УДК 004.65

В. Ч. К. Ал-Исауи В.В. Смелов , Л. С. Мороз
Белорусский государственный технологический университет

ОБОБЩЕННАЯ МОДЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

Исследованы механизмы обеспечения информационной безопасности систем управления базами данных (СУБД) Oracle 12C, IBM DB2 и Microsoft SQL Server 2012. Построена обобщенная модель информационной безопасности СУБД, включающая: девять уровней объектов базы данных и сервера СУБД, три процесса (аутентификации, авторизации и аудита), а также три уровня поверхности базы данных. Описаны принципы межуровневого взаимодействия модели, перечислены основные объекты каждого уровня, выявлены механизмы обеспечения информационной безопасности на каждом уровне.

Предлагается применять предложенную модель для сравнительного анализа механизмов информационной безопасности СУБД.

Ключевые слова: информационная безопасность, база данных, система управления базами данных, модель информационной безопасности.

V. Ch. K. Al-Isaui, V. V. Smelov, L. S. Moroz

GENERALIZED MODEL OF INFORMATION SECURITY DATABASE MANAGEMENT SYSTEM

Belarusian State Technological University

The article investigates the mechanisms for Information Security in the database. Researched mechanisms of information security management systems (DBMS) Oracle 12C, IBM DB2 and Microsoft SQL Server 2012. Built model is generalized information security database, which includes nine levels of objects database and database server, including three processes (authentication, authorization, and accounting), and three surface level database. The principles of the inter-layer interaction models are the main objects of each level, to identify the mechanisms of information security at every level.

It is proposed to apply the proposed model for the comparative analysis of the mechanisms of information security database.

Keywords: information security, database, database management system, the model of information security

Введение. Технологии хранения и управления данными за последние четверть века претерпели революционное развитие, объемы хранимых данных увеличились на несколько порядков. Базы данных, размеры которых исчисляются петабайтами, с ежедневным приростом данных в несколько гигабайтов данных сегодня не являются редкостью. При этом технологии семейства AllwaysOn позволяют обеспечить непрерывный доступ к данным.

Программной реализацией технологий управления данными являются системы управления базами данных (СУБД). Помимо надежного хранения, эффективного поиска и обновления данных, на СУБД возлагаются задачи информационной безопасности, включающие: аутентификацию, авторизацию, секретность и аудит.

На рисунке представлена обобщенная модель информационной безопасности современной СУБД. Модель построена на основе анализа трех наиболее технологически развитых СУБД: Oracle 12c, IBM DB/2 и Microsoft SQL Server 2012 [1 - 3]. Модель является обобщенной в том смысле, что в полной мере ей не соответствует ни одна из реальных систем (можно говорить только о степени соответствия), но описывает принципы и методы решения задач информационной безопасности в современных СУБД.

Модель представляет собой девять взаимодействующих пронумерованных

компонент (см. рисунок). Причем компоненты с более высоким номером включают компоненты с меньшим номером. Каждая компонента имеет собственный набор объектов, а также объекты, входящие во вложенные в нее компоненты. Собственный набор самой внешней, девятой компоненты включает объекты операционной системы (файлы, процессы и потоки, службы операционной системы). Самая внутренняя, первая компонента, содержит реляционные таблицы базы данных, состоящие из столбцов и строк.

В модели рассматриваются три процесса (обозначены направленными стрелками): процесс аутентификации, процесс авторизации и процесс аудита.

Кроме того, модель выделяет уровни поверхностей базы данных. Под поверхностью понимается совокупность объектов, представляющих базу данных подключившемуся пользователю. Поверхность представляется в виде набора таблиц (поверхность 1), набора представлений (поверхность 2) или набора процедур и функций (поверхность три). В реальных базах данных могут сосуществовать все три уровня одновременно.

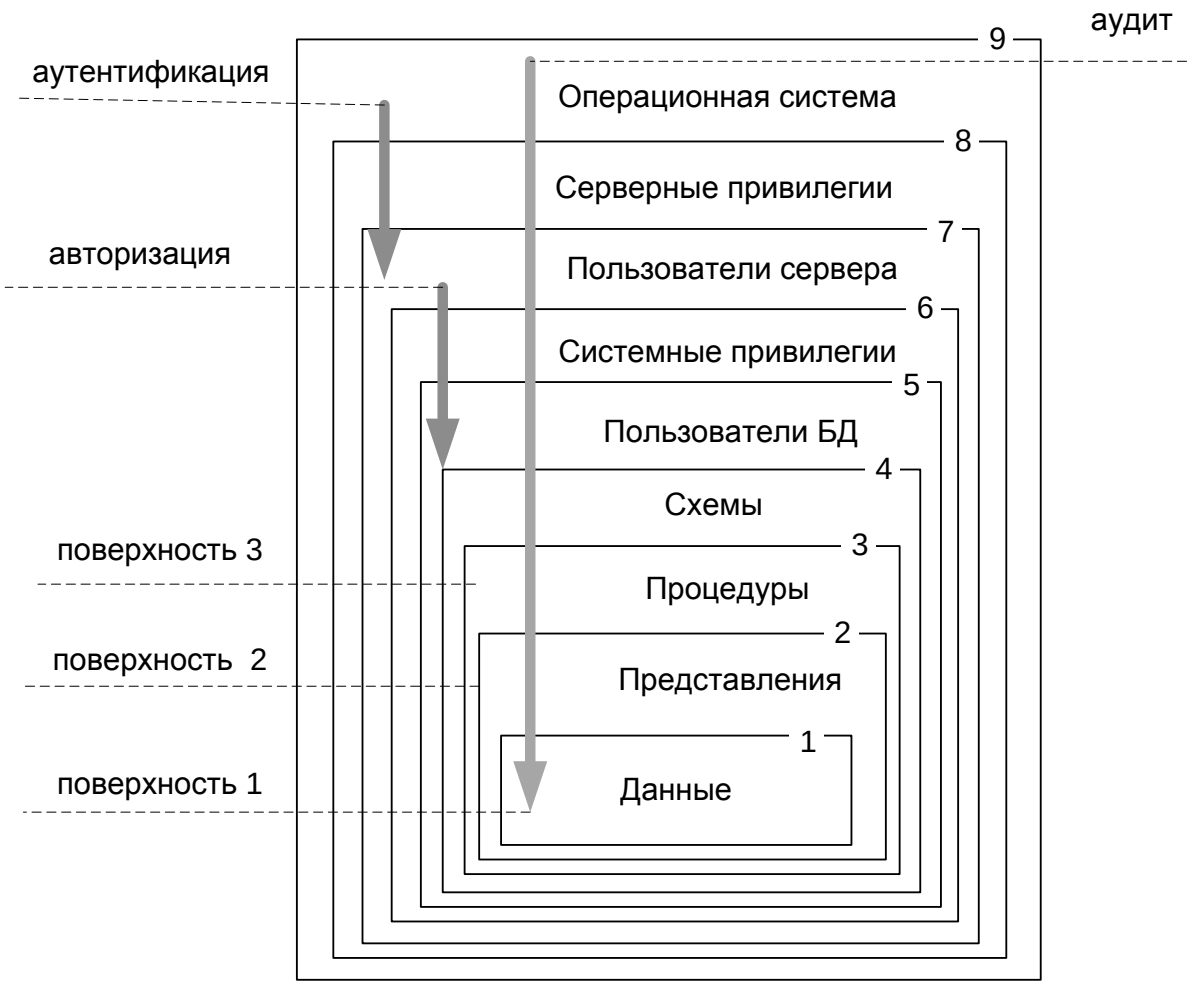

Рисунок. Обобщенная модель информационной безопасности СУБД

Основная часть. В дальнейшем будем говорить об уровнях модели. Каждый уровень соответствует компоненте с тем же номером. При этом будем считать, что уровень содержит собственные объекты соответствующей компоненты.

1. Уровень данных**.** Собственными объектами уровня данных являются реляционные таблицы базы данных. На этом уровне нет объектов и механизмов, регулирующих доступ к данным. Пользователю базы данных может быть предоставлен прямой доступ к содержимому таблицы или отдельных столбцов (для чтения, модификации и удаления) с помощью назначенных ему объектных привилегий средствами пятого уровня модели. Создание изменение и удаление таблиц базы данных определяется наличием соответствующих системных привилегий, рассматриваемых на шестом уровне модели.
2. Уровень представления**.** Собственными объектами этого уровня являются представления (view), являющиеся поименованными и хранящимися в базе данных SELECT-запросами. С точки зрения информационной безопасности представления являются механизмом позволяющим создать промежуточный слой между пользователем (пятый уровень) и таблицами данных (первый уровень). Создание такого слоя позволяет скрыть от пользователя наличие столбцов и строк в существующих таблицах, или наоборот создать иллюзию работы с таблицей, которой в реальности не существует. Доступ к объектам этого уровня регулируется таким же образом, как и таблицам. Уровень представления может быть использован в качестве поверхности базы данных. Другими словами, пользователю будут доступны для работы только представления.
3. Уровень процедур**.** Для создания объектов этого уровня применяются встроенные системы программирования (такие как Transact-SQL или PL/SQL). Объекты уровня процедур представляют собой программные структуры: процедуры, функции, триггеры, пакеты процедур и функций, а так же пользовательские типы. Важнейшим механизмом, действующим на этом уровне является механизм имперсонизации, позволяющим назначать привилегии программным объектам. Часто этот уровень является поверхностью базы данных, то есть база данных может быть представлена пользователю как набор программных объектов: процедур, функций, типов и пр. Доступ к объектам этого уровня регулируется с помощью механизма объектных привилегий (пятый уровень). Возможность создания, изменения и удаления программных объектов определяется наличием соответствующих системных привилегий, рассматриваемых на шестом уровне модели.
4. Уровень схем. Схемы представляют собой поименованную совокупность объектов базы данных. Схему можно рассматривать, как пространство имен для объектов низших уровней модели. С точки зрения информационной безопасности схема может определять группу объектов, доступных пользователю для выполнения заданного перечня операций. Применение схемы требует указания двухкомпонентных имен объектов (имя схемы и имя объекта). Доступ к схемам регулируется с помощью механизма объектных привилегий, рассматриваемого на пятом уровне модели. Для создания и удаления схем необходимы системные привилегии (уровень шесть).
5. Уровень пользователей базы данных**.** Основными объектами этого уровня являются пользователи базы данных, объектные привилегии и роли уровня базы данных. Пользователь базы данных является принципалом (объект безопасности, которому могут быть назначены привилегии), которому могут быть назначены объектные и системные привилегии. Любой создаваемый в базе данных объект создается пользователем,

который становится владельцем этого объекта. Роль базы данных – это принципал, представляющий собой поименованный набор привилегий, который может быть назначен пользователю или другой роли. Объектные привилегии – набор элементарных разрешений, которые может выдать пользователь-владелец объекта другому пользователю для его использования. Как правило, на уровне базы данных всегда предопределены два пользователя: один – с максимальными системными привилегиями, другой – с минимальными. Первый является владельцем базы данных (всех ее объектов) и предназначен для выполнения административных функций, второй предназначен для подключения к базе данных незарегистрированных функций. Каждый пользователь базы данных связываются с пользователем сервера, определенном на седьмом уровне модели.

6. Уровень системных привилегий. Системная привилегия – это элементарное разрешение, которое связано с типом объекта (например, привилегия на создание или удаление таблиц). Как правило, системные привилегии назначает привилегированный пользователь, выполняющий роль администратора. На этом уровне могут существовать предопределенные фиксированные роли – роли не позволяющие изменять заданный перечень системных привилегий.
7. Уровень пользователей сервера. Пользователь сервера СУБД предназначен для установки соединения клиентского приложения с сервером СУБД в рамках процедуры аутентификации. Каждый пользователь сервера проецируется на одного пользователя базы данных (уровень пять), привилегии которого определяют возможности в этой базе данных.
8. Уровень серверных привилегий. Собственными объектами уровня серверных привилегий являются серверные роли (фиксированные и пользовательские) и профили безопасности. Серверная роль – поименованная совокупность серверных привилегий (разрешений на уровне сервера).

Фиксированные серверные роли являются предустановленными и не допускают изменения заданных ими перечней привилегий. Серверные роли могут быть назначены пользователю сервера или другой нефиксированной роли. Профиль безопасности – поименованный перечень лимитов, связанных с процессом подключения серверного пользователя (максимальное количество попыток неправильного ввода пароля, строк действия пароля, максимальная продолжительность сеанса и т.п.). Обычно профиль безопасности связывается с серверным пользователем (уровень семь) и определяет свойства его подключения к серверу СУБД. Кроме того к этому уровню относят словарь данных СУБД (другое название – системный каталог СУБД, представляющий собой набор системных представлений, описывающих структуру базы данных и сервера.

9. Уровень операционной системы. На уровне операционной системы база данных представляет собой набора файлов, а сервер в виде нескольких серверных и фоновых процессов. Доступ к файлам данных и памяти процессов регулируется средствами операционной системы.

Заключение. Принцип построения предложенной выше модели информационной безопасности СУБД основывается на разбиении объектов базы данных и сервера СУБД на девять уровней по следующему правилу – безопасность каждого уровня модели определяется объектами и механизмами, определенными на более высоких уровнях. Модель может быть использована для анализа и сравнения систем информационной безопасности различных СУБД.

Литература

1. Oracle Database 12c Enterprise Edition [Электронный ресурс] / Oracle Corporation, 2015. – Режим доступа: http://oracle.com/database. – Дата доступа: 09.03.2015.
2. IBM DB2 Database software [Электронный ресурс] / IBM, 2015. – Режим доступа: http://www-01.imb.com/software/data/db2 . – Дата доступа: 09.03.2015.
3. Microsoft SQL Server Editions [Электронный ресурс] / Microsoft Corporation, 2015. – Режим доступа: http://www.microsoft.com/sqlserver/ru/ru/sql-2012-editions.aspx. – Дата доступа: 09.03.2015.

References

1. Oracle Database 12c Enterprise Edition [Electronic resource] / Oracle Corporation, 2015. – Access mode: http://oracle.com/database. – Date of access: 09.03.2015.
2. IBM DB2 Database software [Electronic resource] / IBM, 2015. – Access mode: http://www-01.imb.com/software/data/db2 . – – Date of access: 09.03.2015.
3. Microsoft SQL Server Editions [Electronic resource] / Microsoft Corporation, 2015. – Access mode: http://www.microsoft.com/sqlserver/ru/ru/sql-2012-editions.aspx. – – Date of access: 09.03.2015.

Информация об авторах

Ал-Исауи Висам Чяад Карим − магистрант кафедры кафедры информационных систем и технологий. Белорусский государственный технологический университет (220006, г. Минск, ул. Свердлова 13а, Республика Беларусь). E-mail: awessam@mail.ru

Смелов Владимир Владиславович − кандидат технических наук, доцент кафедры информационных систем и технологий. Белорусский государственный технологический университет (220006, г. Минск, ул. Свердлова 13а, Республика Беларусь). E-mail: smw60@mail.ru

Мороз Леонида Станиславовна – ассистент кафедры информационных систем и технологий. Белорусский государственный технологический университет (220006, г. Минск, ул. Свердлова 13а, Республика Беларусь). E-mail: morozls@tut.by

Information about the authors

V. Ch. K. Al-Isaui Visam Chjad Karim undergraduate, Department of Informational Systems and Technologies, Belarusian State Technological University (13a, Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: smw60@mail.ru

Smelov VladimirVladislavovich − Ph. D. Engineering, assistant professor, Department of Informational Systems and Technologies, Belarusian State Technological University (13a, Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: smw60@mail.ru

Moroz Leonida Stanislavovna assistant, Department of Informational Systems and Technologies, Belarusian State Technological University (13a, Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: morozls@tut.by

Поступила 09.03.2015

УДК 004.65

В. Ч. К. Ал-Исауи В.В. Смелов , Л. С. Мороз
Белорусский государственный технологический университет

ОБОБЩЕННАЯ МОДЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

V. Ch. K. Al-Isaui, V. V. Smelov, L. S. Moroz

GENERALIZED MODEL OF INFORMATION SECURITY DATABASE MANAGEMENT SYSTEM

Belarusian State Technological University