МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования
«Оренбургский государственный университет»

Кафедра программного обеспечения вычислительной техники и автоматизированных систем

УТВЕРЖДАЮ
Проректор по учебно-методической работе
Т.П. Петухова
(подпись, расшифровка подписи)
“____”_____2011 г

РАБОЧАЯ ПРОГРАММА

УЧЕБНОЙ ДИСЦИПЛИНЫ

«БЕЗОПАСНОСТЬ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ»

Направление подготовки
231000.68 Программная инженерия
(код и наименование направления подготовки)

Профиль подготовки
Разработка программно-информационных систем
(наименование профиля подготовки)

Квалификация (степень) выпускника
Магистр

Форма обучения
Очная

Оренбург 2011

Рецензент:
старший преподаватель кафедры вычислительной техники,
кандидат технических наук Кручинин Александр Юрьевич.

Рабочая программа дисциплины «Безопасность информационно-телекоммуникационных систем» /сост.А.С. Цыганков – Оренбург: ОГУ, 2011. - 15 с.

Рабочая программа предназначена для преподавания дисциплины вариативной части профессионального цикла студентам очной формы обучения по направлению подготовки 231000.68 Программная инженерия в 3 семестре.

Рабочая программа составлена с учетом Федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 231000.68 Программная инженерия, утвержденного приказом Министерства образования и науки Российской Федерации от "9" ноября 2009 г. № 542.

Составитель _____ А.С. Цыганков
(подпись)
10.10.2011 г.

© Цыганков А.С., 2011
© ОГУ, 2011

Содержание

1 Цели и задачи освоения дисциплины 4
2 Место дисциплины в структуре ООП ВПО 4
3 Требования к результатам освоения содержания дисциплины 4
4 Содержание и структура дисциплины 6
4.1 Содержание разделов дисциплины 6
4.2 Структура дисциплины 7
4.3 Лабораторные работы 7
4.4 Курсовая работа 8
4.5 Самостоятельное изучение разделов дисциплины 9
5 Образовательные технологии 9
5.1 Интерактивные образовательные технологии, используемые в аудиторных занятиях 9
6 Оценочные средства для текущего контроля успеваемости и промежуточной аттестации 10
7 Учебно-методическое обеспечение дисциплины 12
7.1 Основная литература 12
7.2 Дополнительная литература 12
7.3 Периодические издания 12
7.4 Интернет-ресурсы 12
7.5 Программное обеспечение современных информационно-коммуникационных технологий 13
8 Материально-техническое обеспечение дисциплины 14
Лист согласования рабочей программы дисциплины 14

1 Цели и задачи освоения дисциплины

Цели освоения дисциплины

Основная цель курса «Безопасность информационно - телекоммуникационных систем» заключается в систематическом рассмотрении теории защиты компьютерной информации, а так же основных принципов, методов и алгоритмов обеспечения информационной безопасности информационно-телекоммуникационных систем.

Задачи курса:

- раскрыть основные принципы обеспечения информационной безопасности информационно-телекоммуникационных систем;
- сформировать компетентности в области информационной безопасности;
- обучить студентов проектировать и разрабатывать программное обеспечение, обеспечивающее информационную безопасность существующих систем.
- ознакомить с современными тенденциями в области защиты информации(в том числе и криптографией).

2 Место дисциплины в структуре ООП ВПО

Дисциплина относится к вариативной части учебного цикла – М2 профессиональный цикл.

Изучение дисциплины требует базовой подготовки в объеме рабочих программ дисциплин «Информатика и программирование», «Теория вероятностей и математическая статистика», «Операционные системы и сети»

Знания, умения и навыки, приобретенные при изучении данной дисциплины, используются студентами в дисциплинах «Разработка и реализация сетевых протоколов», «Автоматизация и проектирование информационно-телекоммуникационных систем», а так же в дипломном проектировании.

3 Требования к результатам освоения содержания дисциплины

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВПО и ООП ВПО по данному направлению подготовки:

а) общекультурных (ОК):

- владение культурой мышления, способность к обобщению, анализу, восприятию информации, постановке цели и выбору путей её достижения (ОК-1);
- готовность использовать основные законы естественнонаучных дисциплин в профессиональной деятельности, применять методы математического анализа и моделирования, теоретического и экспериментального исследования (ОК-10).

б) профессиональных (ПК):

- умение отбирать и разрабатывать методы исследования объектов профессиональной деятельности на основе общих тенденций развития программной инженерии (ПК-1);

- умение проводить анализ, синтез, оптимизацию решений с целью обеспечения качества объектов профессиональной деятельности (ПК-2);

- умение выполнять оценки степени трудности, рисков, бюджета и времени в течение выполнения проекта, осуществлять контроль рабочего времени (ПК-5);

- способность рассчитывать и оценивать условия и последствия принимаемых организационно – технических решений (ПК-14).

В результате освоения дисциплины обучающийся должен:

Знать:

- математические основы криптографических методов защиты информации;

- способы обеспечения информационной безопасности информационно – телекоммуникационных систем;

- принципы функционирования основных программно-аппаратных средств обеспечения информационной безопасности.

Уметь:

- самостоятельно формировать рекомендации по обеспечению безопасности информационно-телекоммуникационных систем;

- реализовывать криптографические методы защиты компьютерной информации;

- конфигурировать основные средства защиты информации.

Владеть:

- стандартной терминологией и положениями теории защиты информации и информационной безопасности

- методологией оценки рисков нарушения безопасности информационно-телекоммуникационных систем.

Приобрести опыт деятельности:

разработки программного обеспечения для обеспечения безопасности информационно-телекоммуникационных систем.

4 Содержание и структура дисциплины

4.1 Содержание разделов дисциплины

№ раздела	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Введение	Законодательство РФ в области защиты информации. Основные понятия и определения. Современные тенденции в области обеспечения и нарушения информационной безопасности. Классификация криптографических методов.	Т
2	Математические основы криптографии	Арифметика остатков. Расширенный алгоритм Евклида. Теорема Лагранжа. Китайская теорема об остатках. Поиск простых чисел	ЛР, Т
3	Вычислительная сложность	Основы теории вычислительной сложности. Оценка сложность алгоритмов. Машина Тьюринга. P и NP - задачи. Односторонние функции.	Т
4	Криптография	Стеганография. Потоковые шифры. Симметричные шифры. Ассиметричные шифры. Шифры замены и перестановки. Хэширование паролей. Цифровая подпись.	ЛР
5	Средства защиты информации	Антивирусы. Межсетевые экраны. VPN. Системы обнаружения вторжений.	ЛР
6	Протоколы защиты информации	Протоколы аутентификации. Протоколы обмена ключами. Шифрование сетевого трафика. Анализ протоколов распределения ключей. BAN –логика.	Т
6	Модели безопасности операционных систем	Избирательная модель. Изолированная среда. Полномочная модель. Системы управления средствами защиты информации. Анализ рисков. Защита программного обеспечения.	Т

4.2 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы (144 часа)

Вид работы	Трудоемкость, часов	
	3 семестр	Всего
Общая трудоемкость	**144**	**144**
Аудиторная работа:	**39**	**39**
Лекции (Л)	13	13
Практические занятия (ПЗ)		
Лабораторные работы (ЛР)	26	26
Самостоятельная работа:	**78**	**78**
Курсовой проект (КП), курсовая работа (КР)	52	52
Расчетно-графическое задание (РГЗ)		
Реферат (Р)		
Эссе (Э)		
Самостоятельное изучение разделов	8	8
Контрольная работа (К)		
Самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам, рубежному контролю и т.д.).	10	10
Подготовка и сдача экзамена	8	8
Вид итогового контроля (зачет, экзамен)	экзамен	

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	2	3	4
1	4	Стеганография.	2
2	2	Поиск 10-ти значных простых чисел	4
3	4	Шифры замены и перестановки	4
4	4	Симметричные шифры	4
5	4	Ассиметричные шифры	4
6	5	Анализ сетевого трафика	4
7	5,4	VPN	4

4.4 Курсовая работа

Тема курсовой работы: «Повышение информационно безопасности электронного документооборота».

Цель курсовой работы:

- закрепление теоретических знаний в области защиты компьютерной информации;
- формирование практических умений и навыков разработки программного обеспечения для защиты информационно-телекоммуникационных систем;
- закрепление практических навыков самостоятельного решения инженерных задач, развитие творческих способностей студентов и умений пользоваться технической, нормативной и справочной литературой.

Постановка задачи к курсовой работе

Разработать программное средство, предназначенное для защиты электронного документооборота, в соответствии с индивидуальным вариантом .Программное средство должно состоять из двух частей - серверной и клиентской.
Функции клиентской части:

1) Реализовать запрос к серверу для получения сеансовых ключей.
2) Осуществлять шифрование электронных документов, передаваемых по локальной сети ассиметричным методом с помощью полученных от сервера сеансовых ключей.

Функции серверной части:

1) Реализация протокола распределения ключей
2) Генерация сеансовых ключей.

Требования к содержанию курсовой работы

Курсовая работа должна иметь следующую структуру и состоять из разделов.

Введение
1 Постановка задачи
2 Анализ криптографических методов защиты информации
2.1 Анализ симметричных методов
2.2 Анализ ассиметричных методов
3 Спецификация протокола распределения ключей
4 Спецификация разработанного протокола обмена сообщениями
5 Разработка алгоритмов криптографических методов
6 Установка и эксплуатация программного средства
7 Руководство пользователя
Заключение
Список использованных источников
Приложение А – Текст программы
Приложение Б – Контрольный пример

Индивидуальные варианты заданий

1 Протокол Нидхейма - Шредера. DES (режим CBC), RSA
2 Протокол Нидхейма - Шредера. DES (режим OFB), RSA
3 Протокол Нидхейма - Шредера. DES (режим ECB), RSA
4 Протокол Нидхейма - Шредера. DES (режим CFB), RSA
5 Протокол Широкоротой лягушки. DES (режим CBC), RSA
6 Протокол Широкоротой лягушки. DES (режим OFB), RSA
7 Протокол Широкоротой лягушки. DES (режим ECB), RSA
8 Протокол Широкоротой лягушки. DES (режим CFB), RSA
9 Протокол Цербер. DES (режим CBC), RSA
10 Протокол Цербер. DES (режим OFB), RSA
11 Протокол Цербер. DES (режим ECB), RSA
12 Протокол Цербер. DES (режим CFB), RSA
13 Протокол Отвей - Рииса. DES (режим CBC), RSA
14 Протокол Отвей - Рииса. DES (режим OFB), RSA
15 Протокол Отвей - Рииса. DES (режим ECB), RSA
16 Протокол Отвей - Рииса. DES (режим CFB), RSA

4.5 Самостоятельное изучение разделов дисциплины

№ раздела	Вопросы, выносимые на самостоятельное изучение	Кол-во часов
1	2	3
4	Отечественные достижения в области криптографии	4
5	Средства прослушивания сетевого трафика.	4

5 Образовательные технологии

5.1 Интерактивные образовательные технологии, используемые в аудиторных занятиях

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
3	Л	Проблемные лекции, лекции-визуализации, мастер-класс	10
	ЛР	Ролевые игры	10
Итого:			20

6 Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Перечень вопросов к экзамену

1. Законодательство Российской Федерации в области защиты информации.
2. Криптография. Основные понятия.
3. Стеганогра́фия.
4. Шифры замены.
5. Шифры перестановки.
6. Классификация криптоалгоритмов.
7. БЛОЧНЫЕ ШИФРЫ. Сеть Фейштеля.
8. Шифр DES.
9. Режимы шифра DES.
10. Потоковые шифры. Скремблеры.
11. Арифметика остатков. Группы и кольца. Функция Эйлера. Малая теорема Ферма.
12. Алгоритм Евклида, расширенный алгоритм Евклида.
13. Ассиметричные криптоалгоритмы.
14. Алгоритм RSA.
15. Алгоритмы возведения в степень
16. Нахождение простых чисел.
17. Технологии цифровых подписей.
18. Цифровые сертификаты.
19. Управление симметричными ключами. Распределение симметричных ключей.
20. Протокол широкоротой лягушки
21. Протокол Нидхейма-Шредера
22. Протокол Отвей-Рииса
23. Алгоритм Цербер
24. Хеширование паролей.
25. Классификация угроз ИС.
26. Уровни сетевых атак согласно модели OSI.
27. Технологии межсетевого экранирования.
28. Назначение заголовков сетевых пакетов (Протоколы IP, TCP, UDP, ICMP)
29. Вирусы, черви, трояны.
30. Антивирусные механизмы.
31. Технологии VPN.
32. Протоколы аутентификации.
33. Защита ПО
34. Модели безопасности информационных систем.

Образцы тестов для проведения текущего контроля

1 Какие из перечисленных ниже алгоритмов не являются симметричными?
а) Подстановочные шифры;
б) Перестановочные шифры;
в) Шифры гаммирования;
г) Блочные шифры;
д) Поточные шифры исключений.

2 Какую длину имеет секретный ключ в криптосистеме DES?
а) 16бит;
б) 32 бита
в) 64 бита;
г) 128бит;
д).256 бит.

3.Сетевые черви -это:
а) Вредоносные программы, устанавливающие скрытно от пользователя другие вредоносные программы и утилиты
б) Вирусы, которые проникнув на компьютер, блокируют работу сети;
в) Вирусы, которые внедряются в документы под видом макросов;
г) Утилиты управляющие удаленным доступом компьютера;
д) Вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей.

4 К биометрической системе защиты относятся**:**
а) Защита паролем;
б) Физическая защита данных;
в) Антивирусная защита;
г) Идентификация по радужной оболочке глаз;
д) Защита PIN-кодом.

5 Вирус внедряется в исполняемые файлы и при их запуске активируется. Это...:
а) Загрузочный вирус;
б) Макровирус;
в) Файловый вирус;
г) Сетевой червь;
д) Троян.

6 Выделите три наиболее важных метода защиты информации от нелегального доступа:
а) Использование антивирусных программ;
б) Архивирование (создание резервных копий);
в) Использование специальных «электронных ключей»;
г) Установление паролей на доступ к информации;

д) Шифрование.

7 Основными математическими задачами, лежащими в основе асимметричных криптосистем, являются:

а) Задача поиска «больших» простых чисел;

б) Задача поиска неприводимых многочленов в поле Галуа;

в) Задача дискретного логарифмирования;

г) Задача факторизации;

д) Задача вычисления значения функции Эйлера.

8 Показателями безопасности информации являются::

а) вероятность предотвращения угрозы;

б) время, необходимое на взлом защиты информации;

в) время, в течение которого обеспечивается определённый уровень безопасности;

г) вероятность возникновения угрозы информационной безопасности;

д) интенсивность потока информационных атак.

7 Учебно-методическое обеспечение дисциплины

7.1 Основная литература

1 Торстейнсон, П.. Криптография и безопасность в технологии . NET/ П. Торстейнсон, Г. А. Ганеш; пер. с англ. В. Д. Хорева ; под ред. С. М. Молявко. - М. : Бином, 2007. - 480 с.

2 Смарт, Н. Криптография / Н. Смарт; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. - Москва: Техносфера, 2006. - 528 с.

3 Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства: учеб. пособие для студентов вузов, обучающихся по направлению 230100 "Информатика и вычислительная техника" / В. Ф. Шаньгин. - М. : ДМК Пресс, 2008. - 544 с.

4 Семененко, В. А. Программно-аппаратная защита информации: учеб. пособие для вузов / В. А. Семененко, Н. В. Федоров. - М. : МГИУ, 2007. - 340 с.

7.2 Дополнительная литература

1. Бернет, С.. Криптография. Официальное руководство RSA Security = RSA Security's Official Guide to Cryptography / С. Бернет, С. Пэйн ; пер. с англ. под ред. А. И. Тихонова. - М. : Бином, 2009. - 382 с.

2 Лукацкий, А. Обнаружение атак/ А. Лукацкий . - СПб. [и др.] : БХВ - Санкт-Петербург, 2001. - 624 с.

7.3 Периодические издания

– «Программирование»;

– «Программные продукты и системы»;

– «Информационные технологии».

7.4 Интернет-ресурсы

Образовательные порталы:
• Интернет университет информационных технологий: http://www.intuit.ru/
• Все образование в Интернете http://all.edu.ru/
• Сервер Центра информатизации Министерства общего и профессионального образования Информика http://www.informika.ru/

Виртуальные учебные курсы и сайты дистанционного образования:
• Дистанционное образование в Интернете http://www.lessons.ru/
• Центр дистанционного образования http://www.eidos.ru/
• Центр дистанционного обучения http://www.cdo.ru/

Энциклопедии и справочные сайты:
• Море аналитической информации http://www.citforum.ru
• RSDN-magazine http://rsdn.ru/

7.5 Программное обеспечение современных информационно-коммуникационных технологий

Программное обеспечение по видам занятий:
- операционные системы Windows XP/7;
- языки программирования C++, C#
- среды программирование MS Visual Studio 2010, NetBeans, Eclipse.

8 Материально-техническое обеспечение дисциплины

Занятия по дисциплине проводятся в аудиториях, оснащенных компьютерными и мультимедийными средствами.

Лекционные занятия проводятся в аудитории № 14419, имеющей материально-техническое обеспечение:

- компьютер модели Intel Celeron-S -1шт.;
- монитор модели Samsung 793 DF – 1шт.;
- экран настенный стационарный – 1шт.;
- проектор модели Viewsonic PJ510 – 1шт.;
- источник бесперебойного питания – 1шт.;
- сервер модели Intel Xeon – 1шт.;
- сервер модели 2x DualCore AMD Opteron 2218 – 1шт.

Лабораторные работы и практические занятия проводятся в компьютерных классах кафедры ПОВТАС – ауд. №№ 14406 (а, б), 14422, 14423, 14424.

В компьютерных классах установлено оборудование:

- системные блоки модели Intel Celeron – 10шт.;
- мониторы модели Samsung 793 DF – 10шт.;
- принтер лазерный модели Canon LBP-3000 – 1шт.;
- проектор модели NEC PORTABLE PROJEKTOR VT46/G – 1шт.;
- экран настенный стационарный – 1шт.;
- источник бесперебойного питания – 10шт.

ЛИСТ
согласования рабочей программы дисциплины

Направление подготовки: 231000.62 Программная инженерия
Шифр и наименование

Профиль подготовки: Разработка программно-информационных систем
Шифр и наименование

Дисциплина: Безопасность информационно-телекоммуникационных систем

Форма обучения: очная
(очная, очно-заочная, заочная)

Учебный год 2011/2012

РЕКОМЕНДОВАНА на заседании кафедры ПОВТАС
наименование кафедры

протокол № ____от "___" _____ 20__г.

Ответственный исполнитель, заведующий кафедрой

ПОВТАС		Н.А. Соловьев	
наименование кафедры	*подпись*	*расшифровка подписи*	*дата*

Исполнители:

доцент		А.С. Цыганков	
должность	*подпись*	*расшифровка подписи*	*дата*
должность	*подпись*	*расшифровка подписи*	*дата*

ОДОБРЕНА на заседании методической комиссии, протокол № ___ от "___" _____ 20__ г.",

Председатель методической комиссии по направлению подготовки

231000.62 Программная инженерия		Н.А. Соловьев	
шифр наименование	*личная подпись*	*расшифровка подписи*	*дата*

СОГЛАСОВАНО:

Заведующий кафедрой _____
наименование кафедры личная подпись расшифровка подписи дата

Заведующий кафедрой _____
наименование кафедры личная подпись расшифровка подписи дата

Заведующий отделом комплектования научной библиотеки

	И.В. Пащенко	
личная подпись	*расшифровка подписи*	*дата*

Декан Факультета информационных технологий _____ А.М. Пищухин
наименование факультета (института) личная подпись расшифровка подписи дата

Рабочая программа зарегистрирована в УСИТО под учетным номером ____ на правах учебно-методического электронного издания.

Начальник УСИТО _____ Е.В. Дырдина
личная подпись расшифровка подписи дата