



Министерство образования и науки Республики Казахстан  
Павлодарский государственный университет им. С. Торайгырова  
Кафедра «Вычислительная техника и программирование»

# **РАБОЧАЯ УЧЕБНАЯ ПРОГРАММА**

дисциплины «Основы информационной безопасности»

для студентов специальности 050704 – «Вычислительная техника и программное обеспечение»

Лист утверждения рабочей учебной программы, разработанной на основании государственного общеобразовательного стандарта образования специальности типовой программы



Ф СО ПГУ 7.18.3/31

**УТВЕРЖДАЮ**

Проректор по УР

\_\_\_\_\_ Н.Э.Пфейфер  
« \_\_\_\_ » \_\_\_\_\_ 2010г.

Составители: \_\_\_\_\_ ст. преподаватель, м.и., Глазырина Н.С.

Кафедра «Вычислительная техника и программирование»

### **РАБОЧАЯ УЧЕБНАЯ ПРОГРАММА**

по дисциплине «Основы информационной безопасности»

для студентов специальности 050704 «Вычислительная техника и программное обеспечение» для дневной и заочной формы обучения на базе общего среднего, на базе среднего профессионального образования

Рабочая программа разработана на основании ГОСО РК 5.03.330-2006 050704 и типовой программы специальности и утверждена протокольным решением Республиканского учебно-методического совета высшего и послевузовского образования «22» июня 2006 г.

Рекомендована на заседании кафедры от «\_\_» \_\_\_\_\_ 20\_\_ г.

Протокол № \_\_\_\_ .

Заведующий кафедрой \_\_\_\_\_ О.Г. Потапенко «\_\_» \_\_\_\_\_ 20\_\_ г.  
(подпись)

Одобрена учебно-методическим советом факультета ФМиИТ  
«\_\_» \_\_\_\_\_ 20\_\_ г. Протокол № \_\_\_\_ .

Председатель УМС \_\_\_\_\_ Ж.Г. Муканова «\_\_» \_\_\_\_\_ 20\_\_ г.  
(подпись)

**СОГЛАСОВАНО**

Декан факультета ФМиИТ \_\_\_\_\_ Ж.К.Нурбекова «\_\_» \_\_\_\_\_ 20\_\_ г.  
(подпись)

**ОДОБРЕНО**

Начальник ОПиМОУП \_\_\_\_\_ А.А. Варакута «\_\_» \_\_\_\_\_ 20\_\_ г.  
(подпись)

Одобрена учебно-методическим советом университета  
«\_\_» \_\_\_\_\_ 20\_\_ г. Протокол № \_\_\_\_

**1 Цель дисциплины** – изучение студентами теоретических основ и методов защиты информации, математической структуры секретных систем, рассмотрение математического представления информации, методов анализа информационных характеристик и избыточности языковых систем, теоретических основ коррекции и восстановления информационных характеристик произвольных текстов, построение систем защиты информации, освоение основных методов и средств защиты информации.

**Задачи дисциплины** - изучение и освоение:

- источников и форм атак на информацию;
- моделей безопасности (в том числе, основных операционных систем);
- разновидностей вредоносных программ;
- криптографических и административных методов защиты;
- администрирование корпоративных и локальных сетей, методы защиты сетей и протоколов;
- алгоритмов аутентификации пользователей.

В результате изучения дисциплины студенты должны иметь представление:

- о методах и средствах защиты информации;
- знать:
- определение и основные информационно-статические характеристики языковых систем;
  - математическое представление секретных систем;
  - методы анализа текстов и определение их избыточности;
  - методы построения систем трансформации информационно-статических характеристик текстов;
- уметь:
- практические способы построения систем защиты информации;
  - анализировать тексты и определять их избыточность;
  - разрабатывать системы трансформации информационно-статистических характеристик текстов;
  - разрабатывать системы защиты информации;
  - подбирать и применять методы защиты информации;
  - подбирать и применять средства защиты информации

## **2 Пререквизиты:**

Для освоения данной дисциплины необходимы знания, умения и навыки приобретенные при изучении следующих дисциплин: «Высшая математика: дифференциальное и интегральное исчисления»; «Информатика»; «Программирование на языке высокого уровня (Delphi 6, 7; Borland – Pascal 7.0)»

### 3 Постреквизиты

Знания, умения и навыки, полученные при изучении дисциплины необходимы для освоения следующих дисциплин: «Компьютерные сети»; «Сетевые технологии».

### 4 Содержание дисциплины

#### 4.1 Тематический план дисциплины

##### 4.1.1 Тематический план дисциплины для студентов очной формы обучения на базе ОСО, СПО

№ п/п	Наименование тем дисциплины	Очная на базе среднего обр. 2008				Очная на базе среднего проф. 2009			
		Лек.	Прак.	Лаб.	СРС	Лек.	Прак.	Лаб.	СРС
1	Защита информации	1			4	1			4
2	Безопасность информации	1	4	1	5	1	4	1	5
3	Анализ программной и аппаратной платформы информационных систем	2	2	1	9	2	2	1	9
4	Модели безопасности информационных систем	2	2	1	9	2	2	1	9
5	Примеры практической реализации систем защиты и безопасности	1	2,5	1	9	1	2,5	1	9
6	Основные характеристики защищенной информационной системы	1	4	1	9	1	4	1	9
7	Методология корректности информационной защиты	1	4	1	9	1	4	1	9
8	Мера защиты информации	1	4	1	9	1	4	1	9
9	Оптимальное управление процессами защиты	1		0,5	9	1		0,5	9
10	Оценка системы защиты	2			9	2			9
11	Безопасность компьютерных систем	2			9	2			9
	ИТОГО:	15	22,5	7,5	90	15	22,5	7,5	90

4.1.2 Тематический план дисциплины для студентов заочной формы обучения на базе СПО, ВПО

№ п/п	Наименование тем дисциплины	Заочная на базе среднего проф. 2008				заочная на базе ВПО 2009			
		Лек.	Прак.	Лаб.	СРС	Лек.	Прак.	Лаб.	СРС
1	Защита информации	0,5			9	0,5			9
2	Безопасность информации	0,5	2	0,5	9	0,5	2	0,5	9
3	Анализ программной и аппаратной платформы информационных систем	0,5	1	0,5	10	0,5	1	0,5	10
4	Модели безопасности информационных систем	0,5	2	0,2	10	0,5	2	0,2	10
5	Примеры практической реализации систем защиты и безопасности	1	1	0,3	10	1	1	0,3	10
6	Основные характеристики защищенной информационной системы	0,5	1	0,2	11	0,5	1	0,2	11
7	Методология корректности информационной защиты	0,5	1	0,3	11	0,5	1	0,3	11
8	Мера защиты информации	0,5	1	0,5	10	0,5	1	0,5	10
9	Оптимальное управление процессами защиты	0,5			10	0,5			10
10	Оценка системы защиты	0,5			17	0,5			17
11	Безопасность компьютерных систем	0,5			10	0,5			10
	<b>Итого:</b>	<b>6</b>	<b>9</b>	<b>3</b>	<b>117</b>	<b>6</b>	<b>9</b>	<b>3</b>	<b>117</b>

## 4.2 Содержание тем дисциплины

### Тема 1 Введение. Защита информации

Понятие национальной безопасности. Виды безопасности: государственная, экономическая, общественная, военная, экологическая, информационная. Роль и место системы обеспечения информационной безопасности в системе национальной безопасности. Информационные угрозы. Противодействие информационным угрозам. Характеристические свойства систем защиты информации. Методы защиты информации. Предмет защиты. Средства защиты.

### Тема 2 Безопасность информации

Характеристические свойства систем обеспечения безопасности информации. Методы обеспечения безопасности информации. Средства обеспечения безопасности информации.

Тема 3 Анализ программной и аппаратной платформы информационных систем

Архитектура электронных систем обработки данных. Архитектура программного обеспечения. Системные средства обработки данных. Прикладные средства обработки данных. Аппаратные средства информационной защиты. Программные средства информационной защиты.

### Тема 4 Модели безопасности информационных систем

Формальные модели. Модели безопасности. Политика безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Стандарты по оценке защищенных систем.

### Тема 5 Примеры практической реализации систем защиты и безопасности

Построение парольных систем; особенности применения криптографических методов. Способы реализации криптографической подсистемы; особенности реализации систем с симметричными и несимметричными ключами; способы реализации стенографических систем.

### Тема 6 Основные характеристики защищенной информационной системы

Концепция защищенного ядра. Методы верификации. Защищенные домены. Применение иерархического метода для построения защищенной операционной системы.

### Тема 7 Методология корректности информационной защиты

Исследование корректности систем защиты; методология обследования и проектировании защитных механизмов; модель политики контроля целостности.

### Тема 8 Мера защиты информации

Определение необходимой меры защиты информационных ресурсов; методы оценки меры защиты информации; основные показатели оценки уровня защиты информации; характеристики мер защиты.

### Тема 9 Оптимальное управление процессами защиты

Модели и методы оптимального управления процессами обеспечения безопасности при:

- проектирование аппаратных средств защиты;
- проектирование программных средств защиты;
- проектирование организационных мер защиты.

#### Тема 10 Оценка системы защиты

Комплексная оценка системы защиты информации. Тестирование программного обеспечения. Проблема тестирования программных продуктов, автоматическое тестирование, принципы написания самотестирующихся программных продуктов. Установка тестов в готовые программные продукты. Оценка надежности защитных механизмов. Принципы оценки надежности защиты.

#### Тема 11 Безопасность компьютерных систем

Защита в локальных сетях. Программные средства индивидуальной защиты информации. Использование экспертных систем для распознавания попыток несанкционированного доступа.

### 4.3 Перечень и содержание практических и лабораторных занятий

#### Содержание практических занятий

Тема 2 Математическая структура секретных систем

Тема 3 Теоретическая секретность

Тема 4 Практическая секретность

Тема 5 Классификация защищаемых объектов

Тема 6 Типы информационных ресурсов

Тема 7 Классы защиты информации

Тема 8 Определение необходимой меры защиты по различным критериям оценки степени защиты

Тема 8 Составление модели оптимального управления процессами защиты

#### Содержание лабораторных занятий

Тема 2 Исследование классических систем шифрования

Тема 3 Исследование несимметричных систем шифрования

Тема 4 Разработка программ моделирования оптимального управления защитой

Тема 5 Разработка программ тестирования защитных процедур

Тема 6 Разработка процедур защиты от отладчика и дизассемблера

Тема 7 Исследование и комплексная оценка сложности процедур защиты

Тема 8 Разработка программы определения надежности защиты

Тема 9 Разработка экспертной системы для контроля атаки

#### 4.4 Содержание самостоятельной работы студента

##### 4.4.1 Перечень видов СРС

##### 4.4.1.1 Перечень видов СРС для студентов очной формы обучения на базе ОСО, СПО

Вид СРС	Форма отчёта	Вид контроля	Объём в часах
подготовка к лекционным занятиям		участие на занятии	22,5
подготовка к практическим и лабораторным занятиям, выполнение курсовой работы		допуск к лабораторной работе	22,5
подготовка отчёта и защита всех видов работ	отчёт	защита лабораторной работы	22,5
проработка дополнительных тем, не вошедших в лекционный материал	конспект	семинар	18
подготовка к контрольным мероприятиям		РК1 - тесты, РК2 - тесты, экзамен - тесты	4,5
Всего			90

##### 4.4.1.2 Перечень видов СРС для студентов заочной формы обучения на базе СПО, ВПО

Вид СРО	Форма отчёта	Вид контроля	Объём в часах
подготовка к лекционным занятиям		участие на занятии	25,25
подготовка к практическим и лабораторным занятиям, выполнение курсовой работы		допуск к практ. работе	25,25
подготовка отчёта и защита всех видов работ	отчёт	защита практ. работы	25,25
проработка дополнительных тем, не вошедших в лекционный материал	конспект	семинар	18,4
подготовка к контрольным мероприятиям		РК1 - тесты, РК2 - тесты, экзамен - билеты	4,85
Всего			117

##### 4.4.2 Перечень тем, вынесенных на самостоятельное изучение студентами

1) Роль и место системы защиты и безопасности информации в современном информационном процессе

2) Системы защиты информации. Особенность и основные характеристики



3) Система безопасности информации. Особенности и основные характеристики

4) Структура стандартов в области информационной защиты и безопасности Республики Казахстан

5) Законодательные и нормативные акты Республики Казахстан в области защиты и безопасности информации

#### 4.4.3 Тематика курсовых работ

1) Разработать модель оптимального управления защитой комплекса ЭВМ, связанных локальной сетью на основе операционной системы WINDOWS–95,98, NT,2000.

2) Разработать алгоритм тестирования защитной программы на основе имеющегося исходного текста программы.

3) Дать оценку комплекса защитных процедур сети на основе операционных систем WINDOWS–95,98, NT,2000.

4) Разработать программу для фиксации попыток атаки на защищаемый объект.

### **5 Список основной и дополнительной литературы:**

Основная:

1) Шеннон К. Теория связи в секретных системах/Сб.: «Работы по теории информации в кибернетике». – М.: Иностранная литература, 1963. – С.333-402

2) Диффи У., Хеллман Н.Э. Защищённость и помехостойкость. Введение в криптографию.//ТИИЭР, 1979.-Т.667.-N3.-С.71-109.

3) Симионс Г.Дж. Обзор методов аутентификации информации//ТИИЭР, 1988.-Т.76.-n5.-С.105-125.

4) Борсуков В. Бизнес и безопасность связи//Монитор Аспект, 1993.-N1.-С.56-62.

5) Герасименко В.А. Защита информации в автоматизированных системах. Ч. 1,2. М.: «Высшая школа», 1995.

Дополнительная:

6) Законодательные акты РК в области защиты и безопасности информации.

7) Нормативные документы РК в области защиты и безопасности информации.

8) Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации.-М.: «Яхстмен»,1996.-71 с.

9) Хореев А.А. Способы и средства защиты информации. Учебное пособие.-М.: МО РФ, 2000.- 316 с.

10) Уолкер Б. Дж., Блек Я.Ф. Безопасность ЭВМ и организация их защиты: Пер. с англ.-М.: Связь. 1980.-112 с.



**Выписка из рабочего учебного плана специальности(ей)  
050704 Вычислительная техника и программное обеспечение**

(шифр и полное название специальности(ей))

**Наименование дисциплины Основы информационной безопасности**

Форма обучени я	Трудоемкость дисциплины			Формы контроля по семестрам				Сем естр	Объем работы студентов по семестрам						
	кред итов	академических часов							кред итов	аудиторных занятий (ак. часов)			СРС (ак. часов)		
		всег о	ауд	СРС	экз.	зач.	КП			КР	всег о	лек	пр.	лаб	всего
очная на базе ОСО 2008	3	135	45	90	6			6	3	45	15	22,5	7,5	90	45
очная на базе СПО 2009	3	135	45	90	3			3	3	45	15	22,5	7,5	90	45
заочная на базе СПО 2008	3	135	18	117	6			6	5	6	6				
									6	3	12		9	3	117
заочная на базе ВПО 2009	3	135	18	117	4			4	3	6	6				
									4	3			9	3	117

Заведующий кафедрой \_\_\_\_\_ « \_\_\_\_ » \_\_\_\_\_ 201\_\_ г  
(подпись) (Ф.И.О.)