МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ
УТВЕРЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ

УТВЕРЖДАЮ
Проректор МГТУ ГА по УР
_____Криницин В.В.
_____ 2007 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

ОПД Ф.02.

Специальность 090106 – Информационная безопасность телекоммуникационных систем

Факультет - АСК
Кафедра - общей радиотехники и защиты информации
Курс - IV, форма обучения дневная, семестр VII
Общий объем учебных часов на дисциплину — 80 час.
Лекции - 20 (час)
Практические занятия - 18 (час)
Лабораторные работы - 12 (час)
Самостоятельная работа - 30 (час)
Экзамен - VII семестр

Москва — 2007 г.

Рабочая программа составлена на основании примерной учебной программы дисциплины и в соответствии с Государственным образовательным стандартом высшего профессионального образования (1 Гос. Регистрации 285 инф./сп.), определяющим требования к минимуму и уровню подготовки выпускника по специальности 090106 — информационная безопасность телекоммуникационных систем.

Рабочую программу составил

Кузяков Б.А., к.ф. – м.н. _____

Рабочая программа рассмотрена и утверждена на заседании кафедры ОРТ ЗИ.

Протокол № от «___» _____2007 г.

Зав. кафедрой Емельянов В.Е., д.т.н., профессор _____

Председатель методического совета по спец. 090106

Емельянов В.Е., д.т.н., профессор _____

Протокол № от «____» _____ 2007 г.

Рабочая программа согласована с учебно-методическим управлением (УМУ)

Нач. УМУ, доц., к.т.н. Логачев В.П _____ 2007 г.

1. Цель и задачи дисциплины

1.1. Цель преподавания дисциплины

Дисциплина «Основы информационной безопасности» имеет целью подготовку студентов по специальности “Информационная безопасность телекоммуникационных систем в области основ построения аппаратуры, используемой в системах телекоммуникации и обработки информации. При этом предусматривается обучение студентов методам сбора, обработки, рассылки, хранения, сопровождения и отображения информации.

Дисциплина помогает заложить теоретические основы технологии, методам и алгоритмам решения основных функциональных задач обеспечения информационной безопасности.

Дисциплина является базовой для изучения дисциплин по системам передачи информации, по техническим средствам и методам защиты информации по аппаратным средствам обеспечения информационной безопасности. Знания и практические навыки, полученные при изучении курса «Основы информационной безопасности»

используются обучаемыми при изучении дисциплин специализации и при разработке отдельных вопросов курсовых работ, дипломных и курсовых проектов.

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

1.1.1. **Иметь представление:**

• об основах государственной политики Российской Федерации в области информационной безопасности;

• об информационной безопасности в системе национальной безопасности Российской Федерации;

• о видах угроз информационной безопасности Российской Федерации. Угрозы конституционным правам и Свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

• об основных направлениях обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.

1.1.2. Знать:

- основные понятия и общеметодологические принципы теории информационной безопасности;

- роль информационной безопасности в обеспечении национальной безопасности государства;

- основные методы нарушения конфиденциальности, целостности и доступности информации.

- основные причины, виды, каналы утечки и искажения информации;

- основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.

1.2.3. Уметь:

- подбирать и использовать соответствующие правовые, организационно-технические и экономические методы обеспечения информационной безопасности выбранных объектов;

1.1.3. Иметь навыки

- анализа информационной инфраструктуры государства;
- формальной постановки и решения задачи обеспечения информационной безопасности
выбранного объекта телекоммуникационной системы.

Содержание дисциплины.

2.1. Наименование тем, их содержание, объем в часах лекционных занятий.

Тема 1. Введение — 2 часа

Лекция 1.1. Введение. Основные термины и определения. Информационная безопасность в системе национальной безопасности Российской Федерации.

Тема 2. Основы государственной политики Российской Федерации в области информационной безопасности (4 часа). Интересы общества в информационной Сфере. Интересы государства в информационной сфере. Основные составляющие национальных интересов Российской Федерации в информационной сфере.

Лекция 2.2. Источники угроз информационной безопасности Российской Федерации.
Внешние источники угроз. Внутренние источники угроз. Виды безопасности и сферы жизнедеятельности личности, общества и государства. Безопасность экономическая внутриполитическая, социальная, международная информационная, военная, пограничная, экологическая и другие.

Лекция 2.3. Организационно- правовые, технические и криптографические методы обеспечения информационной безопасности. Основная законодательная база обеспечения информационной безопасности.

Тема 3. Используемые методы нарушения конфиденциальности, целостности и доступности информации. (4 часа)

Лекция 3.4. Перечень главных причин перехвата информации. Виды, каналы утечки и искажения информации. Особенности технических каналов утечки информации.

Лекция 3.5. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в

условиях информационной войны. Учёт внешних и внутренних потенциальных угроз безопасности объектов.

Тема 4. Основы комплексного обеспечения информационной безопасности (4 часа).
Критерии выбора политики информационной безопасности предприятия.

Лекция 4.6. Проблемы региональной информационной безопасности. Модели, стратегии и системы обеспечения информационной безопасности.

Лекция 4.7. Методы и средства обеспечения информационной безопасности компьютерных систем. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Анализ моделей действия «нарушителя».

Тема 5. Методы противодействия утечки информации по техническим каналам (4 часа).

Лекция 5.8. Методы противодействия утечки информации по оптическому каналу. Основные параметры технических систем, используемых в оптических каналах нарушения конфиденциальности информации.

Лекция 5.9. Методы противодействия утечки информации по акустическому каналу. Спектры частот и резонансов акустических колебаний в различных материалах. Методы анализа и синтеза при расчётах акустического экрана.

Тема 6. Новейшие средства обеспечения информационной безопасности объектов (2 часа).

Лекция 6.10. Последние разработки средств обеспечения информационной безопасности объектов. Примеры оценки стоимости информационных материалов. Анализ технических средств доступа к выделенным источникам информации.

2.2. Перечень тем практических занятий и их объем в часах.

ПЗ-1. Оценки временных параметров передвижения на модели «нарушителя» (2 часа).

ПЗ-2. Методы расчета коэффициентов ослабления акустических колебаний в различных материалах (2 часа).

ПЗ-3. Анализ спектра частот и резонансов акустических колебаний в различных материалах (2 часа).

ПЗ-4. Применение методов анализа и синтеза при расчётах акустического экрана (2 часа).

ПЗ-5. Оценки параметров технических систем, используемых в оптических каналах нарушения конфиденциальности информации (2 часа).

ПЗ-6. Оценочный расчёт разрешающей способности аппаратуры типа «Фотоснайпер»
(2 часа).

ПЗ-7. Примеры оценочных расчётов стоимости информационных материалов (2 часа).

ПЗ-8. Многофакторный анализ выбора соответствующих технических средств доступа к выделенным источникам информации (2 часа).

ПЗ-9. Анализ критериев выбора соответствующих технических средств доступа к выделенным источникам информации (2 часа).

2.3. Перечень тем лабораторных занятий и их объем в часах.

№ 1. Оптический канал утечки информации. Анализ схемы возможных действий нарушителя с помощью ПК (4 часа), графическое представление результатов.

№ 2. Акустический канал утечки информации. Синтез акустического экрана с помощью ПК, графическое представление результатов (4 часа).

№ 3. Основы защиты волоконных оптических линий связи от несанкционированного
доступа. Расчёты уровней рассеянных сигналов от различных неоднородностей ВОЛС
с помощью ПК (4 часа), графическое представление результатов.

2.4. Тематика курсовых проектов (работ) — учебным планом не предусмотрено.

2.5. Тематика контрольных домашних заданий - учебным планом не предусмотрено.

2.6. Перечень деловых игр - учебным планом не предусмотрено.

2. Рекомендуемая литература:

Автор (ы)	Наименование, издательство, год издания
	Основная литература:
Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А	Основы информационной безопасности. Учебное пособие для вузов. М.: Горячая линия-Телеком, 2006. – 544 с.
Башлы П.Н.	Информационная безопасность. Ростов, И/Д: «Феникс», 2006. -253 с.
Соболев А.Н., Кириллов В.М.	Физические основы технических средств обеспечения информационной безопасности. М., «Гелиос АРВ», 2004.- 216 с.

	Дополнительная литература.
Шинкин Г.П.	Ценность информации. Вопросы теории и приложений. М., Филоматик, 2004.- 144 с.
Максимов Ю.Н., Сонников В.Г., Петров В.Г. и др.	Технические средства защиты информации. СПб.: ООО «Изд. Полигон», 2000. – 320 с.
Симонович С. В. и др.	Информатика: Базовый курс. – СПб.: Питер –2002.
Макарова Н.В. и др.	Информатика: Учебник / под ред. Проф. Н.В. Макаровой. - М.: Финансы и статистика, 1997.

4. Рекомендуемые электронные учебные материалы по дисциплине:

Mathcad 8.0, Quick Basic, Multysim 7.0, Mathlab 7, 8.