

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
10.03.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Криптографическая защита информации

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 РУТ (МИИТ)
ID подписи: 4196
Подписал: заведующий кафедрой Желенков Борис
Владимирович
Дата: 04.06.2026

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):

ОПК-3 - Способен на основании совокупности математических методов, физических законов и моделей разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.

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;
- порядок тестирования функций программных и программно-аппаратных (в том числе криптографических) средств защиты информации.

Уметь:

- оценивать уровень безопасности КС и сетей;
- применять стандарты и другие нормативные документы по информационной безопасности для оценки защищенности КС;
- проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации.

Владеть:

- навыками работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации;

- навыками поддержания бесперебойной работы программных и программно- аппаратных (в том числе криптографических) средств защиты информации в ИТКС;

- навыками использования средств криптографической и технической защиты информации для решения задач профессиональной деятельности.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 9 з.е. (324 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 196 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	5 СЕМЕСТР ЗАЩИТА ИНФОРМАЦИИ Рассматриваемые вопросы: - требования ФСТЭК по защите информации; - рекомендации по технической защите данных; - классы средств защиты данных.
2	ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ Рассматриваемые вопросы: - меры по обеспечению информационной безопасности; - документы ФСТЭК по ИБ; - сертифицированные средства ИБ ФСТЭК.
3	ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ Рассматриваемые вопросы: - порядок обеспечения информационной безопасности; - криптографическая защита информации.
4	КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ Рассматриваемые вопросы: - методы защиты виды, классификация; - шифрование, стенография, кодирование, сжатие и др..
5	КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ Рассматриваемые вопросы: - средства криптографической защиты информации (СКЗИ); - сертифицированные криптографические средства защиты информации в России.
6	ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ Рассматриваемые вопросы: - алгоритм Евклида, соотношение Безу; - Диофантовы линейные уравнения; - теорема Ферма, функция и теорема Эйлера; - квадратичные вычеты, символы Лежандра и Якоби.
7	ТЕСТИРОВАНИЕ ЧИСЕЛ НА ПРОСТОТУ И ПОСТРОЕНИЕ Рассматриваемые вопросы: - элементарные методы проверки простоты чисел; - алгоритмы Коныгина-Померанса, Миллера; - вероятностные тесты на простоту и детерминированный полиномиальный алгоритм проверки простоты чисел.
8	ФАКТОРИЗАЦИЯ ЦЕЛЫХ ЧИСЕЛ С ЭКСПОНЕНЦИАЛЬНОЙ СЛОЖНОСТЬЮ Рассматриваемые вопросы: - методы Ферма, Полларда, Шермана-Лемана, - алгоритмы Ленстры и Полларда-Штрассена; - $(P + 1)$ -метод Уильямса и его обобщения.
9	ФАКТОРИЗАЦИЯ ЦЕЛЫХ ЧИСЕЛ С СУБЭКСПОНЕНЦИАЛЬНОЙ СЛОЖНОСТЬЮ Рассматриваемые вопросы: - методы Диксона, Шнорра-Ленстры, Ленстры-Померанса;

№ п/п	Тематика лекционных занятий / краткое содержание
	<ul style="list-style-type: none"> - алгоритм Бриллихарт-Моррисона; - алгоритмы решета числового поля.
10	<p>АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ: ГРУППЫ, КОЛЬЦА, ПОЛЯ</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - группы, морфизмы групп, кольца, поля; - поля Гауа или конечные поля; - задача дискретного логарифмирования в конечных полях; - кольцо многочленов.
11	<p>ПРИМЕНЕНИЕ КРИВЫХ ДЛЯ ПРОВЕРКИ ПРОСТОТЫ И ФАКТОРИЗАЦИИ</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - эллиптические кривые и их свойства; - алгоритм Ленстры для факторизации целых чисел с помощью эллиптических кривых; - вычисление порядка группы точек эллиптической кривой над конечным полем; - тестирование чисел на простоту с помощью эллиптических кривых.
12	<p>АЛГОРИТМЫ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - детерминированные методы; - дискретное логарифмирование в простых полях, в полях Гауа; решето числового поля; - частное Ферма и дискретное логарифмирование по составному модулю.
13	<p>ФАКТОРИЗАЦИЯ МНОГОЧЛЕНОВ НАД КОНЕЧНЫМИ ПОЛЯМИ</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - вероятностный алгоритм решения алгебраических уравнений в конечных полях; - решение квадратных уравнений; - вероятностный алгоритм проверки неприводимости многочленов над конечными полями.
14	<p>ПРИВЕДЕННЫЕ БАЗИСЫ РЕШЕТОК И ИХ ПРИЛОЖЕНИЯ</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - решетки и базисы; - LLL-приведенный базис и его свойства; - алгоритм Фергюсона-Форкейда.
15	<p>Рассматриваемые вопросы:</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - LLL-алгоритм факторизации; - факторизация многочленов с использованием приближенных вычислений.
16	<p>ДИСКРЕТНОЕ ПРЕОБРАЗОВАНИЕ ФУРЬЕ</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - вычисление дискретного преобразования Фурье; - применение дискретного преобразования Фурье в алгоритме Полларда-Штрассена.
17	<p>6 СЕМЕСТР ЦЕЛОЧИСЛЕННАЯ АРИФМЕТИКА МНОГОКРАТНОЙ ТОЧНОСТИ</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - основные операции; - алгоритмы модулярной арифметики.
18	<p>СИСТЕМЫ ЛИНЕЙНЫХ УРАВНЕНИЙ НАД КОНЕЧНЫМИ ПОЛЯМИ</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - решение систем линейных уравнений в целых числах; - гауссово и структурированное гауссово исключение; - алгоритмы Ланцоша и Видемана.

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

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

4.2. Занятия семинарского типа.

Практические занятия

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

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

№ п/п	Тематика практических занятий/краткое содержание
19	ИССЛЕДОВАНИЕ И ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МЕТОДОВ ШИФРОВАНИЯ Результатом работы является отлаженная программа, реализующая предложенный студентом алгоритм шифрования.
20	СОВРЕМЕННЫЕ СИММЕТРИЧНЫЕ И АССИМЕТРИЧНЫЕ КРИПТОСИСТЕМЫ Результатом работы является отлаженная программа, реализующая заданный студенту криптографический алгоритм.
21	ОБЩИЕ КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ Результат работы – навыки практического применения соответствующего стандарта.
22	ОЦЕНКА БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ Результат работы – список угроз и мер по разработке безопасного ПО, согласно ГОСТ Р 58412-2019.
23	ЗАЩИТА СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ Результат работы - получение навыков практического применения Руководящего документа.
24	РАЗРАБОТКА СИСТЕМЫ ИНФОРМАЦИОННОЙ ЗАЩИТЫ ОБЪЕКТА ИНФОРМАТИЗАЦИИ 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 х9.9.
- 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	Кодирование и защита информации в документообороте: метод. указ. к практ. и лаб. раб. для студ. спец. Прикладная информатика (в экономике) по дисц. Информационная безопасность / В.И. Морозова, К.Э. Врублевский; МИИТ. Каф. Экономическая информатика. - М.: МИИТ, 2010. - 56 с.	https://library.miit.ru/bookscatalog/metod/03_19830.pdf (дата обращения 08.03.2026) Текст : непосредственный.004.056.57 М 80

2	<p>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.</p>	<p>https://library.miiit.ru/bookscatalog/metod/04-46051.pdf. (дата обращения 08.03.2026) Текст : непосредственный.004 К 72</p>
3	<p>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.</p>	<p>https://library.miiit.ru/bookscatalog/metod/03-42764.pdf. (дата обращения 08.03.2026) Текст : непосредственный.004 Г60</p>
4	<p>Информационная безопасность персональных компьютеров: учеб. пособие для студ. спец. САПР и строительных спец. по курсу Методы и средства защиты компьютерной информации. Ч.2 / В.Ю. Смирнов, О.В. Смирнова; МИИТ. Каф. САПР транспортных конструкций и сооружений.М.: МИИТ, 2010. - 88 с.</p>	<p>https://library.miiit.ru/miiitpublishing/10-2256.pdf. (дата обращения 08.03.2026) Текст : непосредственный.681.3.066 С 50</p>
5	<p>Разработка мер защиты информационных ресурсов в корпоративной сети с выходом в интернет: учебно-метод. пособие по курс. работе для специалистов напр. Компьютерная безопасность / В.</p>	<p>https://library.miiit.ru/bookscatalog/metod/DC-435.pdf. (дата обращения 08.03.2026) Текст : непосредственный.004 А-47</p>

<p>М. Алексеев; МИИТ. Каф. Управление и защита информации. - М.: РУТ(МИИТ), 2017. - 9 с.</p>	
--	--

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/>

Поисковые системы: Yandex, Mail.

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).

Microsoft Internet Explorer (или другой браузер).

Операционная система Microsoft Windows.

Microsoft Office.

Специализированное программное обеспечение не требуется.

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

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования.

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:

доцент, к.н. кафедры
«Вычислительные системы и
квантовые коммуникации»

Я.М. Голдовский

Согласовано:

Заведующий кафедрой ВССиИБ
Председатель учебно-методической
комиссии

Б.В. Желенков

Н.А. Андриянова