ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

Государственное образовательное учреждение высшего профессионального образования
«Уральский государственный университет им. А.М. Горького»

ИОНЦ «Информационная безопасность»

математико-механический факультет

кафедра алгебры и дискретной математики

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС

Информационная безопасность АИС, баз и банков данных

Программа дисциплины

Автор: профессор кафедры алгебры
и дискретной математики
Н.А. Гайдамакин

Екатеринбург
2008

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

“____”_____2008 г., протокол №____.

Председатель Методической комиссии _____

АННОТАЦИЯ СОДЕРЖАНИЯ ДИСЦИПЛИНЫ

Дисциплина "Информационная безопасность автоматизированных информационных систем, баз и банков данных" объединяет и систематизирует наиболее важные понятия в сфере информационной безопасности АИС, БД и БнД, раскрывает вопросы моделей, механизмов и технологий обеспечения конфиденциальности, целостности и правомерной доступности информации в АИС, БД и БнД, обеспечения безопасности функций АИС и БнД.

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Дисциплина "Информационная безопасность автоматизированных информационных систем, баз и банков данных" имеет целью раскрыть содержание основных понятий, методов и механизмов обеспечения информационной безопасности АИС, БД и БнД.

Содержание дисциплины определяется апробированными в практической реализации методами и механизмами обеспечения конфиденциальности, целостности и доступности информации в АИС, БД и БнД, 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 интеграции, углубления и систематизации знаний, полученных студентами в ходе изучения общепрофессиональных дисциплин, усилению практической направленности обучения по специальности.

Знания и умения, приобретенные в ходе изучения курса «Информационная безопасность автоматизированных информационных систем, баз и банков данных» используются студентами при разработке курсовых и дипломных работ.

Задачи дисциплины – дать основы:

- системного и комплексного подхода к анализу и обеспечению информационной безопасности АИС, БД и БнД в процессах их создания и эксплуатации (администрирования);
- представления, анализа и обоснования моделей, методов и механизмов обеспечения информационной безопасности АИС, БД и БнД;
- практических навыков работы с нормативно-методическими документами (стандартами) в сфере информационной безопасности автоматизированных информационных систем.

2 ТРЕБОВАНИЯ К УРОВНЮ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате изучения дисциплины студенты должны

2.1 Знать

1. Понятие, виды и структуру автоматизированных информационных систем
2. Функции и структуру СУБД, реляционную модель организации данных
3. Понятие и составляющие информационной безопасности АИС, БД и БнД, схемы анализа и каталогизации угроз безопасности
4. Субъектно-объектный подход в моделях и методах обеспечения информационной безопасности, понятия и структуру функциональной и системной архитектуры АИС, ядра (монитора, системы) безопасности АИС
5. Систематику методов и механизмов обеспечения информационной безопасности АИС

6. Основные политики, дискреционные и мандатные модели разграничения доступа к информации в АИС
7. Структуру системных таблиц и основные инструкции языка SQL, реализующие дискреционные и мандатные механизмы разграничения доступа в реляционных СУБД
8. Понятие и механизмы перекрытия скрытых каналов утечки информации
9. Ролевую политику и технологии индивидуально-группового доступа к разделяемым информационным ресурсам
10. Основные виды и архитектуру документальных АИС, методы и модели разграничения доступа к информации (документам) в документальных АИС
11. Виды и программно-техническую структуру распределенных АИС
12. Особенности политики и систем безопасности в распределенных АИС
13. Источники изъянов безопасности, основы активного аудита безопасности в распределенных АИС
14. Понятие и режимы поддержания целостности данных в реляционных СУБД
15. Механизм событий, триггеров и процедур в процессах обеспечения целостности данных
16. Дискреционные и мандатные модели обеспечения целостности данных, особенности объединения (интегрирования) моделей разграничения доступа и моделей обеспечения целостности данных в архитектуре и процедурах функционирования современных СУБД
17. Основы механизмов и протоколов реализации транзакций, обеспечивающих целостность данных в клиент-серверных СУБД
18. Понятие и схемы резервирования, архивирования и журнализации баз данных в современных СУБД
19. Основы технологий репликации данных как одного из видов архитектуры, принципов создания и функционирования распределенных АИС
20. Методологию стандартизации требований к архитектуре, функциям и критериям оценки подсистем безопасности в АИС
21. Показатели защищенности СВТ/СУБД и классификация АС/АИС по требованиям защиты от НСД к информации
22. Идеологию и общую характеристику критериев оценки безопасности информационных технологий ("Общие критерии")
23. Порядок разработки и структуру профилей защиты СУБД
24. Содержание процессов администрирования и эксплуатации АИС

2.2 Уметь

1. Анализировать функциональную и системную архитектуру АИС в контексте обеспечения информационной безопасности
2. Применять инструкции языка SQL для реализации установок дискреционного доступа, техники представлений
3. Планировать и анализировать структуру индивидуально-группового доступа к разделяемым ресурсам
4. Анализировать и применять политику тематико-иерархического разграничения доступа в документальных АИС
5. Анализировать и обосновывать политику и механизмы обеспечения информационной безопасности, ее аудита в распределенных АИС

6. Планировать и реализовывать в СУБД ограничения целостности данных, определять целесообразные режимы репликации данных
7. Анализировать и определять функциональные требования безопасности по классам защищенности АИС и СУБД
8. Вырабатывать перечень процедур и работ по администрированию защищенных АИС

2.3 Владеть

1. Навыками работы с нормативно-методическими документами в сфере информационной безопасности автоматизированных информационных систем

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	42ч
Практические занятия или семинары	26ч
Самостоятельная работа студентов	68
Экзамен	10 семестр

4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Определяется квалификационными требованиями ГОС, апробированными в практической реализации методами и механизмами обеспечения конфиденциальности, целостности и доступности информации в АИС, БД и БнД, 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 (час)	ПЗ или С (час)	ЛР (час)	Кон.Р (час)
1 Общие положения по информационной безопасности АИС, БД и БнД	**8**	**2**	**-**	**-**
1.1 Понятие, виды и структура АИС	4	1	-	
1.2 Общая характеристика составляющих, методов и механизмов обеспечения информационной безопасности АИС	4	1	-	
2 Методы, модели и механизмы обеспечения конфиденциальности данных	**14**	**10**	**-**	**2**
2.1 Дискреционные и мандатные модели разграничения доступа к информации в АИС, БД и БнД	4	3	-	
2.2 Модели ролевого доступа и технологии рабочих групп пользователей	2	2	-	
2.3 Тематическое разграничение доступа к информации в документальных АИС	4	2		
2.4 Основы обеспечения информационной безопасности в распределенных АИС	4	3		
3 Методы, модели и механизмы обеспечения целостности данных	**4**	**4**	**-**	**1**
3.1 Механизмы обеспечения целостности данных, реализуемые реляционными СУБД	1	-		
3.2 Модели обеспечения целостности данных в процессах коллективного доступа к разделяемым информационным ресурсам	1	2	-	
3.3 Механизмы транзакций и обеспечение целостности данных в клиент-серверных СУБД	2	2		
4 Методы, механизмы и технологии обеспечения сохранности и правомерной доступности информации в АИС, БД и БнД	**4**	**2**	**-**	**1**

4.1 Резервирование, архивирование и журнализация БД	2	1		
4.2 Технологии репликации данных в распределенных АИС	2	1		
5 Критерии и стандарты информационной безопасности (защищенности) АИС	**8**	**6**	**-**	**2**
5.1 Стандартизация требований к архитектуре, функциям и критериям оценки подсистем безопасности в АИС	2	2		
5.2 Классификация автоматизированных систем по требованиям защиты от несанкционированного доступа к информации	2	2		
5.3 Критерии оценки безопасности информационных технологий. Профили защиты СУБД	4	2		
6 Организационное обеспечение информационной безопасности АИС	**4**	**2**	**-**	**-**
6.1 Администрирование и эксплуатация АИС	4	2	-	

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 Общие положения по информационной безопасности АИС, БД и БнД

4.2.1.1 Понятие, виды и структура АИС

Информация и данные, информационные технологии и информационные системы. Автоматизированные информационные системы. Структура и классификация автоматизированных информационных систем. Информационная база АИС, понятия "база данных", "система управления базами данных", "банк данных".

Виды автоматизированных систем. Виды автоматизированных информационных систем по типу представления данных и функциям.

Структура автоматизированных информационных 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.

Системы управления базами данных (СУБД). Архитектура СУБД. Логическая и физическая структура баз данных. Реляционная модель данных и ее структурная, манипуляционная и целостная составляющие.

Язык SQL для описания (формирования) логической структуры данных и манипулирования данными. Встроенные языки и виды СУБД.

4.2.1.2 Общая характеристика составляющих, методов и механизмов обеспечения информационной безопасности АИС

Понятие "безопасность автоматизированной информационной системы". Безопасность информации в АИС и ее составляющие – конфиденциальность, целостность и правомерная доступность информации.

Субъекты и объекты безопасности. Угрозы безопасности. Нарушители безопасности.

Субъекты и объекты безопасности в БД АИС, созданных на основе реляционных СУБД.

Угрозы безопасности объектам АИС, БД и БнД, способы их осуществления (несанкционированный доступ к файлам БД в операционной среде; несанкционированный доступ к информации и манипулирование данными в среде АИС/СУБД; чрезмерное использование ресурсов АИС, приводящее к отказу в обслуживании (отказу функций); сбои ПО, оборудования АИС, приводящие к разрушению/потери данных, отказу в обслуживании). Каталогизация угроз безопасности.

Систематика методов и механизмов обеспечения безопасности в АИС:

непосредственно обеспечивающие конфиденциальность, целостность и доступность информации (разграничение доступа к данным, контроль, управление информационной структурой данных, установление и контроль ограничений целостности данных, шифрование данных, механизмы ЭЦП данных в процессах их передачи и хранения, защита/удаление остаточной информации на носителях данных и в освобождаемых областях оперативной памяти);

общеархитектурного характера (идентификация/аутентификация пользователей, устройств, данных, управление памятью, потоками, изоляция процессов, управление транзакциями);

инфраструктурного характера (управление (контроль) конфигурацией, управление сеансами, управление удаленным доступом с рабочих станций, управление сетевым соединениями, управление инфраструктурой сертификатов криптоключей)

обеспечивающего (профилактирующего) характера (протоколирование, аудит событий, резервирование данных, журнализация процессов изменения данных, профилактика, учет и контроль использования носителей данных, нормативно-организационная регламентация использования АИС, обучение. нормативно-административное побуждение и принуждение пользователей по вопросам информационной безопасности АИС).

4.2.2 Методы, механизмы и технологии обеспечения конфиденциальности данных

4.2.2.1 Дискреционные и мандатные модели разграничения доступа к информации в АИС, БД и БнД

Дискреционный принцип разграничения доступа. Тройки доступа; субъект-операция-объект. Матрица доступа. Принудительное и добровольное управление доступом. Администраторы системы и владельцы объектов. Привилегии и предоставление (распространение) прав доступа.

Разграничение доступа на уровне логических объектов (таблиц) в реляционных СУБД. Структурно-логическая реализации матрицы доступа. Системные (внутренние) таблицы пользователей и прав доступа.

Разграничение доступа на уровне табличных строк-кортежей и полей таблиц в реляционных СУБД. Представления. Элементы языка SQL для установки и управления правилами разграничения доступа.

Мандатный принцип разграничения доступа. Уровни (решетка) безопасности. Уровни конфиденциальности объектов и уровни доверия субъектов доступа. Правила мандатного доступа. Модель Белла-ЛаПадуллы и ее расширения. Особенности реализации мандатного доступа в реляционных СУБД. Метки доступа логических и физических объектов, их установление, изменение. Многоуровневая система доступа. Системные таблицы параметров мандатного доступа.

Скрытые каналы утечки информации в АИС. Скрытые каналы по памяти и времени, статистические скрытые каналы. Теоретические и технологические основы устранения скрытых каналов. Технологии представлений и разрешенных процедур. SQL-запросы с агрегатными функциями и представления данных.

4.2.2.2 Модели ролевого доступа и технологии рабочих групп пользователей

Проблемы проектирования и установления дискреционной системы прав доступа, управления (администрирования) системой доступа при большом количестве субъектов и объектов доступа.

Агрегирование прав доступа в функционально-обособленные сущности предметной области АИС – роли пользователей. Роль как типизованный субъект доступа, соответствующий должностным обязанностям и правам по определенной должности в организационно-штатном расписании организации, предприятия.

Двухфазная организация ролевого доступа – создание системы ролей с правами доступа и назначение ролей пользователям АИС. Сеансовый характер функционирования АИС с системой ролевого доступа. Авторизация пользователей с предоставленными ролями в сеансе работы с АИС.

Разновидности систем ролевого доступа – взаимоисключающие роли, совместимые роли, системы с иерархической организацией ролей.

Технологии рабочих групп пользователей. Групповое назначение прав доступа. Владелец и группа владельца объектов доступа. Проектирование групповой структуры пользователей АИС. Меры близости рабочих групп пользователей в пространстве доступа.

Различие рабочих групп и ролей пользователей. Отношение групп – вхождение одних рабочих групп в другие, доверительные отношения рабочих групп.

Роли пользователей в контексте безопасности. Системный администратор, пользователь, пользователь-владелец, аудитор (администратор безопасности).

4.2.2.3 Тематическое разграничение доступа в документальных АИС

Каталожные документальные системы (информационно-поисковые каталоги) и разграничение доступа к документам. Право чтения и право "прохода" каталога. Проблема техники "представлений" в иерархических каталогах для перекрытия скрытых каналов утечки информации по памяти.

Документальные информационно-поисковые системы (ИПС), основанные на тематическом индексировании (классификации) документов. Дескрипторные, иерархические и фасетные (многоаспектно-иерархические) тематические классификаторы.

Архитектура индексных информационно-поисковых систем. Поисковые образы (тематико-содержательные индексы) документов и поисковые образы поисковых запросов пользователей. Пертинентность и релевантность документов.

Тематический принцип разграничения (ограничения) доступа к документам в индексных документальных ИПС. Тематические полномочия пользователей.

Частичный порядок (уже, шире, несравнимо) и решетки на множестве тематических индексов документов при дескрипторной и иерархической классификации. Монорубрицированная и мультирубрицированная классификация на основе тематических иерархических рубрикаторах. Мультирубрики. Решетка мультирубрик.

Модель тематико-иерархического разграничения доступа в индексных документальных ИПС. Особенности информационного поиска и разграничения доступа.

4.2.2.4 Основы обеспечения информационной безопасности в распределенных многопользовательских АИС

Виды и программно-техническая структура распределенных АИС: системы "клиент-сервер", протокол ODBC, объектное связывание данных, технологии репликаций. Разновидности "клиент-серверных" АИС. Системы, основанные на технологиях терминального доступа. Системы, основанные на Web-интерфейсе.

Понятие распределенности АИС в аспекте безопасности. Монитор (ядро) безопасности АИС и его программно-техническая и информационно-структурная составляющая.

Особенности угроз и задач обеспечения безопасности в распределенных АИС.

Организация рабочих мест (сетевых рабочих станций) и привязка к ним пользователей. Контроль и управление доступом к БД с рабочих станций пользователей: по временному принципу (временному графику), по списку рабочих станций, с которых пользователю разрешен доступ, по количеству одновременных активных соединений (задач) пользователя с одной рабочей станции.

Защита вывода информации БД на внешний носитель данных. Удаление остаточной информации на носителях данных.

Механизмы и протоколы аутентификации в распределенных АИС. Авторизация пользователей.

Понятие уязвимости систем защиты. Характеристика основных уязвимостей.

Протоколирование и аудит в распределенных АИС. События и параметры, подлежащие протоколированию.

Атаки на распределенные АИС. Типология атак. Атаки в системах, основанных на IP-протоколах (SQL-инъекции и др.). Системы активного аудита (системы обнаружения атак). Сканеры безопасности.

4.2.3 Методы, модели и механизмы обеспечения целостности данных

4.2.3.1 Механизмы обеспечения целостности данных, реализуемые реляционными СУБД

Понятие целостности данных. Целостность данных в контексте логической модели данных (целостность значений полей и связей). Целостность данных, определяемая организационно-технологическими правилами предметной области АИС ("правилами бизнеса"). Ограничения целостности данных при проектировании таблиц и схемы БД.

Ограничения целостности данных, устанавливаемые и контролируемые ядром СУБД. Режимы обеспечения целостности связей таблиц при удалении данных.

Механизм событий, триггеров и хранимых процедур. Изменение данных как событие. Установление и контроль целостности данных на основе триггеров и хранимых процедур. Элементы языка SQL встроенный процедурный язык СУБД для установления и выполнения триггеров и хранимых процедур.

4.2.3.2 Модели обеспечения целостности данных в процессах коллективного доступа разделяемым информационным ресурсам

Дискреционная модель Кларка-Вильсона. Объекты, требующие контроля целостности (*constrained data items*), процедуры проверки целостности **(***integrity verification procedures***)**, корректно сформированные транзакции (не нарушающие ограничения целостности), тройки "субъект-транзакция-объект".

Мандатная модель К.Биба. Уровни целостности данных. Уровни доверия пользователям. Правила мандатного доступа, не нарушающие целостность данных (запрет "чтения вниз", запрет "записи вверх") как инверсия правилам мандатного доступа, не нарушающим конфиденциальность данных (в модели Белла-Лападуллы).

Проблемы и разновидности совместимости в практической реализации моделей Белла-ЛаПадуллы и К.Биба: на основе двух разных решеток безопасности (отдельных систем уровней конфиденциальности и целостности), на основе одной общей решетки, но с двумя отдельными метками для объектов и субъектов (на чтение, на запись).

4.2.3.3 Механизмы транзакций и обеспечение целостности данных в клиент-серверных СУБД

Транзакционная парадигма коллективной (одновременной) обработки данных в клиент-серверных АИС. Принципы "атомарности" (неделимости), "изоляции" транзакций. Проблема быстродействия сервера СУБД и параллельное выполнение транзакций. Фиксация (COMMIT) и откат транзакций (ROLLBACK).

Нарушения целостности, возникающие при совместной обработке данных, одновременном (параллельном) выполнении транзакций пользователей. Понятие и виды "грязных" (dirty) данных – "грязное чтение" (dirty read), "потерянные изменения" (lost update) и "неповторяющееся чтение" (unrepeatable read).

Протоколы выполнения и фиксации транзакций. Протоколы, основанные на "захватах" блокировках объектов. Двухфазной протокол выполнения и фиксации транзакций ("пессимистичный" режим выполнения транзакций). Тупики (*Deadlock*), их обнаружение и разрушение. Механизмы изоляции транзакций, основанные на временных метках объектов ("оптимистичный" режим выполнения транзакций).

4.2.4 Методы, механизмы и технологии обеспечения сохранности и правомерной доступности информации в АИС, БД и БнД

4.2.4.1 Резервирование, архивирование и журнализация БД

Предотвращение последствий угроз разрушения, потери данных в АИС в результате программно-аппаратных сбоев или некорректных действий пользователей на основе резервного сохранения и восстановления БД.

Организационные, технологические и программно-технические принципы политики резервирования и архивирования БД (временной режим/периодичность в зависимости от динамики изменений данных, размещение резервных копий и архивов на отдельных от рабочей БД носителях, сочетание средств ОС, СУБД и специальных утилит, нормативная регламентация хранения копий/архивов и процедур восстановления БД).

Резервные копии и архивы БД. Создание резервных копий БД путем пофайлового сохранения БД средствами ОС.

Архивирование БД или отдельных ее объектов (таблиц) средствами СУБД. Специальный формат файлов архива БД. Автономное (без останова и участия ядра СУБД) архивирование БД или ее отдельных объектов специальными утилитами СУБД.

Оперативное сохранение (журнализация) изменений данных ядром СУБД. Синхронная и асинхронная журнализация. Полное и инкрементное сохранение БД. Сценарии архивирования/журнализации и их языковое задание средствами встроенного языка СУБД.

Системы реального времени. "Горячее" резервирование. Главный/резервный серверы. "Прозрачность" для приложений. Автоматическое переключение серверов, "поднятие" "упавшего" сервера.

4.2.4.2 Технологии репликации данных в распределенных АИС

Технологии репликации как альтернатива технологиям "Клиент-сервер" в создании многопользовательских распределенных систем, основанных на "общей" БД. Понятие реплики БД, разрешение проблемы быстродействия обработки данных и повышение степени надежности сохранности данных.

Параллельная обработка и изменение данных реплик БД. Проблема целостности обрабатываемых данных – непрерывной согласованности значений и структуры данных во всех репликах системы.

Синхронная репликация данных (непрерывное тиражирование транзакций с любой реплики на все другие реплики). Двухфазный протокол реализации транзакций. Тупики и их разрешение.

Системы с отложенными обновлениями и временной несогласованностью данных. Обновление данных на основе отложенного выполнения транзакций, выполненных на разных репликах системы (асинхронная репликация). Программно-техническая структура репликации – БД-источник и/или БД приемник данных репликации, серверы репликации, хранилище данных репликации (очереди репликации). Правила (временной режим) синхронизации реплик. Устойчивость систем асинхронной репликации к выходу из строя одного из серверов репликации.

Частичные реплики. Повышение эффективности процессов репликации и решение проблем разграничения доступа на основе техники частичных реплик.

Тиражирование (репликация) изменений структуры данных. Метод "главной" реплики.

4.2.5 Критерии и стандарты защищенности АИС

4.2.5.1 Стандартизация требований к архитектуре, функциям и критериям оценки подсистем безопасности в АИС

Системная и функциональная архитектура защищенных АИС. Ядро ПО АИС и монитор безопасности. Функции ядра и функции монитора безопасности АИС.

Каталогизация (стандартизация) функциональных требований безопасности компьютерных систем. Номинально-ранговый подход к проблеме оценки (измерения) защищенности компьютерных систем. Каталоги функциональных требований, система уровней (классов) защищенности.

История и общая характеристика национальных, зарубежных и международных стандартов безопасности компьютерных систем.

4.2.5.2 Показатели защищенности СВТ/СУБД и классификация АС/АИС по требованиям защиты от несанкционированного доступа к информации

Руководящие документы ГосТехКомиссии (ныне ФСТЭК России) по защите информации от несанкционированного доступа. Концепция защиты, СВТ и АС.

Структура функциональных требований по защите от НСД к информации в СВТ/СУБД. Классы защищенности СВТ/СУБД и характеристика функциональных требований к их реализации. СУБД, сертифицированные по требованиям защиты от НСД к информации.

Структура функциональных требований по защите от НСД к информации в АС/АИС. Группы АС, классы защищенности АС и характеристика функциональных требований к ним.

4.2.5.3 Критерии оценки безопасности информационных технологий. Профили защиты СУБД

Концепция международного стандарта ИСО/МЭК 15408-2000 (российский национальный стандарт ГОСТ Р ИСО/МЭК 15408-2002): продукты и системы ИТ (изделия ИТ), объект и среда безопасности, каталог функциональных требований для всех видов изделий ИТ, профили защиты (ПЗ) для конкретных видов изделий ИТ и их сертификация, задание по безопасности (ЗБ) при разработке/создании конкретного изделия ИТ, парадигма доверия реализации разработчиками требований безопасности изделия ИТ через оценку изделия ИТ, оценочные уровни доверия, каталог требований доверия безопасности.

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).

Пример профиля защиты для СУБД. Основные функциональные требования безопасности СУБД. Требования безопасности для среды СУБД – базовой операционной системы. Требования доверия безопасности по (ОУД3).

4.2.6 Организационное обеспечение информационной безопасности АИС

4.2.6.1 Администрирование и эксплуатация АИС

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 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 АИС – 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).

5 ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Не предусмотрен учебным планом специальности

6 УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Рекомендуемая литература

6.1.1 Основная литература

1. *Смирнов С.Н.* Безопасность систем баз данных. – М.: Гелиос-АРВ, 2007. – 352с.
2. *Гайдамакин Н.А.* Информационная безопасность, автоматизированные информационные системы, базы и банки данных. Вводный курс. (электронный информационный ресурс)
3. *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.
4. *Емельянова Н.З, Партыка Т.Л., Попов И.И.* Основы построения автоматизированных информационных систем: Учебное пособие. – М.: ФОРУМ, ИНФРА-М, 2007. – 416с.

6.1.2 Дополнительная литература

1. *Гайдамакин Н.А.* Разграничение доступа к информации в компью-терных системах. - Екатеринбург: изд-во Урал. Ун-та, 2003. – 328 с.
2. *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.

3. *Романов В.П., Емельянова Н.З., Партыка Т.Л.* Проектирование экономических информационных систем: методология и современные технологии: Учебное пособие / - М.: «Экзамен», 2005.- 256с.
4. *Вендров А.М.* Проектирование программного обеспечения экономических информационных систем: Учебник / - М.: Финансы и статистика, 2000. – 347с.

6.1.3 Нормативно-методические документы

1. РД по стандартизации 50-680-88. Методические указания. Автоматизированные системы. Основные положения
2. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию
3. РД ГосТехКомиссии России. АС. Защита от НСД к информации. Классификация АС и требования по защите информации
4. ГОСТ Р 50739-95. СВТ. Защита от НСД к информации. Общие технические требования
5. ГОСТ Р 51624-2000
6. 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
7. РД ГосТехКомиссии России. Безопасность информационных технологий. Руководство по разработке профилей защиты и заданий по безопасности
8. ГОСТ 34.601-90. Информационная технология. Автоматизированные системы. Стадии создания
9. РД ГосТехКомиссии России. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты
10. РД ГосТехКомиссии России. Безопасность информационных технологий. Положение о разработке профилей защиты и заданий по безопасности
11. ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие вирусов. Типовое руководство
12. ГОСТ Р ИСО/МЭК 14764-2002. Информационная технология. Сопровождение программных средств
13. ГОСТ 34.603-92. Информационная технология. Виды испытаний автоматизированных систем

6.2 Средства обеспечения освоения дисциплины

6.2.1 Перечень средств обеспечения

В процессе изучения дисциплины используются:

1. Система компьютерных презентаций по материалам лекций

6.2.2 Программно-информационное обеспечение дисциплины

Справочные материалы на электроном 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

Специальные требования не предъявляются

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 "Общие положения по информационной безопасности АИС, БД и БнД"

1. Информация, данные, информационные технологии, автоматизированные информационные системы, СУБД
2. Информационная безопасность, угрозы, методы и механизмы обеспечения информационной безопасности в АИС и СУБД
3. Функциональная и системная архитектура АИС в контексте обеспечения информационной безопасности

По разделу "Методы, модели и механизмы обеспечения конфиденциальности данных"

1. Политика и модели разграничения доступа
2. Инструкции языка SQL для реализации установок дискреционного доступа, техники представлений
3. Разработка и анализ системы рабочих групп пользователей в АИС
4. Разработка и анализ системы разграничения доступа в информационно-поисковых каталогах и на основе иерархических рубрикаторах в индексно-тематических документальных АИС
5. Идентификация, аутентификация и аудит безопасности в распределенных АИС

По разделу "Методы, модели и механизмы обеспечения целостности данных "

1. Решение задач по обоснованию и установлению ограничений целостности данных при проектировании реляционных БД
2. Интегрирование мандатных моделей разграничения доступа и обеспечения целостности данных
3. Протоколы реализации и фиксации транзакций в клиент-серверных СУБД

По разделу "Методы, механизмы и технологии обеспечения сохранности и правомерной доступности информации в АИС, БД и БнД"

1. Резервирование, архивирование и журнализация данных
2. Репликация баз данных

По разделу "Критерии и стандарты информационной безопасности (защищенности) АИС"

1. Основные стандарты информационной безопасности АИС и их методология
2. Классы защищенности и функциональные требования их реализации в АС
3. Профили защиты СУБД

По разделу "Критерии и стандарты информационной безопасности (защищенности) АИС"

1. Особенности организации эксплуатации АИС
2. Администрирование защищенных АИС

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 профиля защиты СУБД

8.7 Перечень тем контрольных работ

- Методы, модели и механизмы обеспечения конфиденциальности данных
- Методы, модели и механизмы обеспечения целостности и правомерной доступности данных
- Стандарты информационной безопасности АИС

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 информационных систем
2. Функции и структура СУБД
3. Реляционная модель данных и язык SQL
4. Безопасность АИС, ее составляющие
5. Субъекты и объекты обеспечения информационной безопасности в АИС
6. Принципы, основные методы и механизмы обеспечения безопасности информации в АИС
7. Классификация (каталогизация), идентификация и спецификация угроз безопасности в АИС
8. Политика, модели и механизмы дискреционного разграничения доступа
9. Политика, модели и механизмы мандатного разграничения доступа
10. Скрытые каналы утечки информации в АИС, БД и БнД

11. Политика и модели ролевого доступа
12. Технологии индивидуально-группового доступа
13. Общая характеристика, виды и архитектура документальных АИС
14. Разграничение доступа в информационно-поисковых каталогах
15. Тематическое разграничение доступа в индексных документальных информационно-поисковых системах
16. Виды и программно-техническая структура распределенных АИС
17. Особенности политики и систем безопасности в распределенных АИС
18. Уязвимости систем защиты, системы активного аудита безопасности в распределенных АИС
19. Целостность данных в реляционных СУБД
20. Механизм событий, триггеров и процедур в процессах обеспечения целостности данных
21. Дискреционная модель обеспечения целостности данных Кларка-Вильсона
22. Мандатная модель обеспечения целостности даны Кена Биба
23. Объединение мандатных моделей Белла-ЛаПадуллы и Кена Биба
24. Транзакции и нарушения целостности данных
25. Протоколы выполнения и фиксации транзакций в клиент-серверных СУБД
26. Резервирование, архивирование и журнализация в базах данных
27. Технологии репликации данных в распределенных АИС
28. Стандартизация требований к архитектуре, функциям и критериям оценки подсистем безопасности в АИС
29. Показатели защищенности СВТ/СУБД и классификация АС/АИС по требованиям защиты от НСД к информации
30. Критерии оценки безопасности информационных технологий. Профили защиты СУБД
31. Общие положения по эксплуатации АИС
32. Особенности эксплуатации и администрирования защищенных АИС

8.11 Перечень ключевых слов дисциплины

Автоматизированные системы, автоматизированные информационные системы, базы данных, системы управления базами данных, модель организации данных, информационная безопасность, защита информации, угрозы безопасности, конфиденциальность, разграничение доступа, матрица доступа, дискреционное разграничение доступа, мандатное разграничение доступа, роли, рабочие группы, целостность данных, ограничения целостности, правомерная доступность информации, сохранность данных, клиент-серверные системы, транзакции, протоколы фиксации транзакций, журнализация данных, репликация баз данных, стандарты информационной безопасности, классы защищенности, функциональные требования защищенности, профили защиты, эксплуатация, администрирование