Титульный лист программы
обучения по дисциплине
(Syllabus)

Форма
Ф СО ПГУ 7.18.3/37

Министерство образования и науки Республики Казахстан

Павлодарский государственный университет им. С. Торайгырова

Факультет физики, математики и информационных технологий

Кафедра «Вычислительная техника и программирование»

ПРОГРАММА ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (Syllabus)

Основы защиты информации

для студентов специальности 050719 – «Радиотехника, электроника и телекоммуникации»

Павлодар

Лист утверждения программы
обучения по дисциплине
(Syllabus)

Форма
Ф СО ПГУ 7.18.3/38

УТВЕРЖДАЮ
Декан факультета ФМиИТ
_____ Ж.К. Нурбекова
«____»_____2010 г.

Составитель: старший преподаватель _____ З.Р. Ахмерова

Кафедра «Вычислительная техника и программирование»

Программа обучения по дисциплине (Syllabus)

«Основы защиты информации»

для студентов очной формы обучения специальности 050719 – «Радиотехника, электроника и телекоммуникации»

Программа разработана на основании рабочей учебной программы, утвержденной « ___» _____ 2010 г.

Рекомендована на заседании кафедры от «____»_____2010 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)

1 Сведения о преподавателе и контактная информация

Фамилия, имя, отчество: Ахмерова Зарема Равильевна

Ученая степень, звание, должность: старший преподаватель

Кафедра «Вычислительная техника и программирование» находится в ГУК по адресу Ломова 64, аудитория 329, контактный телефон 673646.

2 Данные о дисциплине

Название: «Основы защиты информации»

Количество часов – 135.

Курс читается в 6 семестре.

Для студентов на базе общего среднего образования в течение семестра предусмотрено 30 часов лекционных, 15 часов практических и 90 часов самостоятельных занятий.

Место проведения занятий - согласно расписанию.

Форма контроля по дисциплине – экзамен.

3 Трудоемкость дисциплины

Для студентов на базе общего среднего образования

Семестр	Количество кредитов	Количество контактных часов по видам аудиторных занятий				Количество часов самостоятельной работы студента		Формы контроля
		всего	лекции	практические	лабораторные	всего	СРСП	
6	3	135	30	15	н/п	90	45	Экзамен
Всего		135	30	15	н/п	90	45	

4 Цель и задачи дисциплины

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, администрирования корпоративных и локальных сетей, методов защиты сетей и протоколов, алгоритмов аутентификации пользователей.

5 Требования к знаниям, умениям и навыкам

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 определения их избыточности, методы построения систем трансформации информационно-статических характеристик текстов, практические способы построения систем защиты информации. Также в результате изучения дисциплины студенты должны уметь анализировать тексты и определять их избыточность, разрабатывать системы трансформации информационно-статистических характеристик текстов, разрабатывать системы защиты информации, подбирать и применять методы защиты информации.

6 Пререквизиты

Для освоения данной дисциплины необходимы знания, умения и навыки приобретенные при изучении следующих дисциплин: «Информатика (базовый курс)», «Высшая математика».

7 Постреквизиты

Знания, умения и навыки, полученные при изучении дисциплины необходимы для освоения дисциплины «Основы преобразовательных устройств и информационная безопасность», а также в процессе дипломного проектирования.

8 Тематический план

№ п/п	Наименование тем дисциплины	Очная на базе ОСО 2008		
		Лек.	Прак	СРС
		6 семестр		
1	Введение. Защита информации	2	0	4
2	Безопасность информации	2	2	5
3	Анализ программной и аппаратной платформы информационных систем	3	2	9
4	Модели безопасности информационных систем	4	2	9
5	Примеры практической реализации систем защиты и безопасности	3	4	9
6	Основные характеристики защищенной информационной системы	2	2	9
7	Методология корректности информационной защиты	2	2	9
8	Мера защиты информации	2	1	9
9	Оптимальное управление процессами защиты	2	0	9
10	Оценка системы защиты	4	0	9

11	Безопасность компьютерных систем	4	0	9
	ИТОГО:	30	15	90

9 Краткое описание дисциплины

Защита информации в современных условиях становится все более сложной проблемой, что обусловлено рядом обстоятельств, основными из которых являются: массовое распространение средств электронной вычислительной техники (ЭВТ); усложнение шифровальных технологий; необходимость защиты не только государственной и военной тайны, но и промышленной, коммерческой и финансовой тайн; расширяющиеся возможности несанкционированных действий над информацией.

Кроме того, в настоящее время получили широкое распространение средства и методы несанкционированного и негласного добывания информации.

Необходимо помнить, что естественные каналы утечки информации образуются спонтанно, в силу специфических обстоятельств, сложившихся на объекте защиты.

Что касается искусственных каналов утечки информации, то они создаются преднамеренно с применением активных методов и способов получения информации. Активные способы предполагают намеренное создание технического канала утечки информации с использованием специальных технических средств. К ним можно отнести незаконное подключение к каналам, проводам и линиям связи, высокочастотное навязывание и облучение, установка в технических средствах и помещениях микрофонов и телефонных закладных устройств, а также несанкционированный доступ к информации, обрабатываемой в автоматизированных системах (АС) и т.д.

Поэтому особую роль и место в деятельности по защите информации занимают мероприятия по созданию комплексной защиты

Таким образом, проблема защиты информации и обеспечения конфиденциальности приобретает актуальность.

10 Компоненты курса

10.1 Перечень тем лекционных занятий

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:

- проектировании аппаратных средств защиты;
- проектировании программных средств защиты;
- проектировании 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. Инсталляция 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.

10.2 Перечень тем практических занятий

1) Тема 2. Математическая структура секретных систем
2) Тема 3. Теоретическая секретность
3) Тема 4. Моделирование оптимального управления защитой
4) Тема 5. Исследование классических систем шифрования
5) Тема 5. Исследование несимметричных систем шифрования
6) Тема 6. Определение необходимой меры защиты по различным критериям оценки степени защиты
7) Темы 7, 8. Разработка экспертной системы для контроля атаки

10.3 Содержание самостоятельной работы студентов

Перечень видов СРС для студентов на базе ОСО

Вид СРС	Форма отчетности	Вид контроля	Объем в часах
Подготовка к лекционным занятиям		участие на занятии	20
Подготовка к практическим занятиям, выполнение домашних заданий	рабочая тетрадь	участие на занятии	25
Подготовка отчета и защита всех видов работ	отчет	защита практической работы	20
Проработка дополнительных тем, не вошедших в лекционный материал	конспект	семинар	20
Подготовка к контрольным мероприятиям		РК1 - тесты, РК2 - тесты, экзамен – тесты, билеты	5
Всего			90

10.4 Календарный график контрольных мероприятий текущей успеваемости для студентов на базе ОСО

1 рейтинг (6 семестр)												
Недели		Макс. балл за 1 занятие	1	2	3	4	5	6	7	8	Всего
Максимальный балл			13		37		28		22		100
Посещение и подготовка к лекциям	Вид СРС/форма отчетн.		ДЗЛ 1,2		ДЗЛ 3,4		ДЗЛ 5,6		ДЗЛ 7,8		16
	Форма контроля		У		У		У		У		
	Макс. балл	2	4		4		4		4		
Посещение и подготовка к практическим занятиям	Вид СРС/форма отчетн.		ДЗП1,2,3		ДЗП4,5,6		ДЗП7,8,9		ДЗП10,11,12		32
	Форма контроля		У		У		У		У		
	Макс. балл	4	8		8		8		8		
Оформление и защита практических работ	Вид СРС/форма отчетн.			О		О		О		О	8
	Форма контроля			ЗЛ1		ЗЛ2		ЗЛ3		ЗЛ4	
	Макс. балл	1	2		2		2		2		
Самостоятельное изучение материала	Вид СРС/форма отчетн.					ДЗ СИ1		ДЗ СИ2			20
	Форма контроля					К		К			
	Макс. балл					10		10			
Контроль знаний по темам дисциплины	Вид СРС/форма отчетн.				ПТД			ПДТ			24
	Форма контроля				Т1			Т2			
	Макс. балл				12			12			
2 рейтинг (6 семестр)											
Недели		Макс. балл за 1 занятие	1	2	3	4	5	6	7		Всего
Максимальный балл			13		38		28		21		100
Посещение и подготовка к лекциям	Вид СРС/форма отчетн.		ДЗЛ 1,2		ДЗЛ 3,4		ДЗЛ 5,6		ДЗЛ 7		14
	Форма контроля		У		У		У		У		
	Макс. балл	2	4		4		4		2		
Посещение и подготовка к практическим занятиям	Вид СРС/форма отчетн.		ДЗП1,2,3		ДЗП4,5,6		ДЗП7,8,9		ДЗП10,11		28
	Форма контроля		У		У		У		У		
	Макс. балл	4	8		8		8		4		
Оформление и защита практических работ	Вид СРС/форма отчетн.			О		О		О	О		7
	Форма контроля			ЗЛ1		ЗЛ2		ЗЛ3	ЗЛ4		
	Макс. балл	1	2		2		2		1		
Самостоятельное изучение материала	Вид СРС/форма отчетн.					ДЗ СИ1		ДЗ СИ2			23
	Форма контроля					К		К			
	Макс. балл					11		12			
Контроль знаний по темам дисциплины	Вид СРС/форма отчетн.				ПТД			ПДТ			28
	Форма контроля				Т1			Т2			
	Макс. балл				14			14			

Условные обозначения: ДЗЛ 1 – домашнее задание на подготовку к лекциям №1; У –участие в учебном процессе; ДЗП 1 – домашнее задание на подготовку к практическим занятиям №1; ДЗлаб 1 – домашнее задание на подготовку к лабораторным занятиям №1; Д- допуск; О – отчет; ЗЛ1 - защита лабораторной работы №1; РКР1 – раздел №1 курсовой работы; П – проверка; ДЗСИ1 – домашнее задание №1 на самостоятельное изучение материала; К- коллоквиум; Е1 – тест №1.

Методика расчета итогового рейтинга по дисциплине:

Итоговый контроль по дисциплине, в соответствии с рабочим учебным планом, предусмотрен в виде экзамена и курсовой работы. Итоговый рейтинг

по дисциплине в баллах определяется по формуле:

$$И = РД \cdot ВД_{РД} + ИК \cdot ВД_{ИК},$$

где РД – рейтинг допуск, т. е. баллы, набранные по итогам первого и второго рейтинга,

ИК – соответственно баллы, набранные на экзамене, определяемые по 100-бальной шкале;

ВДРД, ВДИК – весовые доли текущей успеваемости в течение семестра и видов итогового контроля в итоговом рейтинге по дисциплине.

$$РД = ((Р1 + Р2) * 0,7) / 2 + КР * 0,3$$
$$Р1(2) = ТУ1(2) * 0,7 + РК1(2) * 0,3$$

где Р1 и Р2 – баллы, набранные по итогам первого и второго рейтинга,
КР – баллы, набранные за курсовую работу,
ТУ – итоговые оценки текущей успеваемости,
РК – баллы, набранные во время рубежного контроля.

Весовые доли по видам итогового контроля и текущей успеваемости

№ п/п	Вид итогового контроля	Вид контроля	Весовые доли
1	Экзамен (зачет)	Экзамен (зачет)	0,4
		Контроль текущей успеваемости	0,6

Итоговый рейтинг по дисциплине в баллах (И), в соответствии со шкалой оценки знаний обучающихся, переводится в цифровой эквивалент, буквенную и традиционную оценку и вносится в «Журнал учебных достижений обучающихся» и «Рейтинговую ведомость».

Шкала оценки знаний обучающихся

Итоговая оценка в баллах (И)	Цифровой эквивалент баллов (Ц)	Оценка в буквенной системе	Оценка по традиционной системе	
			Экзамен, диф. зачет	Зачет
95-100	4,00	A	Отлично	Зачтено
90-94	3,67	A-		
85-89	3,33	B+	Хорошо	
80-84	3,00	B		
75-79	2,67	B-		
70-74	2,33	C+	Удовлетворительно	
65-69	2,00	C		
60-64	1,67	C-		
55-59	1,33	D+		

50-54	1,00	D		
0-49	0,00	F	Неудовлетворительно	Не зачтено

В ведомость промежуточной аттестации по дисциплине и зачетную книжку студента проставляется итоговая оценка в традиционной форме.

Если обучающийся получил на экзамене оценку F, то его итоговый рейтинг по дисциплине не определяется, а в ведомости заносится оценка «неудовлетворительно».

11 Политика курса

Каждый студент должен посещать все виды занятий, активно участвовать в обсуждениях и работе группы. Опоздания на любые виды аудиторных занятий мешают их нормальному проведению, поэтому опоздавшие более чем на 10 минут, не отмечаются как присутствующие на занятиях. Любые нарушения правил поведения на занятиях будут наказываться, вплоть до удаления из аудитории, а активная работа – поощряться.

За неоднократное демонстративное невыполнение заданий, неучастие в тестах или занятиях предусмотрены штрафные санкции в виде вычитания баллов, количество которых равно числу баллов, установленных по данному виду занятий.

Подготовка к каждому занятию обязательна, также как прочтение всего заданного материала. Она будет проверяться опросами во время практических занятий и тестами после изучения соответствующего раздела дисциплины (рубежный контроль - РК).

В семестре предусмотрено проведение рубежного контроля в виде тестирования по пройденному материалу из соответствующих разделов дисциплины.

При отсутствии студента во время проведения контрольного мероприятия по какой-либо причине его повторное проведение специально для пропустившего не предусмотрено.

В семестре предусмотрено два рубежных контроля по пройденному материалу соответствующих разделов дисциплины.

12 Список литературы

Основная:

1) Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос; ПБОЮЛ Н.А. Егоров, 2001.

2) Скляров Д.В. Искусство защиты и взлома информации. — СПб.: БХВ-Петербург, 2004.

3) Жельников В. Криптография от папируса до компьютера. – М.: Dore Print, 1999.

4) Сёмкин С.Н., Беляков Э.В., Гребенёв С.В., Козачёк В.И. Основы организационного обеспечения информационной безопасности объектов информатизации. – М.: «Гелиос АРВ», 2005.

5) Саломаа А. Криптография с открытым ключом: Пер. с англ. — М.: Мир, 1995.

6) Хорошко В.А.. Чекатков. Методы и средства защиты информации. — Вінниця: ВДТУ, 2003.

Дополнительная:

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

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

9) Грушко А.А., Тимонина Е.Е. Теоретические основы защиты информации.-М.: «Яхстмен»,1996.

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