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

«Основы построения защищенных компьютерных сетей»

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

Целью изучения дисциплины «Основы построение защищенных компьютерных сетей» является теоретическая и практическая подготовка обучающихся к деятельности, связанной с построением защищенных сетевых автоматизированных систем, а также обучение принципам и методам защиты информации в компьютерных сетях.
Задачи дисциплины:
- изучение типовых угроз безопасности в компьютерных сетях;
- изучение криптографических и программно-аппаратных методов обеспечения информационной безопасности в компьютерных сетях;
- приобретение навыков настройки и эксплуатации средств обеспечения безопасности в компьютерных сетях;
- овладение средствами и методами проектирования и построения защищенных сетевых автоматизированных систем;
- овладение средствами и методами выявления и нейтрализации попыток нарушения безопасности в компьютерных сетях.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Основы построения защищенных компьютерных 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:

ОПК-10	Способен администрировать подсистемы и средства защиты информации в компьютерных системах и сетях
ОПК-16	Способен оценивать эффективность реализации действующих политик безопасности операционных систем и систем управления базами данных
ОПК-17	Способен контролировать корректность функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях
ПКО-7	Способен проводить анализ информационной безопасности объектов и систем, принимать участие в организации и сопровождении аттестации объекта информатизации на предмет соответствия требованиям защиты информации
ПКО-9	Способен участвовать в управлении информационной безопасностью компьютерной системы, разрабатывать предложения по ее совершенствованию
ПКО-11	Способен проводить проверки эффективности и выполнять работы по восстановлению работоспособности программных, программно-аппаратных и технических средств, подсистем защиты информации
ПКО-12	Способен выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности, проводить мониторинг и анализ эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах

4. Общая трудоемкость дисциплины составляет

4 зачетные единицы (144 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Основы построения защищенных компьютерных систем» осуществляется в форме лекций, лабораторных работ и практических занятий.В соответствии с требованиями ФГОС ВПО по направлению 10.05.01 «Компьютерная безопасность» с целью формирования и развития профессиональных навыков студентов предусмотрено использовать и проводить разбор презентаций лучших дипломных проектов по данной специализации. Кроме того, предусмотрены мастер-классы специалистов из:- академии ФСБ- компании «Информзащита»- лаборатории Касперского-РОСАТОМА.

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

РАЗДЕЛ 1
КС и их организация / Сетевые атаки.

Тема: Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI

РАЗДЕЛ 2
Механизмы реализации атак в сетях TCP/IP./

Тема: Методы сканирования портов. Методы обнаружения пакетных снифферов. Методы обхода МЭ.

РАЗДЕЛ 3
Методы перехвата сетевых соединений в сетях TCP/IP./

Тема: Технические меры защиты от сетевых атак. Атаки направленные на сетевую инфраструктуру

РАЗДЕЛ 4
Примеры сетевых атак в сетях TCP/IP.
Устные опросы, выполнение практических заданий

Тема: Технические меры защиты от сетевых атак

Тема: Принуждение к ускоренной передаче..

Тема: Атаки, направленные на отказ в обслуживании.

Тема: Изменение конфигурации и состояния хостов. Программно-технические меры защиты от сетевых атак

РАЗДЕЛ 5
Криптографические методы защиты информации в компьютерных сетях.

Тема: Криптографические протоколы обеспечения безопасности.

Тема: Протоколы аутентификации на прикладном уровне. Протокол Kepberos.

Тема: Протоколы аутентификации на транспортном уровне: протокол SSI/TLS/

РАЗДЕЛ 6
Защита виртуальных частных сетей (VPN).

Тема: Назначение, основные возможности и варианты реализации VPN.

Тема: Достоинства и недостатки применения VPN

Тема: Протокол IPSEC/ Протоколы AH и ESP.

Тема: Использование протокола L2TP для организации виртуальных частных сетей.

РАЗДЕЛ 7
Разработка защищенных сетевых приложений.

Тема: Аутентификация, шифрование, обеспечение целостности с использованием программного интерфейса SSPI.

Тема: Программный интерфейс Open SSI.

РАЗДЕЛ 8
Программно-аппаратные средства обеспечения безопасности в компьютерных сетях.

Тема: Средства защиты локальных сетей при подключении к Интернет.

Тема: Место и роль МЭ в обеспечении сетевой безопасности. Основные возможности и схемы развертывания МЭ

РАЗДЕЛ 9
Методы сетевой трансляции адресов (NAT).
Устный опрос, выполнение практических заданий

Тема: Построение правил фильтрации. Реализация сетевой политики безопасности с использованием МЭ.

Тема: Методы обхода межсетевых экранов

РАЗДЕЛ 10
Защита серверов и рабочих станций.

Тема: Системы обнаружения вторжений (СОВ). Место и роль СОВ в общей системе обеспечения сетевой безопасности. Классификация СОВ.

РАЗДЕЛ 11
Средства и методы предотвращения в обнаружении вторжений.

Тема: Выявление атак на основе сигнатур атак и выявление аномалий. Аудит прикладных служб. Средства обнаружения уязвимостей сетевых служб. Системы виртуальных ловушек (Honey Pot и Paded Geet).

РАЗДЕЛ 12
Курсовая работа

Экзамен