## Тема: *Принципы построения защищенных систем баз данных*

Разработать универсальную защищенную систему баз данных скорее всего нереально. При любом разумном методе измерения уровня защищенности этот уровень является неубывающей функцией от затрат на построение системы защиты. Следовательно, в любом практическом случае, когда существуют ограничения на бюджет системы защиты, существует и некоторый предельный уровень информационной безопасности, который теоретически может быть достигнут.

В настоящее время отсутствует общепринятая методология разработки защищенных автоматизированных информационных систем и, в частности, систем баз данных. В подобных случаях традиционно используется подход, основанный на анализе лучшего мирового опыта решения некоторого класса проблем и формулировании руководящих принципов построения соответствующих систем, концентрирующих накопленный опыт. Именно таким образом для проблемы обеспечения безопасности информационных систем разрабатывался британский стандарт BS 7799 и созданный на его основе международный стандарт ISO 17799.

Анализ наиболее успешных решений в области обеспечения информационной безопасности баз данных позволил сформулировать несколько полезных принципов, которыми можно руководствоваться при проектировании систем защиты:

     экономическая оправданность механизмов защиты;

     открытое проектирование;

     распределение полномочий между различными субъектами в соответствии с правилами организации;

     минимально возможные привилегии для пользователей и администраторов;

     управляемость системы при возникновении отказов и сбоев;

     психологическая приемлемость работы средств защиты данных.

Первый из этих принципов — экономическая оправданность механизмов защиты — предписывает использование простейшего из всевозможных вариантов проекта, который обеспечивает достижение желаемой цели. Хотя этот принцип относится ко многим аспектам проектирования систем, он наиболее пригоден при разработке механизмов защиты, так как ошибки проектирования и реализации, которые ведут к неконтролируемым способам доступа к данным, могут быть не замечены в ходе нормального использования системы. Строгое соблюдение этого принципа приводит к применению на практике таких методов, как проверка «строка за строкой» программных средств и физическая проверка аппаратных средств, реализующих механизмы защиты.

В соответствии с принципом открытого проектирования, технология систем защиты не должна базироваться на «секретных» алгоритмах. Этот принцип широко используется при проектировании безопасных систем и сетей связи. Высокое качество систем защиты обеспечивается не недостатком знаний у возможных нарушителей, а использованием широко опробованных (как правило, открытых) стандартов и правильной организацией управления ключевой информацией. Использование алгоритмов, основанных на открытых стандартах в области информационной безопасности, повышает степень доверия пользователей к системе защиты и формирует правильную психологическую установку на необходимость внимательности и аккуратности при работе с ключевой информацией.

Принцип распределения полномочий состоит в том, что для критически важных приложений целесообразно использовать многокомпонентные схемы доступа к данным. То есть для выполнения соответствующей операции необходимо провести аутентификацию нескольких ее обязательных участников. Физический аналог этого принципа можно наблюдать в конструкциях банковских сейфов, когда для того, чтобы открыть сейф, необходимо наличие двух ключей, которые обычно хранятся у различных людей. Ясно, что механизмы защите, требующие двух ключей для доступа к информации, являются более устойчивыми, чем механизмы, которые разрешают доступ на основе предъявления единственного ключа. В то же время подобные многокомпонентные процедуры требуют больших затрат и, как правило, более сложных процедур управления ключами (включая хранение резервной копии).

При проектировании многокомпонентных схем доступа за прообраз берется существующая в организации практика. Действительно, переход в автоматизированном контуре на более сложные, чем использовались «в доавтоматизированную эру», технологии может вызвать психологический дискомфорт и раличные формы скрытого саботажа системы.

Принцип минимально возможных привилегий для пользователей и администраторов предписывает, чтобы каждый пользователь (процесс) системы оперировали с данными, используя наименьший из возможных набор привилегий, необходимых для выполнения конкретной функции. Применение данного принципа нацелено на минимизацию ущерба, который может быть нанесен в случае сбоя, ошибки программного обеспечения или компрометации элементов системы защиты данных. Принцип минимальных привилегий, используемый при создании пользователей Oracle, — пример реализации этого принципа. Использование точек входа SYSTEM и, особенно, SYS должно быть предметом особого регламента. Хорошей практикой является использование администратором безопасности нескольких точек входа: обычной, с набором привилегий, достаточным для выполнения основных работ, и особой (типа SYSTEM), используемой только при возникновении необходимости выполнения действий, требующих высоких привилегий.

Согласно принципу управляемости системы при отказах и сбоях, проектирование информационной системы, реализованной на базе СУБД, должно осуществляться в предположении, что ошибки операционной системы и СУБД, а также сбои аппаратуры неизбежны. При создании системы возможность реализации таких событий должна быть учтена: при проектировании процедур и функций должны быть обработаны все исключительные ситуации, при обработке данных, содержащих конфиденциальную информацию, должны быть минимизированы риски восстановления этих данных по дампам оперативной памяти и содержимому временных файлов и т. п. Также должны быть разработаны документы, регламентирующие действия участников процесса обработки данных (как пользователей, так и обслуживающего персонала) при возникновении нештатных ситуаций. Персонал должен проходить регулярные инструктажи и тренинги по обучению действиям в нештатных ситуациях, с иерархией передачи данных.

И наконец, в соответствии с принципам психологической приемлемости работы средств защиты данных взаимодействие людей с системой (и подсистемой защиты) не должно быть сложным. Пользователи должны шаблонно и автоматически применять имеющиеся механизмы защиты. Чрезмерное усложнение механизмов защиты может вызывать их внутреннее неприятие и побуждать к использованию различных форм скрытого саботажа. Осознанное принятие используемых средств и методов обеспечения информационной безопасности и оценка комплекса применяемых мер как необходимых приводит к уменьшению числа ошибок поль- зователей. В этом случае аномальное поведение потенциального нарушителя становится более заметным и проще устанавливается. Принцип психологической приемлемости является важным при выборе процедур аутентификации и модели управления доступом.