УДК 004.056.53

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМАХ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

Паламареноко А.С., Мартыненко А.А.
ГВУЗ «Национальный горный университет», http://nmu.org.ua, Palamarenkoas@yandex.ru

В статье анализируются особенности решения проблемы защиты информации в системах управления базами данных, обеспечение надежной и эффективной работоспособности системы баз данных.

Ключевые слова – защита информации, базы данных, системах управления базами данных.

ВВЕДЕНИЕ

По степени универсальности различают два класса Систем Управления Базами Данных (СУБД):

• *системы общего назначения*. СУБД общего значения – это сложные программные комплексы, предназначенные для выполнения всей совокупности функций, связанных с созданием и эксплуатацией базы данных информационной системы.

• *специализированные системы*. Специализированные СУБД создаются в редких случаях при невозможности или нецелесообразности использования СУБД общего значения.

Для систем управления базами данных (СУБД) важны три основных аспекта информационной безопасности - конфиденциальность, целостность и доступность. Политика безопасности определяется администратором данных. Абсолютная защита данных практически не реализуема, поэтому обычно довольствуются относительной защитой информации – гарантированно защищают ее на тот период времени, пока несанкционированный доступ к ней влечет какие-либо последствия.

На производительность СУБД оказывают влияние два фактора:

СУБД, которые следят за соблюдением целостности данных, несут дополнительную нагрузку, которую не испытывают другие программы; производительность собственных прикладных программ сильно зависит от правильного проектирования и построения базы данных.

СУБД, как правило, разделяют по используемой модели данных (как и базы данных) на следующие типы: иерархические, сетевые, реляционные и объектно-ориентированные.

ТРЕБОВАНИЯ, ВЫПОЛНЯЕМЫЕ СУБД

1. Функциональность – описание необходимых функций СУБД, возможность и правила работы с ними.

2. Производительность – время исполнения запроса, ёмкость БД, количество обслуживаемых клиентов.

3. Безопасность – ограничиваются возможностями использования данных для обработки.

4. Масштабируемость – возможность увеличения количества полей, записей полей, пользователей, периодичность передачи данных.

5. Возможность изменения конфигураций – показывает, насколько заказчик может изменять программное обеспечение с помощью разработчика.

6. Совместимость – возможность совместимости работы с разными СУБД.

7. Доступность – определяет количество часов обслуживания пользователей, длительность проведения работ.

8. Простота эксплуатации – определяет условия, которые создают удобства использования СУБД.

9. Простота освоения СУБД – определяет допустимую длительность освоения приёмов управления СУБД.

Среди многочисленных аспектов проблемы безопасности СУБД необходимо отметить следующие:

• Организационные вопросы (например, как в рамках предприятия, обладающего некой системой, организован доступ к данным);

• Вопросы реализации управления (например, если используется метод доступа по паролю, то, как организована реализация управления и как часто меняются пароли);

• Аппаратное обеспечение (обеспечиваются ли меры безопасности на аппаратном уровне, например, с помощью защитных ключей или привилегированного режима управления);

• Безопасность операционной системы (например, затирает ли базовая операционная система содержание структуры хранения и файлов с данными при прекращении работы с ними);

• Некоторые вопросы, касающиеся непосредственно самой системы управления базами данных (например, существует ли для базы данных некоторая концепция предоставления прав владения данными).

В современных СУБД поддерживается один из двух широко распространенных подходов к вопросу обеспечения безопасности данных, а именно избирательный подход или обязательный подход. В обоих подходах единицей данных или "объектом данных", для которых должна быть создана система безопасности, может быть как вся база данных целиком или какой-либо набор отношений, так и некоторое значение данных для заданного атрибута внутри некоторого кортежа в определенном отношении. Эти подходы отличаются следующими свойствами:

• В случае избирательного управления некий пользователь обладает различными правами (привилегиями или полномочиями) при работе с

разными объектами. Более того, разные пользователи обычно обладают и разными правами доступа к одному и тому же объекту. Поэтому избирательные схемы характеризуются значительной гибкостью;

В случае обязательного управления, наоборот, каждому объекту данных присваивается некоторый классификационный уровень, а каждый пользователь обладает некоторым уровнем допуска. Следовательно, при таком подходе доступом к определенному объекту данных обладают только пользователи с соответствующим уровнем допуска. Поэтому обязательные схемы достаточно жестки и статичны.

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Независимо от того, какие схемы используются - избирательные или обязательные, все решения относительно допуска пользователей к выполнению тех или иных операций принимаются на стратегическом, а не техническом уровне. Поэтому они находятся за пределами досягаемости самой СУБД, и все, что может в такой ситуации сделать СУБД – это только привести в действие уже принятые ранее решения. Исходя из этого, можно отметить следующее:

- Результаты стратегических решений должны быть известны системе (т.е. выполнены на основе утверждений, заданных с помощью некоторого подходящего языка) и сохраняться в ней (путем сохранения их в каталоге в виде правил безопасности, которые также называются полномочиями);
- Очевидно, должны быть некоторые средства регулирования запросов доступа по отношению к соответствующим правилам безопасности. (Здесь под "запросом, доступа" подразумевается комбинация запрашиваемой операции, запрашиваемого, объекта и запрашивающего пользователя.) Такая проверка выполняется подсистемой безопасности СУБД, которая также называется подсистемой полномочий;
- Для того чтобы разобраться, какие правила безопасности к каким запросам доступа применяются, в системе должны быть предусмотрены способы опознания источника этого запроса, т.е. опознания запрашивающего пользователя. Поэтому в момент входа в систему от пользователя обычно требуется ввести не только его идентификатор (например, имя или должность), но также и пароль (чтобы подтвердить свои права на заявленные ранее идентификационные данные). Обычно предполагается, что пароль известен только системе и некоторым лицам с особыми правами.

ЗАКЛЮЧЕНИЕ

Современные информационные системы основаны на концепции интеграции данных, характеризующихся большими объектами хранимых данных, сложной организацией, необходимостью удовлетворять разнообразные требования многочисленных пользователей. Для управления этими данными и обеспечения эффективности доступа к ним были созданы системы управления данными.

Таким образом, СУБД называют программную систему, предназначенную для создания ЭВМ общей базы данных для множества приложений, поддержания ее в актуальном состоянии и обеспечения эффективности доступа пользователей к содержащимся в ней данным в рамках предоставленных им полномочий.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Уткин, В.Б. Информационные системы в экономике : учебник / В.Б. Уткин, К. В. Балдин. – 3-е изд., стер. – М. : Академия, 2006. – 288 с.

2. Хоменко, А. Д. Основы современных компьютерных технологий: учебник / А. Д. Хоменко. - М.: Гардарики, 2005. - 415 с.

3. Вычислительные машины, системы и сети: учебник/ В.Ф.Мелехин, Е.Г. Павловский. – М. : Академия, 2006. – 560с.

4. Информатика : Учебник / под ред. Н. В.Макаровой. – 3-е перераб. изд. – М. : Финансы и статистика, 2005. – 768с.

5. Давыдова, Л.А. Информационные системы в экономике в вопросах и ответах : учебное пособие. / Л. А. Давыдова. – М. : ТК Велби, Издательство Проспект, 2006. – 280с.