

**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ГРАЖДАНСКОЙ АВИАЦИИ**

Утверждаю

Проректор МГТУ ГА по УР

(подлинник подписан) Криницин В.В.

" ___ " _____ 200_ г.

Рабочая программа дисциплины

«Сертификация и аттестация объектов информационной защиты»

Шифр – СД.01

Специальность – 090106

Факультет авиационных систем и комплексов.

Кафедра Основ радиотехники и защиты информации.

Курс – V.

Форма обучения - дневная.

Общий объем учебных часов на дисциплину – 180 час.

Аудиторные занятия – 84 (час).

Лекции – 44 (час).

Практические занятия – 40 (час).

Самостоятельная работа – 96 (час).

Зачет – X семестр.

Москва – 2008 г.

Рабочая программа составлена в соответствии с Государственным образовательным стандартом высшего профессионального образования, определяющим требования к минимуму и уровню подготовки выпускника по специальности 090106 – «Информационная безопасность телекоммуникационных систем».

Рабочую программу составил

Болелов Э. А., к.т.н., доцент _____

Рабочая программа рассмотрена и утверждена на заседании кафедры ОРТ ЗИ

Протокол № 2 от "06" октября _____ 2008 г.

Зав. кафедрой Емельянов В.Е., проф. _____

Рабочая программа одобрена методическим советом специальности «Информационная безопасность телекоммуникационных систем», протокол № 1 от "16" октября _____ 2008 г.

Председатель методического совета по специальности 090106

Емельянов В.Е., проф. _____

Рабочая программа согласована с учебно-методическим управлением (УМУ)

Нач. УМУ доц., д.т.н. Логачев В.П. _____

" _____ " _____ 2008 г.

1. Цели и задачи дисциплины

1.1. Цель преподавания дисциплины

Дисциплина «Сертификация и аттестация объектов информационной безопасности» имеет целью дать студентам систематизированные знания об организации мероприятий по информационной безопасности на объекте информатизации и об их правовом обеспечении. Дисциплина раскрывает основные понятия и виды защищаемой информации в соответствии с законодательством РФ, дает знания о системе защиты государственной тайны, конфиденциальной информации.

Дисциплина «Сертификация и аттестация объектов информационной защиты» дает студентам систематизированные знания по вопросам организации системы государственного лицензирования в области защиты информации, сертификации и аттестации объектов защиты информации.

1.2. Задачи изучения дисциплины - дать основы:

- знаний в области информационного законодательства РФ и международного законодательства в области защиты информации;
- организации государственного лицензирования в области защиты информации;
- организации системы сертификации и аттестации объектов защиты информации.

2. Требования к уровню освоения содержания дисциплины

2.1. Иметь представление:

- об основах организации защиты информации на объектах информатизации;
- о назначении, задачах и структуре, средствах и способах работы

подразделений службы безопасности;

- правовом режиме участия в международном обмене.

2.2. Знать:

- основные угрозы информационной безопасности объекта информатизации и их классификацию;

- классификацию мероприятий по защите информации;

- правила лицензирования и сертификации в области защиты информации;

- порядок проведения аттестации объектов информационной защиты;

- типовые методики испытаний объектов информатики по требованиям защиты информации;

- типовые формы документов по подготовке и проведению сертификации и аттестации объектов защиты информации;

- специальные защитные знаки и их классификацию.

2.3. Уметь:

- определять угрозы объекту информатизации;

- определять рациональные способы и средства защиты информации на объекте информатизации;

- организовывать мероприятия по защите информации на объекте информатизации.

3. Содержание дисциплины

3.1. Разделы дисциплины и виды занятий

№ п/п	Раздел дисциплины	Лекции (час)	ПЗ или С (час)	ЛР (час)
1.	Основы правового обеспечения информационной безопасности	20	14	-
2.	Сертификация и аттестация объектов информационной защиты	24	26	-

3.2. Содержание лекций и ссылки на литературу

Раздел 1. Основы правового обеспечения информационной безопасности. - 20 часов, [1-9].

Лекция 1-1. Основы законодательства РФ в области информационной безопасности и защиты информации (4 ч.)

Информация, как объект правового регулирования. Законодательство РФ в области информации и информационной безопасности. Международное право в сфере защиты информации.

Лекция 1-2. Понятие и виды информации, защищаемой законодательством РФ. (4 ч.)

Основные определения. Понятие и виды информации, защищаемой законодательством РФ. Классификация информации по категориям доступа.

Лекция 1-3. Государственная тайна и ее защита (4 ч.).

Государственная тайна - особый вид защищаемой информации. Система защиты государственной тайны. Организационные и технические способы защиты государственной тайны.

Лекция 1-4 Конфиденциальная информация и ее защита (4 ч.).

Коммерческая тайна. Служебная тайна. Профессиональная тайна. Персональные данные.

Лекция 1-5. Электронная цифровая подпись (4 ч.).

Основные определения. Государственные стандарты, образующие систему ЭЦП. Цифровые сертификаты.

СРС – 22 ч.

Раздел 2. Сертификация и аттестация объектов информационной защиты - 24 часа, [2-4].

Лекция 2-1. Лицензирование деятельности в области защиты информации. (4 ч.)

Общие положения. Организационная структура системы государственного лицензирования. Порядок проведения лицензирования и контроль за деятельностью лицензиатов.

Лекция 2-2. Сертификация средств защиты информации по требованиям безопасности информации (4 ч.).

Общие положения. Организационная структура системы сертификации. Порядок проведения сертификации и контроля. Требования к нормативным и методическим документам по сертификации средств защиты информации.

Лекция 2-3. Система сертификации средств криптографической защиты информации (4 ч.).

Общие положения. Система сертификации продукции по требованиям безопасности информации. Порядок подготовки и проведения сертификации. Контроль и надзор за проведением сертификации и стабильностью характеристик сертифицированной продукции.

Лекция 2-4. Лаборатории для проведения сертификационных испытаний средств информационной защиты (4 ч.).

Задачи и функции испытательной лаборатории. Права, обязанности и ответственность испытательной лаборатории.

Лекция 2-5. Аттестация объектов информатизации по требованиям безопасности информации (2 ч.)

Цели и задачи аттестационных проверок и испытаний. Условия и порядок проведения испытаний. Оформление отчетных материалов по результатам испытаний.

Лекция 2-6. Испытания объектов информационной защиты (4 ч.)

Общая характеристика методов проведения испытаний. Испытания объекта на соответствие организационно-техническим требованиям по защите информации. Испытания объекта на соответствие требованиям по защите информации от утечки по каналам ПЭМИН. Испытания объекта на соответствие требованиям по защите информации от НСД. Испытания объекта на соответствие требованиям по защите информации от утечки по акустическим каналам.

Лекция 2-7 Классификация специальных защитных знаков (2 ч.).

Общие положения. Специальные защитные знаки.

СРС – 24 ч.

3.3. Перечень практических занятий

- ПЗ 1. Законодательство РФ в области защиты информации. – 4 часа.
- ПЗ. 2 Правовые режимы защиты информации. – 6 часов.
- ПЗ. 3 Изучение норм административного права в сфере защиты информации. – 4 часа.
- ПЗ. 4 Изучение порядка проведения лицензирования и видов деятельности предприятий в области защиты информации – 4 часа.
- ПЗ 5. Изучение перечня средств защиты информации, подлежащих сертификации в системе сертификации ФСТЭК. – 4 часа.
- ПЗ. 6 Изучение положения о сертификации средств вычислительной техники по требованиям безопасности информации. – 4 часа.
- ПЗ. 7 Изучение положения об аккредитации испытательных лабораторий и органов сертификации средств защиты информации по требованиям безопасности информации. – 4 часа.
- ПЗ. 8 Методика испытаний объектов информатики по требованиям безопасности информации. – 6 часов.
- ПЗ. 9 Концепция защиты средств вычислительной техники и АС от несанкционированного доступа к информации. – 4 часа.

СРС – 50 ч.

Рекомендуемая литература

4.1 ОСНОВНАЯ:

1. Семкин С.Н. и др. Основы информационного обеспечения информационной безопасности объектов информатизации. Учебное пособие. – М.: Гелиос-АРВ, 2005.

2. Казанцев С.Я. и др. Правовое обеспечение информационной безопасности. Учебное пособие для студентов вузов. – М.: Изд. центр «Академия», 2005.

3. Снытников А.А. Лицензирование и сертификация в области защиты информации. – М.: Гелиос-АРВ, 2003.

4. Гринсберг А.С., Горбачев Н.Н., Теплякова А.А. Защита информационных ресурсов государственного управления. Учебное пособие для вузов. – М.: Юнити-Дана, 2003.

4.2. ДОПОЛНИТЕЛЬНАЯ:

5. Федеральный закон от 20.02.1995 №24-ФЗ «Об информации, информатизации и защите информации».

6. Закон РФ от 21.07.1993 №5485-1 «О государственной тайне».

7. Федеральный закон от 29.07.2004 №98-ФЗ «О коммерческой тайне».

8. Организация и современные методы защиты информации. Информационно-справочное пособие. – М.: Ассоциация «Безопасность», 1996.

9. Практика защиты коммерческой тайны в США. Пер. с англ. – М.: СП «Крокус Интернешнел», 1993.

5. Рекомендуемые программные средства и компьютерные системы обучения и контроля знаний студентов

5.1.

5.2. Обучение возможности в сети «Интернет».

<http://www.fsb.ru/>, <http://www.inside-zi.ru/>, и др.

5.3. Средства обеспечения освоения дисциплины.

Компьютерный класс с современным программным обеспечением.

6. Рекомендуемое разделение содержания дисциплины на блоки:

не предусмотрено.

Дополнения и изменения в рабочей программе учебной дисциплины на
200__/200__ учебный год.

В рабочую программу внесены следующие изменения:

Рабочая программа пересмотрена и одобрена на заседании кафедры.

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

протокол № ____ от " ____ " _____ 200__ г.

Внесенные сведения верны

Нач. УМУ доц., д.т.н. Логачев В.П. _____