МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

Кафедра «Железнодорожная автоматика, телемеханика и связь»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Основы построения защищенных вычислительных сетей»

Направление подготовки:	09.04.03 – Прикладная информатика
Магистерская программа:	Прикладная информатика в обеспечении безопасности бизнеса
Квалификация выпускника:	Магистр
Форма обучения:	заочная
Год начала подготовки	2019

1. Цели освоения учебной дисциплины

Целью освоения учебной дисциплины «Основы построения защищенных вычислительных сетей» является формирование у обучающихся компетенцийв соответствии с требованиями самостоятельно утвержденного образовательного стандарта высшего образования (СУОС) по специальности «Прикладная информатика» и приобретение ими:
- знаний о принципах построения защищенных вычислительных сетей, технологиях построения защищенных сетей;
- умений пользоваться средствами настройки и конфигурации средств сетевой защиты (межсетевые экраны, средства VPN и др.), необходимыми для реализации систем защиты информации в сетях;
- навыков настройки и конфигурирования средств сетевой защиты.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Основы построения защищенных вычислительных сетей" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

3. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ПКС-51	Способен обеспечить кибербезопасность в бизнес-процессах при проектировании и эксплуатации информационных систем, управлении проектами в области информационных технологий

4. Общая трудоемкость дисциплины составляет

4 зачетные единицы (144 ак. ч.).

5. Образовательные технологии

Образовательные технологии, используемые для реализации компетентностного подхода и с целью формирования и развития профессиональных навыков студентов по усмотрению преподавателя в учебном процессе могут быть использованы в различных сочетаниях активные и интерактивные формы проведения занятий, включая: Лекционные занятия. Информатизация образования обеспечивается с помощью средств новых информационных технологий - ЭВМ с соответствующим периферийным оборудованием; средства и устройства манипулирования аудиовизуальной информацией; системы машинной графики, программные комплексы (операционные системы, пакеты прикладных программ).Лабораторные занятия. Информатизация образования обеспечивается с помощью средств новых информационных технологий - ЭВМ с соответствующим периферийным оборудованием; виртуальные лабораторные работы. Практические занятия. Информатизация образования обеспечивается с помощью средств новых информационных технологий - ЭВМ с соответствующим периферийным оборудованием; системы машинной графики, программные комплексы (операционные системы, пакеты прикладных программ).Самостоятельная работа. Дистанционное обучение - интернет-технология, которая обеспечивает студентов учебно-методическим материалом, размещенным на сайте академии, и предполагает интерактивное взаимодействие между преподавателем и студентами. Контроль самостоятельной работы. Использование тестовых заданий, что предполагает интерактивное взаимодействие между преподавателем и студентами. При изучении дисциплины используются технологии

электронного обучения(информационные, интернет ресурсы, вычислительная техника) и, при необходимости, дистанционные образовательные технологии, реализуемые в основном с применениеминформационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающегося и педагогических работников..

6. Содержание дисциплины (модуля), структурированное по темам (разделам)

РАЗДЕЛ 1
Раздел 1. Защита информации в локальных вычислительных сетях

Программно-аппаратные средства обеспечения информационной безопасности инфраструктуры сети. Защита административного интерфейса активного сетевого оборудования Cisco. Виртуальные локальные сети (VLAN) как средство защиты информации. Протокол магистральных каналов VLAN VTP (VLAN Trunk Protocol). Стандартные и расширенные списки доступа. Фильтрация трафика с помощью списков доступа

РАЗДЕЛ 2
Раздел 2. Защита периметра вычислительной сети

Классификация межсетевых экранов (МЭ). Программные и аппаратно-программные МЭ. Принципы построения и функционирования межсетевых экранов. Особенности межсетевого экранирования на различных уровнях модели OSI. Системы обнаружения и предотвращения компьютерных атак.
Обеспечение целостности информации. Политика AAA (Аутентификация, Авторизация и Аудит).

РАЗДЕЛ 3
Раздел 3. Защита удаленного доступа

Технологии виртуальных частных сетей (VPN). Протоколы VPN. Технологии IPsec. Туннельный и транспортный режимы IPSec. Ассоциация защиты IPSec. Протокол IKE. Согласование ключей по схеме Диффи-Хеллмана.

РАЗДЕЛ 4
Раздел 4. Конфигурирование серверов доступа Cisco ASA 5500

Режимы работы серверов доступа ASA5500. Настройка NAT и PAT. Конфигурирование доступа через ASA5500 с помощью списков доступа. Сервисные политики.

РАЗДЕЛ 5
допуск к зачету

РАЗДЕЛ 1
Зачет с оценкой

РАЗДЕЛ 5
допуск к зачету
тест КСР

РАЗДЕЛ 1
Зачет с оценкой