

**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  
09.03.01 Информатика и вычислительная техника,  
утвержденной первым проректором РУТ (МИИТ)  
Тимониным В.С.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Защита компьютерных сетей**

Направление подготовки: 09.03.01 Информатика и вычислительная техника

Направленность (профиль): 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: 03.06.2026

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

Целями освоения учебной дисциплины «Защита компьютерных сетей» являются формирование компетенций по основным разделам теоретических и практических основ организации средств защиты информации, дать необходимые навыки по использованию средств защиты компьютерных сетей от несанкционированного доступа и овладению методами решения соответствующих задач.

Студенты должны научиться применять современные средства защиты информации предоставляемые сетевым оборудованием, являющимся самым уязвимым местом при попытке несанкционированного доступа.

Основными задачами дисциплины являются:

- Ознакомление с основными терминами и определениями.
- Ознакомление с основными типами угроз и атак.
- Изучение механизмов защиты административного интерфейса и разграничения прав доступа.
- Изучение технологии AAA.
- Изучение способов защиты информации в сетях.
- Изучение принципов построения виртуальных частных сетей.

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

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

**ПК-4** - Способность планировать и проводить регламентные работы по восстановлению сетевой инфокоммуникационной системы;

**ПК-5** - Способность администрировать процесс управления безопасностью сетевых устройств, программного обеспечения, средств обеспечения безопасности удаленного доступа.

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

### **Знать:**

- понятия информационной безопасности, составные элементы подсистем и их характеристики;
- правила эксплуатации используемых подсистем информационной безопасности;

- методы и средства конфигурирования и контроля работоспособности средств безопасности, предоставляемых аппаратно-программными комплексами;

- порядок обслуживания криптографических средств защиты информации;

- методы и принципы проведения аудита информационной безопасности.

**Уметь:**

- контролировать работу подсистем и изменять конфигурационные параметры при необходимости;

- применять методы и средства контроля работоспособности средств безопасности, предоставляемых аппаратно-программными комплексами, обслуживать технические средства защиты информации;

- организовывать и проводить аудит работоспособности и эффективности применяемых средств защиты информации.

**Владеть:**

- навыками по настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

- навыками прогнозирования поведения подсистемы информационной безопасности объекта при изменении внешних воздействий;

- навыками эксплуатации подсистем управления информационной безопасностью предприятия построенных с использованием современного оборудования;

- навыками оценивания оптимальности выбора программно-аппаратных средств защиты информации.

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 №8
Контактная работа при проведении учебных занятий (всего):	50	50
В том числе:		
Занятия лекционного типа	30	30
Занятия семинарского типа	20	20

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 58 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	Защита информации Рассматриваемые вопросы: - Основные термины и определения. - Рассматриваются основные термины и определения в соответствии с ГОСТ Р 50922-2006. - Рассматриваются основные направления действия системы защиты информации и принципы ее организации.
2	Политика защиты Рассматриваемые вопросы: - Сетевая безопасность. - Рассматриваются вопросы безопасности сети предприятия, определяются направления действия политики защиты. - Приводятся примерные варианты реализации политик защиты.
3	Политика защиты(продолжение) Рассматриваемые вопросы: - Анализ угроз безопасности. - Описываются типы угроз и общие рекомендации по борьбе с ними.
4	Политика защиты(продолжение) Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	<ul style="list-style-type: none"> <li>- Вирусы.</li> <li>- Описываются типы вирусов, среда обитания, способы заражения, вредоносное воздействие.</li> </ul>
5	<p><b>Защита сети</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Защита административного доступа к сетевым устройствам.</li> <li>- Рассматриваются вопросы защиты доступа к административным интерфейсам.</li> <li>- Описываются методы усиления парольной защиты и разделения уровней привилегий.</li> </ul>
6	<p><b>Защита сети (продолжение)</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Защита связи между маршрутизаторами.</li> <li>- Приводятся методы обеспечения защиты связи между маршрутизаторами с использованием аутентификации протоколов маршрутизации.</li> <li>- Приводятся методы ограничения объявлений маршрутной информации и фильтрации входящего сетевого трафика.</li> </ul>
7	<p><b>Защита сети (продолжение)</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Технология защиты AAA.</li> <li>- Рассматриваются методы аутентификации и авторизации.</li> <li>- Представлена технология защиты AAA, принципы ее работы и конфигурирования, TACACS+, RADIUS.</li> </ul>
8	<p><b>Защита сетевых соединений</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Модели обороны.</li> <li>- Рассматриваются существующие модели обороны, их преимущества и недостатки.</li> </ul>
9	<p><b>Защита сетевых соединений(продолжение)</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Защита периметра сети.</li> <li>- Описывается зонная архитектура защиты сети и ее компоненты.</li> <li>- Контроль сервисов TCP/IP.</li> <li>- Рассматриваются средства контроля сервисов TCP/IP на уровне глобальной конфигурации и конфигурации интерфейсов.</li> </ul>
10	<p><b>Защита сетевых соединений(продолжение)</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Контроль доступа.</li> <li>- Описываются средства контроля доступа с использованием рефлексивных, динамических и временных списков доступа, СВАС и их конфигурация, а также настройка средств защиты от синхронных атак.</li> </ul>
11	<p><b>Шифрование</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Механизмы шифрования.</li> <li>- Рассматриваются различные варианты построения систем шифрования и их свойства.</li> </ul>
12	<p><b>Шифрование(продолжение)</b></p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> <li>- Блочное шифрование и цифровая подпись.</li> <li>- Рассматривается алгоритм шифрования с использованием сетей Фейстеля, алгоритмы DES, 3DES, AES.</li> </ul>

№ п/п	Тематика лекционных занятий / краткое содержание
13	<b>Шифрование(продолжение)</b> Рассматриваемые вопросы: - Рассматривается алгоритм шифрования с использованием сетей Фейстеля ГОСТ 28147, RSA, RC5.
14	<b>Шифрование(продолжение)</b> Рассматриваемые вопросы: - Рассматривается назначение и схемы построения цифровой подписи, алгоритм DSA. - Шифрование на сетевом уровне. - Приводится обзор задач и средств шифрования на сетевом уровне.
15	<b>Построение виртуальных частных сетей с использованием IPSec</b> Рассматриваемые вопросы: - Обзор технологии виртуальных частных сетей. - Приводится обзор технологии виртуальных частных сетей (VPN), их топологий и средств поддержки. - Механизмы IPSec. - Рассматриваются принципы работы и настройки механизмов IPSec с использованием IKE. - Настройка IPSec VPN. - Описывается настройка политики ISAKMP, определение наборов преобразований IPSec и настройка криптографических карт.

## 4.2. Занятия семинарского типа.

### Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	<b>Вирусы</b> В результате выполнения работы студент получит понимание принципов работы вирусов.
2	<b>Вирусы(продолжение)</b> В результате выполнения работы студент получит навыки по борьбе с вирусами.
3	<b>Защита административного доступа и связи между маршрутизаторами</b> В результате выполнения работы студент получит практические навыки по защите административного доступа к маршрутизаторам.
4	<b>Защита административного доступа и связи между маршрутизаторами(продолжение)</b> В результате выполнения работы студент получит практические навыки по защите связи между маршрутизаторами.
5	<b>Настройка системы защиты AAA</b> В результате выполнения работы студент получит практические навыки по настройке и применению системы защиты AAA с использованием локальной базы данных и серверов защиты TACACS+ и RADIUS.
6	<b>Защита периметра сети с помощью средств контроля доступа</b> В результате выполнения работы студент получит практические навыки по защите периметра сети с помощью сложных списков доступа - Reflexive ACL, Dynamic ACL, Time-Based ACL.
7	<b>Защита периметра сети с помощью средств контроля доступа(продолжение)</b> В результате выполнения работы студент получит практические навыки по защите периметра сети с помощью CBAC.

№ п/п	Наименование лабораторных работ / краткое содержание
8	Изучение методов шифрования В результате выполнения работы студент получит практические навыки по реализации алгоритмов шифрования с помощью программных средств на примере DES и 3DES
9	Изучение методов шифрования(продолжение) В результате выполнения работы студент получит практические навыки по реализации алгоритмов шифрования с помощью программных средств на примере ГОСТ 28147.
10	Конфигурирование VPN-соединения В результате выполнения работы студент получит практические навыки: - по конфигурированию VPN-соединения с использованием IKE; - по настройке политики ISAKMP; - по конфигурированию VPN-соединения с заданными параметрами на сетевом оборудовании.

#### 4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
2	Подготовка к лабораторным работам
3	Подготовка к промежуточной аттестации.
4	Подготовка к текущему контролю.

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

№ п/п	Библиографическое описание	Место доступа
1	Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2015. — 284 с.	<a href="https://e.lanbook.com/book/110336">https://e.lanbook.com/book/110336</a> (дата обращения: 28.04.2025)
2	Технологии защиты информации в компьютерных сетях : Курс лекций / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суоров — Москва : Интуит НОУ, 2016. — 368 с.	<a href="https://book.ru/book/918258">https://book.ru/book/918258</a> (дата обращения: 28.04.2025)
3	Голдовский Я.М., Желенков Б.В., Сафонова И.Е., Криптографическая защита компьютерной информации. Методические указания к лабораторным работам. М.: МИИТ, 2013. 36с. УДК 681.3 Г60	<a href="http://library.miit.ru/bookscatalog/metod/03-42764.pdf">http://library.miit.ru/bookscatalog/metod/03-42764.pdf</a> (дата обращения: 28.04.2025)

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

Научно-техническая библиотека РУТ(МИИТ) <http://library.miiit.ru/>

Официальный сайт по поддержке решений Cisco <https://www.cisco.com/>

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

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

Тематический форум по информационным технологиям  
<http://habrahabr.ru/>

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

Microsoft Windows

Microsoft Office

Интернет-браузер (Yandex и др.)

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

Учебная аудитория (Компьютерный класс) для проведения учебных занятий (занятий лекционного типа, практических занятий):

- компьютер преподавателя, мультимедийное оборудование, рабочие станции студентов, доска.

Аудитория подключена к сети «Интернет».

9. Форма промежуточной аттестации:

Экзамен в 8 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