирического методов. |
| 32 | ПРОЕКТИРОВАНИЕ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ<br>Рассматриваемые вопросы:<br>- принципы построения систем защиты конфиденциальной информации;<br>- основы политики безопасности (понятие политики безопасности, реализация политики безопасности, модели безопасности);<br>- основные этапы проектирования. |

## 4.2. Занятия семинарского типа.

### Практические занятия

| № п/п | Тематика практических занятий/краткое содержание |
|---|---|
| 1 | СЕМЕСТР 5 КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ<br>В результате работы студентом будут исследованы и проанализированы криптографические методы и средства защиты информации, подготовлен отчет. |
| 2 | ФАКТОРИЗАЦИЯ ЦЕЛЫХ ЧИСЕЛ С ЭКСПОНЕНЦИАЛЬНОЙ<br>Результат работы – реализация алгоритмов Ленстры и Полларда-Штрассена. |
| 3 | ФАКТОРИЗАЦИЯ ЦЕЛЫХ ЧИСЕЛ С СУБЭКСПОНЕНЦИАЛЬНОЙ СЛОЖНОСТЬЮ |

| № п/п | Тематика практических занятий/краткое содержание |
|---|---|
| | Результат работы – реализация алгоритмов Бриллхарта-Моррисона и алгоритмов решета числового поля. |
| 4 | ДИСКРЕТНОЕ ЛОГАРИФМИРОВАНИЕ<br>Результат работы – отчет с решением задач по теме «Дискретное логарифмирование в простых полях и в полях Галуа». |
| 5 | ВЕРОЯТНОСТНЫЙ АЛГОРИТМ РЕШЕНИЯ АЛГЕБРАИЧЕСКИХ УРАВНЕНИЙ<br>Результат работы – реализация вероятностного алгоритма проверки неприводимости многочленов над конечными полями. |
| 6 | РЕШЕТКИ И БАЗИСЫ<br>Результат работы – реализация алгоритма Фергюсона-Форкейда. |
| 7 | ФАКТОРИЗАЦИЯ МНОГОЧЛЕНОВ<br>Результат работы – решение задач по теме «Факторизация многочленов с использованием приближенных вычислений». |
| 8 | ПРЕОБРАЗОВАНИЕ ФУРЬЕ<br>Результат работы – отчет с исследованием применения дискретного преобразования Фурье в алгоритме Полларда-Штрассена. |
| 9 | СЕМЕСТР 6 АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ: ГРУППЫ, КОЛЬЦА, ПОЛЯ<br>Результат работы – получение практических навыков решения задач. |
| 10 | ЦЕЛОЧИСЛЕННАЯ АРИФМЕТИКА МНОГОКРАТНОЙ ТОЧНОСТИ<br>Результат работы – отчет с результатами проведенного анализа алгоритмов модулярной арифметики. |
| 11 | РЕШЕНИЕ СИСТЕМ ЛИНЕЙНЫХ УРАВНЕНИЙ НАД КОНЕЧНЫМИ ПОЛЯМИ<br>Результат работы – реализация алгоритмов Ланцоша и Видемана. |
| 12 | ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ И ИХ СВОЙСТВА<br>ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ И ИХ СВОЙСТВА |
| 13 | ХРАНЕНИЕ КЛЮЧЕЙ<br>Результат работы – отчет с результатами исследования методов и средств хранения ключей. |
| 14 | ГЕНЕРАЦИЯ КЛЮЧЕЙ<br>Результат работы – отчет, где представлены схемы и алгоритмы генерации сеансового ключа. |
| 15 | ИССЛЕДОВАНИЕ ПРОТОКОЛА БЛЮМА<br>Результат работы – отлаженная программа, реализующая протокол привязки к биту (протокол Блюма - схема Блюма-Микали). |
| 16 | Результат работы – отлаженная программа, реализующая протокол привязки к биту (протокол Блюма - схема Блюма-Микали).<br>Студент получит навыки применения соответствующих стандартов, будет знать процессы формирования и проверки ЭП, особенности использования функции хэширования в схемах ЭП. |
| 17 | ФУНКЦИЯ ХЭШИРОВАНИЯ<br>Студент получит навыки применения соответствующих стандартов, будет знать особенности использования функции хэширования в схемах ЭП. |
| 18 | ИЗУЧЕНИЕ МЕТОДОВ ШИФРОВАНИЯ<br>Результат работы – зашифрованное сообщение с использованием традиционных методов шифрования (предварительно выбрав ключ). |

| № п/п | Тематика практических занятий/краткое содержание |
|---|---|
| 19 | ИССЛЕДОВАНИЕ И ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МЕТОДОВ ШИФРОВАНИЯ<br>Результатом работы является отлаженная программа, реализующая предложенный студентом алгоритм шифрования. |
| 20 | СОВРЕМЕННЫЕ СИММЕТРИЧНЫЕ И АССИМЕТРИЧНЫЕ КРИПТОСИСТЕМЫ<br>Результатом работы является отлаженная программа, реализующая заданный студенту криптографический алгоритм. |
| 21 | ОБЩИЕ КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.<br>Результат работы – навыки практического применения соответствующего стандарта. |
| 22 | ОЦЕНКА БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ.<br>Результат работы – список угроз и мер по разработке безопасного ПО, согласно ГОСТ Р 58412-2019. |
| 23 | ЗАЩИТА СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ<br>Результат работы - получение навыков практического применения Руководящего документа. |
| 24 | РАЗРАБОТКА СИСТЕМЫ ИНФОРМАЦИОННОЙ ЗАШИТЫ ОБЪЕКТА ИНФОРМАТИЗАЦИИ<br>В результате выполнения работы студентом будет подготовлен отчет с описанием системы защиты информации. |

4.3. Самостоятельная работа обучающихся.

| № п/п | Вид самостоятельной работы |
|---|---|
| 1 | Изучение дополнительной литературы |
| 2 | Работа с лекционным материалом |
| 3 | Подготовка к практическим занятиям |
| 4 | Выполнение курсовой работы. |
| 5 | Подготовка к промежуточной аттестации. |
| 6 | Подготовка к текущему контролю. |

4.4. Примерный перечень тем курсовых работ

- Реализация алгоритма Ривеста.

- Реализация алгоритма DES – режим сцепления блоков в CBC шифре.

- Реализация алгоритма DES – режим работы ECB (электронный блокнот).

- Реализация алгоритма DES – режим работы CFB – обратная связь по шифротексту.

- Реализация алгоритма DES – OFB – обратная связь по выходу.

- Алгоритм федерального стандарта x9.9.

- Алгоритм криптографического преобразования – общий.

- Алгоритм криптографического преобразования в режиме простой замены.

- Алгоритм криптографического преобразования в режиме гаммирования с обратной связью

- Алгоритм криптографического преобразования в режиме имитовставки.

- Алгоритм, основанный на схеме шифрования Эль Гамаля.

- Алгоритм, основанный на комбинированном методе шифрования

- Открытое распределение ключей Диффи-Хеллмана

- Алгоритм электронной подписи RSA.

- Алгоритм электронной подписи DSA.

- Отечественный стандарт электронной подписи.

- Алгоритм цифровой подписи с дополнительными функциями по схеме «слепой подписи».

- Алгоритм цифровой подписи с дополнительными функциями по схеме «неоспоримой подписи».

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

| № п/п | Библиографическое описание | Место доступа |
|---|---|---|
| 1 | Фильтрация набора данных: учебно-метод. пособие для бакалавров по напр. Управление в технических системах профиля Управление и информатика в технических системах, а также специалистов по спец. Компьютерная безопасность специализации Информационная безопасность объектов информатизации на базе компьютерных систем / М. А. Васильева, О. А. Тимофеева, К. М. Филипченко; МИИТ. | https://library.miit.ru/bookscatalog/metod/DC-1196.pdf |

| | | |
|---|---|---|
| | Каф. Управление и защита информации. - Москва: РУТ (МИИТ), 2020. - 31 с. - Б. ц. | |
| 2 | Фильтрация набора данных. Рекомендации по выполнению работы и перечень типовых заданий. : Учебно - методическое пособие для бакалавров по направлению Управление в технических системах, а также специалистов по специальности Компьютерная безопасность специализации Информационная безопасность объектов информатизации на базе компьютерных систем / М. А. Васильева , Д. О. Хобта; РУТ(МИИТ). Кафедра Управление и защита инофрмации . - - 122 с. - Б. ц. | https://library.miit.ru/bookscatalog/upos/DC-1625.pdf |
| 3 | Шифрование с открытым ключом: метод. указ. к лаб. раб. по дисц. Информационная безопасность и защита информации для студ. спец. Автоматизированные системы обработки информации и управления, Информационные системы и технологии / Э.И. Костюковская, А.М. Удалов; МИИТ. Каф. Автоматизированные системы управления. - М.: МИИТ, 2008. - 28 с | https://library.miit.ru/bookscatalog/metod/04-46051.pdf |
| 4 | Криптографическая защита компьютерной информации: метод. указ. к лаб. раб. по дисц. Теоретические основы компьютерной безопасности для студ., обуч. по напр. Информационная безопасность / Я. М. Голдовский, Б. В. Желенков, И. Е. Сафонова; МИИТ. Каф. Вычислительные системы и сети. - М.: МГУПС(МИИТ), 2013. - 36 с. | https://library.miit.ru/bookscatalog/metod/03-42764.pdf |

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

Форум специалистов по информационным технологиям http://citforum.ru/

Интернет-университет информационных технологий http://www.intuit.ru/

Официальный сайт РУТ (МИИТ) (https://www.miit.ru/).

Научно-техническая библиотека РУТ (МИИТ) (http:/library.miit.ru).

Образовательная платформа «Юрайт» (https://urait.ru/).

Общие информационные, справочные и поисковые системы «Консультант Плюс», «Гарант».

Электронно-библиотечная система издательства «Лань» (http://e.lanbook.com/).

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

ОС Microsoft Windows.
Microsoft Office
Интернет-браузер (Yandex и др.)

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

Учебная аудитория для проведения учебных занятий (занятий лекционного типа, практических занятий, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций):

- компьютер преподавателя, мультимедийное оборудование, доска.

Аудитория подключена к сети «Интернет».

9. Форма промежуточной аттестации:

Зачет в 5 семестре.
Курсовая работа в 6 семестре.
Экзамен в 6 семестре.

10. Оценочные материалы.

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

Авторы:

заведующий кафедрой, доцент, к.н.
кафедры «Вычислительные системы
и квантовые коммуникации» Б.В. Желенков

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова