ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет автоматики и вычислительной техники

"УТВЕРЖДАЮ"

Декан АВТФ

профессор, д.т.н. Гужов Владимир Иванович

"___"_____ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Технология построения защищенных систем

ООП: специальность 090104.65 Комплексная защита объектов информатизации

Шифр по учебному плану: ОПД.В.1.1

Факультет: автоматики и вычислительной техники очная форма обучения

Курс: 5, семестр: 9

Лекции: 34

Практические работы: - Лабораторные работы: 16

Курсовой проект: - Курсовая работа: - РГЗ: 9

Самостоятельная работа: 50

Экзамен: 9 Зачет: -

Всего: 100

Новосибирск

2011

Рабочая программа составлена на основании Государственного образовательного стандарта высшего профессионального образования по направлению (специальности): 075400 Комплексная защита объектов информатизации.(№ 331 инф/сп от 14.04.2000)

ОПД.В.1.1, дисциплины по выбору студента

Рабочая программа обсуждена на заседании кафедры Защита информации протокол № от

Программу разработал

старший преподаватель, Крюков Юрий Дмитриевич

Заведующий кафедрой

с.н.с., к.т.н. Трушин Виктор Александрович

Ответственный за основную образовательную программу

с.н.с., к.т.н. Трушин Виктор Александрович

1. Внешние требования

Таблица 1.1

Шифр дисциплины	Содержание учебной дисциплины	Часы
	Понятие сложной системы: элементы и подсистемы, управление и информация, самоорганизация; основные принципы системного подхода при создании сложных систем; понятие качества и эффективности: характеристики качества, показатели и критерии эффективности, методические вопросы оценки эффективности сложных систем; функциональная и обеспечивающая часть сложной системы; технология функционирования сложной системы; цели и задачи проектировании; структуризация предметной области; классификация объектов проектирования; жизненный цикл автоматизированной системы; этапы проектирования системы; организация работ, функции заказчиков и разработчиков; практические методы реализации моделей безопасности; ядра безопасности; мониторинг взаимодействий в системе; архитектура защищенных систем; принципы построения защищенных информационных систем; технологический цикл реализации защищенной системы обработки и хранения информации; реализация систем контроля доступа; способы представления информации о правах доступа.	**100**

2. Особенности (принципы) построения дисциплины

Таблица 2.1

Особенности (принципы) построения дисциплины

Особенность (принцип)	Содержание
Основания для введения дисциплины в учебный план по направлению или специальности	Дисциплина относится к циклу дисциплин федерального компонента, включенных в учебный план подготовки специалистов по защите ин-формации по специальности 090104 . Основанием для введения в учебный план являются требования ГОС.
Адресат курса	Дисциплина преподается на кафедре ЗИ и предназначена для сту-дентов, обучающихся по специальности 090104
Основная цель (цели) дисциплины	Цель дисциплины "Технология построения защищённых автоматизированных систем" - заложить фундамент комплексного подхода к решению задач построения защищённых автоматизированных систем, научить правильно проводить комплексный анализ автоматизированных систем, организовывать поэтапное внедрение проектируемых автоматизированных систем с обеспечением информационной безопасности, приобрести навыки анализа угроз информационной безопасности, знать основные общеметодологические принципы создания комплексных систем обеспечения информационной безопасности; изучение

	методов и средств проектирования систем обеспечения информационной безопасности, методов оценки качества систем и моделей информационной безопасности.
Ядро дисциплины	
Связи с другими учебными дисциплинами основной образовательной программы	
Требования к первоначальному уровню подготовки обучающихся	Для изучения дисциплины студенты должны иметь представление и ознакомиться с основными стандартами, необходимыми для построения защищенных автоматизированных систем; должны иметь представление о государственной политике в области защиты информации в автоматизированных системах и о системах оценок защищенности автоматизированных систем.
Особенности организации учебного процесса по дисциплине	

3. Цели учебной дисциплины

Таблица 3.1

После изучения дисциплины студент будет

знать	
1	- технологию построения защищенных автоматизированных систем; - методы оценок защищенности автоматизированных систем; - основные положения РД ФСТЭК (Гостехкомиссии) России; - основные положения стандартов информационной безопасности;
уметь	
2	- работать на современных ПЭВМ на уровне пользователя под управлением основных операционных систем; - оценивать защищенность автоматизированных систем; - анализировать риски в автоматизированных системах.

4. Содержание и структура учебной дисциплины

Лекционные занятия

Таблица 4.1

(Модуль), дидактическая единица, тема	Часы	Ссылки на цели
Семестр: 9		
Введение в теорию информационных систем. Основные определения.	2	
Понятие сложной информационной системы. Цели и задачи построения информационной системы. Состав сложной информационной системы, элементы и подсистемы, управление элементами системы и оценка информации. Самоорганизация ИС.	2	
Системный подход при создании ИС. Характеристики ИС, понятие качества и эффективности ИС. Характеристики качества ИС, критерии и показатели эффективности. Методические вопросы оценки эффективности сложных систем. Функциональная и обеспечивающая часть сложной системы;	2	
Порядок разработки сложных систем. технология функционирования сложной системы; цели и задачи проектирования; структуризация предметной области; классификация объектов проектирования; жизненный цикл автоматизированной системы	2	
Классификация ИС. Разработка и производство ИС. Структура и типовые компоненты ИС. Принципы	2	

построения систем защиты информации.		
Типовые компоненты ИС. Проблемы защиты ИС. Защита для открытых ИС. Практические методы реализации моделей безопасности. Ядра безопасности. Мониторинг взаимодействий в системе.	2	
Определение информационных и технических ресурсов, подлежащей защите. Структура и задачи органов, осуществляющих защиту информации. Создание службы информационной безопасности. Организационно-правовой статус и структура службы информационной безопасности.	2	
Политика Информационной безопасности. Реализация политики безопасности. Принципы и виды политики безопасности. Организационно-технические мероприятия. Организация секретного делопроизводства.	2	
Внедрение и использование средств защиты в автоматизированной системе. Принятие административных решений по уровням обеспечения ЗИ. Обеспечение ЗИ на стадиях проектирования ИС. Этапы выполнения работ по создания и внедрению СЗИ. Процесс создания механизмов защиты ИС. Этапы построения СЗИ. Порядок проведения работ по ЗИ. Реализация организационных мер защиты.	2	
Программно-технические методы и средства защиты информации. Службы и механизмы защиты. Реализация систем контроля доступа; Управление доступом. Контроль за работой пользователей. Управление доступом к рабочим местам. Регламентация парольного доступа. Защита целостности программ	2	
Управление системой ЗИ. Принципы организации и контроля системы защиты. Управление защитой в распределённых сетях. Методы разработки защищённых ИС. Модели управления доступом. Проблемы внедрения систем управления доступом.	2	
Этапы построения систем защиты информации. Определение информации, подлежащей защите. Защита государственной тайны. Сведения, составляющие государственную либо коммерческую тайну.	2	
Оценка уязвимости и рисков. Анализ рисков. Разработка методологии оценки. Этапы оценки. Определение и анализ угроз.	2	
Требования к системам защиты информации.	2	
Выбор средств защиты. Модель ИС как объекта защиты. Механизмы обеспечения безопасности. Выбор средств защиты.	2	
Внедрение и использование выбранных мер защиты. Основные решения по обеспечению ЗИ. Содержание	2	

и последовательность работ по ЗИ. Построение системы ЗИ. Порядок проведения работ по ЗИ. Реализация организационных и технических мер защиты. Приемка, определение полноты и качества.		
Контроль целостности СЗИ. Сертификация.	2	

Практические занятия Таблица 4.2

(Модуль), дидактическая единица, тема	Учебная деятельность	Часы	Ссылки на цели
Семестр: 9			
Разработка эскизного и аванпроекта защищенной автоматизированной системы		4	
Разработка перечня угроз автоматизированной системы. Составление модели нарушителя. Выбор способов защиты. Оценка качества защиты автоматизированной системы		4	
Разработка политики безопасности предприятия		4	
Разработка технического проекта реальной автоматизированной системы		4	

5. Самостоятельная работа студентов

Семестр- 9, Индив. работа
Изучение ГОСТов по построению автоматизированных систем
Изучение правовых актов в области защиты информации
Изучение инженерной документации общего назначения
Изучение систем парольной защиты в различных операционных системах
Изучение моделей защищенных автоматизированных систем
Анализ отечественных и зарубежных стандартов информационной безопасности
Изучение организационно-технических способов, направленных на повышение безопасности автоматизированных систем
Изучение влияния человеческого фактора на работу автоматизированной системы
Изучение методов создания защищенных систем
Виды атак на автоматизированные системы, каналы утечки и искажения информации

6. Правила аттестации студентов по учебной дисциплине

Оценка теоретических знаний студентов проводится на экзамене, по ответам на контрольные вопросы, в соответствии с настоящей рабочей программой. Содержание контрольных вопросов соответствует названиям тем теоретических занятий по рабочей программе. Экзаменационный билет содержит два теоретических вопроса.

Оценка практических знаний проводится непосредственно на практическом занятии путем опроса.

7. Список литературы

7.1 Основная литература

В печатном виде

1. Основы организационного обеспечения информационной безопасности объектов информатизации : [учебное пособие по специальностям в области информационной безопасности] / С. Н. Сёмкин [и др.]. - М., 2005. - 185, [1] с. : ил. - Рекомендовано УМО.
2. Галатенко В. А. Основы информационной безопасности : курс лекций : учебное пособие для студентов вузов, обучающихся по специальностям в области информационных технологий / В. А. Галатенко ; под ред. В. Б. Бетелина. - М., 2006. - 205 с. : ил.
3. Малюк А. А. Введение в защиту информации в автоматизированных системах : учебное пособие / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. - М., 2001. - 147 с.

7.2 Дополнительная литература

В печатном виде

1. Семкин С. Н. Основы информационной безопасности объектов обработки информации : науч.-практ. пособие / С. Н. Семкин, А. Н. Семкин. – М. : [б. и.], 2000. – 300 с.
2. Зегжда Д. П. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. – М. : Горячая линия Телеком, 2000. – 452 с.

8. Методическое и программное обеспечение

8.1 Методическое обеспечение

9. Контролирующие материалы для аттестации студентов по дисциплине

Контрольные вопросы

1. Структура и понятие информационной системы, управление и информация
2. Влияние случайных факторов на функционирование системы
3. Самоорганизация сложной системы
4. Эффективность и надежность сложных систем
5. Качество управления сложными системами, помехозащищенность, устойчивость.
6. Этапы разработки сложных систем
7. Классификация сложных систем
8. Структура сложной информационной системы
9. Этапы создания систем защиты информации
10. Типовые компоненты информационной системы
11. Проблемы защиты открытых систем "клиент-сервер"
12. Модели защиты информации для анализа систем защиты, реализующих дискреционную политику безопасности, и ее основного элемента - матрицы доступов
13. Модели защиты информации для анализа систем защиты, реализующих мандатное (полномочное) разграничение доступа
14. Мониторинг взаимодействий в системе
15. Структура и задачи органов, осуществляющих защиту информации.
16. Определение информационных и технических ресурсов, подлежащих защите.
17. Внешние угрозы информационной безопасности
18. Внутренние угрозы информационной безопасности
19. Случайные угрозы информационной безопасности
20. Назначение и структура службы информационной безопасности
21. Модель нарушителя информационной безопасности
22. Состав организационно-технических мероприятий по обеспечению информационной безопасности
23. Организация защиты государственной тайны
24. Состав документации по защите информации на стадии проектирования автоматизированной системы
25. Программно-аппаратные методы и средства защиты информации
26. Реализация систем контроля доступа
27. Управление защитой информации
28. Методы разработки защищенных систем
29. Модель управления доступом
30. Оценка эффективности систем защиты информации. Сертификация.