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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программно-аппаратные средства защиты 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: 22.04.2024

1. Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины «Программно-аппаратные средства защиты информации» 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):

ОПК-1.2 - Способен администрировать средства защиты информации в компьютерных системах и сетях;

ОПК-10 - Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты ;

ПК-1 - способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации ;

ПК-6 - способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации .

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 средств 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 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 №7
Контактная работа при проведении учебных занятий (всего):	64	64
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	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 80 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.

№ п/п	Тематика лекционных занятий / краткое содержание
	- 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: - Вирусы. - Описываются типы вирусов, среда обитания, способы заражения, вредоносное воздействие.
5	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.
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.
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.
8	Защита сетевых соединений Рассматриваемые вопросы: - Модели обороны. - Рассматриваются существующие модели обороны, их преимущества и недостатки.
9	Защита сетевых соединений(продолжение) Рассматриваемые вопросы: - Защита периметра сети. - 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.
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.

№ п/п	Тематика лекционных занятий / краткое содержание
11	Шифрование Рассматриваемые вопросы: - Механизмы шифрования. - Рассматриваются различные варианты построения систем шифрования и их свойства.
12	Шифрование(продолжение) Рассматриваемые вопросы: - Блочное шифрование и цифровая подпись. - Рассматривается алгоритм шифрования с использованием сетей Фейстеля, алгоритмы DES, 3DES, AES.
13	Шифрование(продолжение) Рассматриваемые вопросы: - Рассматривается алгоритм шифрования с использованием сетей Фейстеля ГОСТ 28147, RSA, RC5.
14	Шифрование(продолжение) 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	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.
16	Построение виртуальных частных сетей с использованием IPSec(продолжение) Рассматриваемые вопросы: - 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	Вирусы В результате выполнения работы студент получит понимание принципов работы вирусов.
2	Вирусы(продолжение) В результате выполнения работы студент получит навыки по борьбе с вирусами.
3	Защита административного доступа и связи между маршрутизаторами В результате выполнения работы студент получит практические навыки по защите административного доступа к маршрутизаторам.
4	Защита административного доступа и связи между маршрутизаторами(продолжение) В результате выполнения работы студент получит практические навыки по защите связи между маршрутизаторами.
5	Настройка системы защиты AAA В результате выполнения работы студент получит практические навыки по настройке и применению

№ п/п	Наименование лабораторных работ / краткое содержание
	системы защиты AAA с использованием локальной базы данных.
6	Настройка системы защиты AAA(продолжение) В результате выполнения работы студент получит практические навыки по настройке и применению системы защиты AAA с использованием сервера защиты TACACS+.
7	Настройка системы защиты AAA(продолжение) В результате выполнения работы студент получит практические навыки по настройке и применению системы защиты AAA с использованием сервера защиты RADIUS.
8	Защита периметра сети с помощью средств контроля доступа В результате выполнения работы студент получит практические навыки по защите периметра сети с помощью Reflexive PACL.
9	Защита периметра сети с помощью средств контроля доступа(продолжение) В результате выполнения работы студент получит практические навыки по защите периметра сети с помощью Dynamic ACL.
10	Защита периметра сети с помощью средств контроля доступа(продолжение) В результате выполнения работы студент получит практические навыки по защите периметра сети с помощью Time-Based ACL.
11	Защита периметра сети с помощью средств контроля доступа(продолжение) В результате выполнения работы студент получит практические навыки по защите периметра сети с помощью CBAC.
12	Изучение методов шифрования В результате выполнения работы студент получит практические навыки по реализации алгоритмов шифрования с помощью программных средств на примере DES.
13	Изучение методов шифрования(продолжение) В результате выполнения работы студент получит практические навыки по реализации алгоритмов шифрования с помощью программных средств на примере 3DES.
14	Изучение методов шифрования(продолжение) В результате выполнения работы студент получит практические навыки по реализации алгоритмов шифрования с помощью программных средств на примере ГОСТ 28147.
15	Конфигурирование VPN-соединения В результате выполнения работы студент получит практические навыки по конфигурированию VPN-соединения с использованием IKE.
16	Конфигурирование VPN-соединения(продолжение) В результате выполнения работы студент получит практические навыки: - 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	Выполнение курсовой работы.
4	Подготовка к промежуточной аттестации.

5	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

Разработать защищенное пространство обработки, хранения и передачи данных в соответствии с вариантом задания.

Разработать защищенное пространство обработки и хранения данных.

Для всех вариантов выбрать в качестве интересного трафика протокол ICMP

1. 1 шлюз, AAA - Tacacs, ACL-, IPSec – ESP, DES, MD-5, PSK.
2. 2 шлюза, AAA - Tacacs, ACL-DYN, IPSec – ESP, 3DES, MD-5, PSK.
3. 1 шлюз, AAA - Tacacs, ACL-REF, IPSec – ESP, AES, MD-5, PSK.
4. 2 шлюза, AAA - Tacacs, ACL- TIME, IPSec – ESP, AES, SHA-1, PSK.
5. 1 шлюз, AAA - Tacacs, ACL- CBAC, IPSec – ESP, 3DES, SHA-1, PSK.
6. 2 шлюза, AAA - Tacacs, ACL- DYN, IPSec – ESP, AES, SHA-1, PSK.
7. 1 шлюз, AAA - Tacacs, ACL- REF, IPSec – ESP, DES, SHA-1, RSA.
8. 2 шлюза, AAA - Tacacs, ACL- TIME, IPSec – ESP, 3DES, SHA-1, RSA.
9. 1 шлюз, AAA - Tacacs, ACL- CBAC, IPSec – ESP, AES, SHA-1, RSA.
10. 2 шлюза, AAA - Tacacs, ACL- DYN, IPSec – ESP, DES, MD-5, RSA.
11. 1 шлюз, AAA - Tacacs, ACL- REF, IPSec – ESP, 3DES, MD-5, RSA.
12. 2 шлюза, AAA - Tacacs, ACL- TIME, IPSec – ESP, AES, MD-5, RSA.
13. 1 шлюз, AAA - Radius, ACL-, IPSec – ESP, DES, MD-5, PSK.
14. 2 шлюза, AAA - Radius, ACL-DYN, IPSec – ESP, 3DES, MD-5, PSK.
15. 1 шлюз, AAA - Radius, ACL-REF, IPSec – ESP, AES, MD-5, PSK.
16. 2 шлюза, AAA - Radius, ACL- TIME, IPSec – ESP, AES, SHA-1, PSK.
17. 1 шлюз, AAA - Radius, ACL- CBAC, IPSec – ESP, 3DES, SHA-1, PSK.
18. 2 шлюза, AAA - Radius, ACL- DYN, IPSec – ESP, AES, SHA-1, PSK.
19. 1 шлюз, AAA - Radius, ACL- REF, IPSec – ESP, DES, SHA-1, RSA.
20. 2 шлюза, AAA - Radius, ACL- TIME, IPSec – ESP, 3DES, SHA-1, RSA.
21. 1 шлюз, AAA - Radius, ACL- CBAC, IPSec – ESP, AES, SHA-1, RSA.
22. 2 шлюза, AAA - Radius, ACL- DYN, IPSec – ESP, DES, MD-5, RSA.

23. 1 шлюз, AAA - Radius, ACL- REF, IPSec – ESP, 3DES, MD-5, RSA.

24. 2 шлюза, AAA - Radius, ACL- TIME, IPSec – ESP, AES, MD-5, RSA.

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

-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».

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

- Учебная аудитория для проведения занятий лекционного типа, практических занятий, лабораторных работ

Рабочие станции для студентов, 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:

Курсовая работа в 7 семестре.

Экзамен в 7 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