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

«Программно-аппаратные средства защиты информации»

Направление подготовки:	10.03.01 – Информационная безопасность
Профиль:	Безопасность компьютерных систем
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2018

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 «Программно-аппаратные средства защиты информации» 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 аппаратно-программные 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 аппаратно-программной защиты сетевых соединений.
• Изучение принципов построения виртуальных частных сетей.

Дисциплина формирует знания и умения для решения следующих профессиональных задач (в соответствии с видами профессиональной деятельности):

Эксплуатационная:
• установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;
• администрирование подсистем информационной безопасности объекта, участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;

Проектно-технологическая:
• сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
• проведение проектных расчетов элементов систем обеспечения информационной
• безопасности;
• участие в разработке технологической и эксплуатационной документации;
• проведение предварительного технико-экономического обоснования проектных расчетов;

Экспериментально-исследовательская деятельность:
• сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
• проведение экспериментов по заданной методике, обработка и анализ их результатов;
• проведение вычислительных экспериментов с использованием стандартных программных средств.

Организационно-управленческая деятельность:
- осуществление организационно-правового обеспечения информационной безопасности

объекта защиты;
- организация работы малых коллективов исполнителей;
- участие в совершенствовании системы управления информационной безопасностью;
- изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;
- контроль эффективности реализации политики информационной безопасности объекта защиты.?

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Программно-аппаратные средства защиты информации" 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:

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
ПК-9	способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности

4. Общая трудоемкость дисциплины составляет

5 зачетных единиц (180 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Программно-аппаратные средства защиты информации» осуществляется в форме лекций и лабораторных работ. Лекции проводятся в традиционной классно-урочной организационной форме в объеме 36 часов, по типу управления познавательной деятельностью и являются традиционными классически-лекционными (объяснительно-иллюстративными). Лабораторные работы организованы с использованием технологий развивающего обучения. Курс лабораторных работ (36 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 (49 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, ограничения объявлений маршрутной информации и фильтрации входящего сетевого трафика.

Тема: Технология защиты AAA.
Выполнение лаб.работ 20%

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: 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 по ACL.
Описываются средства контроля доступа с использованием рефлексивных, динамических и временных списков доступа.

Тема: Контроль доступа по CBAC
Описываются средства контроля доступа с 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.
Рассматривается алгоритм шифрования с использованием сетей Фейстеля, алгоритмы DES, 3DES.

Тема: Блочное шифрование.
Рассматривается алгоритм шифрования AES, ГОСТ 28147, RSA RC5.

Тема: Цифровая подпись.
Выполнение лаб.работ 80%

Тема: Цифровая подпись.
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.

РАЗДЕЛ 7
Итоговая аттестация