Система разграничения доступа к данным на уровне записей и ячеек

А. В. Федоров,
a.fedorov@center-inform.ru
В. М. Пьянков,
v.pyankov@center-inform.ru
П. С. Вихлянцев,
p.vihlyantsev@center-inform.ru
М. В. Симонов

info@center-inform.ru
www.center-inform.ru

ФГУП «ЦентрИнформ»

Предназначение большинства информационных систем подразумевает хранение и использование больших объемов информации, а также доступ к ним широкого круга лиц. В то же время защита данных от несанкционированного доступа является важнейшей задачей при разработке и функционировании любой информационной системы.

Взаимодействие пользователей и программных приложений с базами данных осуществляется под контролем системы управления базами данных (СУБД), которая является доминирующим инструментом в обеспечении требуемого уровня безопасности информационной системы.

Большинство известных корпоративных СУБД реализуют управление доступом именованных пользователей к именованным объектам, что частично обеспечивается СУБД, поддерживающими стандарт SQL.

Обычно разграничение доступа к поименованным информационным объектам базы данных (таблицам, представлениям, процедурам и т. п.) ограничивается полным набором данных, предоставляемым тем или иным пользователям. В то же время существуют задачи, требующие управления доступом на более низком уровне. Так, в информационной системе поликлиники списки пациентов и их диагнозы могут храниться в одном файле или таблице. Врачи должны иметь доступ к данным только своих пациентов (разграничение на уровне записей), а сотрудники регистратуры – к необходимой общей информации о пациенте.

Аналогичные требования могут предъявляться к информационным системам другого назначения, в частности, тем, в которых хранятся персональные данные.

Ячейка таблицы является минимальным уровнем, на котором необходимо разграничение доступа к информации в базе данных.

В реляционных СУБД можно выделить следующие пять уровней разграничения доступа:

- сервер СУБД;
- база данных;
- таблица;
- запись таблицы;
- ячейка записи.

Разграничение доступа на первых трех уровнях реализуют механизмы, встроенные в СУБД и/или предусмотренные операционными системами.

В современной терминологии разграничение доступа к информации в базах данных на уровне записей носит название RLS (row level security), а на уровне ячеек – CLS (cell level security).

Большинство СУБД вообще не имеют встроенных средств контроля доступа к данным на уровне записей и ячеек. Тем не менее, некоторые СУБД содержат функциональность, потенциально достаточную для реализации разграничений доступа на этих уровнях. К указанным СУБД относится и Microsoft SQL Server[1].

В СУБД семейства Oracle, начиная с версии 8.1, реализовано расширение FGAC (Fine Grained Access Control – детальный контроль доступа), предоставляющее возможность детального разграничения доступа и работающее в связке с контекстами защищенных приложений (Secure Application Contexts)[2].

Имеется ряд коммерческих продуктов, в той или иной степени удовлетворяющих детальному разграничению доступа. В частности, к таким продуктам можно отнести расшире-

[1] *http://technet.microsoft.com. «Implementing Row- and Cell-Level Security in Classified Databases Using SQL Server 2005».*
[2] *http://www.oracle.com.*

ния Data Security for SQL Server NetLib Encryptionizer for SQL Server[3] и SQL Server 2005 Label Security Toolkit[4].

Однако указанные расширения являются лишь технической основой для создания полноценного решения. Необходима разработка системы, предоставляющая механизм, автоматически применяющий заданную логику отбора данных по правам, предоставляемым пользователю. Указанная логика должна основываться на контексте пользователя и данных и позволять управлять доступом на уровне записей и ячеек. Кроме этого, система должна иметь удобные средства администрирования.

На практике пользователи практически никогда напрямую не общаются с базой данных и с СУБД. Как правило, все действия производятся посредством клиентских приложений, в которые встраивают функциональности разграничения доступа.

В многоуровневых системах разграничение доступа может быть реализовано, например, на уровне бизнес-логики. В двухуровневой системе клиент-серверного приложения это может быть реализовано в клиентской части.

К недостатками таких подходов следует отнести:

- необходимость изменения кода приложения при смене политики безопасности;
- вероятный несанкционированный доступ к данным в обход приложений.

Другим часто применяемым подходом является реализация доступа к данным через хранимые процедуры. При таком подходе пользователям предоставляется доступ на выполнение хранимых процедур, реализующих необходимую логику фильтрации. Недостатком разграничения доступа через хранимые процедуры является необходимость переписывания кода большого числа хранимых процедур при изменении политики безопасности.

Следует отметить, что в обоих вышеуказанных подходах не обеспечивается защита данных при хищении резервных копий баз данных.

Предлагаемая система управления доступом к данным на уровне записей и ячеек (система CRLS) разработана для Microsoft SQL Server. Основным ее отличием является независимость от специфики приложений, которые взаимодействуют с СУБД.

В системе CRLS реализовано единое средство администрирования, позволяющее управлять ролями пользователей и задавать для них всю совокупность прав и ограничений. Посредством системы CRLS решается задача реализации политики разграничения доступа к данным на уровне записей/ячеек при условии максимального удобства администрирования. Имеется возможность как ручного управления доступом, так и автоматического разграничения доступа к данным в соответствии с определяемыми настройками.

Основой данного решения является изолирование пользователя от прямого доступа к объекту защиты и создание отображения (представления), через которое пользователь может осуществить доступ к объектам. Разграничение доступа посредством созданного представления реализуется инфраструктурой системы CRLS, основная часть которой располагается на уровне базы данных. Инфраструктура, располагающаяся на уровне SQL-сервера, реализует контекст безопасности.

В системе CRLS поддерживается построение иерархии ролей и назначение ролей пользователям, а также поддерживаются иерархии ролей, определенных в рамках базы данных SQL-сервера. Система CRLS однозначно идентифицирует пользователя, от лица которого осуществляется доступ к данным. Для идентифицированного пользователя вычисляется набор ролей (эффективные роли) непосредственно, а также косвенно через наследование ролей в иерархии.

Для системы разграничения доступа на уровне записей объектом является запись таблицы и данные ее полей, а операция представляет собой одно из действий над записью: select, insert, update, delete.

На уровне ячейки объектом доступа является содержимое ячейки. Операция ограничивается доступностью или недоступностью содержимого ячейки в момент выполнения операции над записью.

Система CRLS, как и большинство других систем разграничения доступа, позволяет администратору безопасности в ручном режиме назначить конкретному пользователю разрешения на выполнение операций с конкретными записями или ячейками. Данный режим работы – не основной.

Основным режимом работы системы CRLS является автоматический режим. Обуславливается это спецификой баз данных, заключающейся в большом количестве объектов разграничения доступа в рамках даже одной таблицы. Кроме этого, отсутствует какая-либо иерархия объектов разграничения, например, подобно иерархии каталогов файловой системы.

Возможность автоматизации разграничения доступа в системе CRLS достигается благодаря использованию правил (условий), формируемых с помощью модуля администрирования. Основная задача правила состоит в однозначной классификации комбинации трех сущностей: пользователя, объекта доступа и операции.

Введение и использование правил позволяет расширить возможности администратора по настройке разграничения доступа. В отличие от ручной привязки разрешений к конкретным объектам, в автоматическом режиме разграничение доступа сводится к привязке разрешений к правилам, классифицирующим контекст доступа согласно требованиям безопасности. Таким образом, система CRLS автоматически применяет правила и вычисляет разрешения в моменты доступа к данными защищаемой таблицы.

Разрешение, которое привязывается к правилу разграничения на

[3] *http://www.netlib.com/sql-server-encryption.asp.*

[4] *http: //blogs.msdn.com/publicsector/archive/2006/11/16/sql-server-2005-label-security-toolkit.aspx.*

уровне записи, представляет собой сочетание трех сущностей:
- роли (пользователя);
- операции;
- разрешено/запрещено.

Разрешение, которое привязывается к правилу разграничения на уровне ячейки представляет собой сочетание двух сущностей:
- роли (пользователя);
- разрешено/запрещено.

Благодаря введению механизма правил система CRLS в момент выполнения пользователем операции над защищаемым объектом получает все необходимые знания для реализации разграничения (см. рисунок):
- разрешения, вычисленные в результате применения правил;
- текущая операция;
- субъект, осуществляющий доступ (пользователь и его эффективные роли).

На основании этих знаний система CRLS однозначно определяет, разрешено ли пользователю осуществлять запрашиваемую операцию над защищаемым объектом.

Система CRLS обладает следующими характеристиками:
- поддерживает модель безопасности Microsoft SQL Server;
- интегрируется в приложения, архитектура которых предполагает работу с базой данных через фиксированное соединение;
- реализует механизм идентификации и последующей имперсонализации пользователя на уровне базы данных, позволяющий интегрировать систему CRLS в информационные системы, построенные на основе web-технологии, где разграничение доступа к данным реализуется на уровне бизнес-логики (web-сервера), а работа с базой данных ведется с использованием фиксированного соединения или пула соединений;
- обеспечивает прозрачный доступ средствами, предоставляемыми Microsoft SQL Server к данным, защищенным системой CRLS;
- имеет средства администрирования, не зависящие от специфики приложений, взаимодействующих с базой данных.

Кроме этого архитектура системы CRLS позволяет встраивать средства криптографической защиты информации (СКЗИ).

Шифрование данных отдельных полей возможно ключами различных пользователей. Это обеспечит защиту данных в случае несанкционированного копирования базы данных или кражи файлов базы данных.

Работа системы CRLS может снижать производительность доступа к данным из-за необходимости проверки прав пользователей и осуществления операций шифрования/дешифрования данных, которые занимают определенное время. Степень влияния системы CRLS на производительность СУБД зависит от сложности реализуемой бизнес-логики, от конфигурирования правил и ролей в системе доступа. Однако задание бизнес-логики в правилах и ролях системы CRLS снимает необходимость ее реализации в бизнес-приложениях и, соответственно, не приводит к снижению общей производительности информационной системы.

В некоторых случаях система CRLS может даже повысить производительность информационной системы в целом, так как в конечное приложение будет доставляться не вся информация из таблиц, а только та ее часть, правом доступа к которой обладает пользователь, что сокращает перебор и обработку записей.

Сделаем выводы из вышеизложенного.

1. Система CRLS имеет механизмы, расширяющие возможности по управлению доступом к данным и их защите и обеспечивающие гибкость настройки доступа к информации для разных пользователей.

2. Система CRLS имеет возможности для реализации требований по защите информации в соответствии с руководящими документами ФСТЭК России.

3. Применение системы CRLS предоставляет следующие преимущества:
- исключается несанкционированный доступ к защищенным данным посредством любых нелегитимных приложений;
- средства отчетности работают с представлениями, в которых уже учтена необходимая политика безопасности, и при ее изменении не требуется переписывания кода приложения – достаточно применить соответствующие настройки в системе;
- наличие ролей разного уровня позволяет использовать как существующие SQL-роли, так и вводить логические роли посредством системы CRLS, что дает возможность получить большую гибкость в реализации разграничения доступа.

4. Использование предлагаемой системы CRLS целесообразно в информационных системах, содержащих конфиденциальную информацию, в том числе и персональные данные.

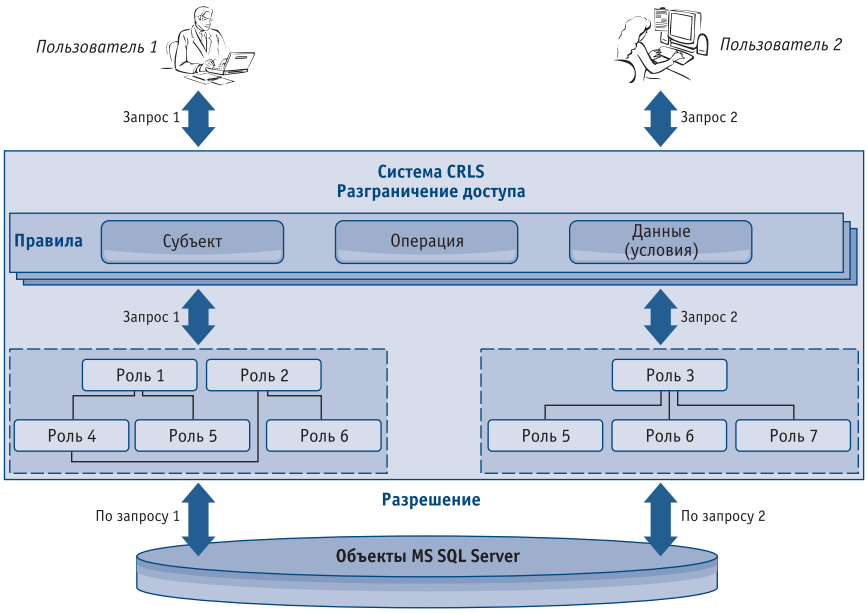

Рисунок. ***Схема формирования разрешений на доступ к данным***