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
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

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;

-изучение способов защиты информации в сетях;

-изучение принципов построения виртуальных частных сетей.

Дисциплина предназначена для получения знаний, необходимых для решения следующих профессиональных задач (в соответствии с видами деятельности):

Производственно-технологическая деятельность

-разработка технических спецификаций на компоненты вычислительной техники и компьютерных сетей;

-осуществляет разработку тестовых документов на компьютерные сети и их компоненты;

-разработка технологических решений при проектировании защищенных компьютерных сетей;

-разработка технологических решений управления сетями;

-коррекция производительности сетевой инфокоммуникационной системы;

-выполнение регламентных работ по поддержке операционных систем сетевых устройств инфокоммуникационной системы;

-восстановление параметров программного обеспечения сетевых устройств.

Проектная деятельность

-проектирование и дизайн ИС;

-разработка, проектирование и модернизация защищенных компьютерных сетей;

-разработка систем управления сетями.

Организационно-управленческая

-контроль использования компьютерных сетей и программного обеспечения;

-оценка производительности компьютерных сетей.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-3 - Способность администрировать процесс контроля использования сетевых устройств и программного обеспечения ;

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:

- общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети;

- архитектуру аппаратных, программных и программно-аппаратных средств администрируемой сети;

- протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем;

- модель ISO для управления сетевым трафиком;

- модели IEEE;

- регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе.

Уметь:

-настраивать параметры современных программно-аппаратных межсетевых экранов;

-сегментировать элементы администрируемой сети;

-инсталлировать операционные системы сетевых устройств;

-осуществлять мониторинг администрируемых сетевых устройств;

-пользоваться нормативно-технической документацией в области инфокоммуникационных технологий;

-работать с контрольно-измерительными аппаратными и программными средствами;

-комплектовать составные элементы сетевого оборудования.

Владеть:

- навыками по параметризации операционных систем дополнительных средств защиты администрируемой сети от несанкционированного доступа;

- установкой специализированных программных средств защиты сетевых устройств администрируемой сети от несанкционированного доступа;

-установкой межсетевых экранов, гибких коммутаторов, средств предотвращения атак виртуальной частной сети;

-навыками инвентаризации оборудования и параметров операционных систем сетевых устройств;

-перезагрузкой операционных систем сетевых устройств;

-регламентное обслуживание оборудования в соответствии с рекомендациями производителя; анализа параметров производительности администрируемой сети за установленный период (сутки, неделя, месяц, квартал, год).

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 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):	72	72
В том числе:		
Занятия лекционного типа	36	36
Занятия семинарского типа	36	36

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 72 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	1. Защита информации. Рассматриваемые вопросы: -основные термины и определения в соответствии с ГОСТ Р 50922-2006; -основные направления действия системы защиты информации и принципы ее организации. 2. Политика защиты.Сетевая безопасность. Рассматриваются вопросы: - безопасность сети предприятия; - определение направления действия политики защиты, примерные варианты реализации политик защиты; -анализ угроз безопасности; - типы угроз и общие рекомендации по борьбе с ними; -вирусы; - типы вирусов, среда обитания, способы заражения, вредоносное воздействие. 3. Защита сети. Рассматриваются вопросы: Защита административного доступа к сетевым устройствам. -защиты доступа к административным интерфейсам; - методы усиления парольной защиты и разделения уровней привилегий. Защита связи между маршрутизаторами. - методы обеспечения защиты связи между маршрутизаторами с использованием аутентификации протоколов маршрутизации; -методы ограничения объявлений маршрутной информации и фильтрации входящего сетевого трафика. Технология защиты AAA. -методы аутентификации и авторизации; -представлена технология защиты AAA, принципы ее работы и конфигурирования. 4. Защита сетевых соединений.

№ п/п	Тематика лекционных занятий / краткое содержание
	Рассматриваются вопросы: .Модели обороны. - существующие модели обороны, их преимущества и недостатки; Защита периметра сети. -зонная архитектура защиты сети и ее компоненты; Контроль сервисов TCP/IP. -средства контроля сервисов TCP/IP на уровне глобальной конфигурации и конфигурации интерфейсов; Контроль доступа. -средства контроля доступа с использованием рефлексивных, динамических и временных списков доступа, CBAC и их конфигурация, а также настройка средств защиты от синхронных атак. 5. Шифрование. Рассматриваются вопросы: Механизмы шифрования. -различные варианты построения систем шифрования и их свойства; Блочное шифрование и цифровая подпись; - алгоритм шифрования с использованием сетей Фейстеля, алгоритмы DES, 3DES.AES, ГОСТ 28147, RSARC5; -назначение и схемы построения цифровой подписи, алгоритм DSA; Шифрование на сетевом уровне. - обзор задач и средств шифрования на сетевом уровне. 6. Построение виртуальных частных сетей с использованием IPSec. Рассматриваются вопросы: Обзор технологии виртуальных частных сетей; -приводится обзор технологии виртуальных частных сетей (VPN), их топологий и средств поддержки; Механизмы IPSec. -принципы работы и настройки механизмов IPSec с использованием IKE; Настройка IPSecVPN. -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	1. Лабораторная работа №1. Вирусы. В результате выполнения работы студент получит понимание принципов работы вирусов и способов борьбы с ними. 2. Лабораторная работа №2. Защита административного доступа и связи между маршрутизаторами. В результате выполнения работы студент получит практические навыки по защите административного доступа и связи между маршрутизаторами. 3. Лабораторная работа №3. Настройка системы защиты AAA. В результате выполнения работы студент получит практические навыки по настройке и применению системы защиты AAA.

№ п/п	Наименование лабораторных работ / краткое содержание
	4. Лабораторная работа №4. Защита периметра сети с помощью средств контроля доступа. В результате выполнения работы студент получит практические навыки по защите периметра сети с помощью средств контроля доступа. 5. Лабораторная работа №5. Изучение методов шифрования. В результате выполнения работы студент получит практические навыки по реализации алгоритмов шифрования с помощью программных средств. 6. Лабораторная работа №6. Конфигурирование VPN-соединения. В результате выполнения работы студент получит практические навыки 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	Желенков Б.В. Основы построения опорных сетей ISP : учеб. пособие по дисц. "Сети ЭВМ и телекоммуникации" для студ. 4 курса спец. "Вычислительные машины, комплексы, системы и сети", магистров напр. "Информатика и выч. техника" / МИИТ. Каф. "Вычислительные системы и сети". - М. : МИИТ, 2009. - 148 с. : ил. - Библиогр.: с. 147.	URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/upos/10-1299.pdf. (дата обращения 04.10.2022) Текст : непосредственный 004 Ж51

	- 100 экз. - (в пер.) : 111.13 р.	
2	Голдовский Я.М. Проектирование кампусных сетей : учеб. пособие по дисц. "Сети ЭВМ и телекоммуникации" для студ. спец. "Информатика и вычислительная техника" /; МИИТ. Каф. "Вычислительные системы и сети". - М. : МИИТ, 2009. - 130 с. : ил. - - Библиогр.: с. 130. - 100 экз. - (в пер.) : 99.86 р.	URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/upos/10-1289.pdf. (дата обращения 04.10.2022)Текст : непосредственный. 004 Г60
3	Голдовский Я.М., Желенков Б.В., Сафонова И.Е. Криптографическая защита компьютерной информации : метод. указ. к лаб. раб. по дисц. "Теоретические основы компьютерной безопасности" для студ., обуч. по напр. "Информационная безопасность" / МИИТ. Каф. "Вычислительные системы и сети". - М. : МГУПС(МИИТ), 2013. - 36 с. : ил. - Библиогр.: с. 46. - 100 экз. - (в пер.) : 39.78 р.	URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/metod/03-42764.pdf. (дата обращения 04.10.2022)Текст : непосредственный.004 Г60

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

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

Для проведения лекционных занятий необходима специализированная лекционная аудитория с мультимедиа аппаратурой. Компьютер должен быть обеспечен лицензионными программными продуктами:

Microsoft Windows

Microsoft Office

Для проведения лабораторных работ необходимы персональные компьютеры с рабочими местами. Компьютер должен быть обеспечен лицензионными программными продуктами:

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 проведении занятий с применением электронного обучения и дистанционных образовательных технологий может понадобиться 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

Аудиовизуальное оборудование для аудитории, АРМ управляющий, проектор, экран проекционный Аудитория подключена к интернету МИИТ.

- Учебная аудитория для проведения занятий лекционного типа,

практических занятий, лабораторных работ

Рабочие станции для студентов, коммутатор CISCO, маршрутизатор CISCO, межсетевой экран Cisco, сетевое оборудование, рабочая станция преподавателя, проектор, экран.

В случае проведении 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:

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,
сети и информационная
безопасность» Б.В. Желенков

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А.Клычева