МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

Кафедра «Вычислительные системы, сети и информационная безопасность»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Защита информации в вычислительных сетях»

Направление подготовки:	09.03.01 – Информатика и вычислительная техника
Профиль:	Вычислительные машины, комплексы, системы и сети
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2019

1. Цели освоения учебной дисциплины

Целями освоения учебной дисциплины «Защита информации в вычислительных сетях» являются формирование компетенции по основным разделам теоретических и практических основ организации средств защиты информации, дать необходимые навыки по использованию средств защиты информации в компьютерных системах и овладению методами решения соответствующих.
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.

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

Организационно-управленческая
- разработка политики информационной безопасности
- разработка регламентов и аудит системы безопасности данных
-контроль использования сетевых устройств и программного обеспечения
- оценка производительности сетевых устройств и программного обеспечения
-администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)

Производственно-технологическая
- осуществляет разработку тестовых документов, включая план тестирования
- разработка автоматизированных процедур выявления попыток несанкционированного доступа к данным
- разработка архитектуры ИС
- коррекция производительности сетевой инфокоммуникационной системы
- установка специальных средств управления безопасностью администрируемой сети

Проектная
- планирование восстановления сетевой инфокоммуникационной системы
- планирование модернизации сетевых устройств
- разработка тестовых программ или генераторов тестовых программ для модели ИС на языках программирования целевой системы

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Защита информации в вычислительных сетях" относится к блоку 1 "Дисциплины (модули)" и входит в его вариативную часть.

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

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ПКР-3	Способность администрировать процесс управления безопасностью сетевых устройств, программного обеспечения, средств обеспечения безопасности удаленного доступа

4. Общая трудоемкость дисциплины составляет

4 зачетные единицы (144 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Защита информации в вычислительных сетях» осуществляется в форме лекций и лабораторных работ.Лекции проводятся в традиционной классно-урочной организационной форме в объеме 24 часов, по типу управления познавательной деятельностью и являются традиционными классически-лекционными (объяснительно-иллюстративными).Лабораторные работы организованы с использованием технологий развивающего обучения. Курс лабораторных работ (24 часов) проводится с использованием сетевого оборудования и на специальных программных симуляторах, разработанных на кафедре, основанных на интерактивных (диалоговых) технологиях, в том числе на сетевом оборудовании (решение проблемных поставленных задач с помощью современной вычислительной техники и исследование моделей); технологий, основанных на коллективных способах обучения, а также использованием компьютерной тестирующей системы. Самостоятельная работа студента организована с использованием традиционных видов работы. К традиционным видам работы (38 часов) относится отработка лекционного материала и отработка отдельных тем по учебным пособиям, подготовка к интерактивным практическим и лабораторным работам.Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 6 разделов, представляющих собой логически завершенный объем учебной информации. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания (решение конкретных задач, работа с данными) для оценки умений и навыков. Теоретические знания проверяются путем применения таких организационных форм, как индивидуальные и групповые опросы..

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

РАЗДЕЛ 1
Защита информации.

Тема: 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.

РАЗДЕЛ 2

Политика защиты

Тема: Сетевая безопасность
Рассматриваются вопросы безопасности сети предприятия, определяются направления действия политики защиты. Приводятся примерные варианты реализации политик защиты.

Тема: Анализ угроз безопасности.
Описываются типы угроз и общие рекомендации по борьбе с ними.

Тема: Вирусы.
Описываются типы вирусов, среда обитания, способы заражения, вредоносное воздействие

РАЗДЕЛ 3
Защита сети.

Тема: Защита административного доступа к сетевым устройствам.
Рассматриваются вопросы защиты доступа к административным интерфейсам. Описываются методы усиления парольной защиты и разделения уровней привилегий.

Тема: 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.

Тема: Технология защиты AAA.
Рассматриваются методы аутентификации и авторизации. Представлена технология защиты AAA, принципы ее работы и конфигурирования.

РАЗДЕЛ 4
Защита сетевых соединений

Тема: Модели обороны.
Рассматриваются существующие модели обороны, их преимущества и недостатки.

Тема: Модели обороны.
Вып. лаб. работ №1-3

Тема: Защита периметра сети.
Описывается зонная архитектура защиты сети и ее компоненты.

Тема: Контроль сервисов TCP/IP.
Рассматриваются средства контроля сервисов TCP/IP на уровне глобальной конфигурации и конфигурации интерфейсов.

Тема: 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.

РАЗДЕЛ 5
Шифрование.

Тема: Механизмы шифрования
Рассматриваются различные варианты построения систем шифрования и их свойства.

Тема: Блочное шифрование и цифровая подпись.
Вып. лаб. работ №4-5

Тема: Блочное шифрование и цифровая подпись.
Рассматривается алгоритм шифрования с использованием сетей Фейстеля, алгоритмы DES, 3DES. AES, ГОСТ 28147, RSA RC5. Рассматривается назначение и схемы построения цифровой подписи, алгоритм DSA.

Тема: Шифрование на сетевом уровне
Приводится обзор задач и средств шифрования на сетевом уровне.

РАЗДЕЛ 6
Построение виртуальных частных сетей с использованием IPSec.

Тема: Обзор технологии виртуальных частных сетей.
Приводится обзор технологии виртуальных частных сетей (VPN), их топологий и средств поддержки.

Тема: Механизмы IPSec.
Рассматриваются принципы работы и настройки механизмов IPSec с использованием IKE.

Тема: Настройка IPSec VPN.
Описывается настройка политики ISAKMP, определение наборов преобразований IPSec и настройка криптографических карт.

Экзамен