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

Методические указания

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

Екатеринбург
2008

СТУДЕНТАМ при изучении содержания дисциплины обратить особое внимание на ряд следующих **узловых моментов** по темам разделов

По теме "**Понятие, виды и структура АИС**"

Автоматизированные информационные системы – основной инструментарий современных информационных технологий.

АИС – человеко-машинная организационно-технологическая система, автоматизирующая процессы информационного обеспечения различных видов человеческой деятельности. Включает компоненты различной природы (информационную базу, программное и математическое обеспечение, технические средства хранения, отображения, обработки и выдачи информации, организационную и технологическую составляющую).

Два принципиально различных вида АИС – фактографического и документального характера.

В основе АИС – базы данных и специфическое ПО – СУБД.

Концепция баз данных как специфической формы организации, хранения и обработки информации в компьютерных системах, независимая от программных средств создания и обработки данных.

Природа СУБД как специфического вида программного обеспечения, обладающего одновременно общесистемным (добавлении к функциям операционных систем) и прикладным характером.

По теме "**Общая характеристика составляющих, методов и механизмов обеспечения информационной безопасности АИС**"

Особенность и специфичность информационных технологий (автоматизированных информационных систем) – существенное повышение значения и требований по обеспечению информационной безопасности, заключающейся в обеспечении безопасности информации и надежности функций АИС. Отсюда – требования безопасности не просто обеспечивающая сторона АИС, непременное условие их функциональности

Формализация АИС в контексте информационной безопасности – субъекты (процессы, процедуры, инициируемые пользователями АИС) и объекты (данные в виде организационных элементов БД), потоки информации, вызываемые действиями субъектов над объектами, которые могут приводить к нарушению конфиденциальности, целостности и доступности данных. Отсюда необходимость наличия в архитектуре ПО АИС на уровне ядра специального компонента обеспечения безопасности.

Каталоги угроз как основа обеспечения полноты анализа, идентификации и учета (противодействия) угроз при создании и эксплуатации АИС.

Важность учета принципов обеспечения информационной безопасности, в особенности принципов разумной достаточности, системности/комплексности, непрерывности, управляемости, унификации/оригинальности при разработке функциональной и системной архитектуры подсистем безопасности АИС.

Систематика методов и механизмов обеспечения информационной безопасности АИС, как основа реализации принципов комплексности, системности и целенаправленности.

По теме "**Дискреционные и мандатные модели разграничения доступа к информации в АИС, БД и БнД**"

Дискреционные модели и механизмы разграничения доступа – максимальная зернистость (детальность) разграничения доступа, простота и обработанность (особенно в СУБД) программно-технических и информационно-организационных механизмов реализации, наличие в языке SQL реляционных СУБД инструкций для программной реализации конкретной политики разграничения доступа. С другой стороны – слабые защитные характеристики дискреционного доступа, большие объемы работы администраторов АИС по установлению и поддержанию систем разграничения доступа, отсюда вероятность ошибок администрирования в виде предоставления излишних (необоснованных) прав доступа или наоборот, непредставление пользователям требуемых прав доступа, сложности в реализации целенаправленной политики разграничения доступа при большом количестве пользователей и объектов доступа (логических элементов данных).

Мандатные модели и механизмы разграничения – теоретически доказанная безопасности информационных потоков при мандатном доступе (изъяны, бреши безопасности могут возникать только из-за ошибок в архитектурной и программной реализации), возможность построения АИС, удовлетворяющих нормативным требованиям по работе со сведениями, составляющими государственную тайну. С другой стороны – определенная абстрактность (схематичность) мандатных механизмов в отношении их реализации в современном ПО, и, в особенности, в реляционной модели организации данных, отсюда – необхомость дополнительных программных и вычислительных ресурсов для реализации мандатных механизмов на уровне ядра и интерфейса АИС, и вследствие этого – снижение функциональности и эффективности функционирования АИС.

Скрытые каналы утечки информации как наиболее сложная проблема информационной безопасности АИС. Теоретико-вероятностная природа возникновения скрытых каналов утечки информации, методология и технологии их перекрытия в АИС.

По теме "**Модели ролевого доступа и технологии рабочих групп пользователей**"

Роли и рабочие группы пользователей – приемы и технологии организации и повышения управляемости разграничением доступа при большом количестве пользователей и объектов доступа.

В основе формирования и использования ролей и системы рабочих групп – функционально-организационная и организационно-технологическая структура предметной области АИС, коллектива пользователей АИС.

Два подхода к проектированию и анализу системы рабочих групп – "сверху" по функциональной и организационной структуре пользователей АИС, и "снизу" по схожести потребностей пользователей в доступе к данным. Использования в процедурах разработки и анализа индивидуально-групповой структуры коллектива пользователей АИС количественных мер близости субъектов в пространстве доступа.

По теме "**Тематическое разграничение доступа к информации в документальных АИС**"

Принципиальные отличия документальных АИС от фактографических по принципу организации и выдачи данных (единичным элементом данных выступает неструктурированный текстовый документ).

Архитектура индексных АИС, суть и виды индексирования текстов,. Иерархические тематические каталоги, индексные полнотекстовые системы и системы на основе иерархических рубрикаторов как три основные разновидности документальных информационно-поисковых систем.

Особенности и проблемы разграничения доступа к каталогах (каталожных ИПС).

Тематико-иерархический принцип и модель разграничения доступа. Возможность сочетания программно-процедурных механизмов поиска и разграничения доступа как способа сочетания высокой функциональности и защищенности документальных ИПС.

По теме "**Основы обеспечения информационной безопасности в распределенных АИС**"

Принципы создания, функционирования распределенных АИС (независимость от физической структуры размещения данных, "изолированность" пользователей). Основные виды программно-технической реализации распределенных АИС (клиент-серверные системы на основе протоколов ODBC, системы объектного связывания данных, системы, основанные на Web-интерфейсах, системы терминального доступа и системы репликаций БД).

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.

Принципиальное значение для обеспечения безопасности механизмов и протоколы аутентификации. Основные виды и протоколы процедур идентификации/аутентификации.

Понятие и природа уязвимостей (брешей) в системах защиты.

Сущность и политика аудита безопасности. Системы активного аудита и сканеры безопасности как специальный инструментарий администраторов безопасности в распределенных АИС и компьютерных сетях.

По теме "**Механизмы обеспечения целостности данных, реализуемые реляционными СУБД**"

Целостность данных как одна из составляющих защищенности (безопасности) информации.

Целостная составляющая реляционной модели данных.

Ограничения целостности данных, определяемые правилами предметной области АИС.

Механизм событий, триггеров и хранимых процедур как основная парадигма обработки и обеспечения целостности данных в современных СУБД.

По теме "**Механизмы транзакций и обеспечение целостности данных в клиент-серверных СУБД**"

Транзакционная технология коллективной (одновременной) обработки данных в клиент-серверных АИС как основа реализации принципа "изоляции пользователей" в распределенных АИС, обеспечения быстродействия и эффективности распределенных АИС.

Виды и суть нарушений (коллизий) целостности данных при "параллельном" осуществлении транзакций с общими данными.

Монитор транзакций как важнейший программный элемент ядра клиент-серверных СУБД. Разновидности протоколов осуществления и фиксации транзакций, "тупики" их обнаружение и разрешение.

По теме "**Резервирование, архивирование и журнализация БД**"

Резервирование, архивирование и журнализация процессов изменения данных – как основная мера профилактики и восстановления данных после сбоев и разрушений.

Должна разрабатываться и реализовываться средствами СУБД, ОС и организационно-технологическими процедурами специальная политика резервирования, архивирования и журнализации данных в зависимости от динамики изменения данных в предметной области АИС и особенности функционирования АИС.

Программно-процедурные режимы журнализации в современных СУБД.

По теме "**Технологии репликации данных в распределенных АИС**"

Репликация баз данных как альтернатива технологиям клиент-сервер и объектного связывания данных при создании распределенных АИС.

Репликация баз данных как метод обеспечения сохранности и правомерной доступности данных.

Программно-техническая структура и режимы репликации.

По теме "**Стандартизация требований к архитектуре, функциям и критериям оценки подсистем безопасности в АИС**"

Методология измерения (оценки) защищенности (безопасности) АИС. Номинально-ранговый подход. Уровни (классы) защищенности и тематические каталоги функциональных требований к архитектуре и механизмам защиты по соответствующим классам/уровням.

История и направления развития стандартов информационной безопасности.

Основные национальные и международные стандарты в сфере информационной безопасности АИС.

По теме "**Показатели защищенности СВТ/СУБД и классификация АС/АИС по требованиям защиты от несанкционированного доступа к информации**"

Особенности классов защищенности и функциональных требований, устанавливаемых Руководящими документами Гостехкомиссии России по защите от НСД к АС по сравнению с идеологией "Оранжевой книги".

Требования по уровням защищенности СВТ (ОС, СУБД) для создания АС/АИС соответствующих классов защищенности.

По теме "**Критерии оценки безопасности информационных технологий. Профили защиты СУБД**"

"Общие критерии" – обобщение мирового опыта по механизмам обеспечения информационной безопасности в компьютерных системам.

Главная особенность ОК – охват всех возможных видов продуктов и систем ИТ, а также всех этапов и процессов жизненного цикла изделий ИТ.

Основная схема ОК – полный каталог известных функциональных требований (механизмов) обеспечения ИБ – формирование на этой основе требований по конкретным видам и группам продуктов ИТ в виде т.н. профилей защиты, которые подлежат сертификации – разработка изделий ИТ на основе заданий по безопасности, формируемый по соответствующим профилям защиты.

Особое внимание в контексте информационной безопасности АИС – профили защиты СУБД, структуры и содержания их основных разделов.

По теме "**Администрирование и эксплуатация АИС**"

Администрирование и эксплуатация защищенных КС представляет собой особый вид профессиональной деятельности, включающий комплекс работы специфичных для эксплуатации технических изделий, обеспечения бесперебойного и правильного функционирования ПО, сохранности и целостности информационной базы, управление средствами защиты информации, анализ и устранение угроз безопасности, возникающих па этапе использования КС и ряд других операций и процедур.

П Р Е П О Д А В А Т Е Л Ю целесообразно использовать следующие методические приемы и формы проведения занятий.

Изложение материала сопровождать примерами в отношении программно-алгоритмических механизмов современных СУБД, на базе которых строятся АИС.

На самостоятельную работу слушателям давать задания по изучению и отработке основных стандартов, регламентирующих функциональные требования к архитектуре и механизмам защиты АИС.

Знания закреплять на семинарских занятиях и контрольных работах.

Практические занятия строить на основе решения задач по тематикам проектирования и анализа систем индивидуально-группового разграничения доступа, установления системы уровней допуска и грифов конфиденциальности объектов мандатного доступа и т.д., закрепляющих и углубляющих знания по моделям и механизмам обеспечения информационной безопасности. Часть практических заданий и задач целесообразно отрабатывать в среде СУБД, обеспечивающей соответствующие механизмы и процедуры, например в среде СУБД MS Access, Линтер. С этой целью целесообразно разработать учебный БнД (базу данных и прикладной компонент АИС).

Также целесообразным является отработка индивидуальных заданий студентам по тематике спецкурса, которые коррелируют с их дипломным и/или курсовым проектированием.

На практических занятиях и в ходе самостоятельной работы студентов необходимо использовать информационные электронные базы соответствующих нормативно-методических документов (стандартов).