УДК 004.056:004.652

Л. С. Сорока, доктор технических наук,
и. о. ректора Академии таможенной службы Украины
В. И. Есин, кандидат технических наук,
доцент кафедры безопасности информационных
систем и технологий Харьковского национального
университета им. В. Н. Каразина
М. В. Есина, студентка факультета компьютерных
наук Харьковского национального университета
им. В. Н. Каразина

ТРАДИЦИОННЫЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ДАННЫХ, РЕАЛИЗОВАННЫЕ В БАЗЕ ДАННЫХ С УНИВЕРСАЛЬНОЙ МОДЕЛЬЮ ДАННЫХ

Формулюється проблема безпеки даних у базах даних. Описуються потенційні загрози базам даних. Розкриваються методи й засоби захисту даних, які реалізовані за допомогою можливостей, закладених у системах управління базами даних, з урахуванням особливостей реалізації схеми бази даних з універсальною моделлю даних. А саме: авторизація користувачів, застосування уявлень, резервне копіювання і відновлення, підтримка цілісності, шифрування, використання відмовостійкої апаратури.

Формулируется проблема безопасности данных в базах данных. Описываются потенциальные угрозы базам данных. Раскрываются методы и средства защиты данных, реализованные с помощью возможностей, заложенных в системах управления базами данных, с учетом особенностей реализации схемы базы данных с универсальной моделью данных. А именно: авторизация пользователей, применение представлений, резервное копирование и восстановление, поддержка целостности, шифрование, использование отказоустойчивой аппаратуры.

The problem of data security in databases is formulated. Potential threats for databases are described. Methods and data protection resources which realize possibilities of database management system, taking into account the features of realization of database schema with a universal data model (user authorization, use of views, backup and recovery, support of integrity, encryption, use of fault-tolerant hardware) are disclosed.

Ключевые слова. База данных с универсальной моделью данных, безопасность данных, защита данных, средства управления доступом, целостность, шифрование, доступность.

Введение. Проблема безопасности данных сегодня является актуальной, что подтверждает собрание авторитетных представителей исследовательского сообщества баз данных в виде положений Лоуэллского отчета: “Безопасность, ориентированная на данные, превалировала в 80-е гг. прошлого века, но потом это направление перестало развиваться. Участники собрания считают, что его нужно возродить, но с несколько другой ориентацией. В настоящее время следует обратиться к принципам и механизмам поддержки разнообразных индивидуальных средств контроля информации, хранимой вовне. Сообщество баз данных может заняться системами безопасности, включающими компонент, который имеет дело с ожидаемым использованием данных. Решения о правомерности доступа должны основываться не только на том, кто запрашивает данные, но и на том, что он собирается с ними делать” [1, 2]. Именно поэтому вопросы безопасности данных в базе данных с их универсальной моделью представляют интерес.

Постановка задачи. Как известно, под *безопасностью базы данных* понимается защищенность данных от нежелательного их разглашения-использования (нарушения конфиденциальности), искажения (нарушения целостности), потери или снижения меры доступности. *Защита базы данных* – это совокупность методов и средств, обеспечивающих целостность, конфиденциальность, достоверность, аутентичность и доступность данных в условиях воздействия на них любых преднамеренных или непреднамеренных угроз.

При этом понятие защиты относится не только к данным, хранящимся в базе данных. Бреши в системе защиты могут возникать и в других частях информационной системы (оборудование, программное обеспечение, персонал, линии связи), что, в свою очередь, подвергает опасности и саму базу данных. Для эффективной реализации защиты необходимы соответствующие средства контроля, которые определяются конкретными

требованиями, вытекающими из особенностей эксплуатируемой системы. Необходимость защищать данные, которая раньше очень часто отвергалась или которой просто пренебрегали, в настоящее время вся яснее осознается различными организациями. Поводом для такой перемены послужили участившиеся случаи разрушения компьютерных хранилищ корпоративных данных, а также осознание того, что потеря или просто временная недоступность этих данных может стать причиной настоящей катастрофы.

Результаты исследования. База данных представляет собой важнейший корпоративный ресурс, который должен быть надлежащим образом защищен с помощью соответствующих средств и методов. В настоящее время можно выделить следующие потенциальные угрозы базам данных (БД) [3]:

– похищение и фальсификация данных;
– утрата конфиденциальности (нарушение тайны);
– нарушение неприкосновенности личных данных;
– утрата целостности;
– потеря доступности.

В принципе это основные направления, на которых необходимо сосредоточиться всем заинтересованным лицам, и в первую очередь, руководству, чтобы оперативно принимать меры, снижающие степень риска, то есть потенциальную возможность потери или повреждения данных. Как правило, все отмеченные выше угрозы тесно связаны между собой, так что действия, направленные на нарушение защищенности системы в одном направлении, часто приводят к снижению ее защищенности во всех остальных.

Похищение и фальсификация данных могут происходить не только в среде базы данных – вся информационная система той или иной организации так или иначе подвержена этому риску. Поэтому, конечно же, необходимо постоянно следить за всеми возможными каналами утечки информации, которыми потенциально обладает любая информационная система.

Понятие конфиденциальности означает необходимость сохранения данных в тайне. *Конфиденциальная информация* – это информация с ограниченным доступом, которой владеют, пользуются, распоряжаются отдельные физические, юридические лица или государство, порядок доступа к которой устанавливается ими.

Утрата целостности данных приводит к их искажению или разрушению, что может иметь самые серьезные последствия для дальнейшей работы организации (например, утрата надежных позиций в конкурентной борьбе).

В настоящее время множество организаций функционирует в непрерывном режиме, предоставляя свои услуги клиентам 24 часа в сутки и 7 дней в неделю. Потеря доступности данных будет означать: либо данные, либо система, либо то и другое одновременно окажутся недоступными пользователям. А это может подвергнуть опасности и финансовое положение организации, и всевозможные системы управления, использующие базы данных для своих нужд.

Не затрагивая общие вопросы информационной безопасности, а также общие методы и средства защиты информации, рассмотрим традиционные методы и средства защиты данных, реализованные с помощью возможностей, заложенных в системах управления базами данных, с учетом особенностей реализации схемы базы данных с универсальной моделью данных (УМД).

Решение проблемы защиты данных в базе данных с универсальной моделью с помощью традиционных методов и средств защиты направлено на минимизацию потерь, вызванных заранее предусмотренными событиями.

Средства и методы защиты БД в различных СУБД несколько отличаются друг от друга. Но в той или иной степени достаточно часто встречаются следующие из них [4, 5]:

– авторизация пользователей;
– применение представлений;
– резервное копирование и восстановление;
– поддержка целостности;
– шифрование;
– использование отказоустойчивой аппаратуры.

Базе данных с УМД присущи все эти методы и средства в большей или меньшей степени. Далее кратко рассмотрим их.

Механизм авторизации часто называют *средствами управления доступом.* Авторизация подразумевает необходимость наличия процедуры идентификации и аутентификации пользователей информационной системы.

Идентификация пользователей заключается в установлении и закреплении за каждым из них уникального идентификатора. *Аутентификация* заключается в проверке подлинности пользователя по предъявленному им идентификатору, например при входе в систему. Такая проверка должна исключать фальсификацию пользователей в системе и их компрометацию. Без проверки подлинности теряется смысл в самой идентификации пользователей и применении средств разграничения доступа, построенных на базе личных идентификаторов.

Обычно в СУБД для идентификации и проверки подлинности пользователей применяются либо соответствующие механизмы операционной системы, либо SQL-оператор CONNECT. Например, в случае СУБД Oracle оператор CONNECT имеет вид:

CONNECT пользователь[/пароль] [@база_данных];.

Так или иначе, в момент начала сеанса работы с сервером баз данных, пользователь идентифицируется своим именем, а средством аутентификации служит пароль.

Чтобы уменьшить вероятность несанкционированного доступа через общеизвестные учетные записи, после инсталляции 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. Например, некоторые пользователи, их пароли и hash-значения пароля по умолчанию, устанавливаемые в схему БД при инсталляции СУБД Oracle, приведены в [6].

Известно, что как только пользователь получит право доступа к СУБД, ему могут автоматически предоставляться различные привилегии, связанные с его идентификатором. В частности, эти привилегии могут включать разрешение на доступ к определенным таблицам, представлениям, пакетам, процедурам, функциям и т. д., а также на создание этих объектов или же право вызывать на выполнение различные утилиты СУБД. Привилегии предоставляются пользователям, чтобы они могли выполнять задачи, которые относятся к кругу их должностных обязанностей (*принцип обоснованности доступа*). Предоставление излишних или ненужных привилегий может привести к нарушению защиты, поэтому пользователь должен получать только такие привилегии, без которых он не имеет возможности выполнять свою работу.

Например, в СУБД Oracle пользователь может получить привилегию двумя способами:

– привилегии могут предоставляться пользователям явным образом;

– привилегии могут также предоставляться некоторой *роли* (так называется именованная группа привилегий). Роли делают управление привилегиями намного проще, так как можно один раз сконфигурировать привилегии для отдельных типов пользователей и затем назначать эти привилегии ролям. Когда пользователь нуждается в какой-то группе привилегий, можно использовать единственную команду назначения роли, чтобы удовлетворить этого пользователя. Используя этот механизм, можно формировать иерархию ролей. Также можно защитить роль паролем, который пользователь должен ввести для активизации роли.

Привилегии доступа выделяются пользователям, группам, ролям или всем посредством оператора GRANT и изымаются с помощью оператора REVOKE. Все эти правила распространяются на соответствующие объекты БД с УМД, а их реализация при инсталляции схемы базы данных с УМД и при ее эксплуатации возлагается на администратора базы данных.

Механизм *представлений* активно используется в схеме БД с УМД. Он служит мощным и гибким инструментом организации защиты данных, позволяющим скрывать от определенных пользователей некоторые части базы данных. В результате пользователи не будут иметь никаких сведений о существовании любых атрибутов или строк данных, которые не доступны через представления, находящиеся в их распоряжении.

Резервное копирование – это периодически выполняемая процедура получения копии базы данных и ее файла журнала на носителе, хранящемся отдельно от системы. Сегодня практически любая современная СУБД предоставляет средства резервного копирования, позволяющие восстанавливать базу данных в случае ее разрушения. С этой целью рекомендуется создавать резервные копии базы данных с УМД и ее файла журнала с некоторой установленной периодичностью, а также организовывать хранение созданных копий в местах, обеспеченных необходимой защитой. В случае аварийного отказа, в результате которого база данных становится непригодной для дальнейшей эксплуатации, резервная копия и зафиксированная в файле журнала оперативная информация используются для восстановления базы данных до последнего согласованного состояния.

Средства поддержки *целостности данных*, реализованные в БД с УМД (определение данных базовых таблиц, система триггеров и серверных процедур и т. д.), также вносят определенный вклад в общую защищенность базы 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, с одной стороны, доступ к ней необходимо ограничить, а с другой – имеет смысл *зашифровать* ее. Существует множество различных технологий зашифрования данных с целью сокрытия передаваемой информации. 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:

– защита информации, находящейся в БД, должна организовываться с учетом СУБД и ее возможностей по встраиванию защитных механизмов (например, начиная с Oracle Database 10*g*, методы шифрования реализуются с помощью встроенного пакета DBMS_CRYPTO, в более ранних версиях доступен другой пакет – DBMS_OBFUSCATION_TOOLKIT, в котором предлагается подмножество функциональных возможностей пакета DBMS_CRYPTO; по умолчанию для шифрования используется криптографический алгоритм AES с 192-битовым ключом, хотя можно использовать любой из алгоритмов AES (AES128, AES192, AES256) или 3DES168 (168-bit Triple DES – трехкратное применение алгоритма DES) с 168-битовым ключом), а также RC4, кроме этого возможно использование других криптографических примитивов: криптографические алгоритмы кеширования – MD5, SHA-1, MD4; алгоритмы кеширования (MAC) – HMAC_MD5, HMAC_SH1; криптографический генератор псевдослучайных чисел – RAW, NUMBER, BINARY_INTEGER), либо в виде внешних защитных оболочек для систем, работающих без функций защиты, или если штатные средства не удовлетворяют пользователя;

– 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;

– средства шифрования приводит к некоторому снижению производительности информационной системы, использующей базу данных.

Большие объемы данных и избирательный доступ к информации затрудняют реализацию эффективного подхода, когда содержимое предварительно расшифровывается, а затем, после использования, зашифровывается обратно. Поэтому, чтобы сохранить привычный инструментарий и порядок работы, используется метод “прозрачного шифрования”, при котором информация автоматически расшифровывается во время считывания с носителя (если был введен правильный ключ) и автоматически зашифровывается при записи. При выборе продукта следует обращать внимание на то, может ли защита устанавливаться динамически, не прерывая процесса работы, или требуется отключение баз данных на период шифрования, на что может уйти немало времени [7].

Так, например, “*прозрачное шифрование данных*” (TDE – Transparent Data Encryption), введенное как часть Oracle Advanced Security Option (версия 10.2 и выше), позволяет выборочно шифровать уязвимые данные, которые на нижнем уровне хранятся в файлах базы данных, а также все потоковые файловые компоненты, такие как журнальные файлы, архивные журналы и ленты резервного копирования. Основная цель TDE – защитить уязвимые данные, находящиеся в этих файлах операционной системы, и не допустить последующего доступа к диску или ленте резервного копирования для восстановления базы данных или сканирования файлов операционной системы, чтобы получить

персональную идентификационную информацию. Техника TDE присуща не только СУБД Oracle, но и SQL Server, или даже базам данных вообще (пример – патент IBM 7426745) [8].

Шифрование становится особенно актуальным при передаче конфиденциальных данных по незащищенным линиям связи. Например, в случае использования распределенных ИС, для организации репликаций данных по открытым каналам связи целесообразно использовать современные методы шифрования. А так как базу данных с УМД предполагается использовать в распределенных системах, более того, реплицируемая информация будет иметь предопределенную структуру и может быть сугубо конфиденциальной или секретной, то с целью противостояния атакам на основе выбранного открытого текста такую информацию необходимо зашифровывать с помощью современных стойких шифров. При этом возможно использование блочных симметричных шифров, например: *AES, RC6*, *ГОСТ, Serpent* и так далее, а также ассиметричных шифров: *RSA, EPOC-2, ACE Encrypt* и др.

Кроме того, существует множество причин, по которым разработчик не хочет, чтобы кто-то видел исходный код написанных им процедур, функций, пакетов, триггеров. Среди наиболее важных причин можно отметить следующие: права интеллектуальной собственности; коммерческая ценность; код обеспечивает решение задач защиты и распределения прав доступа к данным; недопустимость модификации кода другими пользователями, особенно при установке продукта заказчику (чтобы у последнего не было оснований заявлять после его собственной модификации, считай взлома, о неработоспособности и ненадежности программного обеспечения в соответствующей части). Именно по этим причинам код основных элементов БД с УМД целесообразно скрыть.

Существует несколько способов сокрытия кода. Например, в СУБД Oracle с точки зрения эффективности наиболее подходящим для этой цели является использование специальной утилиты WRAP. Эта утилита весьма просто скрывает PL/SQL-код основных элементов БД с УМД, 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 все равно не смогут понять, что в действительности он делает. Кроме того, такая подмена не сильно сказывается на производительности, в отличие от процедуры зашифрования/расшифрования.

Аппаратное обеспечение, на котором эксплуатируется БД с УМД, должно быть *отказоустойчивым*. Для этого необходимо иметь избыточные компоненты, которые могут быть объединены в систему, сохраняющую свою работоспособность при отказе одного или нескольких компонентов. Как показывает практика эксплуатации компьютерных систем, дисковые накопители являются наиболее уязвимыми среди всех аппаратных компонентов и характеризуются самыми низкими показателями непрерывной работы между отказами.

Идеология надежного и эффективного хранения информации на жестких дисках нашла свое отражение в так называемой технологии RAID. Эта технология реализует концепцию создания блочного устройства хранения данных с возможностями параллельного выполнения запросов и восстановления информации при отказах отдельных блоков накопителей на жестких магнитных дисках.

Выводы. В базе данных, построенной на основе универсальной модели данных, для обеспечения безопасности данных используются как возможности (методы и средства) тех СУБД, на платформе которых она строится, так и собственные средства, разработанные в рамках схемы БД с УМД, естественно, с учетом возможностей СУБД.

Все рассмотренные выше методы и средства защиты данных, нашедшие свою реализацию в базе данных с универсальной моделью, позволяют утверждать, что БД с УМД достаточно хорошо защищена и уровень ее безопасности достаточно высокий.

Литература

1. Кузнецов С. Д. Крупные проблемы и текущие задачи исследований в области баз данных [Электронный ресурс] / Кузнецов С. Д. – Режим доступа : http://www.citforum.ru/database/articles/problems/

2. Кузнецов С. Д. Предвестники новых манифестов управления данными [Электронный ресурс] / Кузнецов С. Д. – Режим доступа : http://www.citforum.ru/database/articles/premanifest/

3. Есин В. И. Безопасность информационных систем и технологий / Есин В. И., Кузнецов А. А., Сорока Л. С. – Х. : ЭДЭНА, 2010. – 656 с.

4. Коннолли Т. Базы данных. Проектирование, реализация и сопровождение. Теория и практика. – 3-е издание : пер. с англ. / Т. Коннолли, К. Бегг. – М. : Вильямс, 2003. – 1440 с. : ил.

5. Фленов М. Безопасность баз данных предприятия, 2007 [Электронный ресурс] / Фленов М. – Режим доступа : http:www.vr-online.www.cydsoft.com/russia

6. Финнеган П. Oracle-пользователи по умолчанию, их пароли и зашифровки [Электронный ресурс] / Финнеган П. – Режим доступа : http://www.oracle.com/global/ru/oramag/january2002/admin_defaultuser.html

7. Иванов А. Особенности применения средств шифрования для защиты баз данных / [Электронный ресурс] / Иванов А. –Режим доступа : http://www.osp.ru/lan/2009/05/8808151/

8. Пржиялковский В. Бумажник Oracle Wallet: использование для шифрования данных на внешнем носителе [Электронный ресурс] / Пржиялковский В. – Режим доступа : http://www.citforum.ru/database/oracle/wallet1/