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 магистратуры
по направлению подготовки
10.04.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Проектирование защищенных компьютерных сетей

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем и сетей

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины (модуля) являются:

- изучение вопросов обеспечения информационной безопасности проектируемой сети;

- изучение теоретических и практических основ проектирования защищенных компьютерных сетей различных масштабов с использованием различных средств ограничения доступа к защищаемым ресурсам.

Основными задачами дисциплины являются:

• Ознакомление с концепцией построения защищенной сети.

• Ознакомление со структурой распределенной сети как иерархической моделью.

• Ознакомление с особенностями проектирования СКС.

• Рассмотрение архитектуры защищенной сети на примере Cisco SAFE.

• Построение модели угроз сети.

• Рассмотрение принципов выбора активного сетевого оборудования для построения защищенной компьютерной сети.

• Изучение технологии передачи данных.

• Изучение принципов проектирования защищенной компьютерной сети с использованием протоколов OSPF и BGP.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-1 - Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

ОПК-2 - Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности ;

ПК-3 - Способность анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

УК-2 - Способен управлять проектом на всех этапах его жизненного цикла.

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

Знать:

- методы поиска и систематизации информации для анализа проблемных ситуаций;
- принципы организации информационно-аналитической деятельности;
- способы формирования описаний объектов и классов объектов в области построения защищенных компьютерных сетей;
- нормативные правовые акты в области защиты информации;
- организационные меры по защите информации;
- принципы построения компьютерных систем и сетей;
- методы и методики оценки безопасности программно-аппаратных средств защиты информации;
- методы оценки эффективности политики безопасности.

Уметь:

- анализировать проблемную ситуацию и применять системный подход к ее решению;
- прогнозировать и оценивать последствия принятых решений;
- оценивать эффективность и качество в задачах прогнозирования, планирования;
- разрабатывать методики оценки защищенности программно-аппаратных средств защиты информации;
- оценивать эффективность защиты информации;
- применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации;
- разрабатывать программы и методики испытаний защиты информации в сетях.

Владеть:

- навыками разработки алгоритмов решения проблемной ситуации и проведения выбора рационального решения из множества альтернативных;
- навыками решения задач прогнозирования, планирования, выработки решений при различной априорной неопределенности имеющейся информации при проектировании защищенных компьютерных сетей;
- оценка эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 5 з.е. (180

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 №3
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	16	16

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 132 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	Научный подход к проблеме проектирования защищённых компьютерных сетей Рассматриваемые вопросы: - объект оценки; - фаза проектированиям; - стратегии проектирования; - структура профиля защиты.
2	Концепция построения защищенной сети Рассматриваемые вопросы: - интегрированная и внедренная защита, факторы интеграции, стратегия интеграции.
3	Особенности организации корпоративных сетей.Характеристики корпоративных

№ п/п	Тематика лекционных занятий / краткое содержание
	сетей Характеристики корпоративных сетей. Рассматриваемые вопросы: - требования, предъявляемые к сетям, и их анализ; - структура распределенной сети; - структура распределенной сети как иерархическая модель, ее уровни и необходимое оборудование.
4	Особенности организации корпоративных сетей.Модульный подход к проектированию сети Модульный подход к проектированию сети. Рассматриваемые вопросы: - рассматривается модульный подход к проектированию сети, на основе Cisco SONA; - структура опорной сети провайдера; - основные сегменты сети, их структурная организация и назначение.
5	Структурированная кабельная система (СКС).Стандарты СКС Рассматриваемые вопросы: - стандарты СКС; - преимущества стандартизации; - преимущества СКС; - особенность проектирования СКС; - функциональные элементы СКС.
6	Структурированная кабельная система (СКС).Иерархия СКС Рассматриваемые вопросы: - приводится иерархия СКС; - подробно рассматриваются элементы СКС: горизонтальная подсистема, вертикальная подсистема, магистральная подсистема, подсистема рабочего места.
7	Структурированная кабельная система (СКС).Разработка СКС Рассматриваемые вопросы: - этапы разработки СКС и требования к ее элементам: обеспечение энергоснабжения, установка разъемов и розеток, прокладка и монтаж кабеля, выбор мест размещения распределительные щиты и коммутационные панели; - требования, предъявляемые при тестировании структурированной кабельной сети, оборудование для тестирования; - правила оформления документации и эксплуатации СКС.
8	Архитектура защищенной сети на примере Cisco SAFE.Архитектура безопасности Cisco SAFE Рассматриваемые вопросы: - целостность системы; - жизненный цикл атаки; - архитектура Cisco SAFE; - возможности, архитектура, дизайн.
9	Архитектура защищенной сети на примере Cisco SAFE.Защищенная сеть кампуса Рассматриваемые вопросы: - анализ информационных потоков; - плоскость атак – человек, сетевые устройства, уровень доступа, уровень распределения, уровень ядра.
10	Архитектура безопасного доступа к облачной среде Рассматриваемые вопросы: - облачные сервисы; - безопасность – как услуга; - подключение удаленных офисов и пользователей;

№ п/п	Тематика лекционных занятий / краткое содержание
	- анализ бизнес-потоков с точки зрения архитектуры безопасного доступа к облачной среде; - элементы обеспечения безопасности.
11	Модель угроз безопасности информации в сети.Оценка угроз безопасности Рассматриваемые вопросы: - задачи, решаемые в ходе оценки угроз безопасности информации; - исходные данные для оценки угроз безопасности информации; - нормативно-правовые и методические документы, используемые для оценки угроз безопасности информации и разработки модели угроз.
12	Модель угроз безопасности информации в сети.Информационная структура предприятия и её характеристика как объекта защиты Рассматриваемые вопросы: - перечень категорий информации ограниченного доступа, обрабатываемой в сети предприятия, и уровень их конфиденциальности; - перечень лиц, имеющих доступ к информационным ресурсам, с указанием их уровня полномочий; - матрица доступа или полномочий субъектов доступа.
13	Выбор оборудования и протоколов маршрутизации.Выбор оборудования Рассматриваемые вопросы: - рассматривается выбор активного сетевого оборудования для каждого уровня иерархии.
14	Выбор оборудования и протоколов маршрутизации.Выбор протоколов маршрутизации Рассматриваемые вопросы: - характерные особенности протоколов маршрутизации и возможности их применения на разных уровнях.
15	Проектирование защищенной сети с маршрутизацией по протоколу OSPF Рассматриваемые вопросы: - особенности проектирования сети с использованием протокола маршрутизации OSPF и его конфигурирование.
16	Проектирование защищенной сети с маршрутизацией по протоколу BGP Рассматриваемые вопросы: - особенности проектирования сети с использованием протокола маршрутизации BGP и его конфигурирование.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Информационные потоки предприятия В результате выполнения работы студент получит практические навыки по анализу информационной инфраструктуры предприятия для построения компьютерной сети.
2	Информационные потоки предприятия(продолжение) В результате выполнения работы студент получит практические навыки по расчету требуемой пропускной способности сети и расчету адресного плана предприятия.
3	Разработка структурированной кабельной системы В результате выполнения работы студент получит практические навыки по составлению проектной документации и управлению проектом на примере разработки структурированной кабельной системы.
4	Разработка структуры сети провайдера В результате выполнения работы студент получит практические навыки по проектированию

№ п/п	Наименование лабораторных работ / краткое содержание
	структуры сети провайдера.
5	Модель угроз безопасности информации в сети В результате выполнения работы студент получит практические навыки по оценке угроз безопасности и построению модели угроз сети.
6	Обеспечение отказоустойчивости при построении сети В результате выполнения работы студент получит практические навыки по обеспечению отказоустойчивости сети на уровне физических соединений и с помощью протоколов резервирования.
7	Разработка структуры сети с использованием протокола OSPF В результате выполнения работы студент получит практические навыки по разработке структуры защищенной сети с использованием протокола OSPF.
8	Разработка структуры сети с использованием протокола BGP В результате выполнения работы студент получит практические навыки по разработке структуры защищенной сети с использованием протокола BGP.

4.3. Самостоятельная работа обучающихся.

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

4.4. Примерный перечень тем курсовых проектов

1. Разработать защищенную корпоративную сеть передачи данных с использованием протоколов OSPF, HSRP.
2. Разработать защищенную корпоративную сеть передачи данных с использованием протоколов OSPF, VRRP.
3. Разработать защищенную корпоративную сеть передачи данных с использованием протоколов OSPF, GLBP.
4. Разработать защищенную корпоративную сеть передачи данных с использованием протоколов BGP в одной AS, VRRP.
5. Разработать защищенную корпоративную сеть передачи данных с использованием протоколов BGP в одной AS, VRRP.
6. Разработать защищенную корпоративную сеть передачи данных с использованием протоколов BGP в одной AS, GLBP.
7. Разработать защищенную корпоративную сеть передачи данных с использованием протоколов BGP в нескольких AS, VRRP.

8. Разработать защищенную корпоративную сеть передачи данных с использованием протоколов BGP в нескольких AS, VRRP.

9. Разработать защищенную корпоративную сеть передачи данных с использованием протоколов BGP в нескольких AS, GLBP.

10. Разработать защищенную корпоративную сеть передачи данных с использованием протоколов OSPF и BGP, HSRP.

11. Разработать защищенную корпоративную сеть передачи данных с использованием протоколов OSPF и BGP, VRRP.

12. Разработать защищенную корпоративную сеть передачи данных с использованием протоколов OSPF и BGP, GLBP.

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. - 100 экз. - (в пер.) : 111.13 р	URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/upos/10-1299.pdf. (дата обращения 04.10.2022)Текст : непосредственный 004 Ж51
2	Голдовский Я.М.Проектирование кампусных сетей : учеб. пособие по дисц. "Сети ЭВМ и телекоммуникации" для студ. спец.	Библиотека РУТ, http://library.miit.ru/URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/upos/10-1289.pdf. (дата обращения 04.10.2022)Текст : непосредственный. 004 Г60

	"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.	
3	В.П. Соловьев, А.Е. Шубарев, Н.Н. Пуцко.Безопасность коммуникационных сетей : учеб. пособие для студ., обуч. по магистерской программе "Безопасность и защита информации" напр. "Информатика и выч. Тех МИИТ. Центр компетентности "Защита и безопасность информации". - М. : МИИТ, 2007. - 86 с. : ил. - (Инновационная образовательная программа - МИИТ). - Библиогр.: с. 84 (4 назв.). - Б. ц. -	- URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/upos/04-35188.pdf.(дата обращения: 04.10.2022)Текст : непосредственный.
4	В.Г.Олифер, Н.А.Олифер. Компьютерные сети. Принципы, технологии, протоколы : учебное пособие для вузов. - 4-е изд. - СПб. : Питер, 2015. - 944 с. : ил. - ("Учебники для вузов"). - Библиогр.: с. 917. - ISBN 978-5-496-00004-8 (в пер.) : 470.00 р.	научно-техническая библиотека МИИТ(дата обращения 04.10.2022)полочный шифр 004 О-54.Текст : непосредственный.20 экз.
5	В.В. Яковлев, А.А. Корниенко. Информационная безопасность и защита	https://e.lanbook.com/book/59172. —(дата обращения: 04.10.2022). — Текст : электронный.

	информации в корпоративных сетях железнодорожного транспорта [Электронный ресурс] : учебное пособие. Москва : УМЦ ЖДТ, 2002. — 328 с	
6	Мэйволд Эрик. Безопасность сетей: курс лекций Москва :Интуит НОУ, 2016. — 572 с. — ISBN 978-5-9570-0046-9.	URL: https://book.ru/book/917577 (дата обращения: 04.10.2022). — Текст : электронный.

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 и лабораторных работ необходима специализированная лекционная аудитория с мультимедиа аппаратурой. Компьютеры должны быть обеспечены лицензионными программными продуктами:

Microsoft Windows

Microsoft Office

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 межсетевой экран, сетевое оборудование, рабочая станция преподавателя, проектор, экран.

9. Форма промежуточной аттестации:

Курсовой проект в 3 семестре.
Экзамен в 3 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