МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (МИИТ)»

Кафедра «Управление и защита информации»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Техническая защита информации»

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	2018

1. Цели освоения учебной дисциплины

Целью дисциплины «Техническая защита информации» является формирование у студентов знаний по основам инженерно-технической защиты информации, а также навыков и умения в применении знаний для конкретных условий. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач инженерно-технической защиты информации с учетом требований системного подхода.
Задачи дисциплины – дать знания:
-по концепции инженерно-технической защиты информации;
-по теоретическим основам инженерно-технической защиты информации;
-по физическим основам инженерно-технической защиты информации;
-по техническим средствам добывания и защиты информации;
-по организационным основам инженерно-технической защиты информации;
-по методическому обеспечению инженерно-технической защиты информации.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Техническая защита 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-7	способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем
ПК-19	способностью производить проверки технического состояния и профилактические осмотры технических средств защиты информации
ПСК-8.3	способностью проводить анализ систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и систем обеспечения информационной безопасности процессов их проектирования, создания и модернизации

4. Общая трудоемкость дисциплины составляет

5 зачетных единиц (180 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Техническая защита информации» осуществляется в форме лекций и практических занятий. Лекции в объеме 28 часов проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью и на 100 % являются традиционными классически-лекционными (объяснительно-иллюстративные.Практические занятия в объеме 28 часов организованы с использованием технологий развивающего обучения. Часть практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач) в объёме 8 часов. Остальная часть практического курса (20 часов) проводиться с использованием интерактивных (диалоговые) технологий, в том числе разбор и анализ конкретных ситуаций, электронный практикум (решение проблемных поставленных задач с помощью современной вычислительной техники и исследование моделей); технологий, основанных на коллективных способах обучения, а так же использованием компьютерной тестирующей

системы. Самостоятельная работа студента организованна с использованием традиционных видов работы и интерактивных технологий. К традиционным видам работы (19 часа) относятся отработка лекционного материала и отработка отдельных тем по учебным пособиям. К интерактивным (диалоговым) технологиям (20 часов) относиться отработка отдельных тем по электронным пособиям, подготовка к промежуточным контролям в интерактивном режиме, интерактивные консультации в режиме реального времени по специальным разделам и технологиям, основанным на коллективных способах самостоятельной работы студентов.Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 8 разделов, представляющих собой логически завершенный объём учебной информации. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания (решение ситуационных задач, анализ конкретных ситуаций, работа с данными) для оценки умений и навыков. Теоретические знания проверяются путём применения таких организационных форм, как индивидуальные и групповые опросы, решение тестов с использованием компьютеров или на бумажных носителях.Internet, сайты и порталы государственных структур и компаний, связанных с информационной безопасностью. Компьютерные презентации лучших дипломных проектов выпускников кафедры по компьютерной безопасности..

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

РАЗДЕЛ 1
Вводная лекция

Тема: Цели и задачи дисциплины. Общие принципы построения защищенной корпоративной сети

РАЗДЕЛ 2
Концепция инженерно-технической защиты информации

Тема: Характеристика инженерно-технической защиты информации как области информационной безопасности. Представление сил и средств защиты информации в виде системы.

РАЗДЕЛ 3
Теоретические основы инженерно-технической защиты информации

Тема: Особенности информации как предмета защиты. Виды, источники и носители защищаемой информации.

Тема: Демаскирующие признаки объектов наблюдения, сигналов и веществ. Основные и вспомогательные технические средства, и системы как источники опасных сигналов.

РАЗДЕЛ 4
Физические основы инженерно-технической защиты информации

Тема: Акустоэлектрические преобразователи. Источники побочных излучений. Характер электромагнитных излучений в ближней и дальней зонах.

Тема: Виды паразитных связей и наводок. Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи.

РАЗДЕЛ 5

Технические средства добывания и инженерно-технической защиты информации

Тема: Визуально-оптические приборы. Фотоаппараты. Оптоэлектрические приборы наблюдения в видимом и инфракрасном диапазонах. Средства управления доступом. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей. Средства видеоконтроля и видеоохраны. Средства маскировки и дезинформирования в оптическом и радиодиапазонах.

Тема: Средства звукоизоляции и звукопоглащения. Средства обнаружения, локализации и подавления сигналов закладных устройств. Средства подавления сигналов акустоэлектрических преобразователей, фильтрации и заземления. Генераторы линейного и пространственного зашумления

РАЗДЕЛ 6
Организационные основы инженерно-технической защиты информации

Тема: Основные задачи, структура и характеристика государственной системы противодействия технической разведке. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке. Основные организационные и технические меры по защите информации.

Тема: Аттестация объектов, лицензирование деятельности по защите информации и сертифицированные ее средства. Виды контроля эффективности инженерно-технической защиты информации. Виды зон безопасности. Методы технического контроля. Особенности инструментального контроля эффективности инженерно-технической защиты.

РАЗДЕЛ 7
Методическое обеспечение инженерно-технической защиты информации

Тема: Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирование объектов защиты. Моделирование угроз безопасности информации.

Тема: Методические рекомендации по выбору рациональных вариантов защиты. Пути оптимизации мер инженерно-технической защиты информации.

РАЗДЕЛ 8
Программные средства защиты информации

Тема: Виртуальные локальные сети VLAN. Протоколы магистральных каналов. Коммутационные массивы. Теггированный трафик на интерфейсах сетевых устройств. Маршрутизация в подсетях. Принципы коммутации подсетей. Определение трансляции сетевых адресов. Списки доступа. Настройка доступа. DMZ Модель прохождения трафика через сетевые интерфейсы. Реализация стека протокола IP. Прохождение пакета через фильтры фаервола.

РАЗДЕЛ 9
Курсовой проект

Экзамен