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.

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	Сем. №8
Контактная работа при проведении учебных занятий (всего):	60	60
В том числе:		
Занятия лекционного типа	30	30
Занятия семинарского типа	30	30

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 84 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	Лекция 1 Тема 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.

№ п/п	Тематика лекционных занятий / краткое содержание
	Лекция 2 Тема 2. Политика защиты. Рассматриваемые вопросы: Сетевая безопасность. Рассматриваются вопросы безопасности сети предприятия, определяются направления действия политики защиты. Приводятся примерные варианты реализации политик защиты. Лекция 3 Политика защиты (продолжение). Рассматриваемые вопросы: Анализ угроз безопасности. Описываются типы угроз и общие рекомендации по борьбе с ними. Лекция 4 Политика защиты (продолжение). Рассматриваемые вопросы: Вирусы. Описываются типы вирусов, среда обитания, способы заражения, вредоносное воздействие. Лекция 5 Тема 3.Защита сети. Рассматриваемые вопросы: Защита административного доступа к сетевым устройствам. Рассматриваются вопросы защиты доступа к административным интерфейсам. Описываются методы усиления парольной защиты и разделения уровней привилегий. Лекция 6 Защита сети (продолжение). Рассматриваемые вопросы: Защита связи между маршрутизаторами. Приводятся методы обеспечения защиты связи между маршрутизаторами с использованием аутентификации протоколов маршрутизации. Приводятся методы ограничения объявлений маршрутной информации и фильтрации входящего сетевого трафика. Лекция 7 Защита сети (продолжение). Рассматриваемые вопросы: Технология защиты AAA. Рассматриваются методы аутентификации и авторизации. Представлена технология защиты AAA, принципы ее работы и конфигурирования,TACACS+, RADIUS. Лекция 8 Тема 4. Защита сетевых соединений. Рассматриваемые вопросы: Модели обороны. Рассматриваются существующие модели обороны, их преимущества и недостатки. Лекция 9 Защита сетевых соединений (продолжение). Рассматриваемые вопросы: Защита периметра сети.

№ п/п	Тематика лекционных занятий / краткое содержание
	Описывается зонная архитектура защиты сети и ее компоненты. Контроль сервисов TCP/IP. Рассматриваются средства контроля сервисов TCP/IP на уровне глобальной конфигурации и конфигурации интерфейсов. Лекция 10 Защита сетевых соединений (продолжение). Рассматриваемые вопросы: Контроль доступа. Описываются средства контроля доступа с использованием рефлексивных, динамических и временных списков доступа, CBAC и их конфигурация, а также настройка средств защиты от синхронных атак. Лекция 11 Тема 5. Шифрование. Рассматриваемые вопросы: Механизмы шифрования. Шифрование на сетевом уровне. Приводится обзор задач и средств шифрования на сетевом уровне. Рассматриваются различные варианты построения систем шифрования и их свойства. Лекция 12 Шифрование (продолжение). Рассматриваемые вопросы: Блочное шифрование и цифровая подпись. Рассматривается алгоритм шифрования с использованием сетей Фейстеля, алгоритмы DES, 3DES,AES, Лекция 13 Шифрование (продолжение). Рассматриваемые вопросы: Рассматривается алгоритм шифрования с использованием сетей Фейстеля ГОСТ 28147, RSA, RC5. Рассматривается назначение и схемы построения цифровой подписи, алгоритм DSA. Лекция 14 Тема 6. Построение виртуальных частных сетей с использованием IPSec. 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. Лекция 15 Построение виртуальных частных сетей с использованием IPSec (продожение). Рассматриваемые вопросы: Настройка IPSecVPN. 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	1. Лабораторная работа №1. Вирусы. В результате выполнения работы студент получит понимание принципов работы вирусов и получит навыки по борьбе с вирусами. 2. Лабораторная работа №2. Защита административного доступа и связи между маршрутизаторами. В результате выполнения работы студент получит практические навыки по защите административного доступа к маршрутизаторам и связи между ними. 3. Лабораторная работа №3. Настройка системы защиты AAA. В результате выполнения работы студент получит практические навыки по настройке и применению системы защиты AAA с использованием локальной базы данных. 4. Лабораторная работа №3. (продолжение). Настройка системы защиты AAA. В результате выполнения работы студент получит практические навыки по настройке и применению системы защиты AAA с использованием сервера защиты TACACS+. 5. Лабораторная работа №3(продолжение). Настройка системы защиты AAA. В результате выполнения работы студент получит практические навыки по настройке и применению системы защиты AAA с использованием сервера защиты RADIUS. 6. 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 Reflexive ACL. 7. Лабораторная работа №4(продолжение). Защита периметра сети с помощью средств контроля доступа. В результате выполнения работы студент получит практические навыки по защите периметра сети с помощью Dynamic ACL. 8. Лабораторная работа №4. (продолжение). Защита периметра сети с помощью средств контроля доступа. В результате выполнения работы студент получит практические навыки по защите периметра сети с помощью Time-Based ACL. 9. Лабораторная работа №4(продолжение). Защита периметра сети с помощью средств контроля доступа. В результате выполнения работы студент получит практические навыки по защите периметра сети с помощью CBAC 10. Лабораторная работа №5. Изучение методов шифрования. В результате выполнения работы студент получит практические навыки по реализации алгоритмов шифрования с помощью программных средств на примере DES.

№ п/п	Наименование лабораторных работ / краткое содержание
	11. Лабораторная работа №5(продолжение). Изучение методов шифрования. В результате выполнения работы студент получит практические навыки по реализации алгоритмов шифрования с помощью программных средствна примере 3DES. 12. Лабораторная работа №5(продолжение). Изучение методов шифрования. В результате выполнения работы студент получит практические навыки по реализации алгоритмов шифрования с помощью программных средствна примере ГОСТ 28147. 13. Лабораторная работа №6. Конфигурирование VPN-соединения. В результате выполнения работы студент получит практические навыки по конфигурированию VPN-соединения с использованием IKE. 14. Лабораторная работа №6(продолжение). Конфигурирование VPN-соединения. В результате выполнения работы студент получит практические навыки по настройке политики ISAKMP 15. Лабораторная работа №6(продолжение). 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	Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2012. — 592 с. — ISBN 978-5-94074-637-9. — Текст : электронный // Лань : электронно-библиотечная система.	https://e.lanbook.com/book/3032 (дата обращения: 29.02.2024)

2	Технологии защиты информации в компьютерных сетях : Курс лекций / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов — Москва : Интуит НОУ, 2016. — 368 с.	https://book.ru/book/918258 (дата обращения: 29.02.2024)
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	http://library.miit.ru/bookscatalog/metod/03-42764.pdf (дата обращения: 29.02.2024)

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 подключенная к интернету МИИТ.

- Учебная аудитория для проведения занятий 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. Андриянова