УДК 004.056: 004.652

МЕХАНИЗМЫ ЗАЩИТЫ ДАННЫХ, РЕАЛИЗОВАННЫЕ В БАЗЕ ДАННЫХ С УНИВЕРСАЛЬНОЙ МОДЕЛЬЮ

В. М. Грачев[2], В. И. Есин[1], Н. Г. Полухина[3], С. Г. Рассомахин[1]

Рассматривается проблема обеспечения безопасности баз данных. На примере базы данных с универсальной моделью рассматриваются средства и методы, обеспечивающие безопасность хранящихся корпоративных данных. Раскрываются механизмы защиты, реализуемые за счет возможностей систем управления базами данных (СУБД) на платформах которых установлены базы данных, и специальные средства защиты данных, реализованные в схеме базы данных с универсальной моделью данных.

Ключевые слова: база данных, база данных с универсальной моделью данных, безопасность баз данных, защита данных, средства управления доступом.

Проблема безопасности баз данных. Темпы развития информационных технологий за последние 20 лет способствовали внедрению средств вычислительной техники во все сферы деяельности человека, что, в свою очередь, отразилось и на обратной стороне этого процесса. А именно, возрос интерес к циркулирующим внутри информационной системы (ИС) данным не только со стороны законных пользователей и владельцев, но и со стороны злоумышленников. Поэтому решение проблемы информационной безопасности компьютерных систем, в том числе и баз данных (БД) как основного элемента ИС, стало одной из первоочередных задач. При этом защита баз данных остается одной из самых сложных задач, стоящих перед подразделениями, отвечающими за обеспечение информационной безопасности. Проблема решения последней усугубляется тем, что часто четкой и ясной методики комплексного ее решения, которую можно было бы

[1] Харьковский национальный университет им. В. Н. Каразина, 61022, Харьков, пл. Свободы, 4.

[2] Национальный исследовательский ядерный университет “МИФИ”, 115409 Россия, Москва, Каширское шоссе, 31.

[3] ФИАН, 119991 Россия, Москва, Ленинский пр-т, 53; e-mail: polukhina@sci.lebedev.ru.

применять во всех случаях, не существует. Объясняется это разнообразием деятельности предприятий, структурой построения информационных сетей, потоков данных, прикладных систем и способов организации доступа к ним и т. д. Поэтому в каждой конкретной ситуации ее приходится решать индивидуально.

Существующие подходы к решению проблемы. Рассмотрим методы и средства, обеспечивающие безопасность базы данных, построенной на основе универсальной модели данных (УМД) [2–4], которую предполагается использовать в корпоративных ИС для надежного, безопасного одновременного хранения больших объемов данных из разных существенно отличающихся предметных областей.

Классическое решение данной проблемы предполагает обследование БД с целью выявления таких угроз, как хищение и фальсификация данных, утрата конфиденциальности и целостности данных, уничтожение, нарушение неприкосновенности личных данных, потеря доступности и т. д. [1]. При этом, в первую очередь, анализируются все или почти все средства и методы защиты БД, имеющиеся в арсенале тех систем управления БД (СУБД), на платформах которых они реализуются или планируются к реализации.

Защита данных средствами СУБД. Как правило, средства и методы защиты БД в различных СУБД несколько отличаются друг от друга, однако существуют такие, которые в той или иной степени встречаются во многих СУБД. Общие методы и средства защиты достаточно подробно описаны в [5, 6]. Они же в полной мере могут и используются для защиты данных, хранящихся в БД с УМД. Это авторизация пользователей (так называемые механизмы управления доступом), применение представлений, резервное копирование и восстановление, поддержка целостности, шифрование, использование отказоустойчивой аппаратуры.

Например, чтобы уменьшить вероятность несанкционированного доступа через общеизвестные учетные записи, после инсталляции схемы БД с УМД администратор базы данных должен проанализировать административные, вспомогательные, учебные учетные записи, которые прописываются в базе данных по умолчанию, поскольку каждая из них имеет один и тот же пароль. И впоследствии удалить или изменить их на другие пароли, причем длина, срок действия и сложность пароля должны отвечать соответствующим требованиям, принятым в СУБД и в организации.

Известно, что как только пользователь получит право доступа к СУБД, ему могут втоматически предоставляться различные привилегии, связанные с его идентификатором. В базах данных, построенных на основе универсальной модели, все привилегии

предоставляются пользователям с учетом принципа обоснованности доступа. То есть только такие привилегии, которые им необходимы для выполнения задач, относящихся к кругу их должностных обязанностей. Предоставление излишних или ненужных привилегий может привести к нарушению защиты, поэтому пользователь должен получать только те, без которых он не имеет возможности выполнять свою работу. Для мониторинга используемых видов привилегий и объектов БД с УМД, к которым выполняется доступ, применяются различные методы аудита, позволяющие получить полезную информацию для обнаружения фактов злоупотребления привилегиями или неправильного их использования.

В схеме БД с УМД активно используется механизм представлений. Он служит мощным и гибким инструментом организации защиты данных, позволяющим скрывать от пользователей определенные части данных базы.

Для осуществления надежности хранения информации в БД с УМД рекомендуется с некоторой установленной периодичностью создавать резервные копии ее данных, а также копии файла журнала. Организовывая при этом хранение созданных копий в местах, обеспеченных необходимой защитой. Сегодня практически любая современная СУБД предоставляет средства резервного копирования, позволяющие восстанавливать базу данных в случае ее порчи. А отказоустойчивое аппаратное обеспечение, на котором планируется эксплуатация БД с УМД, будет этому процессу только способствовать.

Общая защищенность данных в БД с УМД, в том числе, обеспечивается и средствами поддержки целостности данных. Поскольку они предотвращают возможность перехода данных в несогласованное состояние, а значит, исключают угрозу получения ошибочных или неправильных результатов расчетов. Если в базе данных содержится весьма важная конфиденциальная информация, то данные БД с УМД могут быть зашифрованы. Существует множество различных технологий зашифрования данных. Одна из таких – криптографическая защита. Однако задача криптографической защиты баз данных в общем, и БД с УМД в частности, существенно отличается от криптозащиты информации в рамках обычной файловой системы по следующим причинам: а) защита информации, находящейся в БД, должна организовываться с учетом СУБД и ее возможностей по встраиванию защитных механизмов; б) файлы БД – это файлы определенной структуры. Пользователи могут иметь доступ к информации только из определенных частей БД, то есть возникает задача ранжирования прав доступа (избирательной защиты) внутри файла БД; в) средства шифрования приводят к некоторому снижению производительности информационной системы, использующей базу данных.

Об этом следует помнить и соотносить выигрыш от ее использования с затратами.

Кроме того существует множество причин (права интеллектуальной собственности; коммерческая ценность; недопустимость модификации кода другими пользователями и т.д.), по которым разработчик не хочет, чтобы кто-то видел исходный код написанных им процедур, функций, пакетов, триггеров. Код обеспечивает решение задач защиты и распределения прав доступа к данным. Существует несколько способов сокрытия кода. Например, при реализации схемы БД с УМД на платформе СУБД Oracle с точки зрения эффективности наиболее подходящим для этой цели является использование специальной утилиты WRAP. Эта утилита весьма просто скрывает L/SQL-код основных элементов базы данных, преобразуя его в вид, который на первый взгляд кажется бессмысленным, однако сервер может прочитать этот скрытый код, скомпилировать и выполнить его. При этом код изменяется, а не зашифровывается сложными алгоритмами, но пользователи при просмотре исходного кода в словаре данных не смогут понять, что в действительности он делает. При этом такая подмена не сильно сказывается на производительности в отличие от процедуры зашифрования/расшифрования.

Специальные средства защита данных, реализованные в БД с УМД. В дополнении к вышеописанным средствам и методам, при реализации схемы БД с УМД были разработаны специальные средства защиты и механизмы их использования. Так для организации контроля доступа пользователей к объектам схемы БД с УМД была создана дополнительная таблица пользователей, которую на псевдокоде можно записать следующим образом:

USER_ID NUMERIC not null PRIMARY KEY,

USER_NAME VARCHAR not null,

USER_ISUD NUMERIC not null.

Атрибуты этой таблицы определены на следующих доменах:

– атрибут USER_ID – at(USER_ID) – на домене U_1 – множество условных идентификаторов пользователей, то есть dom(USER_ID)=dom(U_1);

– атрибут USER_NAME – at(USER_NAME) – на домене U_2 – множество условных имен пользователей: dom(USER_NAME)=dom(U_2);

– специальный атрибут “Права пользователя” – USER_ISUD – на домене U_3 – множество, элементами которого являются имена (или их идентификаторы) прав, предоставляемых соответствующим пользователям при работе с данными (а именно, какие операции может выполнять пользователь с данными: удалять, добавлять, изменять, просматривать, все перечисленные действия или их комбинации): dom(USER_ISUD)=dom(U_3).

После того как перечень пользователей создан, каждому из них, в соответствии с принципом обоснованности доступа, предоставляются определенные права доступа к данным. Но в этом случае возникает вопрос – может ли он передавать эти права другим пользователям и как? В схеме БД с УМД, если владелец объекта желает передать/отозвать другим авторизованным пользователям принадлежащие ему привилегии, то, кроме предусмотренных традиционных способов передачи/отзыва привилегий посредством операторов языка SQL (используя операторы GRANT/REVOKE), имеется дополнительная возможность, реализованная с помощью специально созданной таблицы "Распределения прав доступа к данным других пользователей":

GRANT_ID NUMERIC not null PRIMARY KEY,

GRANTOR NUMERIC not null,

GRANTEE NUMERIC not null,

USER_ISUD NUMERIC not null,

где атрибут GRANTEE необходим для определения, какому пользователю предоставляются права доступа к данным (определен на домене U_1 – dom(GRANTEE)=dom(U_1)), а атрибут USER_ISUD необходим для уточнения, какие именно необходимо установить права доступа к данным (INSERT, SELECT, UPDATE, DELETE) – определен на домене U_3 – dom(USER_ISUD)=dom(U_3). Чтобы изменить привилегии пользователя, необходимо просто изменить значение атрибута USER_ISUD на новое.

Само по себе наличие этих двух таблиц ничего не дает. Таблицы – только необходимое условие возможности организации защиты данных в схеме БД с УМД. Нужны были еще дополнительные элементы, механизмы, процедуры, программы и т. д., которые будут их использовать. Например, всю защиту можно было бы реализовать в приложении: будь то клиентское приложение (в случае архитектуры клиент-сервер) или сервер приложений (в многоуровневой архитектуре). Такие приложения могут учитывать, кто к ним обращается, и выполнять соответствующий запрос, реализовывая собственный механизм контроля доступа. Однако серьезным недостатком такого подхода является то, что в этом случае данные базы могут безопасно использоваться только соответствующим приложением. Иные приложения, средства создания запросов, средства генерации отчетов и т. п., для обращения к БД использовать нельзя, поскольку в них доступ к данным не будет защищен. Кроме того, если защита встроена в приложение, то это ведет к усложнению развития этого приложения.

Поэтому, чтобы избежать подобных недостатков в схеме БД с УМД, механизм защиты был реализован на стороне сервера (с максимальным учетом всех возможностей,

заложенных в СУБД). Так в реализации схемы БД с УМД на платформе СУБД Oracle, в механизме защиты задействованы: специально созданные триггеры, процедуры, пакеты, вышеназванные таблицы, механизм детального контроля доступа [7]. Например, защита на уровне строк (Row Level Security) осуществляется с помощью встроенного пакета DBMS_RLS [7]. При этом в схеме БД с УМД возможна организация защиты отдельных конкретных элементов данных. Однако следует помнить, что защита отдельных записей данных ведет к потере производительности информационной системы в целом. То есть чем-то приходится жертвовать. Хотите иметь хорошо защищенные данные и гибкую систему распределения прав доступа, приходится идти на заведомо вычислительно-затратные меры.

С помощью определенных триггеров и специально разработанного пакета программ реализована возможность (или невозможность, в зависимости от прав доступа) удаления классов объектов, классов событий, классов параметров объектов, экземпляров объектов, экземпляров событий, их характеристик и так далее. Другие триггеры схемы БД с УМД, не "позволяют" удалять некоторые метаданные предметной области (ПрО), если они присутствуют у данных этой же ПрО.

Для повышения надежности восстановления измененных данных, в схеме БД с УМД некоторые значимые данные хранятся в так называемом, журнале измененных данных, представляющим собой специальную таблицу схемы БД с УМД, в которой отслеживаются (сохраняются) все изменения данных, проводимых пользователями в процессе работы. Функции этого журнала несколько сходны с некоторыми функциями журналов повторного выполнения, которые, как правило, являются неотъемлемой частью всех СУБД. Однако последние используются только для восстановления при сбое или при поддержке резервной БД, в том числе и таблицы журнала измененных данных. Журнал же измененных данных хранит информацию: о пользователе, который производил изменения или удаления с указанием его конкретных действий (вставка, удаление, изменение данных) и времени; об имени базы данных; о специальном операторе языка модели [8], на основании которой можно не только проследить кто, когда и какие изменения производил, но и при необходимости по ней можно восстановить неправильно измененные или утраченные данные, как в самой схеме БД, так и в случае репликаций, в распределенных системах.

Вывод.

1. В базе данных, построенной на основе УМД, для обеспечения безопасности данных используются как методы и средства встроенные в СУБД, на платформе которых она

реализуется, так и собственные механизмы, разработанные в рамках схемы БД с УМД, и включающие: специально созданные триггеры, процедуры, пакеты и таблицы.

2. Средства схемы БД с УМД позволяют прозрачным образом контролировать доступ к объектам базы данных (вплоть до конкретного элемента), осуществлять восстановление утраченных или неправильно измененных данных, обеспечивать их целостность, проводить при необходимости зашифрование конфиденциальных данных, что в целом обеспечивает высокую степень безопасности данных, хранящихся в БД с УМД.

Л И Т Е Р А Т У Р А

[1] В. И. Есин, А. А. Кузнецов, Л. С. Сорока, *Безопасность информационных систем и технологий* (Х., ООО "ЭДЭНА", 2010).

[2] В. И. Есин, *Универсальная модель данных и ее математические основы. Системи обробки інформації* (Х., Харківський університет Повітряних Сил), № 2(92)), 21 (2011).

[3] В. И. Есин, *Универсальная модель данных и ее отличительные особенности.* Вісник Харківського національного університету (Х., Харьковский национальный университет им. В. Н. Каразина), № 960, 141 (2010).

[4] В. И. Есин, Ю. А. Пергаменцев, *Технология проектирования модели предприятия на основе универсальной модели данных.* http://www.citforum.ru/database/articles/udm.

[5] Т. Коннолли, *Базы данных. Проектирование, реализация и сопровождение. Теория и практика* 3-е издание. : Пер. с англ. Т. Коннолли, К. Бегг (М., Издательский дом, "Вильямс", 2003).

[6] М. Фленов, *Безопасность баз данных предприятия.* http:www.vr-online.www.cydsoft.com/russia.

[7] А. Нанда, *Oracle PL/SQL для администраторов баз данных* Пер. с англ. А. Нанда, С. Фейерштейн (СПб, Символ-Плюс, 2008).

[8] В. И. Есин, М. В. Есина, *Язык для универсальной модели данных. Системи обробки інформації* (Х., Харківський університет Повітряних Сил), № 5(95)), 193 (2011).

Поступила в редакцию 24 апреля 2014 г.