**РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ОТКРЫТЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ
МИНИСТЕРСТВА ПУТЕЙ СООБЩЕНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

20/43/1

**Одобрено кафедрой
«Вычислительная
техника»**

**Утверждено деканом
факультета
«Управление процессами
перевозок»**

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

**Рабочая программа
для студентов V курса
специальности**

**220100 ВЫЧИСЛИТЕЛЬНЫЕ МАШИНЫ, КОМПЛЕКСЫ,
СИСТЕМЫ И СЕТИ (ЭВМ)**

Москва – 2004

Рабочая программа составлена в соответствии с Государственным образовательным стандартом высшего профессионального образования и удовлетворяет государственным требованиям к минимуму содержания и уровню подготовки инженера по специальности 220100 (ЭВМ).

Составитель: канд. техн. наук, доц. А.Е. Ермаков

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Рабочая программа

Редактор *Д.Н. Тихонычев*
Корректор *В.В. Игнатова*
Компьютерная верстка *О.А. Денисова*

Тип. зак.	Изд. зак. 171	Тираж 900 экз.
Подписано в печать 14.12.04	Гарнитура Times.	Офсет
Усл. печ. л. 0,5		Формат $60\times90^{1}/_{16}$

Издательский центр РГОТУПСа,
125993, Москва, Часовая ул., 22/2

Участок оперативной печати РГОТУПСа,
125993, Москва, Часовая ул., 22/2

ЦЕЛЬ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Цель изучения дисциплины состоит в формировании системного базового представления, умения и навыков студентов по основам информационной безопасности и защите информации, достаточных для последующей эксплуатации автоматизированных систем (АС) и сетей Федерального железнодорожного транспорта (ФЖТ).

В процессе обучения студенты должны изучить правовую базу информационной безопасности информационных систем, угрозы информационной безопасности корпоративных систем ФЖТ, методы защиты информации (включая криптографические), способы защиты информации от несанкционированного доступа к информации и техническим ресурсам корпоративных сетей ФЖТ, архитектуру и методы организации систем защиты информации.

Этот результат достигается с помощью лекций и выполнения контрольной работы, а также самоподготовки студентов.

2. ТРЕБОВАНИЯ К УРОВНЮ ОСВОЕНИЯ СОДЕРЖАНИЯ ДИСЦИПЛИНЫ

Изучив дисциплину, студент должен.

2.1. Знать и уметь использовать:

• правовую и нормативную базу корпоративных информационных систем ФЖТ;

• информационную структуру и информационные ресурсы сетей ФЖТ как объекта защиты;

• уровни защиты информации;

• криптографические методы защиты информации;

• протоколы взаимной аутентификации объектов сетей;

• методы организации систем защиты информации.

2.2. Владеть:

• навыками работы с межсетевыми экранами и пакетами антивирусных программ;

• навыками самостоятельного проектирования систем защиты информации.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Вид учебной работы	Всего часов	Курс – V
Общая трудоемкость дисциплины	110	
Аудиторные занятия:	16	
Лекции	8	
Практические занятия	4	
Лабораторный практикум	4	
Самостоятельная работа	79	
Контрольная работа	15	1
Вид итогового контроля		Экзамен

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Разделы дисциплины и виды занятий

№ п/п	Раздел дисциплины	Лекции, ч	Практические занятия, ч	Лабораторный практикум, ч
1	Правовая основа информационной безопасности информационных систем.	2		
2	Информационная безопасность и методология защиты информации в корпоративных системах ФЖТ	2		
3	Криптографические методы защиты информации	2	4	
4	Методы защиты от несанкционированного доступа к информации и техническим ресурсам сетей	2		4

4.2. Содержание разделов дисциплины

Раздел 1. **Правовая основа информационной безопасности информационных систем**

Предмет, цели и задачи дисциплины «Методы и средства защиты компьютерной информации». Основные определения и понятия. Общая проблема информационной безопасности информационных систем. Доктрина информационной безопасности РФ. [1; 2, с. 109…120]

Раздел 2. **Информационная безопасность и методология защиты информации корпоративных системах ФЖТ**

Классификация информации, циркулирующей в корпоративных системах ФЖТ. Информационные ресурсы и информационная инфраструктура сетей ФЖТ как объекты защиты. Классификация и анализ угроз информационной безопасности корпоративным системам. Уровни защиты информации: правовой; организационный; аппаратно-программный; криптографический. [2, с. 120…150]

Раздел 3. **Криптографические методы защиты информации**

Классификация криптографических методов. Традиционные (симметричные) криптосистемы. Блоковые и поточные шифры. Стойкость криптосистем. Американский стандарт шифрования данных DES. Отечественный стандарт криптографической защиты ГОСТ 28147-89.

Асимметричные криптосистемы. Математические основы криптографии с открытым ключом. Криптосистема RSA. Криптосистема Эль Гамаля. Криптосистемы без передачи ключей.

Управление ключами. Методы генерации, хранения и распределения ключей. Протоколы управления ключами. Инфраструктура открытых ключей. Цифровые сертификаты. (2 часа, лекция).

Новый стандарт электронной цифровой подписи (ЭЦП) на эллиптических кривых. Стандарт функции хэширования. [2, с. 155…186; 4, с. 82…153]

Раздел 4. **Методы защиты от несанкционированного доступа к информации и техническим ресурсам сетей**

Идентификация и аутентификация объектов сети. Идентификация и подтверждение подлинности пользователей сети.

Применение паролей и биометрических средств аутентификации пользователей. Протоколы взаимной проверки подлинности объектов сети.

Межсетевое экранирование. Принципы построения и функционирования межсетевых экранов (МЭ). Классификация МЭ. Особенности межсетевого экранирования на различных уровнях модели OSI.

Обеспечение целостности информации. Аутентификация информации и электронная цифровая подпись сообщений. Однонаправленные хэш-функции. Коды проверки подлинности информации.

Средства антивирусной защиты. Классификация вирусов и средств защиты. Виды антивирусных программных продуктов. Характеристика наиболее популярных антивирусных пакетов. [2, с. 187…246; 4, с. 154…217]

Раздел 5. **Архитектура и методы организации систем защиты информации**

Архитектура системы защиты информации (СЗИ). Этапы создания СЗИ. Виды обеспечения СЗИ. Принципы разработки СЗИ. Специализированные программно-аппаратные средства защиты информации. Средства и механизмы обеспечения безопасности сетевого оборудования Cisco Systems. Межсетевые экраны (брандмауэры) Cisco. Средства обнаружения атак.

Методы технической защиты информации в сетях железнодорожного транспорта. Угрозы безопасности за счет электромагнитных и акустических факторов, воздействующих на защищаемую информацию. Методы предотвращения перехвата информации через побочные электромагнитные излучения и наводки (ПЭМИН). Защита обслуживающего персонала от физических излучений. [2, с. 255…282]

4.3. Лабораторный практикум

№ п/п	№ раздела дисциплины	Наименование лабораторных работ
1	4	Конфигурирование межсетевого экрана
2	4	Конфигурирование антивирусного пакета

4.4. Практические занятия

№ п/п	№ раздела дисциплины	Наименование практических занятий
1	3	Шифрование информации с помощью алгоритма DES

5. САМОСТОЯТЕЛЬНАЯ РАБОТА

Студенты выполняют контрольную работу по шифрованию своей фамилии, представленной в двоичном коде с помощью кодировки КОИ-8, с помощью симметричного криптографического алгоритма DES.

Пояснительная записка должна включать в себя описание преобразования фамилии студента в двоичный код; определение 64-х разрядного ключа, за основу которого берется представленное в двоичном коде имя студента, описание алгоритма шифрования.

Примерный объем пояснительной записки составляет 15…20 страниц.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Рекомендуемая литература

Основная

1. Доктрина информационной безопасности Российской Федерации. — М.: Совет безопасности РФ, 2000. — 41 с.

2. Яковлев В.В., Корниенко А.А. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта: Учебник для вузов ж.-д транспорта. — М.: УМК МПС России, 2002. — 328 с.

3. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных: Уч. пос. — М.: СИНТЕГ, 2000. — 248 с.

4. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. — М.: Радио и связь, 2001. — 328 с.

Дополнительная

5. Руководящий документ: Защита от несанкционированного доступа к информации. Термины и определения. — М.: Гостехкомиссия России, 1992. — 13 с.

6. Руководящий документ. Концепция защиты СВТ и АС от НСД к информации. — М.: Гостехкомиссия России, 1992.

7. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. — М.: Гостехкомиссия России, 1992.

8. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. — М.: Гостехкомиссия России, 1992.

9. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники. — М.: Гостехкомиссия России, 1992.

10. Руководящий документ: Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. — М.: Гостехкомиссия России, 1992. — 18 с.

11. Руководящий документ: Средства вычислительной техники. Межсетевые экраны. Показатели защищенности от несанкционированного доступа. — М.: Гостехкомиссия России, 1997. — 17 с.

12. ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

13. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

14. ОСТ 45.127-99. Система обеспечения информационной безопасности взаимоувязанной сети связи РФ. Термины и определения.

15. Мельников В.В. Защита информации в компьютерных системах. — М.: Финансы и статистика – Электроинформ, 1997. — 368 с.