**Лекция1 Проблемы обеспечения безопасности ИС**

**1.Постановка задачи обеспечения**

**информационно й безопасности ИС**

Эффективное управление сложными организационными системами требует использования современных средств автоматизации. Основная цель всякой системы обработки информации —полное и своевременное удовлетворение информационных потребностей пользователей. Успешное решение этой задачи возможно только тогда, когда для каждого контингента пользователей автоматизированных систем обработки информации создана отвечающая их потребностям среда обработки данных. Одной из важнейших характеристик качества информационной системы —ядра всякой системы автоматизированного управления — является уровень обеспечения ее информационной безопасности. Важность поиска эффективных методов решения проблемы обеспечения информационной безопасности (ИБ) автоматизированных систем информационного обеспечения управления определена в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации 9 сентября 2000 г.

Основой программных решений, характерных для информационных систем, являются системы управления базами данных, работающие как надстройка над операционной системой, а также специализированные серверы приложений. Средства реализации процессов обработки данных встраивались или интегрировались с СУБД.

Ориентация на использование универсального клиента (браузера) как единого интерфейса доступа к корпоративной информационной инфраструктуре стала общепринятой.

Необходимость и целесообразность интеграции базовых программных технологий обработки данных привела к формированию новых требований по повышению качества, скорости и безопасности программных комплексов, обеспечивающих надежное функционирование программных средств реализации компонент корпоративных информационных систем. Производители программных средств и провайдеры услуг Интернета предприняли усилия по построению схем прямого выхода на потребителя и непосредственной интеграции корпоративной информации в технологические схемы деятельности предприятия или организации и, в частности, взаимодействия автоматизированных систем с деловыми партнерами.

Вопросы информационной безопасности баз данных целесообразно рассматривать с двух взаимодополняющих позиций:

* оценочные стандарты, направленные на классификацию информационных систем и средств их защиты по требованиям безопасности;
* технические спецификации, регламентирующие различные аспекты реализации средств защиты.

Важно отметить, что между этими видами анализа нет четко определенной границы. Оценочные стандарты выделяют важнейшие, с точки зрения ИБ, аспекты автоматизированных информационных систем, играя роль архитектурных спецификаций. Технические спецификации построения средств защиты определяют, каким образом строить информационную систему конкретной архитектуры.

Интеграция программных средств обработки информации и средств ее доставки приводит к необходимости создания комплексных программных систем обеспечения безопасности автоматизированных информационных систем. Комплексная система обеспечения информационной безопасности должна строиться с учетом средств и методов, характерных для четырех уровней информационной системы:

* уровня прикладного программного обеспечения, отвечающего за взаимодействие с пользователем;
* уровня системы управления базами данных, обеспечивающего хранение и обработку данных информационной системы;
* уровня операционной системы, отвечающего за функционирование СУБД и иного прикладного программного обеспечения;
* уровня среды доставки, отвечающего за взаимодействие информационных серверов и потребителей информации.

Система защиты должна эффективно функционировать на всех этих уровнях.

Проблема обеспечения безопасности автоматизированных информационных систем может быть определена как решение трех взаимосвязанных задач по реализации требуемого уровня:

* *конфиденциальности* — обеспечения пользователям доступа только к данным, для которых пользователь имеет явное или неявное разрешение на доступ (синонимы — секретность, защищенность);
* *целостности* — обеспечения защиты от преднамеренного или непреднамеренного изменения информации или процессов ее обработки;
* *доступности* — обеспечения возможности авторизованным в системе пользователям доступа к информации в соответствии с принятой технологией (синоним — готовность).

Методы и средства решения трех отмеченных взаимосвязанных задач характерны для любых автоматизированных информационных систем. В частности, для систем принятия решений задача обеспечения конфиденциальности предусматривает комплекс мер по предотвращению несанкционированного доступа к информации ограниченного пользования. Задача обеспечения целостности предусматривает комплекс мер по предотвращению умышлен­ ного или случайного изменения или уничтожения информации, используемой системой принятия решений. Задача обеспечения доступности информации предусматривает систему мер по поддержке всем уполномоченным пользователям доступа к ресурсам системы в соответствии с принятой технологией (например, круглосуточно).

Решение задачи обеспечения конфиденциальности базируется на том, что существует внешний по отношению к системе объект, который определяет, какой взаимодействующий с системой субъект к какой информации должен иметь доступ. Особенностью, характерной для автоматизированных систем, является тот факт, что доступность или недоступность некоторой информации для конкретного субъекта определяется не только решением внешнего по отношению к системе объекта, но и логической непротиворечивостью соответствующих требований. То есть содержательное решение о разграничении доступа должно вкладываться в модель разграничения доступа, которая поддерживается системой.

Современный уровень развития распределенной обработки данных характеризуется размещением логически единой ин формационной базы в сетевой среде, объединяющей различные компьютеры, асинхронной многопользовательской обработкой с развитыми средствами разграничения доступа. При этом реальная сложность организации управления доступом должна быть скрыта от пользователя. Логическое пространство баз данных должно выглядеть для пользователя единым, то есть, как если бы вся база располагалась на его локальном компьютере.

Современная СУБД—это совокупность взаимодействующих процессов и совместно используемая область оперативной памяти, обеспечивающая логическое управление данными стандартными языковыми средствами в соответствии с предписанной (на­ строенной) технологией. Управляемая система баз данных, как правило, является распределенной, то есть физически может быть размещена на нескольких носителях, а возможно, и в нескольких узлах, взаимодействие которых осуществляется по протоколам транспортного уровня. Логически распределенная база данных может представлять единое целое либо являться совокупностью синхронно или асинхронно обновляемых копий.

Анализ информационной безопасности СУБД должен быть проведен по двум направлениям:

* безопасность архитектурных решений и их программных реализаций, собственно, в СУБД;
* безопасность взаимодействия с внешними по отношению к СУБД программными и аппаратными компонентами.

Анализ безопасности архитектурных решений и их программных реализаций в СУБД должен включать исследование следующих проблем: идентификация и аутентификация субъектов системы, технологии реализации дискреционной, мандатной и ролевой модели доступа к ресурсам системы, реализация аудита действий пользователей.

Широко используемым, простым и эффективным способом реализации разграничения доступа является использование представлений (view). Представление — это поименованная динамически поддерживаемая сервером выборка из одной или нескольких таблиц. Оператор SELECT, определяющий выборку, ограничивает видимые пользователем данные. Кроме того, пред­ ставление позволяет эффективно ограничить данные, которые пользователь может модифицировать. Сервер гарантирует актуальность представления, то есть формирование представления (материализация соответствующего запроса) производится каждый раз при использовании представления. Используя представления, администратор безопасности ограничивает доступную пользователям часть базы данных только теми данными, которые реально необходимы для выполнения его работы.

Специфическим для СУБД средством обеспечения информационной безопасности являются триггеры. Триггеры —это совокупности предложений языка SQL или некоторого иного процедурного языка, автоматически запускаемые сервером при регистрации определенных событий в системе. Триггеры выполняются системой автоматически до или после возникновения предопределенных событий, таких, как выполнения операций INSERT, UPDATE, DELETE в некоторой таблице. Обычно рассматривают два способа использования триггеров для повышения защищенности системы: дополнительный контроль допустимости действий пользователя и ведение специализированного (нестандартного) аудита действий пользователя. Особенностью триггеров является автоматически реализуемая возможность выполнить необходимые проверки полно­ мочий перед выполнением операций над таблицами. Дополнительно отметим, что на одном множестве таблиц может быть определено несколько триггеров. Комбинации триггеров, выполняемых до и после операций, позволяют создавать изощренные механизмы проверки допустимости тех или иных действий в базе данных и фиксации (или откате) их результатов. Современные СУБД промышленного уровня поддерживает триггеры, запускаемые для определенных системных событий, в частности: начала и завершения сессии взаимодействия пользователя с системой, запуска и останова экземпляра сервера баз данных, создания и уничтожения объектов и т.п.

Новым направлением для СУБД промышленного уровня является наличие встроенных механизмов шифрования на уровне столбцов таблиц, в основном на базе алгоритмов DES и AES. Представлены встроенные генераторы псевдослучайных последовательностей и алгоритмы вычисления хеш-функций основных, распространенных в США и Европе стандартов. Реализовано явное и неявное управление ключами.

Анализ безопасности взаимодействия с внешними компонентами должен включать вопросы сопряжения с элементами операционной системы —анализ управляющих и информационных потоков вниз — и вопросы сопряжения с программным обеспечением промежуточного уровня (прослушивающие процессы, HTTP- серверы, мониторы транзакций и т. п.) — анализ управляющих и информационных потоков вверх.

Исследование безопасности СУБД должно включать и изучение инсайдерских рисков: возможностей пользователей СУБД несанкционированно осуществлять чтение и запись в файлы и устройства операционной системы, включая возможность модификации записей аудита, осуществляемых во внешние файлы.

Исследование вопросов сопряжения с программным обес­ печением промежуточного уровня должно включать: выявление портов взаимодействия с внешним программным обеспечением и механизмов их активизации и переназначения (внутренние и внешние); устойчивость к перегрузкам каналов шумовым трафиком и вставкам ложных пакетов; возможности внутреннего и внешнего управления активизацией и перенастройкой параметров протоколов ODBC и JDBC; анализ алгоритмов и технологий линейного шифрования трафика межсерверного обмена и взаимодействия клиентского программного обеспечения с серверами баз данных.

Полноценная система обеспечения безопасности должна обладать развитыми средствами аудита, то есть автоматического ведения протоколов действий пользователей системы. В СУБД средство ведения аудита может быть реализовано в виде набора возможностей, управляемых языковыми средствами системы, или независимой утилиты (пакета). Средства аудита выполняют фиксацию информации об активности пользователей системы в словаре данных или в файле операционной системы — журнале аудита. Информация о настройках системы аудита хранится в специальном конфигурационном файле. Файл настройки или параметры команды активизации аудита определяют перечень событий, которые фиксируются системой аудита. Исследование средств аудита должно включать вопросы устойчивости системы аудита к несанкционированному изменению параметров системы и собственно данных аудита, а также избирательность средств аудита, включая возможность оптимизации параметров при заданных (стоимостных) критериях и ограничениях на объем используемых ресурсов системы.

**2** **Этапы научного формирования проблемы обеспечения информационной безопасности баз данных**

Первоначально проблема обеспечения безопасности данных возникла при расширении круга пользователей ЭВМ и вычислительных систем. Увеличение количества ЭВМ и областей их применения расширило возможности модификации, хищения и уничтожения данных. Появление автоматизированных информационных систем (АИС) еще более усугубило проблему обеспечения безопасности данных. Можно выделить следующие этапы развития концепций обеспечения безопасности данных.

Центральной идеей первого этапа являлось намерение обеспечить безопасность данных механизмами, функционирующими по строго формальным алгоритмам. Для создания таких механизмов использовались технические и, в основном, программные средства. Программные средства защиты включались в состав операционных систем и систем управления базами данных. Слабым звеном разработанных механизмов защиты была технология разграничения доступа пользователей к данным. Поэтому следующим шагом к повышению эффективности защиты стала организация дифференцированного доступа к данным. Однако всесторонние испытания таких систем, как MULTICS и ADEPT-50, показали, что указанные системы, с точки зрения обеспечения безопасности данных, имеют множество недостатков. По мере усложнения программных систем, увеличения числа пользователей АИС и стало ясно, что необходима разработка идей защиты данных на более высоком уровне абстракции.

Главным достижением второго этапа стала разработка концепции и реализации специального программного компонента, управляющего программными и, частично, аппаратными средствами защиты данных — ядра безопасности. В составе операционных систем ядро безопасности реализовывалось как функционально самостоятельная подсистема управления механизмами защиты данных, которая включала технические, программные, и лингвистические средства. Этот этап также характеризовался интенсивным развитием технических и криптографических средств защиты.

Концепции и технологии защиты данных в СУБД в основном состояли из модификаций соответствующих разработок для операционных систем. По мере развития теории моделей данных и языка SQL стало ясно, что проблема обеспечения безопасности баз данных имеет свою специфику, в первую очередь в области информационного и лингвистического обеспечения. По мере осознания роли собственника информации совершенствовалась технология механизмов защиты, которыми могли бы управлять пользователи АИС. Однако, несмотря на принимаемые меры, обеспечение эффективной защиты данных оказалось недостижимым, о чем свидетельствовали многочисленные факты нарушения безопасности данных.

Накопление и осмысление как успешного, так и негативного опыта в сфере инцидентов в области автоматизированной обработки информации составили основное содержание третьего этапа развития проблемы. Проблема обеспечения информационной безопасности трансформировалась от описательного до научного уровня осмысления. Основной отличительной особенностью третьего этапа стало применение принципа системности. Принцип системности требует, чтобы обеспечение безопасности данных представляло собой регулярный процесс, осуществляемый на всех этапах жизненного цикла АИС при комплексном использовании всех средств и механизмов защиты. При этом все средства и механизмы, используемые для защиты данных, объединяются в систему обеспечения безопасности данных, которая должна обеспечивать многоуровневую защиту данных не только от злоумышленников, но и от обслуживающего персонала АИС, а также случайных ошибок пользователей.

Начало этим процессам было положено исследованиями вопросов защиты компьютерной информации, проведенными в конце 70-х — начале 80-х гг. Национальным центром компьютерной безопасности (NCSC —National Computer Security Center) министерства обороны США. Результатом этих исследований явилась публикация министерством обороны США в 1983 г. документа под названием

«Критерии оценки надежных компьютерных систем», впоследствии по цвету обложки получившего название «Оранжевая книга». Этот документ стал фактически первым стандартом в области создания защищенных компьютерных систем и впоследствии основой организации системы сертификации компьютерных систем по критериям защиты информации.

Подходы к построению и анализу защищенных систем, пред­ ставленные в «Оранжевой книге», послужили методологической и методической базой для дальнейших исследований в этой сфере. В 1991 г. NCSC был опубликован документ— Интерпретация

«Критериев оценки надежных компьютерных систем» в приме­ нении к понятию надежной системы управления базой данных. Этот документ, конкретизирующий и развивающий положения «Оранжевой книги» для решения задачи создания и оценки защищенных СУБД, известен также как «Розовая книга».

В конце 80-х-начале 90-х гг. аналогичные исследования по проблемам компьютерной безопасности были проведены во многих странах и созданы соответствующие национальные стандарты в этой сфере. В России Государственной технической комиссией при Президенте Российской Федерации (Гостехкомиссией) были разработаны и в 1992 г. опубликованы «Руководящие документы по защите от несанкционированного доступа к информации», определяющие требования, методику и стандарты построения защищенных средств вычислительной техники и автоматизированных систем.

Во всех перечисленных выше документах уровень безопасности средств вычислительной техники или программного обеспечения характеризуется принадлежностью к одному из иерархически упорядоченных классов. Иерархическая упорядоченность классов защищенности подразумевает, что если наличие некоторого средства защиты от несанкционированного доступа требуется для вычислительной техники или программного обеспечения определенного класса, то это же средство потребуется и для средства вычислительной техники более высокого класса.

Существо требований к оцениваемой системе может только усиливаться при переходе к более высоким классам защищенности. Например, «Руководящие документы по защите от несанкционированного доступа к информации» определяют, что самый низкий класс— седьмой, самый высокий— первый. Наличие некоторых средств защиты от несанкционированного доступа может требоваться только для некоторого множества высоких классов защищенности. Наличие или отсутствие конкретного средства защиты от несанкционированного доступа к данным является показателем защищенности средства вычислительной техники. Всего в руководящих документах сформулирован 21 показатель.

Подобным образом построена система оценки защищенности автоматизированных информационных систем. По защищенности процессов обработки информации все автоматизированные системы делятся на три группы.

Третья группа включает в себя автоматизированные системы, в которых работает один пользователь. Предполагается, что он допущен до всей информации, и информация размещена на носителях одного уровня конфиденциальности. Вторая и первая группы включают многопользовательские системы, в которых информация обрабатывается и хранится на носителях различного уровня конфиденциальности. Если пользователь имеет одинаковые права доступа ко всей обрабатываемой и хранимой информации, то автоматизированная система относится ко второй группе. В тех же случаях, когда не все пользователи имеют права доступа ко всей информации, система относится к первой группе.

Все автоматизированные системы по степени защищенности от несанкционированного доступа подразделяются на девять классов. Внутри каждой группы соблюдается иерархия классов по требованиям к защите, с усилением требований в порядке перечисления классов.

Комплекс программно-технических средств и организационных

мер по защите информации от несанкционированного доступа реализуется системой защиты информации. Система защиты информации должна быть рассмотрена как состоящая из четырех подсистем:

* подсистемы управления доступом;
* подсистемы регистрации и учета;
* криптографической подсистемы;
* подсистемы обеспечения целостности.

Процесс аттестации конкретной автоматизированной информационной системы состоит в проведении экспертизы с целью отнесения системы к определенному классу. Процесс экспертизы состоит из формальной проверки наличия свойств, перечень которых определен в соответствующем руководящем документе (стандарте).

Накопленный опыт в области обеспечения информационной безопасности, развитие теории информационной безопасности стали объективной основой стандартизации в данной сфере. Стандартизация характеризует определенный уровень зрелости области человеческой деятельности. Разработка и внедрение стандартов в области информационной безопасности характеризует следующий, четвертый этап развития. На этом этапе ставится и решается задача управления обеспечением информационной безопасности конкретного объекта, в частности, баз данных. Целью управления является обеспечение требуемого уровня защищенности информационных активов от объективно существующих угроз. Требуемый уровень защищенности определяется как разумный баланс между потенциальным ущербом, связанным с реализациями существующих угроз, и затратами на обеспечение процесса управления.

В 1990 г. представителями государственных организаций США, Канады, Великобритании и ряда других стран были развернуты работы по созданию международного стандарта в области оценки безопасности информационных технологий. Работа по созданию нового стандарта координировалась Международной организации по стандартизации (ISO) и была направлена в первую очередь на унификацию (гармонизацию) национальных стандартов в области оценки безопасности и повышение уровня доверия к оценке безопасности информационных технологий.

Официальный текст международного стандарта ISO/IEC 15408 был издан 1 декабря 1999 г. Принятие этого стандарта, известного также как «Общие критерии», отразило изменения, происходящие в идеологии подхода к построению безопасных информационных технологий, в частности, защищенных информационных систем и их программного ядра — СУБД. В отличие от «Оранжевой книги» и руководящих документов Гостехкомиссии в новом стан­ дарте отсутствует фиксированный набор классов защищенности. Основная идея «Общих критериев» состоит в разделении всех требований безопасности на две категории: функциональные, обеспечивающие безопасность информационных технологий, и требования гарантии оценки, оценивающие правильности и эффективность реализации функциональных требований.

В 2002 г. на основе аутентичного текста ISO/IEC 15408 был принят российский стандарт ГОСТ Р ИСО/МЭК 15408-2002

«Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».

Близкий подход к анализу защищенности ИС был предложен в британском стандарте BS 7799 «Практические правила управления информационной безопасностью», принятом в 1995 г. Содержательное существо стандарта состоит в обобщении опыта обеспечения информационной безопасности ИС различного назначения. Стандарт BS 7799 послужил основой для разработки стандарта ISO 17799, который был принят в конце 2000 г.

Базис стандарта состоит в определении и оценке уязвимых мест в анализируемой информационной системе, оценке уровня существующих угроз и определения комплекса мер, позволяющего снизить риски до приемлемого для организации уровня. Выбор комплекса осуществляется на основе стоимостного анализа потенциальных потерь, связанных с реализацией конкретных угроз.

Стандарт содержит практические правила обеспечения безопасности ИС для всех этапов жизненного цикла системы. Правила интегрированы в комплексный метод и основаны на проверенных практикой приемах и технологиях. Например, стандарт предписывает использовать определенные средства идентификации и аутентификации пользователей (или процессов), средства резервного копирования, антивирусный контроль и т. д.

Соблюдение предписанных технологий обеспечения ин­ формационной безопасности гарантирует некоторый базовый уровень безопасности ИС. В случае повышенных требований к безопасности ИС производится оценка ценности ресурсов, характеристик информационных рисков и уязвимости системы, на основе которых осуществляется выбор системы защиты ин­ формационных ресурсов.

**3.Критерии качества баз данных**

Современные базы данных являются одними из массовых специфических объектов в сфере информатизации, для которых в ряде областей необходимо особенно высокое качество и квалифицированное системное проектирование.

При выполнении анализа безопасности систем баз данных целесообразно рассматривать два компонента: систему программ управления данными и совокупность данных, упорядоченных по некоторым правилам. Поэтому и при анализе качества системы баз данных выделяют два основных компонента:

* + - программные средства системы управления базой данных (СУБД), независимые от сферы их применения, структуры и смыслового содержания накапливаемых и обрабатываемых данных;
    - информацию базы данных, доступную для накопления, упорядочивания, обработки и использования в конкретной проблемно-ориентированной сфере применения.

*Первым компонентом* для системного анализа и требований к качеству является комплекс программ СУБД. Практически весь набор характеристик и атрибутов качества программных систем, изложенный в стандарте ISO 9126, в той или иной степени может использоваться при формировании требований к качеству СУБД. Особенности состоят в адаптации и изменении акцентов при выборе и упорядочении этих показателей. Во всех случаях важнейшими характеристиками качества СУБД являются требования к функциональной пригодности для процессов формирования и изменения информационного наполнения БД администраторами, а также доступа к данным и представления результатов пользователям БД. Качество интерфейса специалистов с БД, обеспечиваемого средствами СУБД, определяется, в значительной степени, субъективно, однако имеется ряд характеристик, которые можно оценивать достаточно корректно.

В зависимости от конкретной проблемно-ориентированной области применения СУБД, приоритет при системном анализе требований к качеству может отдаваться различным конструктивным характеристикам: либо надежности и защищенности применения (финансовая сфера), либо удобству использования малоквалифицированными пользователями (социальная сфера), либо эффективности использования ресурсов (сфера материально- технического снабжения). Однако практически во всех случаях сохраняется некоторая роль ряда других конструктивных показа­ телей качества. Для каждого из них необходимо анализировать и определять его приоритет для конкретной сферы применения, меры и шкалы необходимых и допустимых характеристик качества.

*Вторым компонентом* БД является собственно накапливаемая и обрабатываемая информация. В системах баз данных доминирующее значение приобретают сами данные, их хранение и технология обработки.

Применяемые требования и показатели качества должны быть практически значимы для обладателей информационных ресурсов и пользователей. Кроме того, каждый выделяемый показатель качества систем баз данных должен быть пригоден для достаточно достоверного оценивания или измерения, а также для сравнения с требуемым значением, определенным в техническом задании на проектирование системы.

Характеристики качества систем баз данных можно разделить на функциональные и конструктивные.

*Функциональная пригодность* баз данных при проектировании определяется на основании требований реальным значениям необходимых показателей и критериев качества. Особенно сложной эта задача является для больших и, как правило, распределенных баз данных, связанных с обработкой разнообразной и многоаспектной информацией об анализируемых объектах. Мерой качества функциональной пригодности может быть степень соответствия доступной пользователям информации целям создания, назначения и функциям системы баз данных. Функциональная пригодность систем баз данных также отражается следующими характеристиками:

* + - полнотой накопленных описаний объектов — относи­ тельным числом объектов или документов, имеющихся в БД, к общему числу объектов по данной тематике или по отношению к числу объектов в аналогичных БД того же назначения;
    - идентичностью данных—относительным числом описаний объектов, не содержащих дефекты и ошибки, к общему числу документов об объектах систем баз данных;
    - актуальностью данных — относительным числом устаревших данных об объектах в ИБД к общему числу накопленных и обрабатываемых данных.

К *конструктивным характеристикам* качества информации систем баз данных в целом можно отнести практически все показатели качества программных систем, представленных в стандарте ISO 9126.

Требования к информации баз данных также должны со­ держать особенности обеспечения ее надежности, актуальности (достоверности), эффективности использования вычислительных ресурсов и приемлемого уровня сопровождения. Содержание и сущность этих конструктивных характеристик как базовых понятий и характеристик качества целесообразно использовать при проектировании информационных систем. Меры и шкалы для оценивания конструктивных характеристик в значительной степени могут применяться те же, что при анализе качества программных средств.

Особо выделяются характеристики достоверности данных и защищенности информации.

*Актуальность (достоверность) данных* — это степень соответствия информации об объектах в системе баз данных моделируемым реальным объектам в данный момент времени. Причинами нарушения актуальности данных являются изменения самих объектов, которые могут несвоевременно или некорректно отображаться в их образах в базах данных. При проектировании выбор и установление требований к актуальности баз данных можно оценивать по степени покрытия актуальными и достоверными данными состояния и изменения внешних объектов, которые они отражают.

Важными показателями качества баз данных также являются объемно-временные характеристики обрабатываемых данных:

* + - объем базы данных — относительное число записей описаний объектов или документов в базе данных, доступных для хранения и обработки, по сравнению с полным числом реальных объектов во внешней среде;
    - оперативность — степень соответствия динамики изме­ нения описаний данных в процессе сбора и обработки состояниям реальных объектов или величина допустимого запаздывания между появлением или изменением характеристик реального объекта относительно его отражения в базе данных;
    - глубина ретроспективы — максимальный интервал времени от даты выпуска и/или записи в базу данных самого раннего документа до настоящего времени;
    - динамичность — относительное число изменяемых описаний объектов к общему числу записей в БД за некоторый интервал времени, определяемый периодичностью издания версий БД.

Отдельно отметим такую характеристику как *защищенность информации* БД, которая реализуется, в основном, программными средствами СУБД, однако в сочетании с поддерживающими их средствами организации и защиты данных. Цели, назначение и функции защиты тесно связаны с особенностями функциональной пригодности каждой ИБД. При системном проектировании свойства защищать информацию баз данных от негативных воздействий описываются обычно составом и номенклатурой методов и средств, используемых для защиты от внешних и внутренних угроз. Косвенным показателем ее качества может служить относительная доля вычислительных ресурсов, используемых непосредственно средствами защиты информации БД.

Основное внимание в практике обеспечения безопасности применения БД сосредоточено на защите от злоумышленных разрушений, искажений и хищений информации баз данных. Основой такой защиты является аудит доступа, а также контроль организации и эффективности ограничений доступа. В реальных системах баз данных должны учитываться последствия реализации угроз, источниками которых являются случайные, непредсказуемые, дестабилизирующие факторы или дефекты и отсутствуют непосредственно заинтересованные лица в подобных нарушениях. Качество защиты систем баз можно характеризовать величиной потенциального ущерба, риск возникновения которого при про­ явлении дестабилизирующих факторов и реализации конкретных угроз безопасности удается предотвратить или понизить. Также возможной характеристикой качества может выступать среднее время между возможными проявлениями угроз, преодолевающих защиту данных.

**4 Основные подходы к методам построения защищенных информационных систем**

Разработка теории построения защищенных систем обработки информации в отечественной науке в первую очередь связана с разработкой моделей строгого обоснования надежности систем обеспечения безопасности информации. Данные формальные модели создают методологический фундамент, на котором строится оценка эффективности защиты любой автоматизированной системы.

В настоящее время сложились и наиболее широко реализуются два подхода:

* + - разработка и применение строгих математических моде­ лей, позволяющих аналитически или на ЭВМ получить надлежащие оценки;
    - критериальный подход к оценке надежности автоматизированных систем на всех этапах жизненного цикла.

Каждый из этих подходов имеет свои преимущества и недостатки, свою методологию и особенности реализации. Однако данные подходы не исключают, а дополняют друг друга.

На каждом из упомянутых подходов в течение последних 15-20 лет получено много интересных и важных для практической деятельности по построению информационных систем результатов. Однако на настоящее время имеющиеся теоретические достижения не позволяют с надлежащим уровнем точности дать оценки надежности методической и инструментальной базы обеспечения безопасности информации практически значимых автоматизированных систем.

Поэтому к категории важных следует отнести задачи, связанные с разработкой строгих математических моделей, описывающих механизмы реализации политики безопасности. Логическим продолжением этой деятельности является создание строгой доказательной базы для получения аналитических оценок надежности реализации необходимых политик безопасности с помощью инструментальных средств построения защищенных автоматизированных систем.

Не меньшую значимость имеет задача развития критериального подхода к оценке надежности автоматизированных систем на всех этапах жизненного цикла. Действующие на сегодня в России руководящие документы Гостехкомиссии при Президенте РФ по вопросам защиты информации в автоматизированных системах выпущены в 1991 г. Они во многом устарели и не соответствуют современному уровню доказательной базы надежности инструментальных средств, основанной на критериальном подходе. С другой стороны, реализация более перспективных в этом отношении «Общих критериев» (ISO-15408) в России сопряжена с целым рядом проблем и трудностей не только законодательного и административного уровней их реализации, но и во многом — программно-технического.

Проблема разработки и реализации моделей разграничения доступа, адекватных потребностям современных распределенных автоматизированных систем, —одна из самых насущных и сложных в общем комплексе проблем информационной безопасности. Уровень ее проработки в значительной степени определяет защищенность информационной инфраструктуры государства и, в частности, критически важных элементов инфраструктуры. Управление доступом принято считать одним из основных сервисов программно-технического уровня систем обработки информации. Этот сервис осуществляется соответствующими средствами на трех основных уровнях:

* + - ядро операционной системы;
    - сервер баз данных;
    - сервер приложений или прикладная система.

При использовании данного подхода к построению защищенных систем ключевую роль в системе аппаратно-программных сервисов защиты автоматизированных систем играет монитор безопасности. Основная функция монитора— реализация разграничения доступа различных субъектов системы (пользователи, процессы и т. п.) к объектам системы (файлы, устройства, процессы, сегменты разделяемой памяти и т. д.) в соответствии с принятой политикой безопасности. Основные механизмы разграничения доступа реализуются в ядре защищенной операционной системы или сервера баз данных.

Модели математически строгого описания правил разграничения доступа реализуются, как правило, на основе подхода «Субъект-объект». К таким наиболее часто употребляемым и реализуемым в операционных и автоматизированных информационных системах относятся дискреционная и мандатная модели. Широко распространено мнение, что за счет их развития, разумной комбинации, использования гибких схем и более тонких механизмов разграничения доступа удается получить достаточно хорошие результаты при приемлемых затратах на всех этапах жизненного цикла систем.

Традиционные подходы в совершенствовании уже существующих и разработке новых моделей разграничения доступа связаны с их описанием на основе отношений «субъект-объект». В последние годы, с активным внедрением в практику объектно- ориентированного программирования, появились вполне обоснованные (и адекватные потребностям) подходы к описанию моделей разграничения доступа на основе новых методов. Разработка формальных моделей на новых подходах, их реализация для конкретных информационных систем, функциональных или структурных сервисов представляется важной и перспективной задачей.

Есть два принципиально отличных пути решения задачи построения защищенной автоматизированной системы. Первый путь основан на пересмотре традиционных механизмов автоматизированной системы и создании системы с новой архитек­ турой, предусматривающей использование более тонких схем разграничения доступа в таких ключевых подсистемах, как ядро операционной системы, способов работы с памятью, контроля атомарности вычисления файловых операций и более корректной работы с временными файлами.

Второй путь основан на подходах, направленных на устранение тех же проблем в системе, однако путем анализа и выявлением уязвимых мест, исправления недостатков модернизации уже существующих традиционных систем. Очевидно, что второе направление лучше реализуется для систем с открытыми кодами. К таким системам относятся в первую очередь операционные системы Linux и Free BSD. В работе над данными системами в режиме открытых проектов большими исследовательскими коллективами, распределенными по всему миру, получены важные результаты.

Получение уверенности в правильности проектных решений по построению системы защиты невозможно без применения методов тестирования. В большинстве случаев тестирование не дает абсолютной уверенности в правильности построения систем защиты. Тем не менее целесообразно тщательно готовить и проводить тестирование разумной степени полноты. Проведенное тестирование может дать определенную уверенность в том, что заявленные в документации свойства системы реально реализованы без ошибок.

Тестирование системы защиты позволяет выявить уровень изменения характеристик производительности системы, в зависимости от конфигурации и параметров используемых механизмов защиты, определить устойчивость механизмов защиты в отношении возможных атак. Квалифицированно разработанный тест также может выявить уязвимость в системе защиты.

Традиционно используются два основных метода тестирования:

* тестирование по методу «черного ящика»;
* тестирование по методу «белого ящика».

Тестирование по методу «черного ящика» предполагает отсутствие у тестирующей стороны каких-либо специальных знаний о конфигурации и внутренней структуре объекта испытаний. При этом против объекта испытаний реализуются все известные типы атак и проверяется устойчивость системы защиты в отношении этих атак. Используемые методы тестирования эмулируют действия потенциальных злоумышленников, пытающихся взломать систему защиты. Основным средством тестирования в данном случае являются сетевые сканеры, располагающие базами данных известных уязвимостей.

Метод «белого ящика» предполагает составление программы тестирования на основании знаний о структуре и конфигурации объекта испытаний. В ходе тестирования проверяются

* наличие и работоспособность механизмов безопасности,
* соответствие состава и конфигурации системы защиты требованиям безопасности и существующим рискам.

Выводы о наличие уязвимостей делаются на основании анализа конфигурации используемых средств защиты и системного ПО, а затем проверяются на практике. Основным инструментом анализа в данном случае являются программные агенты средств анализа защищенности системного уровня.

В модели МРД

В процессе исследования дискреционной модели доступа важно обратить внимание на особенности реализации системных привилегий и привилегий доступа к объекту системы, в частности, механизмы предоставления и отзыва привилегий. Основой системы разграничения доступа в большинстве СУБД промышленного уровня является реализация принципа минимальных привилегий. Суть данного принципа состоит в том, что пользователю должно быть явно разрешено выполнение каждого действия в системе. Другими словами, возможность выполнения какого-либо действия в системе (начиная с регистрации пользователя) по умолчанию должна быть отключена или определена в минимально возможном объеме, определяемом объективными условиями эксплуатации системы.

Важнейший вопрос при проведении исследования реализации мандатной модели управления доступом —технология присваивания и изменения меток для объектов и субъектов. Реализация разграничения доступа на уровне кортежей предполагает наличие специального столбца с меткой доступа. Ясно, что технология изменения данных в таком специальном столбце должна отличаться от традиционной. В то же время введение специальных языковых средств — это явный отход от стандарта SQL, что для промышленной СУБД маловероятное решение.

Необходимость исследования ролевой модели доступа определяется широким ее распространением в мировой практике обеспечения защищенных технологий обработки баз данных.

Понятие роли вошло составной частью в последний стандарт SQL и стандарт Common Criteria для коммерческого профиля безопасности. Большое число пользователей, статус которых требует различных привилегий для доступа к ресурсам базы данных, создает значительный объем рутинной работы администратору. Роль — это поименованный набор привилегий, который может быть предоставлен пользователю или другой роли; по сути, языковое средство для автоматизации работы администратора по разграничению доступа. Описание привилегий, характерных для той или иной роли, готовится заранее. При регистрации нового пользователя в системе администратор выполняет только предоставление пользователю привилегий конкретной роли. При необходимости изменить привилегии конкретному приложению достаточно изменить только привилегии соответствующей роли. Все пользователи, отображенные на эту роль, автоматически получат измененные привилегии.

В защ ОС на организационный уровень управления

Подводя итог, можно сформулировать перечень задач, которые необходимо решить на организационном уровне управления системой информационной безопасности:

1. Нормативно оформить организационную инфраструктуру обеспечения безопасности в подразделениях организации, в частности, оформить в должностных обязанностях сотрудников выполнение функций по обеспечению информационной безопасности.
2. Документально оформить политики безопасности для организации в целом, определить и документально оформить стратегии и общие подходы к оцениванию и управлению рисками.
3. Документально оформить и утвердить установленным порядком методики оценивания и управления рисками и процедуры, гарантирующие использование утвержденных методик в практике деятельности организации.
4. Документально оформить проектные решения с обоснованием рациональности выбора средств защиты для рассматриваемой автоматизированной информационной системы.
5. Разработать и документально оформить процессы обслуживания и администрирования информационной системы организации, в частности, процедуры создания резервных копий и технологии восстановления системы.
6. Разработать и документально оформить регламент проведения периодических или выборочных проверок с целью получения значений оценок, характеризующих информационную безопасность системы, и корректировки системы управления рисками.
7. Обеспечить актуальное состояние документации по системе управления информационной безопасностью и регистрации используемых технологий и средств обеспечения информационной безопасности.