МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

УТВЕРЖДАЮ:

Директор ИТТСУ

П.Ф. Бестемьянов

26 мая 2020 г.

Кафедра «Управление и защита информации»

Автор Клепцов Михаил Яковлевич, д.т.н., профессор

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Проектирование и анализ систем обеспечения информационной безопасности объектов информатизации»

Специальность:	10.05.01 – Компьютерная безопасность
Специализация:	Информационная безопасность объектов информатизации на базе компьютерных систем
Квалификация выпускника:	Специалист по защите информации
Форма обучения:	очная
Год начала подготовки	2020

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 10 26 мая 2020 г. Председатель учебно-методической комиссии  С.В. Володин	Протокол № 16 21 мая 2020 г. Заведующий кафедрой  Л.А. Баранов

Москва 2020 г.

1. Цели освоения учебной дисциплины

Целями освоения учебной дисциплины «Проектирование и анализ систем обеспечения информационной безопасности объектов информатизации» 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):
научно-исследовательская;
контрольно-аналитическая;
специализация №8.
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, отечественного и зарубежного опыта по проблемам компьютерной безопасности;
изучение и обобщение опыта работы других учреждений, организаций и предприятий по способам использования методов и средств обеспечения информационной безопасности с целью повышения эффективности и совершенствования работ по защите информации на конкретном объекте;
подготовка научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований.
Контрольно-аналитическая деятельность:
предварительная оценка, выбор и разработка необходимых методик поиска уязвимостей;
применение методов и методик оценивания безопасности компьютерных систем при проведении контрольного анализа системы защиты;
подготовка аналитического отчета по результатам проведенного анализа и выработка предложений по устранению выявленных уязвимостей.
Специализация №8 "Информационная безопасность объектов информатизации на базе компьютерных систем":
разработка проектных решений и анализ систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования, создания и модернизации, в том числе разработка модели угроз и формирование требования к обеспечению информационной безопасности.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Проектирование и анализ систем обеспечения информационной безопасности объектов информатизации" 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	Способен принимать участие в разработке проектных решений по защите информации в автоматизированных системах
ПКР-5	Способен проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации
ПКР-6	Способен принимать участие в разработке архитектуры системы защиты информации автоматизированной системы
ПКР-10	Способен проводить тестирование систем защиты информации автоматизированных систем
ПКР-11	Способен участвовать в разработке эксплуатационной документации на системы защиты информации автоматизированных систем
ПКС-2	Способен разрабатывать план мероприятий по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации
ПКС-3	Способен проводить анализ эффективности систем защиты информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации
ПКС-4	Способен участвовать в создании системы защиты информации процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем
ПКС-5	Способен разрабатывать проекты нормативных правовых актов, руководящих и методических документов предприятия, учреждения, организации, регламентирующих деятельность по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации

4. Общая трудоемкость дисциплины составляет

4 зачетные единицы (144 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Проектирование и анализ систем обеспечения информационной безопасности объектов информатизации» осуществляется в форме лекций и практических занятий.Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью и являются традиционными классически-лекционными (объяснительно-иллюстративными).Курс практических занятий 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 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
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
Сетевая безопасность.
Рассматриваются вопросы безопасности сети предприятия, определяются направления действия политики защиты. Приводятся примерные варианты реализации политик защиты.
Анализ угроз безопасности.
Описываются типы угроз и общие рекомендации по борьбе с ними.
Вирусы.
Описываются типы вирусов, среда обитания, способы заражения, вредоносное воздействие.

РАЗДЕЛ 3
Защита сети
Защита административного доступа к сетевым устройствам.
Рассматриваются вопросы защиты доступа к административным интерфейсам.
Описываются методы усиления парольной защиты и разделения уровней привилегий.
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.
Технология защиты AAA.
Рассматриваются методы аутентификации и авторизации. Представлена технология защиты AAA, принципы ее работы и конфигурирования.

РАЗДЕЛ 4
Защита сетевых соединений
Модели обороны.
Рассматриваются существующие модели обороны, их преимущества и недостатки.
Защита периметра сети.
Описывается зонная архитектура защиты сети и ее компоненты.
Контроль сервисов TCP/IP.
Рассматриваются средства контроля сервисов TCP/IP на уровне глобальной конфигурации и конфигурации интерфейсов.
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
Механизмы шифрования.
Рассматриваются различные варианты построения систем шифрования и их свойства.
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.
Шифрование на сетевом уровне.
Приводится обзор задач и средств шифрования на сетевом уровне.

РАЗДЕЛ 6
Построение виртуальных частных сетей с использованием IPSec
Обзор технологии виртуальных частных сетей.
Приводится обзор технологии виртуальных частных сетей (VPN), их топологий и средств поддержки.
Механизмы IPSec.
Рассматриваются принципы работы и настройки механизмов IPSec с использованием IKE.
Настройка IPSec VPN.
Описывается настройка политики ISAKMP, определение наборов преобразований IPSec и настройка криптографических карт.

Экзамен