МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧЕРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ

«УТВЕРЖДАЮ»
Проректор по УМР и К
_____В.В. Криницин
«___»_____2008 г.

РАБОЧАЯ УЧЕБНАЯ ПРОГРАММА ПО ДИСЦИПЛИНЕ

«ТЕХНИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ». ОПД.Ф.05

Специальность (специализация)	090106 Информационная безопасность телекоммуникационных систем
Факультет	Авиационных систем и комплексов
Кафедра	Основ радиотехники и защиты информации
Курс	5
Форма обучения	дневная
Общий объем учебных часов	100 час.
Лекции	22 час.
Практические занятия	8 час.
Лабораторные занятия	20 час.
Самостоятельная работа	50 час.
Зачёт	5 курс, 9 семестр
Экзамен	5 курс, 9 семестр

Москва 2008

Рабочая программа составлена на основании примерной учебной программы дисциплины и в соответствии с государственными требованиями к минимуму содержания и уровню подготовки выпускника по специальности 090106 - Информационная безопасность телекоммуникационных систем.

Рабочую программу составил:
Илюхин А.А., доцент, к.т.н. _____

Рабочая программа утверждена на заседании кафедры ОРТЗИ, протокол № 1от 9.09. 2008 г.

Заведующий кафедрой Емельянов В.Е., доцент, д.т.н. _____

Рабочая программа одобрена методическим советом по специальности 090106, протокол № от 2008 г.

Председатель методического совета по специальности 090106
Емельянов В.Е. _____

Рабочая программа согласована с Учебно-методическим управлением(УМУ).

Начальник УМУ - Логачёв В.П., к.т.н. _____

1. Цель и задачи дисциплины.

1.1. Цель преподавания дисциплины.

Цель преподавания дисциплины «Технические средства и методы защиты информации»- формирование у студентов знаний по основам инженерно-технической защиты информации, а также навыков и умения в применении знаний для конкретных условий.

1.2. Задачи изучения дисциплины (необходимый комплекс знаний и умений):

1.2.1. Иметь представление:

- о задачах, структуре и возможностях технической разведки, основных этапах и процессах добывания информации;
- о физических процессах в технических средствах и системах, способствующих утечке защищаемой информации;
- о характеристиках используемых и перспективных технических средств добывания и защиты информации;
- о государственной системе защиты информации и ее основных документах.

1.2.2. Знать:

- виды, источники и носители защищаемой информации;
- основные угрозы безопасности информации;
- концепцию инженерно-технической защиты информации;
- основные принципы и методы защиты информации;
- основные руководящие и нормативные документы по инженерно-технической защите информации;
- порядок организации инженерно-технической защиты информации.

1.2.3. Уметь:

- 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;
- контролировать эффективность мер защиты.

1.2.4. Иметь навыки:

- инженерного расчета размеров контролируемой зоны.

2. Содержание дисциплины.

2.1. Наименование разделов, подразделов и тем, объемы в часах.

Содержание лекций, ссылки на литературу.

Раздел 1. Концепция инженерно-технической защиты информации (2 час.).

Лекция 1.1. Системный подход к защите информации. Основные концептуальные положения инженерно-технической защиты информации.

Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической защиты информации. Представление сил и средств защиты информации в виде системы. Основные параметры системы защиты информации.

Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации. Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации. Показатели эффективности инженерно-технической защиты информации.

Литература по разделу: 3.1.1.

Раздел 2. Теоретические основы инженерно-технической защиты информации (8 час.).

Лекция 2.1. Информация как предмет защиты. Источники опасных сигналов.

Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие о текущей и эталонной признаковой структуре.

Понятие об опасном сигнале. Основные и вспомогательные технические средства и системы как источники опасных сигналов. Состав и краткая характеристика основных и вспомогательных технических средств и систем.

Образование опасных сигналов в результате побочных электромагнитных излучений и наводок.

Лекция 2.2. Технические каналы утечки информации.

Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика и возможности.

Лекция 2.3. Методы добывания информации. Методы инженерной защиты и технической охраны объектов.

Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процессы добывания информации технической разведкой. Классификация технической разведки. Возможности видов технической разведки. Основные направления развития технической разведки.

Классификация способов инженерной защиты и технической охраны объектов. Инженерные конструкции. Автономные и централизованные системы охраны. Модели злоумышленника. Подсистемы обнаружения злоумышленника и пожара, видеоконтроля, нейтрализации угроз и управления охраной. Способы повышения помехоустойчивости средств обнаружения злоумышленников и пожара. Автоматизация процессов охраны.

Лекция 2.4. Методы скрытия информации и ее носителей.

Пространственное скрытие объектов наблюдения и сигналов. Структурное и энергетическое скрытие объектов наблюдения. Методы технического закрытия речевых сигналов. Звукоизоляция и звукопоглощение. Энергетическое скрытие радио- и электрических сигналов. Виды и условия зашумления.

Литература по разделу: 3.1.1, 3.1.2, 3.2.1, 3.2.2.

Раздел 3. Технические средства добывания и инженерно-технической защиты информации (8 час.).

Лекция 3.1. Средства технической разведки.

Визуально-оптические приборы. Фотоаппараты. Оптоэлектрические 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.

Лекция 3.2. Средства инженерной защиты и технической охраны.

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 нейтрализации угроз. Средства управления и передачи извещений. Автоматизированные интегральные системы охраны.

Лекции 3.3, 3.4. Средства предотвращения утечки информации по техническим каналам.

Средства маскировки и дезинформации в оптическом и радиодиапазонах. Средства обнаружения, локализации и подавления сигналов закладных устройств. Средства подавления сигналов акустоэлектрических преобразователей, фильтрации и заземления. Генераторы линейного и пространственного зашумления.

Литература по разделу: 3.1.1, 3.1.2, 3.2.1, 3.2.2.

Раздел 4. Организационные основы инженерно-технической защиты информации (2 час.).

Лекция 4.1. Государственная система защиты информации. Контроль эффективности инженерно-технической защиты информации.

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. Аттестация объектов, лицензирование деятельности по защите информации и сертифицирование ее средств.

Виды контроля эффективности инженерно-технической защиты информации. Виды зон безопасности. Методы технического контроля. Особенности инструментального контроля эффективности инженерно-технической защиты информации.

Литература по разделу: 3.1.1.

Раздел 5. Методическое обеспечение инженерно-технической защиты информации (2час.).

Лекция 5.1. Моделирование и принципы оценки эффективности инженерно-технической защиты информации.

Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты. Пути оптимизации мер инженерно-технической защиты информации.

Принципы оценки эффективности охраны объектов защиты. Возможности оценки видовых признаков объектов наблюдения. Подходы к определению безопасности речевой информации в помещении. Принципы оценки размеров зон I и II. Оценка дальности перехвата сигналов.

Литература по разделу: 3.1.1.

2.2. Перечень тем практических занятий и их объём в часах:

П 3-1. Определение разрешения объектов защиты от возможного наблюдения с использованием современных визуально-оптических и оптико-электронных приборов (2час.).

П 3-2. Расчёт уровней речевых сигналов в местах возможного нахождения злоумышленника или его подслушивающих технических средств (2 час.).

П 3-3. Оценка утечки информации по радиоканалу при использовании специальных технических средств (закладных устройств) и за счёт побочных электромагнитных излучений (2 час.).

П 3-4. Расчёт зон 1 и 2 для основных технических средств и систем, размещённых в помещении (2 час.).

2.3. Перечень лабораторных работ и их объём в часах:

ЛР-1. Технические средства защиты речевой информации в телефонных линиях (6 час.).

ЛР-2. Технические средства обнаружения, локализации и нейтрализации специальных технических средств негласного получения информации, излучающих в радио- и инфракрасном диапазонах (4 час.).

ЛР-3. Технические средства обнаружения , локализации и нейтрализации специальных технических средств негласного получения информации, использующих силовые линии сети переменного тока и линии систем пожарной и охранной сигнализаций (2 час.).

ЛР-4. Контроль эффективности защиты речевой информации с помощью программно-аппаратного комплекса «СПРУТ-МИНИ-А» (4 час.).

ЛР-5. Поиск и измерение побочных электромагнитных излучений и наводок с помощью программно-аппаратного комплекса «НАВИГАТОР-ПЗГ» (4 час.).

3. Рекомендуемая литература.

3.1. Основная литература.

3.1.1. Торокин А.А. Инженерно-техническая защита информации. М.: Гелиос АРВ, 2005.

3.1.2. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам. М.: Горячая линия – ТЕЛЕКОМ, 2005.

3.2. Дополнительная литература.

3.2.1. Соболев А.Н., Кириллов В.М. Физические основы технических средств обеспечения информационной безопасности. М.: Гелиос АРВ, 2004.

3.2.2. Кулаков В.Г., Гаранин М.В., Заряев А.В., Новоквашанов О.Н. Информационная безопасность телекоммуникационных систем (технические аспекты). М.: Радио и связь, 2004.

4. Рекомендуемые электронные учебные материалы по дисциплине.

4.1. Электронная версия учебного пособия «Инженерно-техническая защита информации», автор – Торокин А.А., 2005 г.

4.2. Электронные версии технических описаний средств защиты информации, имеющихся на кафедре.