

**МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»**

Кафедра «Железнодорожная автоматика, телемеханика и связь»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Технические средства и методы защиты информации»

Направление подготовки:	<u>09.04.03 – Прикладная информатика</u>
Магистерская программа:	<u>Прикладная информатика в обеспечении безопасности бизнеса</u>
Квалификация выпускника:	<u>Магистр</u>
Форма обучения:	<u>заочная</u>
Год начала подготовки	<u>2019</u>

1. Цели освоения учебной дисциплины

Целью освоения учебной дисциплины «Технические средства и методы защиты информации» является формирование у обучающихся компетенций в соответствии с требованиями самостоятельно утвержденного образовательного стандарта высшего образования (СУОС) по специальности «Прикладная информатика» и приобретение ими:

- знаний о видах, источниках и носителях защищаемой информации, концепции инженерно-технической защиты информации, порядке организации инженерно-технической защиты информации;
- умений выявлять угрозы и технические каналы утечки информации; описывать (моделировать) объекты защиты и угрозы безопасности информации; применять наиболее эффективные методы и средства инженерно-технической защиты информации;
- навыков инженерного расчета размеров контролируемой зоны.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Технические средства и методы 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:

ПКС-51	Способен обеспечить кибербезопасность в бизнес-процессах при проектировании и эксплуатации информационных систем, управлении проектами в области информационных технологий
--------	--

4. Общая трудоемкость дисциплины составляет

6 зачетных единиц (216 ак. ч.).

5. Образовательные технологии

Образовательные технологии, используемые для реализации компетентного подхода и с целью формирования и развития профессиональных навыков студентов по усмотрению преподавателя в учебном процессе могут быть использованы в различных сочетаниях активные и интерактивные формы проведения занятий, включая: Лекционные занятия. Информатизация образования обеспечивается с помощью средств новых информационных технологий - ЭВМ с соответствующим периферийным оборудованием; средства и устройства манипулирования аудиовизуальной информацией; системы машинной графики, программные комплексы (операционные системы, пакеты прикладных программ). Лабораторные занятия. Информатизация образования обеспечивается с помощью средств новых информационных технологий - ЭВМ с соответствующим периферийным оборудованием; виртуальные лабораторные работы. Практические занятия. Информатизация образования обеспечивается с помощью средств новых информационных технологий - ЭВМ с соответствующим периферийным оборудованием; системы машинной графики, программные комплексы (операционные системы, пакеты прикладных программ). Самостоятельная работа. Дистанционное обучение - интернет-технология, которая обеспечивает студентов учебно-методическим материалом, размещенным на сайте академии, и предполагает интерактивное взаимодействие между преподавателем и студентами. Контроль самостоятельной работы. Использование тестовых заданий, что предполагает интерактивное взаимодействие между

преподавателем и студентами. При изучении дисциплины используются технологии электронного обучения(информационные, интернет ресурсы, вычислительная техника) и, при необходимости, дистанционные образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающегося и педагогических работников..

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

РАЗДЕЛ 1

Раздел 1. Концепция инженерно-технической защиты информации

Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической защиты информации. Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации. Показатели эффективности инженерно-технической защиты информации.

РАЗДЕЛ 2

Раздел 2. Теоретические основы инженерно-технической защиты информации

Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процессы добывания информации технической разведкой. Классификация технической разведки. Структура, классификация и основные характеристики технических каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика и возможности.

РАЗДЕЛ 3

Раздел 3. Физические основы защиты информации

Акустоэлектрические преобразования. Источники побочных излучений. Характер электромагнитных излучений в ближней и дальней зонах. Виды паразитных связей и наводок. Утечка опасных сигналов по цепям электропитания и заземления. Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях. Распространение оптических сигналов в атмосфере и в световодах. Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи. Подавление опасных сигналов акустоэлектрических преобразователей. Экранирование и компенсация полей. Подавление опасных сигналов в цепях электропитания и заземления. Зашумление опасных сигналов помехами.

РАЗДЕЛ 4

Раздел 4. Технические средства добывания и инженерно-технической защиты информации

Визуально-оптические приборы. Фотоаппараты. Оптикоэлектрические приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Направленные микрофоны. Структура комплексов перехвата. Особенности сканирующих радиоприемников. Закладные устройства. Средства ВЧ-навязывания и лазерного подслушивания. Автономные средства разведки. Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. Средства управления доступом.

Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей. Средства видеоконтроля и видеоохраны. Средства маскировки и дезинформирования в оптическом и радиодиапазонах. Средства звукоизоляции и звукопоглощения. Средства обнаружения, локализации и подавления сигналов закладных устройств. Средства подавления сигналов акустоэлектрических преобразователей, фильтрации и заземления. Генераторы линейного и пространственного зашумления.

Экзамен