

**МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ**  
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ**  
**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**  
**«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (МИИТ)»**

УТВЕРЖДАЮ:

Директор ИТТСУ



П.Ф. Бестемьянов

25 мая 2018 г.


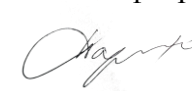
Кафедра «Управление и защита информации»

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

**АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ**

**«Основы построения защищенных компьютерных сетей»**

Специальность:	<u>10.05.01 – Компьютерная безопасность</u>
Специализация:	<u>Информационная безопасность объектов информатизации на базе компьютерных систем</u>
Квалификация выпускника:	<u>Специалист по защите информации</u>
Форма обучения:	<u>очная</u>
Год начала подготовки	<u>2018</u>

<p style="text-align: center;">Одобрено на заседании Учебно-методической комиссии института Протокол № 10 21 мая 2018 г. Председатель учебно-методической комиссии</p>  <p style="text-align: right;">С.В. Володин</p>	<p style="text-align: center;">Одобрено на заседании кафедры</p> <p style="text-align: center;">Протокол № 16 15 мая 2018 г. Заведующий кафедрой</p>  <p style="text-align: right;">Л.А. Баранов</p>
---	--

## 1. Цели освоения учебной дисциплины

Целью изучения дисциплины «Основы построения 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:

ПК-11	способностью участвовать в проведении экспериментально-исследовательских работ при проведении сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации
ПК-15	способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы
ПК-18	способностью производить установку, наладку, тестирование и обслуживание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
ПСК-8.1	способностью разрабатывать модели угроз, формировать требования к обеспечению информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования, создания и модернизации

## 4. Общая трудоемкость дисциплины составляет

5 зачетных единиц (180 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

Тема: 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..

Тема: Протокол Kerberos

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