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

Статья посвящена описанию обобщенной модели информационной безопасности систем управления базами данных (СУБД). Модель построена на основе анализа систем информационной безопасности СУБД Oracle 12c, IBM DB2 и Microsoft SQL Server 2012, но при этом является обобщенной и не соответствует в полной мере ни одной из перечисленных СУБД. Можно говорить лишь о степени соответствия. Модель включает девять поименованных уровней и три процесса. На каждом уровне модели располагаются объекты базы данных, сервера СУБД и операционной системы. Разбиение на уровни осуществляется по следующему принципу: безопасность каждого уровня модели (кроме самого верхнего) определяется объектами и механизмами, определенными на более высоких уровнях. Описание модели включает перечень объектов каждого уровня с пояснением принципов межуровневого взаимодействия. Самый нижний уровень (первый) модели содержит реляционные таблицы базы данных, самый верхний (девятый) – объекты операционной системы (процессы, пользователи, файлы и пр.). В модели вводится понятие поверхности базы данных. Каждая поверхность определяет один из способов логического представления базы данных пользователю. Модель описывает три процесса: аутентификации, авторизации и аудита. Процесс аутентификации затрагивает три верхних уровня, процесс авторизации – три следующих, процесс аудита – все девять уровней модели. Модель может применяться при проектировании информационных систем, при этом она позволяет сформулировать основные требования к информационной безопасности данных до выбора СУБД. Кроме того, модель может быть использована в учебном процессе с целью системного описания технологии обеспечения информационной безопасности, применяемой современными 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
Belarusian State Technological University

THE GENERALIZED MODEL OF AN INFORMATION SECURITY DATABASE MANAGEMENT SYSTEM

The article describes the generalized model of information security management systems (DBMS). The model is constructed based on the analysis of information security systems DBMS Oracle 12c, IBM DB2 and Microsoft SQL Server 2012, but it is generalized and does not fully conform to any of the listed databases. One can only talk about the degree of compliance. The model includes nine levels and named three processes. At each level of the model the database objects are placed as well as, database server and operating system. Layering is done in the following way: the safety of each level (except the top) is determined objects and mechanisms defined at higher levels. The description of the model includes a list of objects at each level to explain the principles of the inter-layer interaction. The lowest level (first) of the model contains the relational database tables, the top (ninth) – operating system objects (processes, users, halyards etc.). The model introduces the concept of the surface of the database. Each surface defines one of the ways a logical view of the database user. The model describes three processes: authentication, authorization, and auditing. The authentication process involves three upperlevels, authorization – the next three, and the audit process – all nine levels of the model. The model can be applied in the design of information systems – its use allows us to formulate the basic requirements for information security data before selecting the database. The model can be used in the educational process its use enables us to give a systematic description of information security technologies applied by modern DBMS.

Key words: information security, database, database management system, the model of information security.

Введение. На сегодняшний день наиболее технологически развитыми СУБД являются: Oracle 11.2g/12c, IBM DB2 и Microsoft SQL Server 2008/2012 [1–3]. Все они поддерживают реляционную модель данных и реализуют архитектуру клиент-сервер. Анализ систем информационной безопасности этих СУБД позволил авторам статьи разработать обобщенную

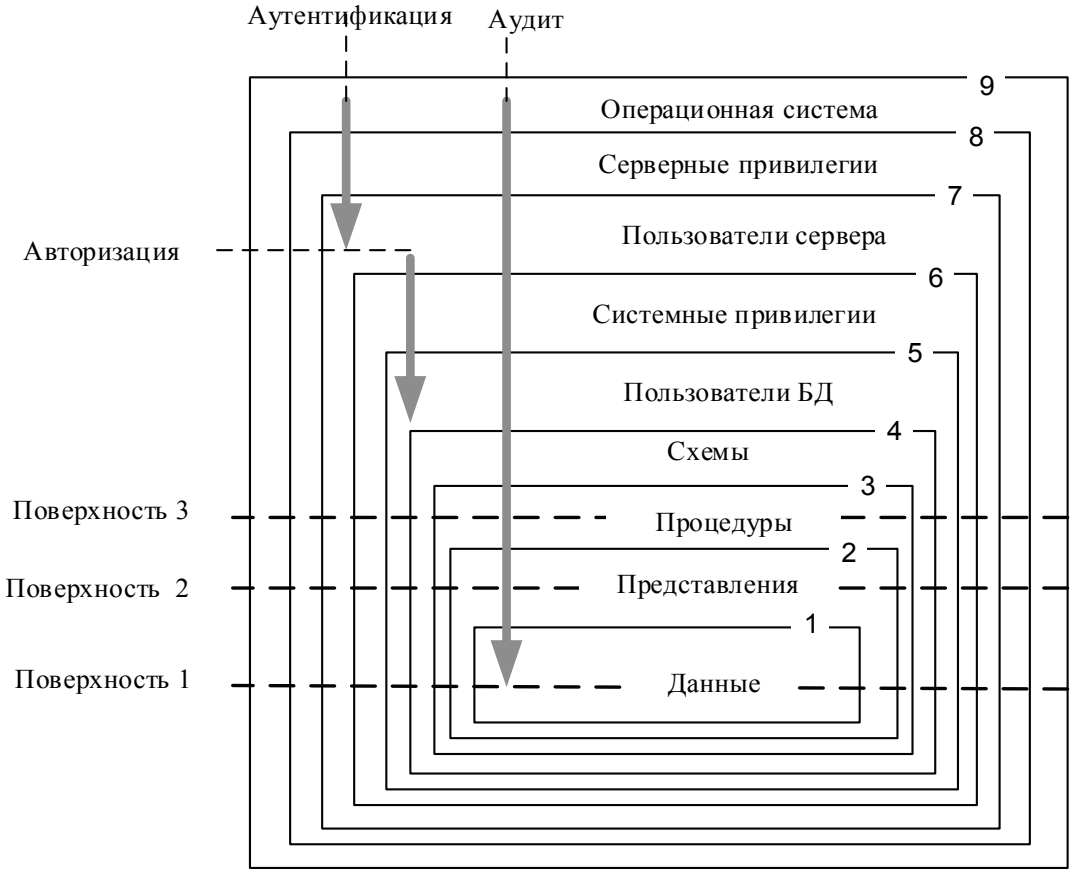
модель информационной безопасности СУБД. Модель является обобщенной в том смысле, что в полной мере ей не соответствует ни одна из реальных систем (можно говорить только о степени соответствия), но описывает общие принципы и методы решения задач информационной безопасности СУБД. Обобщенные модели СУБД рассматриваются и в [4], но все они описывают уровни абстракции данных или принципы хранения данных.

Основная часть. На рисунке приведено графическое изображение обобщенной модели информационной безопасности СУБД. Модель представляет собой девять взаимодействующих пронумерованных и поименованных компонент. Все компоненты, кроме первой, включают в себя компоненты с меньшими номерами. Каждая компонента имеет собственный набор объектов базы данных (БД) или сервера СУБД.

В модели рассматриваются три процесса (обозначены направленными стрелками): аутентификации, авторизации и аудита. Кроме того, вводится понятие поверхностей базы данных (изображены штриховыми горизонтальными линиями). Под поверхностью понимается способ представления БД подключившемуся пользователю. В простейшем случае БД может быть представлена в виде множества таблиц (поверхность 1). В других – в виде набора представлений (поверхность 2) или перечня процедур и функций (поверхность 3). В общем случае могут сосуществовать все три уровня одновременно.

Далее будут использоваться уровни модели. Каждый уровень соответствует компоненте с тем же номером. На каждом уровне будем рассматривать перечень собственных объектов уровня и привилегии – элементарные разрешения на выполнение элементарных операций с объектами сервера или БД.

1. Уровень данных. Собственными объектами уровня данных являются реляционные таблицы БД. На этом уровне нет объектов и механизмов, регулирующих доступ к данным. Доступ к данным осуществляется пользователем БД (уровень 5), которому может быть предоставлен доступ к содержимому таблицы или отдельным столбцам (для чтения, модификации и удаления) с помощью назначенных объектных привилегий (уровень 5). Возможность создания, изменения и удаления таблиц БД определяется наличием соответствующих системных привилегий (уровень 6). Множество собственных объектов уровня данных представляет собой первую поверхность БД.



Обобщенная модель информационной безопасности СУ

2. Уровень представления. Собственными объектами этого уровня выступают представления, являющиеся поименованными и хранящимися в БД SELECT-запросами. Представления являются механизмом, позволяющим создать промежуточный слой между пользователем (уровень 5) и таблицами данных (уровень 1). Создание такого слоя дает возможность скрыть от пользователя наличие реальных таблиц, более того, создать иллюзию работы с таблицами, которых в реальности не существует. Доступ к представлениям регулируется таким же образом, как и к реляционным таблицам. Уровень представления может образовывать вторую поверхность БД. Другими словами, пользователю будут доступны для работы не реальные таблицы, а только представления. При этом операции, выполняемые с представлениями, будут транслироваться в операции с таблицами. В зависимости от вида представления трансляция может выполняться автоматически или с применением триггеров замещения (уровень 3).

3. Уровень процедур. Объекты уровня процедур представляют собой программные структуры: процедуры, функции, триггеры, пакеты процедур, функций и пользовательские типы. Важнейшим механизмом, действующим на этом уровне, является механизм имперсонизации, позволяющий перенести привилегии пользователя на программный объект. Часто этот уровень является поверхностью базы данных (поверхность 3), т. е. БД может быть представлена пользователю как набор программных объектов: процедур, функций, типов и пр. Доступ к объектам этого уровня регулируется с помощью механизмов объектных и системных привилегий (уровни 5 и 6).

4. Уровень схем. Схема – это поименованная совокупность объектов БД. С точки зрения информационной безопасности схема может определять группу объектов, доступных пользователю для выполнения заданного перечня операций. Доступ к схемам регулируется с помощью механизмов объектных и системных привилегий (уровни 5 и 6). Применение схемы дает возможность регулировать доступ пользователей (уровень 5) одновременно ко всем элементам схемы.

5. Уровень пользователей БД. Основными объектами этого уровня являются пользователи базы данных, объектные привилегии и роли уровня базы данных. Пользователь БД является принципалом – объектом безопасности, которому могут быть назначены привилегии. Любой создаваемый в БД объект создается от лица пользователя, который становится владельцем созданного объекта. Роль БД – это тоже принципал, представляющий собой поименованный набор привилегий. Роль может быть назначена пользователю или другой роли. При этом привилегии, закрепленные за исходной ролью, распространяются на пользователя или другую роль. Кроме того, на этом уровне могут быть определены фиксированные роли – роли, обладающие неизменяемым набором привилегий. Объектные привилегии – набор элементарных разрешений, которые может выдать пользователь-владелец объекта другому пользователю для использования объекта. Как правило, на уровне БД всегда предопределены два пользователя: один – с максимальными системными привилегиями (владелец БД), другой – с минимальными (для подключения без привилегий).

6. Уровень системных привилегий. Системная привилегия – это элементарное разрешение, связанное с элементарной операцией для типа объекта (например, привилегия на создание или удаление таблиц, представлений, процедур, функций). Как правило, системные привилегии назначает привилегированный пользователь – администратор БД. На этом уровне могут существовать предопределенные фиксированные роли. Кроме фиксированных ролей могут быть созданы пользовательские роли.

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 в БД (уровень 5), привилегии которого определяют возможности серверного пользователя в этой БД. Возможности серверного пользователя определяются назначенными ему серверными привилегиями (уровень 8).

8. Уровень серверных привилегий. Собственными объектами уровня серверных привилегий являются серверные роли и профили безопасности. Серверная роль – поименованная совокупность серверных привилегий (разрешений на уровне сервера). Серверные роли могут быть фиксированные (не допускающие модифкации) и пользовательские. Серверные роли могут быть назначены пользователю сервера или нефиксированной роли. Профиль безопасности – поименованный перечень лимитов, связанных с процессом подключения серверного пользователя (максимальное количество попыток неправильного ввода пароля, строк действия пароля, максимальная продол-

жительность сеанса и т. п.). Обычно профиль безопасности определяет свойства подключения пользователя к серверу СУБД. К этому же уровню относят словарь СУБД (системный каталог), представляющий собой набор системных представлений, описывающих структуру и состояние БД.

9. Уровень операционной системы. На уровне операционной системы (ОС) БД представляет собой набор файлов (файлы перманентных и временных данных, журналов, резервных копий и архивов, конфигурационные файлы), а сервер в виде нескольких серверных и фоновых процессов (или служб ОС), работающим от лица специальных учетных записей, созданных при инсталляции серверного программного обеспечения. Доступ к файлам данных и памяти процессов регулируется средствами ОС.

Процесс аутентификации. Аутентификация охватывает три верхних уровня модели. На уровне ОС аутентификация выполняется средствами ОС, на уровнях серверных привилегий и пользователей сервера – средствами СУБД. Может быть установлены доверительные отношения между ОС и СУБД, что позволяет применять только аутентификацию, выполненную ОС. Отдельно рассматривается процесс локальной аутентификации пользователя сервера СУБД. Такое подключение необходимо для старта или останова сервера, для перевода его в другие режимы работы, для выполнения серверных команд, требующих эксклюзивного использования сервера СУБД. В этом случае предусматривается аутентификация при отсутствии доступа к БД. На уровне системных привилегий может быть предусмотрена роль для подключения к серверу без аутентификации.

Процесс авторизации. Процесс авторизации выполняется после аутентификации и затрагивает три уровня (уровни 5–7). Он сводится к наделению пользователя БД необходимым перечнем системных и объектных привилегий. Любая работа с объектом БД осуществляется от лица пользователя БД и в соответствии с тем перечнем привилегий, которые он унаследовал от соответствующего пользователя сервера, от фиксированных и пользовательских ролей, а также привилегий, назначенных ему индивидуально.

Аудит. Основное назначение процесса аудита – осуществление контроля за уровнем информационной безопасности базы данных. Процесс охватывает все девять уровней модели и предназначен для выявления: избыточно назначенных привилегий; недостающих привилегий; попыток несанкционированного доступа к данным; авторства выполненных в базе данных операций.

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 является универсальной и не связана с какой-нибудь реализацией СУБД.

Модель может быть использована при проектировании информационных систем. Ее применение позволяет сформулировать требования к системе информационной безопасности БД безотносительно используемой СУБД. Более того, одним из критериев дальнейшего выбора СУБД может служить степень покрытия этой системой сформулированных требований.

Модель может быть применяться в учебном процессе для объяснения принципов построения систем информационной безопасности в современных СУБД.

Кроме того, модель может использоваться для сравнительного анализа систем информационной безопасности различных СУБД.

Литература

1. Oracle Database 12c Enterprise Edition [Электронный ресурс]. 2015. URL: http://oracle.com/database (дата обращения: 09.03.2015).

2. IBM DB2 Database software [Электронный ресурс]. 2015. URL: http://www-01.imb.com/software/data/db2 (дата обращения: 09.03.2015).

3. Microsoft SQL Server Editions [Электронный ресурс]. 2015. URL: http://www.microsoft.com/sqlserver/ru/ru/sql-2012-editions.aspx (дата обращения: 09.03.2015).

4. Дейт К. Дж. Введение в системы баз данных. М.: Вильямс, 2005. 1316 с.

References

1. Oracle Database 12c Enterprise Edition [Electronic resource]. 2015. Available at: http://oracle.com/database (accessed 09.03.2015).

2. IBM DB2 Database software [Electronic resource]. 2015. Available at: http://www-01.imb.com/software/data/db2 (accessed 09.03.2015).

3. Microsoft SQL Server Editions [Electronic resource]. 2015. Available at: http://www.microsoft.com/sqlserver/ru/ru/sql-2012-editions.aspx (accessed 09.03.2015).

4. Deyt K. Dzh. *Vvedeniye v sistemy baz dannykh* [Introduction to Database System]. Moscow, Vil'yams Publ., 2005. 1316 p.

Информация об авторах

Ал-Исауи Висам Чяад Карим – магистрант. Белорусский государственный технологический университет (220006, г. Минск, ул. Свердлова, 13а, Республика Беларусь). E-mail: smw60@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 Леонарда 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

Al-Isaui Visam Chjad Karim – undergraduate. Belarusian State Technological University (13a, Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: smw60@mail.ru

Smelov Vladimir Vladislavovich − Ph. D. (Engineering), Assistant Professor, the Department of Information Systems and Technologies. Belarusian State Technological University (13a, Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: smw60@mail.ru

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

Поступила 09.03.2015