МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ

УТВЕРЖДАЮ
Проректор по УМР

_____ Криницин В.В.

" ___ " _____ 2004 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ "МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ" (ОПД.Ф.12)

Специальность 22.01.00
Кафедра "Вычислительные машины, комплексы, системы и сети"
Факультет "Прикладной математики и вычислительной техники"
Курс 4, форма обучения – дневная, семестр – 7

Общий объем учебных часов на дисциплину – 68 час.

Лекции	– 34 час.
Практические занятия	– 18 час.
Лабораторные занятия	– 16 час.
Самостоятельная работа	–
Курсовой проект	–
Курсовая работа	–
Контрольная работа	–
Домашнее задание	–
Зачет	–
Экзамен	– 4 курс, 7 семестр

Москва – 2004

Рабочая программа составлена в соответствии с Государственным образовательным стандартом высшего и среднего образования по направлению подготовки 654600 – Информатика и вычислительная техника на основании примерной учебной программы дисциплины в соответствии с Государственными требованиями к минимуму содержания и уровню подготовки выпускника по специальности.

Рабочую программу составил
кандидат технических наук, доцент Терентьев А.И.

Рабочая программа утверждена на заседании кафедры,
протокол № _____ от " _____ " _____ 2004 года

Заведующий кафедрой
доктор технических наук, профессор Соломенцев В.В.

Рабочая программа одобрена методическим советом специальности
"Вычислительные машины, комплексы, системы и сети".
Протокол № ____ от " _____ " _____ 2004 года

Председатель методического совета
доктор технических наук, профессор Соломенцев В.В.

Рабочая программа согласована с Учебно-методическим управлением.
Начальник УМУ Логачев В.П.

1. Цель преподавания дисциплины

Öåëüþ ïðåïîäàâàíèÿ äèñöèïëèíû ÿâëÿåòñÿ îçíàêîìëåíèå ñòóäåíòîâ ñ îñíîâíûìè îðãàíèçàöèîííûìè, òåõíè÷åñêèìè, àëãîðèòì÷åñêèìè, ïðîãðàììíûìè è äðóãèìè ìåòîäàìè è ñðåäñòâàìè çàùèòû êîìïüþòåðíîé èíôîðìàöèè, à òàêæå ñ äåéñòâóþùèì çàêîíîäàòåëüñòâîì è ñòàíäàðòàìè â îáëàñòè èíôîðìàöèîííîé áåçîïàñíîñòè.

2. Задачи изучения дисциплины, необходимый комплекс знаний и умений

Â ðåçóëüòàòå èçó÷åíèÿ äèñöèïëèíû ñòóäåíòû äîëæíû:

çíàòü ïðàâîâûå îñíîâû è äåéñòâóþùèå ñòàíäàðòû â îáëàñòè çàùèòû êîìïüþòåðíîé èíôîðìàöèè, àäåêâàòíûå âîçìîæíûì óãðîçàì îðãàíèçàöèîííûå, òåõíè÷åñêèå è äðóãèå ìåòîäû îáåñïå÷åíèÿ öåëîñòíîñòè, êîíôèäåíöèàëüíîñòè è äîñòóïíîñòè êîìïüþòåðíîé èíôîðìàöèè, â òîì ÷èñëå ñîâðåìåííûå ìåòîäû è ñðåäñòâà êðèïòîãðàôè÷åñêîãî ïðåîáðàçîâàíèÿ èíôîðìàöèè, èäåíòèôèêàöèè è àóòåíòèôèêàöèè îáúåêòîâ (ñóáúåêòîâ), çàùèòû ïðîãðàììíîãî îáåñïå÷åíèÿ îò âèðóñîâ è íåñàíêöèîíè-ðîâàííîãî êîïèðîâàíèÿ, ïðîòèâîäåéñòâèÿ òåõíè÷åñêèì ðàçâåäêàì;

óìåòü ïðèìåíÿòü ïîëó÷åííûå çíàíèÿ è íàâûêè íà ïðàêòèêå, â òîì ÷èñëå ïðè ïðîåêòèðîâàíèè è ýêñïëóàòàöèè àâòîìàòèçèðîâàííûõ ñèñòåì îáðàáîòêè èíôîðìàöèè è óïðàâëåíèÿ (ÀÑÎÈÓ), èìåòü ïðåäñòàâëåíèå î íàïðàâëåíèÿõ ðàçâèòèÿ è ïåðñïåêòèâíûõ ìåòîäàõ çàùèòû èíôîðìàöèè.

2. Содержание дисциплины

2.1. Наименование разделов, объем в часах. Содержание лекций

Ðàçäåë 1. Îáùåå ïðåäñòàâëåíèå îá èíôîðìàöèè как объекте защиты (4 часа)

Лекция 1. Введение. Определение, свойства, категории и формы представления информации. Информационные процессы и жизненный цикл информации. Каналы передачи и доступа к информации. Источники и носители информации.

Лекция 2. Объекты защиты информации и их классификация. Информатизация и объекты информатизации. Объекты защиты компьютерной информации. Классификация угроз информации как объекту защиты и их источников. Оценка уязвимости объекта защиты

информации. Оценка рисков по отношению к принятой модели угроз. Методы ранжирования угроз, уязвимостей и рисков. Инциденты в области информационной безопасности.

Ðàçäåë 2. Îáùåå ïðåäñòàâëåíèå î ñèñòåìàõ çàùèòû èíôîðìàöèè è ïðèíöèïàõ èõ ïîñòðîåíèÿ (2 ÷àñà)

Лекция 3. Иерархический принцип организации информационной системы предприятия. Модель потенциального нарушителя. Абстрактные графические модели систем защиты информации. Некоторые критерии и методы оценки эффективности систем защиты информации. Основные этапы и принципы проектирования систем защиты информации.

Ðàçäåë 3. Çàùèòà èíôîðìàöèè от несанкционированного доступа (4 часа)

Лекция 4. Основные понятия и определения. Виды и каналы несанкционированного доступа (НСД) к информации. Основные методы защиты информации от несанкционированного доступа (НСД). Управление доступом к объектам защиты информации: физическое ограничение доступа, инженерно-технические средства и системы охраны, логическое разграничение доступа, протоколирование и аудит происходящих событий.

Лекция 5. Идентификация и аутентификация объекта (субъекта): идентификация и аутентификация личности, технических средств, документов.

Ðàçäåë 4. Êðèòîãðàôè÷åñêèå ìåòîäû çàùèòû êîìïüþòåðíîé èíôîðìàöèè îò íåñàíêöèîíèðîâàííîãî äîñòóïà è ìîäèôèêàöèè (8 ÷àñîâ)

Лекция 6. Основные понятия и определения. Исторический обзор примитивных методов шифрования. Принципы построения и требования к современным криптографическим системам. Симметричные, асиммет-ричные и гибридные криптографические системы.

Лекция 7. Алгоритмы шифрования с секретным ключом. Блочные и поточные шифры. Алгоритм шифрования DES. Алгоритм шифрования ГОСТ 28147-89. Алгоритм шифрования Rijndael. Алгоритм шифрования RC4.

Лекция 8. Алгоритмы шифрования с открытым ключом. Алгоритм шифрования RSA. Алгоритм шифрования Эль-Гамаля. Защита юридической значимости электронных документов. Электронная

цифровая подпись. Определение, свойства и способы реализации функции хэширования. Электронная цифровая подпись по алгоритму Эль-Гамаля.

Лекция 9. Электронная цифровая подпись по алгоритму ГОСТ Р 34.10-94, ГОСТ Р 34.10-01. Управление криптографическими ключами. Некоторые сведения о криптоанализе.

Ðàçäåë 5. Çàùèòà èíôîðìàöèîííûõ ðåñóðñîâ
àâòîìàòèçèðîâàííûõ ñèñòåì îò íåñàíêöèîíèðîâàííîãî âîñòóïà
è ìîäèôèêàöèè (4 ÷àñà)

Лекция 10. Классификация и состав автоматизированных систем. Модель структуризации объектов защиты информации автоматизированных систем. Характерные угрозы и атаки на информационные ресурсы автоматизированных систем. Назначение и функции подсистемы информационной безопасности автоматизированной системы. Политика безопасности. Модели разграничения доступа к информации. Методы и средства защиты информации в ОС Windows NT/2000/XP: идентификация и аутентификация пользователей, объекты и субъекты доступа, методы, права и привилегии доступа, маркер доступа и дескриптор защиты, протоколирование и аудит происходящих событий, средства администрирования ОС Windows NT/2000/XP для защиты информации в автономных ПЭВМ, средства администрирования ОС Windows NT/2000/XP для защиты информации в локальных компьютерных сетях.

Лекция 11. Защита информации в распределенных компьютерных сетях. Межсетевые экраны и маршрутизаторы. Построение и компоненты виртуальных частных сетей (VPN). Защита информации в сети Internet. Защита информации от помех и умышленной модификации с помощью корректирующих кодов. Специализированное архивирование и хранение информации.

Ðàçäåë 6. Çàùèòà ïðîãðàììíîãî îáåñïå÷åíèÿ
îò íåñàíêöèîíèðîâàííîãî êîïèðîâàíèÿ è ðàñïðîñòðàíåíèÿ (2 ÷àñà)

Лекция 12. Классификация методов защиты программного обеспечения от несанкционированного копирования. Структура системы защиты программного обеспечения от несанкционированного копирования. Методы и средства нейтрализации систем защиты от несанкционированного копирования.

Ðàçäåë 7. Çàùèòà èíôîðìàöèè îò êîìïüþòåðíûõ âèðóñîâ
è ïîäñíûõ âîçäåéñòâèé ïî êàíàëàì ðàñïðîñòðàíåíèÿ
ïðîãðàììíûõ ñðåäñòâ (2 ÷àñà)

Лекция 13. Основные виды и классификация вредоносных программ. Некоторые типы программных закладок. Компьютерные вирусы, их классификация и признаки наличия вирусной инфекции. Методы и средства защиты от вредоносных программ.

Раздел 8. Защита информации от технических разведок (4 часа)

Лекция 14. Классификация технических каналов утечки информации. Классификация и характеристика технических средств разведки. Методы и средства противодействия техническим разведкам.

Лекция 15. Защита информации от НСД по каналам побочных электромагнитных излучений и наводок (ПЭМИН). Классификация каналов ПЭМИН. Методы и средства защиты информации от утечки по каналам ПЭМИН.

Раздел 9. Организационно-правовое обеспечение и регулирование в области защиты информации (4 часа)

Лекция 16. Значение и задачи организационно-правового обеспечения в области защиты информации. Информация как объект гражданско-правовых отношений. Законодательные акты Российской Федерации в области информационной безопасности. Система стандартизации и регулирования деятельности в области защиты информации. Государственные стандарты Российской Федерации в области защиты информации.

Лекция 17. Общие технические требования и классы защищенности средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации, установленные руководящими документами Государственной технической комиссии при Президенте Российской Федерации. Критерии оценки безопасности компьютерных систем Министерства обороны США. Общие критерии оценки безопасности информационных технологий (ГОСТ Р ИСО/МЭК 15408-2002).

2.2. Перечень тем практических занятий и их объем в часах

ПЗ–1. Математические методы и операции в криптографии. Проблемы факторизации и дискретного логарифма. Элементы теории сложности арифметических алгоритмов (2 часа).

ПЗ–2. Построение матрицы доступа для физических (охраняемых) объектов. Элементы системы контроля и управления доступом. Современные инженерно-технические средства охраны (2 часа).

ПЗ–3. Ограничение доступа и разграничение полномочий в автоматизированных системах обработки информации и управления. Матрица доступа объектов к субъектам (2 часа).

ПЗ–4. Криптографическая защита информации от несанкционированного доступа. Реализация простейших методов шифрования (2 часа).

ПЗ–5. Способы реализации функции хэширования (2 часа).

ПЗ–6. Защита информации от модификации с помощью числовых корректирующих кодов (2 часа).

ПЗ–7. Современные методы и средства защиты информации от утечки по техническим каналам (2 часа).

ПЗ–8. Разработка политики безопасности и планирование мероприятий по комплексной защите объектов информации (2 часа).

ПЗ–9. Руководящие документы Гостехкомиссии России по защите средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Требования по защите информации от несанкционированного доступа. Оценка класса защищенности средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации (2 часа).

2.3. Перечень лабораторных работ и их объем в часах

ЛР–1. Криптографические методы защиты информации от несанкционированного доступа (4 часа).

ЛР–2. Криптографические методы обеспечения подлинности и целостности электронных документов. Электронная цифровая подпись (4 часа).

ËÐ–3. Ìåòîäû è ñðåäñòâà çàùèòû èíôîðìàöèè â îïåðàöèîííûõ ñèñòåìàõ ñåìåéñòâà Windows NT/2000/XP (4 ÷àñà).

ЛР–4. Методы оценки класса защищенности средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации (4 часа).

2.4. Тематика курсовых проектов, работ

Êóðñîâîé ïðîåêò èëè ðàáîòà ïî äèñöèïëèíå Ó÷åáíûì ïëàíîì íå ïðåäóñìîòðåíû.

2.5. Тематика контрольных работ (домашних заданий)

Контрольные работы (домашние задания) по данной дисциплине не предусмотрены.

2.6. Перечень деловых игр

Деловые игры по данной дисциплине не предусмотрены.

3. Рекомендуемая литература

№	Автор	Наименование, издательство, год издания
		Îñíîâíàÿ
1.	Терентьев А.И.	Введение в информационную безопасность: Учебное пособие. – М.: МГТУ ГА, 2001. – 144 с.
		Учебно-методическая
1.	Терентьев А.И.	Методы защиты информации. Пособие к выполнению лабораторных работ. – М.: МГТУ ГА, 2002. – 40 с.
2.	Терентьев А.И.	Методы защиты информации: Пособие к выполнению лабораторной работы. – М.: МГТУ ГА, 2003. – 48 с.
		Дополнительная
1.	Анин Б.Ю.	Защита компьютерной информации. – СПб.: БХВ – Санкт-Петербург, 2000. – 384 с.: ил.
2.	Учебный курс MCSE	Безопасность сети на основе Windows 2000. Учебный курс MCSE / Пер. с англ. – М.: Издательско-торговый дом "Русская Редакция", 2001. – 912 с.: ил.
3.	Бойс Дж.	Windows 2000: Пер. с англ. – М.: ДМК Пресс, 2001. – 304 с.: ил. (Серия "Защита и администрирование").
4.	Под общ. ред. В.В.Ященко	Введение в криптографию / Под общ. ред. В.В. Ященко. – М.: МЦНМО, "ЧеРо", 1998. – 272 с.
5.	Герасименко В.А.,	Основы защиты информации. – М.: МИФИ,

	Малюк А.А.	1997. – 538 с.
6.	Горбатов В.С., Полянская О.Ю.	Основы технологии PKI. – М.: Горячая линия – Телеком, 2004. – 248 с.: ил.
7.	Запечинков С.В., Милославская Н.Г., Толстой А.И.	Основы построения виртуальных частных сетей: Учеб. пособие для вузов. – М.: Горячая линия–Телеком, 2003. – 249 с.
8.	Зегжда Д.П., Ивашко А.М.	Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.: ил.
9.	Касперский Е.	Компьютерные вирусы: что это такое и как с ними бороться. - М.: СК Пресс, 1998.
10.	Малюк А.А.	Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. – М.: Горячая линия–Телеком, 2004. – 280 с. ил.
11.	Мельников В.В.	Защита информации в компьютерных системах. -М.: Финансы и статистика; Электроинформ, 1997. - 368 с.: ил.
12.	Петраков А.В., Лагутин В.С.	Телеохрана. – М.: Энергоатомиздат, 1998, - 376 с.: ил.
13.	Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф.	Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с.: ил.
14.	Терентьев А.И.	Элементы теории и практики числовых линейных блоковых корректирующих кодов. – М.: Альтекс, 2000. – 204 с.: ил.
15.	Торокин А.А.	Основы инженерно-технической защиты информации. – М.: Издательство "Ось-89", 1998. – 336 с.
16.	Ухлинов Л.М., Сычев М.П., Скиба В.Ю., Казарин О.В.	Обеспечение безопасности информации в центрах управления полетами космических аппаратов / Л.М.Ухлинов, М.П.Сычев, В.Ю.Скиба, О.В.Казарин. – М.: Издательство МГТУ им. Н.Э.Баумана, 2000. – 366 с.
17.	Учебное пособие для вузов	Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учебное пособие для вузов / П.Ю.Белкин, О.О.Михальский, А.С.Першаков и др. – М.: Радио и связь, 1999. – 168 с.: ил.

18.	Учебное пособие для вузов	Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб. пособие для вузов / Проскурин В.Г., Крутов С.В., Мацкевич И.В. – М.: Радио и связь, 2000. – 168 с.: ил.
19.	Учебное пособие для вузов	Теоретические основы компьютерной безопасности: Учебное пособие для вузов / П.Н.Девянин, О.О.Михальский, Д.И.Правиков и др. – М.: Радио и связь, 2000. – 192 с.: ил.
20.	Хорев А.А.	Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учеб. пособие. – М.: Гостехкомиссия России, 1998. – 320 с.
21.	Чмора А.Л.	Современная прикладная криптография. – М.: Гелиос АРВ, 2001. – 256 с.: ил.
22.	Ярочкин В.И.	Система безопасности фирмы. – 2-е издание. - М.: Издательство "Ось-89", 1998. – 192 с.

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

При проведении лабораторных работ и практических занятий используются обучающие и вспомогательные программы, разработанные студентами Московского государственного технического университета гражданской авиации под руководством к.т.н. доцента Терентьева А.И.

5. Рекомендуемое разделение содержания дисциплины на блоки:

Блок 1. Разделы 1, 2, 3.
Блок 2. Раздел 4.
Блок 3. Разделы 5, 6, 7.
Блок 4. Раздел 8.
Блок 5. Раздел 9.

Рабочая программа периодически корректируется. Изменения вносятся в лист изменений (форма 1).

Форма 1

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

В рабочую программу вносятся следующие изменения:

_____
_____
_____
_____

Рабочая программа пересмотрена и одобрена на заседании кафедры "Вычислительные машины, комплексы, системы и сети".

Заведующий кафедрой _____ _____
Протокол № _____ от " ____ " _____ 200 __ г.

Внесенные изменения утверждены.
Начальник УМУ _____ _____