

**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 - программы бакалавриата  
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

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: 24.10.2024

## 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-1** - Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности;

**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 математики 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):	112	48	64
В том числе:			
Занятия лекционного типа	64	32	32
Занятия семинарского типа	48	16	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 176 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	<b>СЕМЕСТР 5 ЗАЩИТА ИНФОРМАЦИИ</b> Рассматриваемые вопросы: - требования ФСТЭК по защите информации; - рекомендации по технической защите данных; - классы средств защиты данных.
2	<b>ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ</b> Рассматриваемые вопросы: - меры по обеспечению информационной безопасности; - документы ФСТЭК по ИБ; - сертифицированные средства ИБ ФСТЭК
3	<b>ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ</b> Рассматриваемые вопросы: - порядок обеспечения информационной безопасности; - криптографическая защита информации.
4	<b>КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ</b> Рассматриваемые вопросы: - методы защиты виды, классификация; - шифрование, стенография, кодирование, сжатие и др..
5	<b>КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ</b> Рассматриваемые вопросы: - средства криптографической защиты информации (СКЗИ); - сертифицированные криптографические средства защиты информации в России.
6	<b>ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ</b> Рассматриваемые вопросы: - алгоритм Евклида, соотношение Безу; - Диофантовы линейные уравнения; - теорема Ферма, функция и теорема Эйлера; - квадратичные вычеты, символы Лежандра и Якоби.
7	<b>ТЕСТИРОВАНИЕ ЧИСЕЛ НА ПРОСТОТУ И ПОСТРОЕНИЕ</b> Рассматриваемые вопросы: - элементарные методы проверки простоты чисел; - алгоритмы Конягина-Померанса, Миллера; - вероятностные тесты на простоту и детерминированный полиномиальный алгоритм проверки простоты чисел.
8	<b>ФАКТОРИЗАЦИЯ ЦЕЛЫХ ЧИСЕЛ С ЭКСПОНЕНЦИАЛЬНОЙ</b> Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	<ul style="list-style-type: none"> <li>- методы Ферма, Полларда, Шермана-Лемана,</li> <li>- алгоритмы Ленстры и Полларда-Штрассена;</li> <li>- <math>(P + 1)</math>-метод Уильямса и его обобщения.</li> </ul>
9	<p><b>ФАКТОРИЗАЦИЯ ЦЕЛЫХ ЧИСЕЛ С СУБЭКСПОНЕНЦИАЛЬНОЙ СЛОЖНОСТЬЮ</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- методы Диксона, Шнорра-Ленстры, Ленстры-Померанса;</li> <li>- алгоритм Бриллхарта-Моррисона;</li> <li>- алгоритмы решета числового поля.</li> </ul>
10	<p><b>АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ: ГРУППЫ, КОЛЬЦА, ПОЛЯ</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- группы, морфизмы групп, кольца, поля;</li> <li>- поля Галуа или конечные поля;</li> <li>- задача дискретного логарифмирования в конечных полях;</li> <li>- кольцо многочленов.</li> </ul>
11	<p><b>ПРИМЕНЕНИЕ КРИВЫХ ДЛЯ ПРОВЕРКИ ПРОСТОТЫ И ФАКТОРИЗАЦИИ</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- эллиптические кривые и их свойства;</li> <li>- алгоритм Ленстры для факторизации целых чисел с помощью эллиптических кривых;</li> <li>- вычисление порядка группы точек эллиптической кривой над конечным полем;</li> <li>- тестирование чисел на простоту с помощью эллиптических кривых.</li> </ul>
12	<p><b>АЛГОРИТМЫ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- детерминированные методы;</li> <li>- дискретное логарифмирование в простых полях, в полях Галуа; решето числового поля;</li> <li>- частное Ферма и дискретное логарифмирование по составному модулю.</li> </ul>
13	<p><b>ФАКТОРИЗАЦИЯ МНОГОЧЛЕНОВ НАД КОНЕЧНЫМИ ПОЛЯМИ</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- вероятностный алгоритм решения алгебраических уравнений в конечных полях;</li> <li>- решение квадратных уравнений;</li> <li>- вероятностный алгоритм проверки неприводимости многочленов над конечными полями.</li> </ul>
14	<p><b>ПРИВЕДЕННЫЕ БАЗИСЫ РЕШЕТОК И ИХ ПРИЛОЖЕНИЯ</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- решетки и базисы;</li> <li>- LLL-приведенный базис и его свойства;</li> <li>- алгоритм Фергюсона-Форкейда.</li> </ul>
15	<p><b>ФАКТОРИЗАЦИЯ МНОГОЧЛЕНОВ НАД ПОЛЕМ РАЦИОНАЛЬНЫХ ЧИСЕЛ</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- LLL-алгоритм факторизации;</li> <li>- факторизация многочленов с использованием приближенных вычислений.</li> </ul>
16	<p><b>ДИСКРЕТНОЕ ПРЕОБРАЗОВАНИЕ ФУРЬЕ</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- вычисление дискретного преобразования Фурье;</li> <li>- применение дискретного преобразования Фурье в алгоритме Полларда-Штрассена.</li> </ul>
17	<p><b>СЕМЕСТР 6 ЦЕЛОЧИСЛЕННАЯ АРИФМЕТИКА МНОГОКРАТНОЙ ТОЧНОСТИ</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- основные операции;</li> <li>- алгоритмы модулярной арифметики.</li> </ul>

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

№ п/п	Тематика лекционных занятий / краткое содержание
	Рассматриваемые вопросы: - проблема аутентификации данных; - подписи с дополнительными функциональными свойствами.
28	<b>АЛГОРИТМЫ ЭП</b> Рассматриваемые вопросы: - алгоритмы электронной подписи (назначение и виды, классификация, подделка ЭП); - слепая ЭП, быстрая, неоспоримая.
29	<b>БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ</b> Рассматриваемые вопросы: - формальные методы доказательства правильности программ и их спецификаций; - методы и средства анализа безопасности ПО; - контрольно-испытательные и логико-аналитические методы.
30	<b>БЕЗОПАСНОСТЬ ТЕХНИЧЕСКИХ СРЕДСТВ КОМПЬЮТЕРНЫХ СИСТЕМ</b> Рассматриваемые вопросы: - требования к техническим средствам; - анализ безопасности технических средств КС; - подходы к оценке информационной безопасности.
31	<b>ОСНОВНЫЕ МЕТОДЫ ДЛЯ РЕШЕНИЯ ПРОБЛЕМЫ ОПРЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ КС</b> Рассматриваемые вопросы: - структура критериев оценки соответствия уровня защищенности; - показатели уязвимости; - использование эмпирического, теоретического и теоретико-эмпирического методов.
32	<b>ПРОЕКТИРОВАНИЕ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b> 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	<b>СЕМЕСТР 5 КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ</b> В результате работы студентом будут исследованы и проанализированы криптографические методы и средства защиты информации, подготовлен отчет.
2	<b>ФАКТОРИЗАЦИЯ ЦЕЛЫХ ЧИСЕЛ С ЭКСПОНЕНЦИАЛЬНОЙ</b> Результат работы – реализация алгоритмов Ленстры и Полларда-Штрассена.
3	<b>ФАКТОРИЗАЦИЯ ЦЕЛЫХ ЧИСЕЛ С СУБЭКСПОНЕНЦИАЛЬНОЙ СЛОЖНОСТЬЮ</b>

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

№ п/п	Тематика практических занятий/краткое содержание
20	<b>СОВРЕМЕННЫЕ СИММЕТРИЧНЫЕ И АССИМЕТРИЧНЫЕ КРИПТОСИСТЕМЫ</b> Результатом работы является отлаженная программа, реализующая заданный студенту криптографический алгоритм.
21	<b>ОБЩИЕ КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.</b> Результат работы – навыки практического применения соответствующего стандарта.
22	<b>ОЦЕНКА БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ.</b> Результат работы – список угроз и мер по разработке безопасного ПО, согласно ГОСТ Р 58412-2019.
23	<b>ЗАЩИТА СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ</b> Результат работы - получение навыков практического применения Руководящего документа.
24	<b>РАЗРАБОТКА СИСТЕМЫ ИНФОРМАЦИОННОЙ ЗАЩИТЫ ОБЪЕКТА ИНФОРМАТИЗАЦИИ</b> 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. Каф. Управление и защита информации. - Москва: РУТ (МИИТ), 2020. - 31 с. - Б. ц.	<a href="https://library.miit.ru/bookscatalog/metod/DC-1196.pdf">https://library.miit.ru/bookscatalog/metod/DC-1196.pdf</a>
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	<a href="https://library.miit.ru/bookscatalog/upos/DC-1625.pdf">https://library.miit.ru/bookscatalog/upos/DC-1625.pdf</a>

	Компьютерная безопасность специализации Информационная безопасность объектов информатизации на базе компьютерных систем / М. А. Васильева, Д. О. Хобта; РУТ(МИИТ). Кафедра Управление и защита информации . - - 122 с. - Б. ц.	
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	<a href="https://library.miit.ru/bookscatalog/metod/04-46051.pdf">https://library.miit.ru/bookscatalog/metod/04-46051.pdf</a>
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.	<a href="https://library.miit.ru/bookscatalog/metod/03-42764.pdf">https://library.miit.ru/bookscatalog/metod/03-42764.pdf</a>

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,  
сети и информационная  
безопасность»

Б.В. Желенков

Согласовано:

Заведующий кафедрой ВССиИБ  
Председатель учебно-методической  
комиссии

Б.В. Желенков

Н.А. Андриянова