МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИУЦТ

С.П. Вакуленко

30 сентября 2019 г.

Кафедра «Вычислительные системы, сети и информационная безопасность»

Автор Желенков Борис Владимирович, к.т.н., доцент

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Защита информации в сетях»

Направление подготовки:	09.04.01 – Информатика и вычислительная техника
Магистерская программа:	Компьютерные сети и технологии
Квалификация выпускника:	Магистр
Форма обучения:	очная
Год начала подготовки	2019

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 2 30 сентября 2019 г. Председатель учебно-методической комиссии Н.А. Клычева	Протокол № 2 27 сентября 2019 г. Заведующий кафедрой Б.В. Желенков

Москва 2019 г.

1. Цели освоения учебной дисциплины

Целями освоения учебной дисциплины «Защита информации в сетях» являются формирование компетенции по основным разделам теоретических и практических основ организации средств защиты информации, дать необходимые навыки по практическому использованию средств защиты информации включая использование различных возможностей ограничения доступа к защищаемым ресурсам.

Основными задачами дисциплины являются:
• ознакомление с внутренней организацией и основными характеристиками различных систем защит информации и их компонентов;
• изучение принципов структурной и архитектурной организации современных средств защиты информации и их настройки;
• рассмотрение и анализ перспектив развития средств защиты информации.

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

Научно-исследовательская деятельность:
• сбор, обработка, анализ и систематизация научно-технической информации по теме исследования, выбор методик и средств решения задачи;
• организация проведения экспериментов и испытаний, анализ их результатов;
• подготовка научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований.

Проектная деятельность:
• подготовка заданий на разработку проектных решений;
• разработка и реализация проектов по интеграции информационных систем в соответствии с методиками и стандартами информационной поддержки изделий, включая методики и стандарты документооборота, интегрированной логистической поддержки, оценки качества программ и баз данных, электронного бизнеса;
• проведение технико-экономического и функционально-стоимостного анализа эффективности проектируемых систем;
• разработка методических и нормативных документов, технической документации, а также предложений и мероприятий по реализации разработанных проектов и программ.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Защита информации в сетях" 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:

ОПК-4	Способен применять на практике новые научные принципы и методы исследований
ПКО-1	Способность формировать технические задания и руководить разработками аппаратно-программных средств вычислительной техники информационные и автоматизированные системы

4. Общая трудоемкость дисциплины составляет

4 зачетных единиц (144 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Защита информации в сетях» осуществляется в форме лекций и лабораторных работ.Лекции проводятся в традиционной классно-урочной организационной форме в объеме 8 часов, по типу управления познавательной деятельностью и являются традиционными классически-лекционными (объяснительно-иллюстративными).Лабораторные работы организованы с использованием технологий развивающего обучения. Курс лабораторных работ (16 часов) проводится с использованием специализированных стендов и на специальных программных симуляторах, разработанных на кафедре, основанных на интерактивных (диалоговых) технологиях, 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 (66 часов) относится отработка лекционного материала и отработка отдельных тем по учебным пособиям, подготовка к интерактивным лабораторным работам.Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 3 раздела, 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. Проведении занятий по дисциплине (модулю) возможно с применением электронного обучения и дистанционных образовательных технологий, реализуемые с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.В процессе проведения занятий с применением электронного обучения и дистанционных образовательных технологий применяются современные образовательные технологии, такие как (при необходимости):- использование современных средств коммуникации;- электронная форма обмена материалами;- дистанционная форма групповых и индивидуальных консультаций;- использование компьютерных технологий и программных продуктов, необходимых для сбора и систематизации информации, проведения требуемых программой расчетов и т.д..

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

РАЗДЕЛ 1
Основы компьютерных сетей
Выполнение и защита лабораторной работы №1, 2

Тема: Компьютерная сеть. Классификация сетей.
Рассматриваются основные направления действия системы защиты информации в сети и принципы ее организации.

Тема: Коммутация каналов, сообщений, пакетов.
Рассматриваются вопросы безопасности сети предприятия, определяются направления действия политики защиты. Приводятся примерные варианты реализации политик защиты.

Тема: Атаки на коммуникационные протоколы.

Рассматриваются компоненты системы защиты информации и их совместное использование.

РАЗДЕЛ 2
Задачи информационной безопасности

Тема: Шифрование данных .Контроль целостности данных. Аутентификация. Протоколирование и аудит. Антивирусная защита.
Рассматриваются варианты внешних угроз беспроводным сетям.

Тема: Средства защиты информации в сетях. Межсетевой экран. Виртуальные частные сети. IPsec.Системы анализа защищенности.
Рассматриваются методы защиты беспроводных сетей и их уязвимости

РАЗДЕЛ 3
Стандарты защиты информации в сетях.
Выполнение и защита лабораторной работы №3, 4

Тема: Система обнаружения атак. Система управления средствами безопасности.
Приводится обзор технологии виртуальных частных сетей (VPN), их топологий и средств поддержки.

Тема: Средства антивирусной защиты. Руководящие документы Гостехкомиссии России.
Рассматриваются принципы работы и настройки механизмов IPSec с использованием IKE

РАЗДЕЛ 4
Итоговая аттестация