Министерство образования и науки Республики Казахстан

Павлодарский государственный университет им. С. Торайгырова

Кафедра радиотехники и телекоммуникаций

РАБОЧАЯ ПРОГРАММА

дисциплины «Информационная безопасность телекоммуникационных систем»
для студентов специальности 050719
«Радиотехника, электроника и телекоммуникации»

Павлодар

Лист утверждения к рабочей программе дисциплины, разработанной на основании каталога элективных дисциплин по специальности

Форма ФСО ПГУ 7.18.1/08

УТВЕРЖДАЮ
Проректор по УР
Н.Э. Пфейфер
"05" ___ *OS* 2008 **г.**

Составитель: старший преподаватель Глухова Н.И..

Кафедра "Радиотехника и телекоммуникации "

РАБОЧАЯ ПРОГРАММА

по дисциплине " Информационная безопасность телекоммуникационных систем"

для студентов специальности 050719 «Радиотехника, электроника и телекоммуникации»

Рабочая программа разработана на основании рабочего учебного плана и каталога элективных дисциплин специальности 050719 «Радиотехника. электроника и телекоммуникации» и утверждена на заседании Учёного совета ПГУ им. С. Торайгырова « *£b* » *cf* 2008 г., протокол №

Рекомендована на заседании кафедры РТиТК от «__/_» *OS>* 2008 **г.**
Протокол № *•/ JJLJ>*
Заведующий кафедрой */Тлм)'* Тастенов А.Д.

Одобрена методическим советом энергетического факультета
" Я " g>j 2008 г.. протокол № *4/*

Председатель МС *c0& Iёё?£—* Кабдуалиева М.М.

СОГЛАСОВАНО
Де кан факул ьтета. Сислов Л.П. «А3 » *&9* 2008 **г.**

ОДОБРЕНО ОПиМО
Начальник ОПиМО А. Головерина Л.Т. « *СУ»* 2008 **г.**

1 ЦЕЛИ И ЗАДАЧИ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1 Цель преподавания дисциплины

Цель преподавания дисциплины - заложить терминологический фундамент, рассмотреть основные общеметодологические принципы теории информационной безопасности, изучить методы и средства обеспечения информационной безопасности, методы нарушения конфиденциальности, целостности и доступности информации.

1.2 Задачи изучения дисциплины

1 Ознакомление студентов с терминологией информационной безопасности.
2 Развитие мышления студентов.
3 Изучение методов и средств обеспечения информационной безопасности.
4 Обучение определению причин, видов, источников и каналов утечки, искажения информации.

13 В результате изучения дисциплины студенты должны знать:

основные понятия и определения, этапы развития информационной безопасности, требования к системе защиты, классификацию и анализ угроз информационной безопасности, методы нарушения конфиденциальности, целостности и доступности информации, функции и задачи защиты информации, причины, виды, каналы утечки информации.

1.4 В результате изучения дисциплины студенты должны уметь:

1 Выполнять основные этапы решения задач информационной безопасности.
2 Правильно проводить анализ угроз информационной безопасности.
3 Использовать методы и средства обеспечения информационной безопасности.
4 Работать с технической литературой.

1.5 Прсреквизиты

Для освоения изучаемой дисциплины студент должен знать следующие дисциплины:
1 Информатика.
2 Основы радиотехники, электроники и телекоммуникаций.
3 Цифровые устройства и микропроцессоры.
4 Теория автоматизированного управления.

2 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1 Тематический план дисциплины для заочной формы обучения на базе высшего технического профессионального образования

ТЕМАТИЧЕСКИЙ ПЛАН ДИСЦИПЛИНЫ					
№ п/п	Наименование тем	Количество часов			
		лек.	прак.	лаб.	СРС
1	**Введение**	0,5	–		–
2	**Основные положения теории информационной безопасности**	2	-	-	-
3	**Угрозы информации**	2		–	–
4	**Методы и модели оценки уязвимости информации**	3		–	
5	**Основы формальной теории защиты информации**	2.5	–		–
6	**Стандарты в информационной безопасности**	2	-	–	
	ИТОГО за семестр	**12**	–	–	–
7	**Функции и задачи защиты информации**	1	1	–	35
8	**Построение систем защиты информации**	1	1	–	35
9	**Архитектура систем защиты информации**	1	1	–	30
10	**КР**				17
	ИТОГО за семестр	**3**	**3**	–	**117**
	ИТОГО по дисциплине	**15**	**3**		**117**

2.2 Содержание теоретического курса

Тема 1. Введение в теорию информационной безопасности. Современная постановка задачи защиты информации.

Тема **2.** Основные положения теории информационной безопасности
2.1 Понятия, определения, объекты, субъекты, термины.
2.2 Ценность информации.
2.3 Конфиденциальность, целостность, доступность информации.
2.4 Методы обеспечения информационной безопасности.

Тема **3.** Угрозы информации
3.1 Классы каналов несанкционированного получения информации
3.2 Причины нарушения целостности информации.
3.3 Виды угроз информационным системам.
3.4 Виды потерь
3.5 Информационные инфекции.
3.6 Убытки, связанные с информационным обменом
3.7 Модель нарушителя информационных систем.

Тема 4. Методы и модели оценки уязвимости информации
4.1 Эмпирический подход к оценке уязвимости информации.
4.2 Система с полным перекрытием.
4.3 Практическая реализация модели «угроза- защита».

Тема 5. Основы формальной теории защиты информации
5.1 Основные определения.
5.2 Формальные модели управления доступом.
5.3 Формальные модели целостности.
5.4 Скрытые каналы передачи.

Тема 6. Стандарты в информационной безопасности
6.1 Общие сведения.
6.2 «Оранжевая книга».

Тема 7. Функции и задачи защиты информации
7.1 Общие положения.
7.2 Методы формирования функций защиты.
7.3 Классы задач защиты информации.
7.4 Функции защиты.
7.4 Стратегии защиты информации.

Тема 8. Построение систем защиты информации
8.1 Модель системы защиты от угроз нарушения конфиденциальности информации.
8.2 Криптографические методы обеспечения конфиденциальности информации.
8.3 Модель системы защиты от угроз нарушения целостности.
8.4 Криптографические методы обеспечения целостности информации.
8.5 Модель системы защиты от угроз нарушения доступности.
8.6 Выводы.

Тема 9. Архитектура систем защиты информации
9.1 Требования к архитектуре СЗИ.
9.2 Построение СЗИ
9.3 Ядро системы защиты информации.
9.4 Ресурсы СЗИ и организационное построении.

23 **Содержание практических занятий**

Цель практических занятий - закрепление студентами теоретического материала с помощью решения задач и выполнения контрольных работ.

СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ (заочная форма обучения)

№ п/п	Наименование тем	Содержание	Вид контроля	Сроки выполнения (по неделям)
1	**2**	**3**	**4**	**5**
1	Функции и задачи защиты информации	Классы задач защиты информации	Домашнее задание	1-2

1	2	3	4	5
2	Построение систем защиты информации	Модели системы защиты	конспект	2
3	Архитектура систем защиты информации.	Требования к архитектуре защиты информации	Домашнее задание	3

2.4 Содержание СРС

СОДЕРЖАНИЕ СРС ДЛЯ ЗАОЧНОЙ ФОРМЫ ОБУЧЕНИЯ				
№	Вид СРС	Форма отчётности	Вид контроля	Объём в часах
1	2	3	4	5
1	Проработка пройденного лекционного материала по конспекту лекций, учебникам и пособиям	конспект	Участие на занятии	0.5*15=7.5
2	Подготовка к практическим занятиям, выполнение домашних заданий	Рабочая тетрадь	Участие на занятии	1*3=3
5	Подготовка к контрольной работе	Рабочая тетрадь	Тестирование	1*6=6
6	Изучение материала, не вошедшего в содержание аудиторных занятий	Конспект	Тестирование, устный ответ	4,3*18=77.5
7	Выполнение контрольной работы	Оформленная по ГОСТу контрольная работа	Защита КР	17*1=17
8	Подготовка к рубежному контролю		РК 1, тестирование	1*6=6
Всего				117

2.4.1 Темы для самостоятельного изучения

2.4.1 .а) Угрозы информации

Подверженность физическому искажению, возможность несанкцианированной модификации, опасность несанкционированного получения информации. ***Литература:*** Основная - 1 . стр. 142-163; 5, стр. 10-12.

2.4.1.6) Функции и задачи защиты информации

. Потенциально возможные умышленные действия в автоматизированных системах обработки данных. ***Литература:*** Основная - 1, стр. 231-241 ; 5, стр. 12-18.

2.4.1 .в) Стандарты в информационной безопасности.

Основные идеи общих критериев, основные положения концепции СВТ и АС от НДС информации. ***Литература:*** Основная - 5, стр. 60-63.

2.4.2 Содержание контрольной работы для студентов заочной формы обучения

СОДЕРЖАНИЕ И ГРАФИК ВЫПОЛНЕНИЯ КОНТРОЛЬНОЙ РАБОТЫ			
№ п/п	Наименование тем	Содержание	Сроки выполнения (по неделям)
1	Основные положения теории информационной безопасности	Конфиденциальность, целостность, доступность. Методы обеспечения ИБ	1-3
2	Построение систем защиты информации.	Защиты от нарушения, конфиденциальности. целостности, доступности.	3-5
3	Угрозы информации	Классификация угроз	5-8
4	Стандарты в области управления И>	Описание содержания основных стандартов	8-11

Выписка из рабочего учебного плана специальности

Форма
ФСО ЛГУ 7.18.1.10

3 Выписка из рабочего учебного плана специальносги 050719 «Радиотехника, элекгроника и телекоммуникации» но дисциплине «Информационная безопасносгь телекоммутационных систем»

№	Форма обучения	Формы контроля						Объем работы студ. в часах всего			Распределение часов по курсам и семестрг м (' асов)								
		Экз.	зач.	кп	кр	р Г р	к. р.	общ	ауд	срс	лек	пр.	лаб	срсп/ срс	лек	пр	лаб	ср сп	срс
1	заочная на базе ВПО	3					3	135	18	117	2 семестр				3 семестр				
											12 |				3 | 3 |			3	114

4 Список рекомендуемой литературы

4.1 **Основная**

1. Белов Е.Б. Основы информационной безопасности: Учебник для вузов. - М.: Горячая линия, 2006.- 546 с.
2. Герасименко В.А. Защита информации в автоматизированных системах обработки данных: В 2 кн.Учебник для вузов. - М.: Энергоатомиздат, 1994.
3. Грушко А.А., Тимонина Е.Е. Теоретические основы защиты информации: Учебник для вузов. - М.: Яхтсмен, 1996.
4. Девянин П.Н. Теоретические основы компьютерной безопасности: Учебное пособие для вузов, - М.: Радио и связь, 2000.-192 с.
5. Цирлов В.Л. Основы информационной безопасности: Учебное пособие для вузов,- М: Феникс. 2008. -119 с.

4.2 **Дополнительная**

6. Анин Б.Ю. Защита компьютерной информации. СПб.: БВХ - Санкт-Петербург, 2000. 168 с.
7. Расторгуев С П. Программные методы защиты информации в компьютерах и сетях. М.: Яхтсмен, 1993.
8. Ярочкин В.И. Системы безопасности фирмы, 2-е изд. М.: Ось - 89, 1999.- 192 с.