

Министерство образования и науки Российской Федерации
Федеральное агентство по образованию
ГОУ ВПО «Уральский государственный университет»

ИОНЦ «Информационная безопасность»

Математико-механический факультет

КАФЕДРА АЛГЕБРЫ И ДИСКРЕТНОЙ МАТЕМАТИКИ

УТВЕРЖДАЮ

Проректор университета

“ ” _____ 2007 г.

**ОСНОВЫ СОЗДАНИЯ И ЭКСПЛУАТАЦИИ ЗАЩИЩЕННЫХ
КОМПЬЮТЕРНЫХ СИСТЕМ**

ПРОГРАММА ДИСЦИПЛИНЫ

Рекомендована Методическим Советом ГОУ ВПО УрГУ
для специальностей и направлений подготовки: Компьютерная безопасность,
квалификация математик

Екатеринбург 2007

Программа составлена в соответствии с Государственным образовательным стандартом высшего профессионального образования (регистрационный номер 285 инф/сп от 05.04 2000 г.) для направления 075000 – Специальности в области информационной безопасности, специальность 075200 – Компьютерная безопасность.

Программа составлена авторами:

1. Профессор, д.т.н. Гайдамакин Николай Александрович, профессор кафедры алгебры и дискретной математики

Рабочая программа одобрена на заседании кафедр

Рабочая программа одобрена на заседании Методической комиссии

“ ____ ” _____ 2007 г., протокол № ____.

Председатель Методической комиссии _____

АННОТАЦИЯ СОДЕРЖАНИЯ ДИСЦИПЛИНЫ

Дисциплина "Основы создания и эксплуатации защищенных компьютерных систем" объединяет и систематизирует наиболее важные понятия в сфере создания и эксплуатации защищенных автоматизированных систем (АС), раскрывает вопросы нормативно-методической регламентации функциональной структуры (архитектуры) подсистем безопасности защищенных компьютерных систем (КС), функциональные требования безопасности к продуктам и системам информационных технологий (ИТ), жизненный цикл, порядок создания и эксплуатации защищенных КС, продуктов и систем ИТ, удовлетворяющих требованиям информационной безопасности.

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Дисциплина "Основы создания и эксплуатации защищенных компьютерных систем" имеет целью раскрыть нормативно-методическое регулирование процессов создания и эксплуатации защищенных автоматизированных систем, безопасных продуктов и систем информационных технологий.

Содержание дисциплины определяется государственными стандартами в области автоматизированных информационных систем и защиты информации, руководящими документами Гостехкомиссии (ныне ФСТЭК России) по защите информации от несанкционированного доступа в автоматизированных системах и в области безопасности информационных технологий.

Данная дисциплина является спецкурсом национально-регионального (вузовского) компонента учебного плана специальности: направление 075000 - Информационная безопасность, специальность 075200 - Компьютерная безопасность, и призвана содействовать усилению практической направленности образования, формированию и укреплению технической, нормативно-методической культуры студентов.

Знания и умения, приобретенные в ходе изучения курса «Основы создания и эксплуатации защищенных компьютерных систем» используются студентами при разработке курсовых и дипломных работ.

Задачи дисциплины – дать основы:

- стандартизации (нормативно-методической регламентации) требований к защищенным КС, процессов их создания и эксплуатации;
- методов и технологий проектирования защищенных КС;
- управления проектированием защищенных КС;
- практических навыков работы с нормативно-методическими документами (стандартами), умений составления основных документов на этапах создания и эксплуатации защищенных КС.

2 ТРЕБОВАНИЯ К УРОВНЮ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате изучения дисциплины студенты должны

2.1 Знать

1. Понятие, виды и структуру автоматизированных систем
2. Понятие и составляющие безопасности автоматизированных систем
3. Схемы каталогизации угроз безопасности КС, способы их идентификации, спецификации и оценивания, роль человеческого фактора в угрозах безопасности КС
4. Понятия функциональной и системной архитектуры КС, ядра (монитора, системы) безопасности КС
5. Общую характеристику и методологию руководящих документов Гостехкомиссии/ФСТЭК по защите СВТ и АС от НСД к информации, классы защищенности и структуру функциональных требований к подсистемам защиты информации

6. Общую характеристику и структуру стандартов по безопасности информационных технологий, виды требований безопасности, общую характеристику структуры классов и семейств функциональных требований безопасности к изделиям ИТ, общую характеристику классов требований доверия безопасности и структуры оценочных уровней доверия
7. Общую характеристику стандартов и особенности регламентации архитектуры систем защиты информации при взаимодействии открытых систем
8. Модель жизненного цикла и порядок создания АС, стандарты и их содержание по регламентации стадий и этапов создания АС, структуру, порядок составления, оформления и утверждения Технического задания по созданию АС, состав и структуру основных документов, обрабатываемых на этапе технорабочего проектирования
9. Особенности создания защищенных АС
10. Модель жизненного цикла и порядок создания изделий ИТ, удовлетворяющих требованиям безопасности, способы задания требований безопасности, структуру, порядок разработки, оценки, утверждения и опубликования профилей защиты изделий ИТ, заданий по безопасности при создании изделий ИТ
11. Основы методов и технологий проектирования защищенных компьютерных систем, понятие и содержание канонического (индивидуального) и типового проектирования
12. Основы управления проектированием КС
13. Основы планирования и графического представления процессов (работ) проектирования КС, общую характеристику автоматизированных систем управления проектами
14. Общие положения по эксплуатации КС
15. Содержание процессов администрирования и эксплуатации КС
16. Основные документы конструкторской эксплуатационной документации на КС, основные эксплуатационные документы на КС в организациях (на предприятиях)

2.2 Уметь

1. Идентифицировать и оценивать угрозы безопасности при формировании требований пользователя к КС
2. Определять и оформлять класс защищенности создаваемой КС
3. Составлять и правильно оформлять основные разделы Технического задания на создание несложных КС (системы защиты информации КС)
4. Составлять отдельные разделы Профиля защиты применительно к простым видам изделий ИТ
5. Составлять диаграммы Ганта и сетевые графики несложных процессов проектирования, осуществлять их анализ и оптимизацию
6. Планировать индивидуально-групповую структуру пользователей КС и структуру разделяемых (коллективных) информационных ресурсов
7. Разрабатывать политику и регламентации технологических процедур генерации, хранения и эксплуатации парольных и других средств аутентификации пользователей КС, архивирования информационных ресурсов, эксплуатации сменных носителей информации

8. Разрабатывать структуру и отдельные разделы Руководства пользователя и Руководства администратора несложных КС, изделий ИТ

2.3 Владеть

1. Навыками работы с нормативно-правовыми актами и нормативно-методическими документами в сфере защиты информации, автоматизированных систем и информационных технологий

3 ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

3.1 Объем в академических часах

Виды учебной работы по дисциплине и формы итогового контроля знаний, с разбивкой объема работы по часам и семестрам для существующих форм обучения для данной профессиональной образовательной программы (ПрОП) приведены в таблице 3.1.

Общая трудоемкость	136ч
Аудиторные занятия	68ч
Лекции	34ч
Практические занятия или семинары	34ч
Самостоятельная работа студентов	68
Экзамен	10 семестр

4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Содержание дисциплины определяется квалификационными требованиями ГОС и государственными стандартами в области автоматизированных информационных систем и защиты информации, руководящими документами Гостехкомиссии (ныне ФСТЭК России) по защите информации от несанкционированного доступа в автоматизированных системах и в области безопасности информационных технологий.

4.1 Разделы дисциплины и виды занятий

Перечень тем разделов с указанием трудоемкости их освоения, в академических часах, по видам учебной работы

Раздел дисциплины	Лекции и (час)	ПЗ или С (час)	ЛР (час)	Кон.Р (час)
4.2.1 Защищенные компьютерные системы и требования к ним	8	4	-	2
4.2.1.1 Понятие, виды и структура автоматизированных систем	2	-	-	
4.2.1.2 Объекты защиты и угрозы безопасности в автоматизированных (компьютерных) системах	2	2	-	
4.2.1.3 Функции и структура (архитектура) подсистем безопасности автоматизированных (компьютерных) систем	4	2	-	
4.2.2 Порядок создания и проектирования защищенных КС	16	18	-	2
4.2.2.1 Жизненный цикл и порядок создания защищенных АС	4	6	-	
4.2.2.2 Порядок создания изделий ИТ, удовлетворяющих требованиям безопасности	4	6	-	
4.2.2.3 Основы методов и технологий проектирования защищенных компьютерных систем	4	3	-	
4.2.2.4 Управление проектированием защищенных КС	4	3	-	
4.2.3 Эксплуатация защищенных КС	10	12	-	2
4.2.3.1 Общие положения по эксплуатации КС	4	2	-	
4.2.3.2 Администрирование и эксплуатация защищенных КС	4	6	-	
4.2.3.3 Эксплуатационная документация защищенных КС	2	4	-	

4.2 Содержание разделов дисциплины

Содержание дисциплины структурировано по разделам и темам. Ниже приведен перечень разделов и тем каждого раздела, трудоемкость освоения каждого раздела показана в таблице 4.1.

4.2.1 Защищенные компьютерные системы и требования к ним

4.2.1.1 Понятие, виды и структура автоматизированных систем

Понятия "система", "автоматизированная система", "информационные технологии", "управление", "автоматизированный процесс", "автоматический процесс". Виды АС по ГОСТ 34.003-90, (РД 50-680-88). Соотношение понятий "автоматизированная система" и "информационная система". Общая характеристика систем автоматизации управленческой деятельности. Информационная база автоматизированных (информационных) систем, понятия "база данных", "система управления базами данных", "банк данных". Структура автоматизированных систем по видам обеспечения (по РД 50-680-88) – назначение и компоненты информационного, технического, программного, математического, лингвистического, организационного и правового обеспечения. Автоматизированные рабочие места, пользователи и эксплуатационный персонал.

Понятие "безопасность автоматизированной системы". Безопасность информации в АС (конфиденциальность, целостность и правомерная доступность информации). Безопасность (надежность) функционирования АС (безотказность функций АС на основе безотказности/надежности программного обеспечения и безотказности/надежности технических средств и коммуникаций АС, аутентичность функций АС на основе целостности ПО и целостности параметров конфигурации ПО). Программно-техническая структура АС с точки зрения защиты информации и обеспечения безопасности функционирования.

4.2.1.2 Объекты защиты и угрозы безопасности в автоматизированных (компьютерных) системах

Понятия "идентификация", "аутентификация", "авторизация", "спецификация", "классификация", "категорирование" и "каталогизация".

Классификационные схемы объектов защиты в автоматизированных (компьютерных) системах. Объекты защиты в АС (по ГОСТ Р 51624-2000). Реестр средств и их классификация по ISO/IEC 17799:2000. Объекты воздействия угроз по BSI (германскому стандарту безопасности ИТ). Защищаемые активы продуктов и систем ИТ (в идеологии «Общих критериев» - по ГОСТ Р ИСО/МЭК 15408-2002 и руководящим документам Гостехкомиссии/ФСТЭК).

Идентификация и спецификация объектов защиты – выявление экземпляра объекта определенного вида и присвоение ему уникального идентификатора, авторизация (установление владельца), локализация местонахождения, оценка абсолютной/относительной стоимости и/или значимости. Методы и способы оценивания стоимости и/или значимости объектов защиты, интервальные и ранговые шкалы оценки (категорирование).

Понятие угрозы, угрозы безопасности информации в компьютерных системах. Классификационные схемы (каталогизация) угроз. Каталог угроз по BSI. ГОСТ Р 51275-99 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию". Примеры угроз защищаемым активам в продуктах и системах ИТ (по РД Гостехкомиссии "Безопасность ИТ. Руководство по разработке профилей защиты и заданий по безопасности").

Идентификация и спецификация (описание) угроз – выявление угрозы определенного типа и присвоение ей уникального идентификатора, определение и описания источника (природы)

угрозы, активов/объектов, подверженных воздействию угрозы, особенностей реализации/осуществления.

Общая схема оценивания угроз – оценка [вероятности] реализации и оценка ущерба. Оценка рисков, методы и шкалы оценки.

Человеческий фактор в угрозах безопасности и модель нарушителя информационной безопасности.

4.2.1.3 Функции и структура (архитектура) подсистем безопасности автоматизированных (компьютерных) систем

Понятия функциональной и системной архитектуры (структуры) автоматизированных (компьютерных) систем. Целевая декомпозиция подсистем безопасности компьютерных систем (цели, задачи, функции, процедуры). Иерархический и функционально-модульный принцип структуры (архитектуры) монитора (ядра, системы) безопасности.

Общая характеристика стандартов безопасности компьютерных систем. Номинально-ранговый принцип оценивания безопасности (защищенности) компьютерных систем (классы/уровни безопасности/защищенности) в зависимости от реализации установленных для соответствующих классов/уровней наборов функциональных требований, сгруппированных в функциональные подсистемы или семейства. Концепция и общая характеристика "Критериев оценки безопасных (надежных) компьютерных систем" (США, 1983г., т.н. "Оранжевая книга").

Система защиты от НСД к информации в СВТ по ГОСТ Р 50739-95. Подсистемы и функциональные требования.

Схема групп и классов защищенности АС по руководящим документам Гостехкомиссии. Система защиты от НСД к информации в АС по ГОСТ Р 51583-2000, РД Гостехкомиссии "АС. Защита от НСД к информации. Классификация АС и требования по защите информации", подсистемы и функциональные требования по классам защищенности.

Концепция и общая характеристика ГОСТ Р ИСО/МЭК 15408-2002 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий" (т.н. "Общие критерии"), изделие (продукт или система) ИТ, объект оценки и среда безопасности, парадигма доверия и система оценочных уровней доверия к реализации требований по безопасности. Представление (система) функциональных требований безопасности к продуктам и системам ИТ – классы функциональных требований, их семейства, компоненты семейств, их функциональные элементы. Пакеты функциональных требований по типам и группам изделий ИТ (ОС, СУБД, МЭ и т.д.).

Архитектура систем защиты информации при взаимодействии открытых систем (ВОС). Структура стандартов в области ВОС (Госпрофиль ВОС – Рекомендации по стандартизации Р 50.1.022-2000 "Информационная технология. Государственный профиль взаимосвязи открытых систем России"). ГОСТ Р ИСО 7498-2-99 "Взаимосвязь открытых систем. Базовая эталонная модель. Ч.2. Архитектура защиты информации". Услуги безопасности, общеархитектурные и специальные механизмы их реализации. Взаимоотношение (размещение) между услугами защиты и уровнями эталонной модели ВОС.

4.2.2 Порядок создания и проектирования защищенных КС

4.2.2.1 Жизненный цикл и порядок создания защищенных АС

Жизненный цикл АС – создание (обоснование необходимости, определение целей создания, требований, задач и функций АС, проектирование, реализация проектных решений, внедрение, ввод в эксплуатацию), эксплуатация и развитие (использование и применение по

назначению, администрирование, сопровождение программных средств, техническое обслуживание и ремонт аппаратных средств), вывод из эксплуатации.

Общие положения и стандарты по созданию автоматизированных систем. Создание АС как продукции единичного производства проектным путем на плановой основе по техническому заданию. Принципы создания и требования по созданию АС (по РД 50-680-88).

Регламентация (по ГОСТ 34.601-90) процесса создания АС: предпроектные работы, их стадии и этапы (формирование требований к АС; разработка концепции АС; разработка, согласование и утверждение Технического задания); проектирование (эскизный проект, технический проект, рабочая документация); ввод в эксплуатацию (ввод в действие, сопровождение). Содержание работ на этапах создания. Методы обследования объекта информатизации, перечень и содержание документов, разрабатываемых на предпроектных стадиях (по РД 50-34.698-90). Особенности предпроектных работ при создании защищенных автоматизированных АС (АС в защищенном исполнении), в т.ч. анализ условий функционирования объекта информатизации и определение факторов, воздействующих на информацию (идентификация, спецификация и оценивание угроз безопасности), анализ категорий важности защищаемой информации, формирование требований по защите информации, принятие решения о классе защищенности АС.

Техническое задание на создание защищенных АС. Структура, порядок разработки, оформления, согласования и утверждения (по ГОСТ 34.602-89).

Состав и содержание работ на стадии технорабочего проектирования. Понятие эскизного, технического и рабочего проекта (рабочей документации), требования к содержанию документов (по РД 50-34.698-90).

Сертификация АС по требованиям безопасности информации. Системы сертификации, органы и схемы сертификации. Аттестация объектов информатизации по требованиям безопасности.

Состав и содержание работ стадиях внедрения и сопровождения.

4.2.2.2 Порядок создания изделий ИТ, удовлетворяющих требованиям безопасности

Жизненный цикл изделий ИТ (продуктов и систем) в контексте обеспечения информационной безопасности (в идеологии "Общих критериев" по ГОСТ Р ИСО/МЭК 15408-2002) – создание изделия ИТ (задание требований, разработка, подтверждение соответствия требованиям информационной безопасности, поставка и ввод в действие); эксплуатация изделия ИТ (планирование и организация применения мер и средств обеспечения безопасности, анализ проблем и устранение недостатков, доработка и модернизация изделия ИТ, поддержка пользователей изделия ИТ); снятие с эксплуатации (архивирование информационных ресурсов, очистка носителей информации).

Виды требований безопасности ИТ (функциональные требования безопасности, требования доверия к безопасности, требования безопасности к среде ИТ). Способы задания требований к изделию ИТ, функциональные пакеты требований безопасности по группам изделий ИТ, базовые пакеты требований доверия к безопасности по классам защищенности изделий ИТ, профиль защиты (ПЗ) и задание по безопасности (ЗБ).

Структура и содержание профиля защиты, организационный порядок его разработки, оценки, сертификации, регистрации и опубликования (по руководящим документам Гостехкомиссии/ФСТЭК России). Примеры профилей защиты (по операционным системам, СУБД и межсетевым экранам).

Структура и содержание задания по безопасности при создании изделия ИТ. Порядок его разработки, оценки и утверждения. Общие положения и особенности разработки Технического задания на создание системы ИТ по требованиям информационной безопасности.

Содержание работ на этапе создания изделия ИТ – разработка и реализация комплекса организационно-технических мер по обеспечению безопасности в процессе разработки; проектирование изделия ИТ (реализация требований ПЗ/ЗБ/ТЗ); управление конфигурацией; разработка эксплуатационной документации; функциональное тестирование; оценка уязвимостей; разработка требований безопасности при эксплуатации изделия ИТ.

Подтверждение соответствия изделия ИТ требованиям информационной безопасности, подготовка к оценке, оценка задания по безопасности и созданного изделия, подтверждение соответствия (сертификация). Органы оценки (испытательные лаборатории) и органы по сертификации. Программа и календарный план испытаний.

Содержание работ на этапе поставки и ввода в действие изделия ИТ. Особенности поставки изделия ИТ, созданного по требованиям информационной безопасности.

4.2.2.3 Основы методов и технологий проектирования защищенных компьютерных систем

Общая характеристика и особенности проектной деятельности. Понятие проекта как результата, понятия методологии, технологий и средств проектирования.

Классификация методов проектирования по типу проектных решений (каноническое/индивидуальное и типовое проектирование), по типу средств и технологий проектирования (ручное и автоматизированное проектирование), по степени адаптивности проектных решений (методы реконструкции, методы параметризации, методы реструктуризации).

Понятие средств проектирования. Некомпьютерные (средства организационно-методического обеспечения операций проектирования – стандарты, руководящие документы, модели и языки формализации проектных решений) и компьютерные средства (среды программирования, СУБД, системы автоматизированного проектирования (CASE-системы – Computer Aided Software Engineering) программного обеспечения и баз данных, пакеты прикладных программ, функциональные пакеты программ и ПО т.н. типовых АС).

Технологический процесс проектирования. Формализация представления процессов проектирования. Технологические схемы (сети) процесса проектирования.

Каноническое (индивидуальное) проектирование на основе каскадной модели жизненного цикла проектируемого изделия. Технологическая схема канонического проектирования на этапе технического проекта.

Типовое проектирование. Понятие типового проектного решения. Разновидности типового проектирования (элементный метод, подсистемный метод, объектный метод). Особенности выбора и применения функциональных пакетов прикладных программ, выбора и использования ПО типовых АС. Понятие реинжиниринга деловых (бизнес) процессов.

Особенности разработки проектной и эксплуатационной документации.

4.2.2.4 Управление проектированием защищенных КС

Общие положения по организации и управлению проектированием, специфика проектирования защищенных КС. Понятие проекта как особого рода деятельности.

Компоненты процесса управления проектом – цель управления, ограничения, объект и субъект управления, контур (цикл) управления, методы и средства управления.

Особенности субъекта управления проектной деятельностью – руководство проектной организации и обеспечивающих (функциональных) подразделений, руководители проектов и проектных групп.

Объекты управления в процессе проектирования, их роли (заказчик, пользователь, администратор и разработчик) и функции.

Схемы взаимоотношений пользователя, заказчика, администратора и разработчика при реализации небольших и больших (сложных) проектов.

Организация-разработчик. Головные и субподрядные организации, порядок их взаимодействия и взаимоотношений. Системные интеграторы.

Организационные формы коллектива разработчиков (проектной группы), функциональный, проектно-целевой и матричный принцип организационной структуры коллектива разработчиков. Разделение труда в коллективе разработчиков на основе операционного и подсистемного подходов, группа главного специалиста, группа системного анализа, группа программирования, группа тестирования, группа документации и административная группа.

Управленческий цикл в процессах проектирования.

Планирование в процессах проектирования. Основные понятия планирования (план, работа, ресурсы, событие, связи предшествования). Графические способы формализованного представления совокупности работ при планировании и управлении, линейные графики Ганта (диаграммы Ганта) и графовые сети (сетевые графики работ).

Этапы планирования и управления проектом – разработка первоначального сетевого плана/графика, анализ его реализуемости (логической, временной с использованием метода критического пути, физической/ресурсной и финансовой реализуемости); оптимизация плана и приведение его в соответствие с ограничениями (параметры оптимизации – время, стоимость, ресурсы, качество); оперативное управление и систематический контроль реализации плана.

Системы управления проектами (СУП) как организационно-технологические комплексы методических, технических, программных и информационных средств, обеспечивающих поддержку и повышение эффективности процессов планирования и управления проектами. Функциональные возможности и предназначение СУП – визуально-графические средства целевой декомпозиции задач проектирования, организационной структуры коллектива разработчиков; визуально-графические средства составления диаграмм Ганта, сетевых графиков, гистограмм распределения ресурсов; встроенные математико-алгоритмические средства анализа и оптимизации сетевых графиков (ПЕРТ-диаграмм, метод критического пути-МКП); централизованное накопление, хранение информации по графикам и планам работ; возможности быстрого анализа и влияния на ход работ, изменений в графике, ресурсном обеспечении и финансировании плана; поддержка автоматизированного составления отчетов и документации по проекту. Обзор и характеристика программных средств (систем) управления проектами (MS Project, Primavera Project Planner, Open Plan, Spider Project).

4.2.3 Эксплуатация защищенных КС

4.2.3.1 Общие положения по эксплуатации КС

Общие положения по эксплуатации изделий, комплексов, средств деятельности. Понятие эксплуатации и системы эксплуатации изделий.

Организационные мероприятия по эксплуатации (планирование эксплуатации, контроль технического состояния, анализ показателей надежности и функционирования, рекламационная и претензионная работа, категорирование, списание), их содержание и общая характеристика.

Технические мероприятия по эксплуатации (применение по назначению, техническое обслуживание, ремонт, [хранение, сбережение, транспортирование, консервация]). Понятие, содержание и виды технического обслуживания (регламентных работ). Виды ремонтов и особенности организации и проведения ремонтных работ. Основы организации хранения изделий и комплексов.

Особенности эксплуатации автоматизированных информационных систем и изделий ИТ как комплекса технических средств обработки информации (ТСОИ – СВТ, коммуникационное оборудование, линии связи), программного обеспечения (ПО), средств информационного обеспечения (информационная база – БД) и средств организационного обеспечения (коллектива пользователей). Составляющие эксплуатации АС и изделий ИТ – работы, мероприятия и процедуры, характерные для эксплуатации технических средств и изделий (ТСОИ); специальные работы по обеспечению функционирования ПО (развертывание, настройка, устранение сбоев и восстановление после них ПО, авторское сопровождение ПО, включая внесение изменений и доработок в ПО, обеспечение требований по авторскому праву на ПО); специальные работы по обеспечению целостности и сохранности информационной базы (устранение нарушений целостности, внесение изменений/доработок в логическую структуру, в настройки, словарно-классификационную базу, резервирование, архивирование, восстановление данных после сбоев); администрирование работы пользователей (регистрация и установление полномочий, ролей и т.д., обучение пользователей, контроль за выполнением пользователями правил эксплуатации и работы и т.д.).

Снятие с эксплуатации защищенных АС и изделий ИТ - архивирование ресурсов информационной базы АС (для последующего возможного использования, в т.ч. функционально-ориентированных данных с соблюдением юридических аспектов); очистка носителей информации (стирание данных и надежное удаление данных); физическое уничтожение носителей данных (в установленных нормативными предписаниями случаях); списание ТСОИ и их утилизация (по требованиям, установленным эксплуатационной документацией, ведомственной и/или локальной нормативной базой, в частности, в отношении компонент, содержащих драгметаллы, ядовитые, опасные вещества и материалы).

4.2.3.2 Администрирование и эксплуатация защищенных КС

Особенности эксплуатации защищенных КС. Угрозы безопасности на стадии эксплуатации и сопровождения КС. Органы системы управления эксплуатацией защищенных КС (АС), функции и компетенции инженерно-технических, ИТ и обеспечивающих подразделений, подразделений по защите информации. Комиссионные органы.

Планирование эксплуатации. Программа обеспечения безопасности при эксплуатации изделия ИТ.

Планирование и организация работы пользователей (планирование структуры информационных ресурсов и коллектива пользователей, регистрация пользователей, установление полномочий, обучение).

Управление конфигурацией ПО, ТСОИ.

Обеспечение целостности и сохранности (в т.ч. восстановление при разрушениях) информационной базы.

Антивирусная защита ПО. Организационные и программно-технологические меры.

Управление функционированием средств защиты информации (реализация политики безопасности в настройках, параметрах и процедурах функционирования КС и СЗИ, устранение изъянов в системах безопасности). Технологические процедуры парольной политики, использования других средств идентификации и аутентификации, криптографических средств.

Организация и обеспечение безопасного содержания и законодательно установленного порядка использования дистрибутивов ПО, модификации, адаптации и восстановления ПО.

Мониторинг, контроль, аудит безопасности в КС. Организационные и программно-технические меры.

Обеспечение безопасного содержания ТСОИ и защиты от воздействия факторов внешней среды.

Техническое обслуживание и ремонт ТСОИ (в т.ч. профилактика носителей информации, обеспечение расходными и пополняемыми комплектующими материалами, носителями данных), ведение эксплуатационной документации, рекламационная и претензионная работа.

Сопровождение ПО.

Организационные аспекты администрирования. Администраторы сетей, КС, безопасности. Нормативное обеспечение администрирования, Положение об администраторе информационной безопасности.

4.2.3.3 Эксплуатационная документация защищенных КС

Конструкторские эксплуатационные документы (руководства/инструкции по эксплуатации и эксплуатационные документы на средства по видам обеспечения – на ТСОИ, ПО).

Структура Руководства пользователя АС (по РД 50-34.698-99). Структура руководства пользователя изделия ИТ (по ГОСТ Р ИСО/МЭК 15408-2002 Ч.3. Класс AGD).

Структура Руководства администратора системы ИТ (по ГОСТ Р ИСО/МЭК 15408-2002 Ч.3. Класс AGD).

Конструкторская эксплуатационная документация на ТСОИ и ПО (по ГОСТ 19.101 и ГОСТ 2.601-95).

Эксплуатационные документы организации – организационно-распорядительная документация (положения, инструкции, приказы) и учетно-отчетная документация по вопросам эксплуатации.

5 ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Не предусмотрен учебным планом специальности

6 УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Рекомендуемая литература

6.1.1 Основная литература

1. Емельянова Н.З., Партыка Т.Л., Попов И.И. Основы построения автоматизированных информационных систем: Учебное пособие. – М.: ФОРУМ: ИНФРА-М, 2007. – 416с.
2. Стандарты информационной безопасности: курс лекций: учебное пособие / Второе издание / В.А. Галатенко. Под редакцией академика РАН В.Б. Бетелина / – М.: ИНТУИТ.РУ "Интернет-университет Информационных технологий", 2006. – 264 с.
3. Гайдамакин Н.А. Автоматизированные информационные системы, базы и банки данных. Вводный курс: Учебное пособие. – М.: Гелиос-АРВ, 2002. – 308с.

4. *Товс А.С., Ципес Г.Л.* Управление проектами: стандарты, методы, опыт. – М.: ЗАО «Олимп-Бизнес», 2003.- 240с.

6.1.2 Дополнительная литература

1. *Смирнова Г.Н.* Проектирование экономических информационных систем: Учебник / Г.Н. Смирнова, А.А.Сорокин, Ю.Ф.Тельнов; Под ред. Ю.Ф.Тельнова. – М.: Финансы и статистика, 2001. – 512с.
2. *Романов В.П., Емельянова Н.З., Партыка Т.Л.* Проектирование экономических информационных систем: методология и современные технологии: Учебное пособие / - М.: «Экзамен», 2005.- 256с.
3. *Вендров А.М.* Проектирование программного обеспечения экономических информационных систем: Учебник / - М.: Финансы и статистика, 2000. – 347с.
4. *Филипс Дж.* Менеджмент ИТ-проектов. На пути от старта до финиша. - М.: «Лори», 2005. – 378с.

6.1.3 Нормативно-методические документы

5. РД по стандартизации 50-680-88. Методические указания. Автоматизированные системы. Основные положения
6. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию
7. РД ГосТехКомиссии России. АС. Защита от НСД к информации. Классификация АС и требования по защите информации
8. ГОСТ Р 50739-95. СВТ. Защита от НСД к информации. Общие технические требования
9. ГОСТ Р 51624-2000
10. ГОСТ Р ИСО/МЭК 15408-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч.1. Введение и общая модель. Ч.2. Функциональные требования безопасности. Ч.3. Требования доверия к безопасности
11. Рекомендации по стандартизации Р 50.1.022-2000. Информационная технология. Государственный профиль взаимосвязи открытых систем России
12. ГОСТ Р ИСО 7498-2-99. Взаимосвязь открытых систем. Базовая эталонная модель. Ч.2. Архитектура защиты информации
13. РД ГосТехКомиссии России. Безопасность информационных технологий. Руководство по разработке профилей защиты и заданий по безопасности
14. ГОСТ 34.601-90. Информационная технология. Автоматизированные системы. Стадии создания
15. ГОСТ 34.602-89. Информационная технология. Техническое задание на создание автоматизированной системы

16. РД ГосТехКомиссии России. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в АС и СВТ
17. ГОСТ Р 51583-2000
18. ГОСТ 34.201-89. Информационная технология. Виды, комплектность и обозначение документов при создании автоматизированных систем
19. РД ГосТехКомиссии России. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты
20. РД ГосТехКомиссии России. Безопасность информационных технологий. Положение о разработке профилей защиты и заданий по безопасности
21. ГОСТ Р ИСО/МЭК 12207. Информационная технология. Процессы жизненного цикла программных средств
22. ГОСТ Р ИСО/МЭК ТО 15271-2002. Информационная технология. Руководство по применению ГОСТ Р ИСО/МЭК 12207 (Процессы жизненного цикла программных средств)
23. ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие вирусов. Типовое руководство
24. ГОСТ Р ИСО/МЭК 14764-2002. Информационная технология. Сопровождение программных средств
25. ГОСТ Р ИСО/МЭК 15910-2002. Информационная технология. Процесс создания документации пользователя программного средства
26. ГОСТ 34.603-92. Информационная технология. Виды испытаний автоматизированных систем
27. РД по стандартизации 50-34.698-90. Автоматизированные системы. Требования к содержанию документов
28. Единая система конструкторской документации (ЕСКД). Комплекс стандартов серии 2.xxx
29. Единая система программной документации (ЕСПД). Комплекс стандартов серии 19.xxx
30. ГосТехКомиссия России. Положение по аттестации объектов информатизации по требованиям безопасности информации
31. ГосТехКомиссия России. Положение о сертификации средств защиты информации по требованиям безопасности информации
32. ISO/IEC 17799:2002. Информационные технологии. Свод правил по управлению защитой информации

6.2 Средства обеспечения освоения дисциплины

6.2.1 Перечень средств обеспечения

В процессе изучения дисциплины используются:

1. Автоматизированная информационно-справочная система *"Нормативно-правовые акты и нормативно-методические документы в сфере создания и эксплуатации защищенных компьютерных систем"*.

6.2.2 Программно-информационное обеспечение дисциплины

Справочные материалы на электронном носителе

7 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1 Общие требования

Лекционный материал должен изучаться в специализированной аудитории, оснащенной современным компьютером с подключенным проектором от видеотерминала персонального компьютера на настенный экран.

7.2 Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Компьютерный класс с доступом к автоматизированным информационно-справочным системам, указанным в п.6.2.1.

8 МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

В настоящем разделе приведены методические рекомендации для преподавателей, студентов. Кроме того, показана тематика самостоятельной работы студентов (СРС), предусмотренная данной рабочей программой дисциплины (см. таблицу 3.1).

8.1 Рекомендации для преподавателя

- глубокое освоение теоретических аспектов тематики курса, ознакомление, проработка литературных источников; составление списка литературы, обязательной для изучения и дополнительной литературы; проведение собственных исследований в этой области;
- разработка методики изложения курса: структуры и последовательности изложения материала; составление тестовых заданий, контрольных вопросов;
- разработка методики проведения и совершенствование тематики практических работ и семинаров;
- разработка методики самостоятельной работы студентов;
- постоянная корректировка структуры, содержания курса.

8.2 Рекомендации для студента

- обязательное посещение лекций ведущего преподавателя; лекции – основное методическое руководство при изучении дисциплины, наиболее оптимальным

образом структурированное и скорректированное на современный материал; в лекции глубоко и подробно, аргументировано и методологически строго рассматриваются главные проблемы темы; в лекции даются необходимые разные подходы к исследуемым проблемам;

- подготовка и активная работа на практических занятиях и семинарах; подготовка к практическим занятиям и семинарам включает проработку материалов лекций, рекомендованной учебной литературы нормативных правовых актов.

8.3 Перечень тем семинаров и практических занятий

По разделу "Защищенные компьютерные системы и требования к ним"

1. Идентификация, спецификация и оценивание объектов защиты и угроз безопасности в КС
2. Классы защищенности и функциональные требования по защите информации в АС
3. Требования безопасности к изделиям ИТ

По разделу "Порядок создания и проектирования защищенных КС"

1. Предпроектные работы при создании АС
2. Разработка Технического задания на создание АС
3. Разработка Профиля защиты изделия ИТ и задания по безопасности при создании изделия ИТ
4. Технологии и средства проектирования АС (КС)
5. Управление проектированием КС, планирование работ

По разделу "Эксплуатация защищенных КС"

1. Содержание и система эксплуатации КС
2. Администрирование КС
3. Эксплуатационная документация КС

8.4 Перечень тем рефератов

Не предусмотрено

8.5 Тематика курсового проектирования

Не предусмотрено учебным планом

8.6 Перечень тем домашних работ

- Изучение стандартов и руководящих документов стандартизации по АС (ГОСТы серии 34.)
- Изучение Руководящих документов Гостехкомиссии по защите от НСД
- Изучение стандарта ГОСТ Р ИСО/МЭК 15408-2002

8.7 Перечень тем контрольных работ

- Автоматизированные системы и требования к ним
- Порядок создания и проектирования защищенных КС

- Эксплуатация защищенных КС

8.8 Перечень тем расчетных работ

Не предусмотрено

8.9 Перечень тем расчетно-графических работ

Не предусмотрено

8.10 Перечень контрольных вопросов для подготовки к итоговой аттестации по дисциплине

1. Понятие, виды и структура автоматизированных систем (по РД 50-680-88)
2. Безопасность АС, ее составляющие. Основные способы и механизмы обеспечения безопасности информации в АС
3. Классификация, идентификация (инвентаризация, каталогизация) и оценивание (категорирование) объектов защиты в АС
4. Классификация (каталогизация), идентификация, спецификация и оценивание угроз безопасности в АС
5. Человеческий фактор в угрозах безопасности. Модель нарушителя безопасности информации в АС (РД Гостехкомиссии)
6. Декомпозиция назначения, целей и задач функционирования АС. Функциональная структура АС и функциональные требования к защищенным СВТ, АС, продуктам и системам ИТ
7. Система и структура функциональных требований по защите от НСД к информации в СВТ (по РД Гостехкомиссии), классы защищенности СВТ
8. Система и структура функциональных требований по защите от НСД в АС (по РД Гостехкомиссии), группы и классы защищенности АС
9. Общая структура требований безопасности к изделиям и системам ИТ, классы функциональных требований безопасности (по ГОСТ Р ИСО/МЭК 15408-2002. Ч.2)
10. Услуги (сервисы) безопасности при взаимодействии открытых систем и механизмы безопасности, их реализующие (по ГОСТ Р ИСО 7498-1-99), взаимоотношение между услугами защиты и уровнями взаимодействия по 7-ми уровневой эталонной модели ВОС
11. Жизненный цикл, стадии создания и содержание работ по созданию АС, особенности создания АС в защищенном исполнении (по ГОСТ 34.601-90, ГОСТ Р 51583)
12. Техническое задание на создание АС, требования по структуре, содержанию, порядку разработки, оформления, согласования и утверждения (по ГОСТ 34.602-89)
13. Особенности Технического задания на создание АС в защищенном исполнении. Составляющие общих требований к АСЗИ и структуру функциональных требований (по ГОСТ Р 51624)
14. Жизненный цикл изделий (продуктов и систем) ИТ, общая схема и последовательность создания изделий ИТ

15. Классификация изделий ИТ и функциональные пакеты требований безопасности. Классы защищенности изделий ИТ и пакеты требований доверия безопасности (по ГОСТ Р ИСО/МЭК 15408-2002 и РД Гостехкомиссии)
16. Структура, порядок разработки, регистрации и опубликования профилей защиты для изделий ИТ (по ГОСТ Р ИСО/МЭК 15408-2002 и РД Гостехкомиссии)
17. Структура, назначение и порядок разработки задания по безопасности при создании изделий ИТ, соотношение между профилем защиты и заданием по безопасности. Техническое задание на создание системы ИТ (по ГОСТ Р ИСО/МЭК 15408-2002 и РД Гостехкомиссии)
18. Содержание процесса разработки и ввода в действие изделий (систем) ИТ. Уровни представления проектных решений
19. Проектирование АС как особый вид деятельности, объекты проектирования при создании АС (по РД 50-680-88)
20. Методология (методы и средства) проектирования АС
21. Каноническое (индивидуальное) проектирование АС. Технологическая схема этапов технического и рабочего проектирования
22. Типовое проектирование АС и его методы. Технологическая схема проектирования
23. Управление процессом проектирования АС, его компоненты и специфика
24. Организационная структура, схемы организации работ при проектировании АС и организационные формы проектного коллектива
25. Содержание и специфика управленческого цикла при проектировании АС
26. Методы планирования и управления проектами. Диаграммы Ганта, сетевые графики проектов
27. Автоматизированные системы управления проектами
28. Общие положения по эксплуатации изделий, комплексов, средств деятельности. Составляющие организационных и технических мероприятий по эксплуатации
29. Особенности эксплуатации КС (АС) и защищенных КС (АС в защищенном исполнении). Администрирование КС (АС)
30. Органы управления и планирования эксплуатации защищенных АС
31. Эксплуатационная документация на АС (изделия ИТ). Руководства пользователя и администратора
32. Конструкторские эксплуатационные документы на ТСО и ПО, эксплуатационные документы предприятия

8.11 Перечень ключевых слов дисциплины

Автоматизированные системы, защищенные компьютерные системы, безопасность, защита информации, угрозы безопасности, классы защищенности, требования по защите информации, функциональная архитектура, информационные технологии, изделие ИТ, функциональные требования по безопасности, требования безопасности среде ИТ, требования доверия безопасности, оценочные уровни доверия, стандарты, создание автоматизированных систем, предпроектные работы, техническое задание, профиль защиты, задание по безопасности, эскизный проект, технический проект, рабочая документация, проектирование, методы проектирования, технологии проектирования, средства проектирования, каноническое (индивидуальное) проектирование, типовое проектирование, проектная документация, эксплуатационная

документация, управление проектированием, планирование проектирования, диаграммы Ганта, сетевые графики, эксплуатация, техническое обслуживание, ремонт, администрирование АС, руководство пользователя АС, руководство администратора АС