Министерство образования Республики Беларусь

Белорусский государственный технологический университет

Ал-Исауи Висам Чяад Карим

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СУБД MICROSOFT SQL SERVERS 2008 И ORACLE 11.2g

Специальность 1-40 80 02 Системный анализ, управление и обработка информации

Магистерская диссертация
на соискание академической степени магистр

Научный руководитель:
к.т.н., доцент Смелов В. В.

Минск 2015

СОДЕРЖАНИЕ

ВВЕДЕНИЕ…….. 6
1. Аналитически обзор литературы……..... 7
1.1. Рынок СУБД……. 7
1.2. Стандарты безопасности……. 8
1.3. СУБД Oracle 11.2g…… 16
1.4. СУБД Microsoft SQL Server 2008…… 18
1.5. Заключение…… 19
2. Объекты информационной безопасности СУБД……... 21
2.1. Архитектура безопасности СУБД……... 21
2.2. Соединение с сервером СУБД …… 25
2.3. Серверные привилегии……. 27
2.4. Привилегии уровня базы данных…… 28
2.5. Роли…… 30
2.6. Имперсонизация……... 34
2.7. Заключение…… 36
3. Обобщенная модель информационной безопасности СУБД…... 38
3.1. Структура модели……. 38
3.2. Уровень данных…… 39
3.3. Уровень представлений……... 39
3.4. Уровень процедур……. 40
3.5. Уровень схем……. 41
3.6. Уровень пользователей базы данных……. 43
3.7. Уровень системных привилегий……. 43
3.8. Уровень пользователей сервера…….. 44
3.9. Уровень серверных привилегий…….. 44
3.10. Уровень операционной системы…… 45
3.11. Поверхности базы данных……... 45
3.12. Процессы аутентификации и авторизации……. 47
3.13. Процесс аудита……. 48
3.14. Заключение…… 49
4. Сравнительная оценка систем безопасности СУБД Oracle 11.2g и Microsoft SQL Server 2008……. 50
4.1. Принципы оценки систем безопасности…… 50
4.2. Метрики системы безопасности СУБД…… 51
4.2.1. Уровень данных…… 51
4.2.2. Уровень представлений……... 51
4.2.3. Уровень процедур……. 51
4.2.4. Уровень схем……. 52
4.2.5. Уровень пользователей базы данных……. 52

4.2.6. Уровень системных привилегий……. 52
4.2.7. Уровень пользователей сервера…….. 53
4.2.8. Уровень серверных привилегий…….. 53
4.2.9. Уровень операционной системы……. 53
4.3. Результаты экспертной оценки……... 54
ЗАКЛЮЧЕНИЕ……. 57
Список литературы…… 58
ПРИЛОЖЕНИЕ 1. Глоссарий терминов…… 60
ПРИЛОЖЕНИЕ 2. Справка о внедрении в учебный процесс..... 66

АННОТАЦИЯ

Пояснительная записка выполнена на 65 страницах, включая 9 таблиц, 33 рисунков.

Цель данной работы: осуществить сравнительный анализ систем безопасности двух систем управления базами данных (СУБД): Microsoft SQL 2008 и Oracle 11.2g.

Для достижения цели сформулированы следующие задачи:

- исследовать методики оценки информационной безопасности, опубликованные в литературе;
- исследовать архитектуру и объекты информационной безопасности СУБД Microsoft SQL 2008 и Oracle 11.2g;
- разработать обобщенную модель системы информационной безопасности СУБД;
- предложить методику сравнения систем информационной безопасности СУБД Microsoft SQL 2008 и Oracle 11.2g;
- получить количественную оценку сравнительного анализа систем безопасности двух СУБД : Microsoft SQL 2008 и Oracle 11.2g.

Диссертация состоит из введение, четырех глав и заключения. Каждая глава завершается заключением к главе. В ведении кратко описывается предмет исследования.

Первая глава посвящена литературному обзору. Материал главы содержит краткую информацию о состоянии рынка СУБД, обзор оценочных стандартов информационной безопасности, а также общие сведения об СУБД Microsoft SQL 2008 и Oracle 11.2g.

Во второй главе анализируется архитектура и объекты информационной безопасности СУБД Microsoft SQL 2008 и Oracle 11.2g.

Третья глава содержит описание обобщенной модели информационной безопасности СУБД.

Четвертая глава является результирующей и содержит описание методики сравнения систем безопасности СУБД, а также численный расчет оценки систем информационной безопасности СУБД Microsoft SQL 2008 и Oracle 11.2g.

الملـــخص

تحتوي هذه الاطروحه على (٦٥) صفحة وعلى (٩) جدول و (٣٣) رسم .
والغرض من هذا العمل هو: أجراء تحليل مقارن لأنظمة الأجهزة الأمنية لأثنين من إدارة قواعد البيانات (DBMS) هما:
مايكروسوفت SQL 2008 و Oracle 11.2g.
لتحقيق هذه المقارنه ونتائجها وضعت المهام التالية:
- دراسة منهجية لتقييم أمن المعلومات التي نشرت في المصادر.
- استكشاف الهندسة المعمارية والملحقات الخاصه بأمن المعلومات في مايكروسوفت SQL 2008 و Oracle 11.2g .
- وضع النموذج العام لقاعدة بيانات لنظم أمن المعلومات.
- اقتراح منهجية المقارنة لنظم أمن المعلومات في مايكروسوفت SQL 2008 و Oracle 11.2g.
- تحديد التحليل المقارن لقواعد البيانات الخاصه بنظم امن المعلومات هما: مايكروسوفت SQL 2008 و Oracle 11.2g .

تتكون الاطروحه من مقدمة وأربعة فصول وخاتمة. ينتهي كل فصل بخاتمه للفصل. يوصف نبذه مختصره لموضوع الفصل المقدم.

ويخصص الفصل الأول لاستعراض المصادر. ويتضمن الفصل الاول ملخصا لحالة سوق قاعدة البيانات، وإعادة النظر في معايير تقييم أمن المعلومات، فضلا عن معلومات عامة عن قاعدة بيانات Microsoft SQL 2008 و Oracle 11.2g.

يوضح الفصل الثاني الهندسة المعمارية والملحقات الخاصه بأمن المعلومات من مايكروسوفت SQL 2008 و Oracle 11.2g.

يتضمن الفصل الثالث وصفا للنموذج المصمم من قاعدة بيانات أمن المعلومات.

الفصل الرابع هو الناتج، ويصف أساليب المقارنة بين أنظمة قواعد البيانات الأمنية وتقييم الحساب العددي لنظم أمن المعلومات من مايكروسوفت SQL 2008 و Oracle 11.2g.

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 Always On [1] 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. Общая идея защиты баз данных состоит в следовании рекомендациям, сформулированным для класса безопасности С2 «Критериях оценки надежных компьютерных систем» [2].

Традиционно основными аспектами информационной безопасности СУБД являются конфиденциальность, целостность и доступность данных.

Под конфиденциальностью в СУБД понимается ее свойство, позволяющее предотвращать несанкционированное извлечение данных. Целостность определяется, как способность СУБД предотвращать несанкционированное изменение, удаление или уничтожение данных. Аспект доступности данных в СУБД требует обеспечения беспрепятственного доступа к данным для их извлечения, изменения или уничтожения пользователям, обладающим соответствующими привилегиями.

Для обеспечения конфиденциальности, целостности и доступности данных все современные СУБД применяют два механизма: аутентификацию и авторизацию. Механизм аутентификации предназначен для идентификации и проверки пользователей СУБД. Обычно, этот механизм реализован в виде процедуры позволяющей пользователю указать свое уникальное имя (идентифицирующее его в системе) и пароль (подтверждающий его подлинность). Механизм авторизации в СУБД представляет собой процедуру проверки возможности аутентифицированному пользователю выполнить извлечение, изменение или удаление определенных данных.

Данная работа посвящена сравнительному анализу систем информационной безопасности двух СУБД: Oracle 11.2g [3] и Microsoft SQL Server 2008 [4]. При этом основное внимание уделено вопросам реализации аспектов и механизмов информационной безопасности на уровне объектов сервера СУБД и базы данных.

1. АНАЛИТИЧЕСКИЙ ОБЗОР ЛИТЕРАТУРЫ

1.1. Рынок систем управление базами данных

Системы управления базами данных (СУБД) является одним из старейших направлений информационных технологий, имеющее более полувековую историю.

Предшественницами СУБД были файловые системы. Данные хранились в плоских файлах, имеющих жесткую структуру. Доступ к участкам файла, к которых были расположены данные, осуществлялся по смещению или по ключу (для файлов с индексным методом доступа).

В середине 60-х годов прошлого века корпорация IBM разработала первую СУБД IMS (Information Management System), основанную на иерархической модели данных [5].

Другим событием этого периода является появление СУБД IDS (Integrated Data Store) компании General Electric. Развитие этой системы привело к созданию сетевых СУБД. Сетевая структура данных значительно сложнее иерархической. Для создания стандартов СУБД сетевых моделей в 1965 году на конференции CODASYL (Conference on Data System Languages) была сформирована рабочая группа List Processing Task Force, переименованная в 1967 году в Data Base Task Group (DBTG) [6].

В 1970 году Э. Кодд, работавший в корпорации IBM, опубликовал статью о реляционной модели данных, позволявшей устранить недостатки прежних моделей. Вслед за этим появилось много экспериментальных реляционных СУБД. Первые коммерческие СУБД появились в конце 70-х годов. Среди них следует выделить СУБД System R, разработанную корпорацией IBM. Этот проект был задуман с целью доказать практичность реляционной модели. На основе этой СУБД был разработан язык SQL, который с тех пор стал стандартом.

В 1980-х годах были созданы первые версии двух знаковых СУБД: IBM DB2 [7] и Oracle корпорации Oracle.

В настоящее время существует несколько сотен различных СУБД для мейнфреймов и персональных ЭВМ.

С начала 90-х годов прошлого в течении 10 лет века бессменными лидерами рынка СУБД являлись две системы IBM DB2 и Oracle. Последний период начался с начала текущего века, когда группу лидеров стала нагонять компания Microsoft со своей СУБД Microsoft SQL Server.

С появлением этого активного игрока конкурентная ситуация резко обострилась, в результате чего начались процессы поглощения ИТ-гигантами специализированных разработчиков, и к середине прошлого десятилетия в данном сегменте установилось относительное спокойствие: корпорации IBM, Oracle и Microsoft прочно удерживают 80% (в денежном выражении) рынка. Говоря о рынке СУБД часто эти три компании называют «большой тройкой».

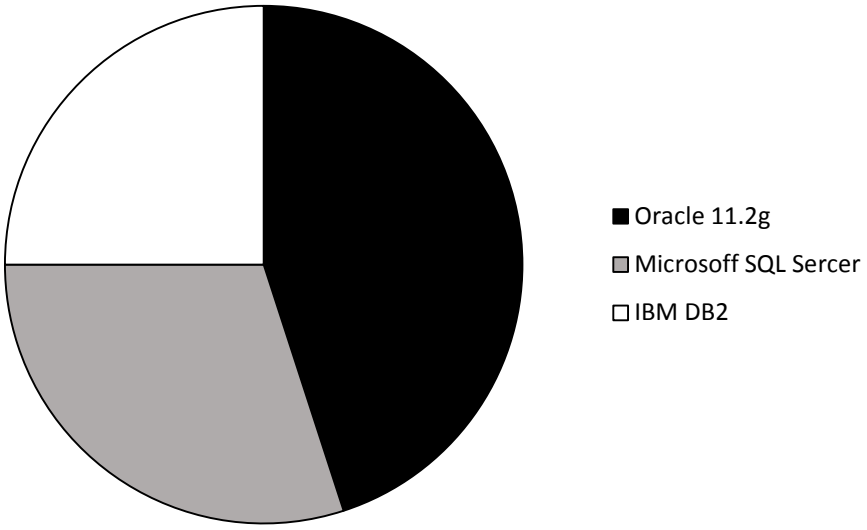

Рис.1.1. Распределение выручки за продажу СУБД в рамках «большой тройки»

В рамках «большой тройки» выручка распределяется в соотношении 45% (Oracle), 35% (Microsoft SQL Server) 20% (IBM DB2) и . Причем по количеству продаж больше всего продана СУБД Microsoft SQL Server, но в следствии значительной разницы в стоимости в денежном выражении лидирует Oracle [8].

1.2. Стандарты безопасности

Специалистам а области информационной безопасности сегодня невозможно обойтись без знаний соответствующих стандартов и спецификаций. Причины этого заключаются в следующем.

1. Формально необходимость следовать стандартам безопасности закрепляется законодательством.
2. Стандарты являются средством совместимости программно-аппаратных систем.

3. Стандарты и спецификации – это одна из форм накопления знаний и апробированных решений.

На самом верхнем уровне можно выделить три группы стандартов:

- оценочные, предназначенные для оценки и классификации информационных систем и средств защиты по требованиям безопасности;
- спецификации, регламентирующие различные аспекты реализации и использования средств и методов защиты;
- мониторинга и аудита, описывающих требования и механизмы систем слежения за работой информационных систем.

Из числа оценочных , следует выделить следующие стандарты.

Критерии оценки доверенных компьютерных систем

Стандарт является первым, получившим международное признание стандартом безопасности в области информационных технологий. Его оригинальное название «Department of Defense Trusted Computer System Evaluation Criteria» или аббревиатура TCSEC, но более он известен под названием (по цвету обложки) «Оранжевая книга». Первая версия стандарта была разработана Министерством обороны США. Без преувеличения можно сказать, что этот стандарт сформулировал понятийный базис информационной безопасности. В нем определены понятия: безопасная и доверенная системы, политика безопасности, уровень гарантированности, подотчетность, доверенная вычислительная база, монитор обращений, ядро и периметр безопасности.

В TCSEC предложены три категории требований безопасности: политика безопасности, аудит и гарантии.

Политика безопасности формулирует требования к возможности доступа субъектов системы к объектам, их идентификации, правилам управления доступом, меткам безопасности, процедура контроля доступа и пр.

Аудит формулирует требования к системе, которые позволяют определить степень ответственности пользователей в системе. Это достигается путем регистрации всех событий в системе в защищенном протоколе (доступ к этой информации имеет только администратор системы).

Гарантии формулируют требование к контролю средств защиты.

Стандарт предусматривает четыре группы критериев, которые соответствуют различным уровням защищенности: D, C, B. A (перечислены в порядке возрастания требований).

Уровень D (минимальная защита). Характеризует минимальную защиту системы. Уровень предназначен для систем, которые были представлены на оценку, но по какой-либо причине ее не прошли.

Уровень С (дискреционная защита). Характеризуется наличием дискреционного управления доступом и аудитом действий субъектов. Уровень включает два класса: С1 и С2.

Класс С1 описывает требования к системам построенным на основе дискреционного разграничения доступа. Системы, соответствующих этому классу защиты, удовлетворяет минимальным требованиям безопасного разделения пользователей и данных. Определяются некоторые формы разграничения доступа на индивидуальной основе, т.е. пользователь имеет возможность защитить свою информацию от ее случайного чтения или уничтожения. Пользователи могут обрабатывать данные, как по отдельности, так и от имени группы пользователей. Система безопасности этого класса должна определять и управлять доступом между поименованными объектами и субъектами (пользователями или их группами) в компьютерной системе (например, при помощи матрицы доступа). Механизм защиты должен позволять пользователям определять и контролировать распределение доступа к объектам по поименованным пользователям и /или их группам. Пользователи должны идентифицировать себя в системе безопасности в случае выполнения ими любых действий, ею контролируемых, при этом должен быть использован хотя бы один из механизмов аутентификации (например, пароль). Данные аутентификации должны быть защищены от доступа неавторизованного пользователя. Система безопасности обеспечивает собственную работу и защиту от внешнего воздействия. Контролируемые системой безопасности ресурсы, являются частью всех ресурсов. Система безопасности должна иметь средства для периодической проверки правильности своей работы. Тестирование системы безопасности должно выполняться согласно документации для обеспечения гарантии того, что нет явных путей обхода системы защиты неавторизованным пользователем или иного расстройства системы защиты.

Документация системы безопасности должна включать:

- описание реализованных в ТСВ механизмов защиты, их взаимодействия и руководство пользователя по их использованию;
- руководство для администратора системы на гарантирование системы защиты;
- документацию по тестам, включающую описание того, как механизмы безопасности должны тестироваться и как интерпретировать резуль-таты тестов;
- документацию по проекту, описывающую философию системы защиты и того, как эта философия реализована в ТСВ (если ТСВ состоит из нескольких модулей, то должен быть описан интерфейс между ними).

Класс С1 рассчитан на многопользовательские системы, в которых осуществляется совместная обработка данных одного уровня конфиден-циальности.

Класс С2 описывает системы, построенные на основе управляемого дискреционного разграничения доступа. Системы, сертифицированные по данному классу, должны удовлетворять всем требованиям, изложенным в классе С1. Однако, системы класса С2 поддерживают более тонкую, чем в классе С1, политику дискреционного разграничения доступа, делающую пользователя индивидуально ответственным за свои действия после процедуры аутентификации в системе, а также аудит событий, связанных с безопасностью системы.

Уровень В (мандатное управление доступом). Основные требования этой уровня – полномочное (мандатное) управление доступом с использованием меток безопасности, реализация некоторой формальной модели политики безопасности, а также наличие спецификаций на функции системы безопасности. Уровень включает три класса: В1, В2 и В3. В системах этого уровня постепенно к классу В3 должен быть реализован монитор ссылок, который должен контролировать все доступы субъектов к объектам системы.

Класс В1 должен удовлетворять всем требованиям класса С2 и некоторым дополнительным требования из В2:

- все субъекты и объекты должны иметь метку системы безопасности;
- аудиту подлежат любые изменения меток секретности;
- система безопасности должна обеспечивать изоляцию процессов системы, через выделение им соответствующего адресного пространства.

Документация В1 должна дополнительно включать описание функций, относящихся к безопасности самой системы безопасности, а также описание путей и методов наилучшего ис-пользования защитных свойств системы; описания выполняемых процедур, предупреждений и привилегий, необходимых для контроля за безопасной работой системы.

Класс В2 (структурированная защита) требует выполнения всех требования класса защиты В1. Кроме того, в системах класса В2 система безопасности основывается на четко определенной и хорошо документированной формальной модели политики безопасности, требующей, чтобы мандатная и дискреционная системы разграничения доступа были распространены на все субъекты и объекты компьютерной системы. Система должна быть четко структурирована на элементы, критичные с точки зрения безопасности и некритичные. Интерфейс системы безопасности должен быть хорошо определен и ее проект и конечный результат должны быть

подвергнуты полной проверке и тестированию. Механизм аудита должен быть усилен, введен контроль за конфигурацией системы. Система должна быть устойчива к внешнему проникновению.

Системы класса B3 (домены безопасности) должны удовлетворять всем требованиям предыдущего класса и удовлетворять дополнительным требованиям к требованиям монитору ссылок, который должен быть:

- защищен от несанкционированного изменения или порчи;
- способен обрабатывать все обращения;
- прост для анализа и тестирования.

Система безопасности класса B3 должна быть структурирована таким образом, чтобы исключить код, не имеющий отношения к безопасности компоненты. Кроме того, должна быть обеспечена поддержка администратора безопасности, расширен механизм аудита с целью сигнализации о любых событиях, связанных с безопасностью, а также поддерживались процедуры восстановления системы.

Уровень A (верифицированная защита). Данная группа характеризуется применением формальных методов верификации корректности работы механизмов управления доступом (дискреционного и мандатного). Требуется, чтобы было формально показано соответствие архитектуры и реализации системы безопасности требованиям. Уровень содержит только один класс A1.

Критерий защиты класса A1 не определяет дополнительные по сравнению с классом B3 требования к архитектуре или политике безопасности компьютерной системы. Дополнительным свойством систем, отнесенных к классу A1, является проведенный анализ системы на соответствие формальным высокоуровневым спецификациям и использование технологий проверки с целью получения высоких гарантий того, что система безопасности функционирует корректно.

Общие критерии

В 1990 году рабочая группа 3 подкомитета 27 Первого совместного комитета (JTC1/SC27/WG3) Международной организации по стандартизации (ISO) приступила к разработке «Критериев оценки безопасности информационных технологий» (Evaluation Criteria of IT Security, ECITS). Несколько позже, в 1993 г., правительственные организации шести стран (Канады, США, Великобритании, Германии, Нидерландов и Франции) занялись составлением так называемых «Общих критериев оценки безопасности информационных технологий» (Common Criteria of IT Security

Evaluation). За этим документом исторически закрепилось более короткое название «Общие критерии» [2].

С 1996 году появилась совместная с Международной организации по стандартизации версия 1.0 «Общих критериев». Соответствующий международный стандарт ISO/IEC введен в действие с 1.12.1999.

Для структуризации пространства требований в «Общих критериях» введена иерархия класс-семейство-компонент-элемент.

Классы определяют наиболее общую (как правило, предметную) группировку требований. Семейства в пределах класса различаются по строгости и другим характеристикам требований. Компонент – минимальный набор требований, фигурирующий как целое. Элемент – неделимое требование. Между компонентами могут возникать зависимости в том случае, если сам по себе компонент не является достаточным для достижения цели безопасности. Соответственно при включении такого компонента надо добавить все связанные с ним компоненты.

«Общие критерии» содержат два вида требований безопасности:

- функциональные, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности и реализующим их механизм;
- требования доверия, которые соответствуют пассивному аспекту, предъявляются к технологии и процессу разработки и эксплуатации стандарта.

К спецификациям относятся следующие стандарты.

Рекомендации семейства X.500

X.500 – это серия стандартов Международного союза электросвязи (International Telecommunication Union, ITU) для службы распределенного каталога сети (службы директорий).

Среди возможностей этой службы, обычно выделяют дружественное именование (обращение к объектам сети по именам) и отображение этих имен в адреса.

Основные понятия службы директорий зафиксированы в рекомендациях X.501 «Служба директорий: модели» и X.511 «Службы директорий: абстрактное определение сервиса»

Информация, доступ к которой посредством службы директорий называется информационной базой директории. Информационная база имеет древовидную структуру. Природа объектов, которая хранится в базе данных, произвольна. Единственное требование состоит в идентифицируемости этих

объектов. Назначение информационной базы – хранение информации о распределенной вычислительной структуре.

В документе X.509 описывается форматы данных и процедуры распределения открытых ключей с помощью сертификатов с цифровыми подписями, которые предоставляются сертификационными органами.

Всего в семейство X.500 включено 10 документов, описывающие различные аспекты службы директорий [2], [9].

Специкая IPSec

IPSec (сокращение от IP Security) – набор протоколов для обеспечения защиты данных, передаваемые по межсетевому протоколу IP. Позволяет осуществлять подтверждение подлинности (аутентификацию) и/или шифрование IP-пакетов. Кроме того, IPSec включает в себя протоколы для защищенного обмена ключами в сети Интернет. В основном применяется для организации виртуальной частной сети [2], [10].

Специкая TLS

TLS (Transport Layer Security) – криптографический протокол, обеспечивающий защищенную передачу данных между узлами сети Интернет. TSL использует ассиметричную криптографию для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности для сохранения целостности сообщений [2], [11].

Общий стандарт оценки уязвимости

Общая система учета уязвимостей (CVSS, Common Vulnerability Scoring System) является открытой платформой для сравнения характеристик и расчета воздействия уязвимостей в информационных системах. CVSS состоит из трех групп: базовой, временной и инфраструктурной. Базовая составляющая отражает общие особенности уязвимости. Результат от временной группы отражает характеристики уязвимости, которые менялись с течением времени. Инфраструктурная составляющая увязывает характеристики уязвимости с уникальной для каждого клиента инфраструктурой, в которой уязвимость найдена.

CVSS дает возможность менеджерам информационных систем, компаниям, ведущим учет уязвимостей, производителям средств информационной защиты, разработчикам программного обеспечения и

исследователям говорить на одном языке, используя общий подход к оцениванию уязвимостей информационных систем.

Каждой уязвимости соответствует CVE-код. CVE – сокращенное название стандарта Common Vulnerabilities and Exposure (общие уязвимости и проблемы), предназначенного для идентификации уязвимостей. CVE определяет справочник имен.

Наиболее известные базы данных зарегистрированных уязвимостей представлены на сайтах [12], [13].

Если говорить о стандартах безопасности, относящихся непосредственно к СУБД, то можно выделить стандарты мониторинга и аудита, перечисленные в таблице 1.1.

Таблица 1.1. Основные стандарты безопасности СУБД

Мониторинг безопасности	COBIT (SOX)	PCI-DSS	ISO 27002	DP&PL	NIST SP 800-53 (FISMA)
Доступ к секретным данным (все запросы SELECT)		+	+	+	+
Изменение схемы (DDL: CREATE, DROP, ALTER)	+	+	+	+	+
Изменение данных (DML: INSERT, DELETE, UPDATE)	+		+		
Инциденты безопасности (ошибки набора пароля, ошибки SQL и пр.)	+	+	+	+	+
Учетные записи, роли, привилегии (DCL: GRANT, REVOKE)	+	+	+	+	+

Строки табл. 1.1 соответствуют событиям базы данных, столбцы – стандартам безопасности. Если на пересечении столбца (стандарта) и строки (события в базе данных) стоит знак +, то это означает, что данный стандарт регулирует процесс мониторинга и/или аудита данного события.

Кратко охарактеризуем стандарты, перечисленные в табл.1.1.

Стандарт **COBIT (Control Objectives Information and Related Technologies)** представляет собой пакет, состоящий и около сорока открытых международных стандартов в области управления и информационными технологиями, аудита и информационной безопасности [14].

PCI-DSS – стандарт безопасности данных, применяемый в индустрии платежных карт. Разработан Советом по безопасности индустрии платежных карт, учрежденным международными платежными системами Visa, MasterCard, American Express, JCB и Discover . Стандарт представляет собой 12 детализованных требований по обеспечению безопасности данных о держателях платежных карт, которые передаются, хранятся и обрабатываются в информационных инфраструктурах организаций [15].

ISO/IEC 27002 – стандарт информационной безопасности. Стандарт озаглавлен «Информационные технологии – Технологии безопасности – Практические правила менеджмента информационной безопасности». Стандарт разработан на базе Британского стандарта BS 7799-1:1999 [16].

NIST SP 800-53 – стандарт Национального института стандартов и технологий США. Стандарт содержит описание контроля безопасности приватных данных для федеральных систем и организаций [17].

DP&PL (Data privacy and protection law) – государственные законы «О персональных» данных. В разных странах этот закон может иметь разные наименования, в некоторых случаях это может быть несколько законов. Например, в Российской Федерации это закон «О персональных данных» № 152-ФЗ от 27.06.2006 , или в Беларуси закон «Об информации, информатизации и защите информации» [18].

1.3. Обзор возможностей СУБД Oracle 11.2.g

СУБД Oracle 11.2.g – система управления объектно-реляционной базой данных американской корпорации Oracle [3]. Первая версия СУБД Oracle была выпущена в 1982 году (под именем Oracle Systems). Рассматриваемая в работе версия 11.2.g стала доступной с 2010 года. СУБД работает на всех основных серверных платформах: Linux, Unix, AIX, z/OS, Mac OS и пр.

СУБД Oracle имеет архитектуру клиент-сервер. Другими словами, программное обеспечение СУБД условно разбито на две части: клиент и сервер. Клиентское программное обеспечение предназначено для формирования и оправки запроса серверу, а также для обработки ответа. Сервер СУБД прослушивает TCP-порт (по умолчанию 1521), принимает и обрабатывает клиентские запросы, формирует и оправляет ответ клиенту. Один экземпляр сервера обеспечивает работу одной базы данных.

База данных Oracle представляет собой совокупность данных, размещенных в одном или нескольких файлах операционной системы.

Главной структурой базы данных Oracle 11.2.g является таблицы. СУБД Oracle 11.2.g поддерживает таблицы нескольких типов:

- реляционные таблицы: используют внутренние типы данных Oracle; применяются для хранения строк, которыми с помощью языка DML может манипулировать приложение;
- объектно-реляционные таблицы: таблица содержащие столбцы, тип данных которых создан пользователем;
- индексно-ориентированные таблицы: таблицы, хранящиеся в индексной структуре (поддерживающей логический порядок строк в таблице);
- внешние таблицы: данные хранящиеся в плоских файлах операционной системы, представляемые в базе данных в виде таблицы, допускающую операцию чтения;
- временные таблицы: таблицы, которые могут быть использоваться несколькими пользователями в рамках одного соединения, при этом каждому пользователю доступны только собственные данные;
- секционированные таблицы: таблицы, строки которых разбиты на секции, которые могут быть физически размещены на разных носителях;
- табличные кластеры: структура, позволяющая хранить общие столбцы нескольких реляционных таблиц.

Для ускорения извлечения данных из таблиц применяются индексы. СУБД Oracle 11.2g поддерживает индексы следующих типов:

- древовидные индексы: стандартный индекс базы данных Oracle типа B*-tree;
- битовые индексы (Bitmap-индексы): индексы повышающие производительность выборки по значениям столбца, в котором мало различных значений;
- секционированные индексы: индексы секционированных таблиц;
- функциональные индексы: индексы, значения которых вычисляются на основе детерминистической функции.

Запросы, формируемые клиентом для отправки серверу, содержат выражения, записанные на Oracle-диалекте языка SQL.

Oracle 11.2g поддерживает представления – поименованные и хранящиеся в базе данных SELECT-запросы, а также материализованные представления – поименованные результаты выполнения SELECT-запросов.

Для разработки программных серверных объектов (процедуры, функции, пакеты, типы, триггеры) предназначена специальная встроенная система программирования PL/SQL.

В состав программного обеспечения входит достаточно много различных утилит: настройки компонент СУБД, резервного копирования, экспорта и импорта, загрузки, командора, средств разработки и пр.

Для доступа к ресурсам базы данных приложение может использовать стандартные программные интерфейсы: JDBC, ODBC, OLE DB, ODAC и пр.

1.4. Обзор возможностей СУБД Microsoft SQL Server 2008

СУБД Microsoft SQL Server 2008 – система управления объектно-реляционной базой данных американской корпорации Microsoft [4]. Первая версия СУБД Microsoft SQL Server была выпущена в 1988 году (версия 1.0). Рассматриваемая в работе версия 2008 стала доступной с 2008 года. СУБД работает только в среде операционной системы Windows и . NET Framework 3.5.

СУБД Microsoft SQL Server 2008 имеет архитектуру клиент-сервер.. Сервер СУБД прослушивает TCP-порт (по умолчанию 1433), принимает и обрабатывает клиентские запросы, формирует и оправляет ответ клиенту. Один экземпляр сервера обеспечивает работу нескольких баз данных. Для управления сервером применяются пять специальных системных баз данных.

База данных Microsoft SQL Server 2008 представляет собой совокупность данных, размещенных в одном или нескольких файлах операционной системы.

Главной структурой базы данных SQL Server 2008 является таблицы. SQL Server 2008 поддерживает таблицы нескольких типов:

- реляционные таблицы: используют внутренние типы данных SQL Server 2008 ; применяются для хранения строк, которыми с помощью языка DML может манипулировать приложение;
- объектно-реляционные таблицы: таблица содержащие столбцы, тип данных которых создан пользователем с помощью языка C#;
- кластерные таблицы: таблицы, хранящиеся в индексной структуре (поддерживающей логический порядок строк в таблице);
- временные таблицы: таблицы, которые могут быть использоваться несколькими пользователями (глобальные временные таблицы) или только одним пользователем (локальные временные таблицы) в рамках одного соединения;
- секционированные таблицы: таблицы, строки которых разбиты на секции, которые могут быть физически размещены на разных носителях;

Для ускорения извлечения данных из таблиц применяются индексы. СУБД SQL Server 2008 поддерживает индексы следующих типов:

- древовидные индексы: стандартный индекс базы данных Oracle типа B*-tree;
- секционированные индексы: индексы секционированных таблиц;
- индексы покрытия: индексы, позволяющие включать неиндексируемые столбцы реляционной таблицы.

Запросы, формируемые клиентом для отправки серверу, содержат выражения, записанные на Microsoft-диалекте языка SQL.

SQL Server 2008 поддерживает представления – поименованные и хранящиеся в базе данных SELECT-запросы, а также кластеризованные представления – поименованные результаты выполнения SELECT-запросов.

Для разработки программных серверных объектов (процедуры, функции, пакеты, типы, триггеры) предназначена специальная встроенная система программирования Transact-SQL и язык C#.

В состав программного обеспечения входит достаточно много различных утилит: настройки компонент СУБД, резервного копирования, экспорта и импорта, загрузки, средств разработки.

Для доступа к ресурсам базы данных приложение может использовать стандартные программные интерфейсы: JDBC, ODBC, OLE DB, ADO.NET и пр.

1.5. Заключение

1. На сегодняшний момент 70% рынка СУБД (в денежном выражении) прочно удерживает «большая тройка»: корпорации Oracle (СУБД Oracle), IBM (DB2) и Microsoft (SQL Server). Причем внутри «большой тройки» в денежном выражении лидирует СУБД Oracle, а по количеству проданных копий Microsoft SQL Server.
2. Система безопасности СУБД не является самодостаточной. СУБД использует механизмы и функции операционной системы. Поэтому к некоторым компонентам СУБД можно получить доступ с помощью средств операционной системы. Таким образом, уровень безопасности СУБД зависит от уровня безопасности (не может его превышать) операционной системы.
3. Сервер СУБД Oracle может работать на нескольких операционных платформах (Linux, Unix, Windows, AIX, z/OS), Microsoft SQL Server только на Windows.

4. Для оценки уровня системы безопасности СУБД используется оценочный стандарт TCSEC. В соответствии классификацией TCSEC уровень защиты всех СУБД «большой тройки» относится к группе C2.
5. Уровень TCSEC-оценки является достаточно грубым и не учитывает внутренних механизмов систем безопасности СУБД.
6. Для более детального сравнительного анализа СУБД, необходимо осуществить анализ на уровне объектов сервера СУБД и базы данных.

2. ОБЪЕКТЫ ИНФОМАЦИОННОЙ БЕЗОПАСНОСТИ СУБД

2.1. Архитектура безопасности СУБД

Современные СУБД имеют архитектуру клиент-сервер (рис. 2.1), подразумевающую наличие как минимум двух компонент: клиента и сервера.

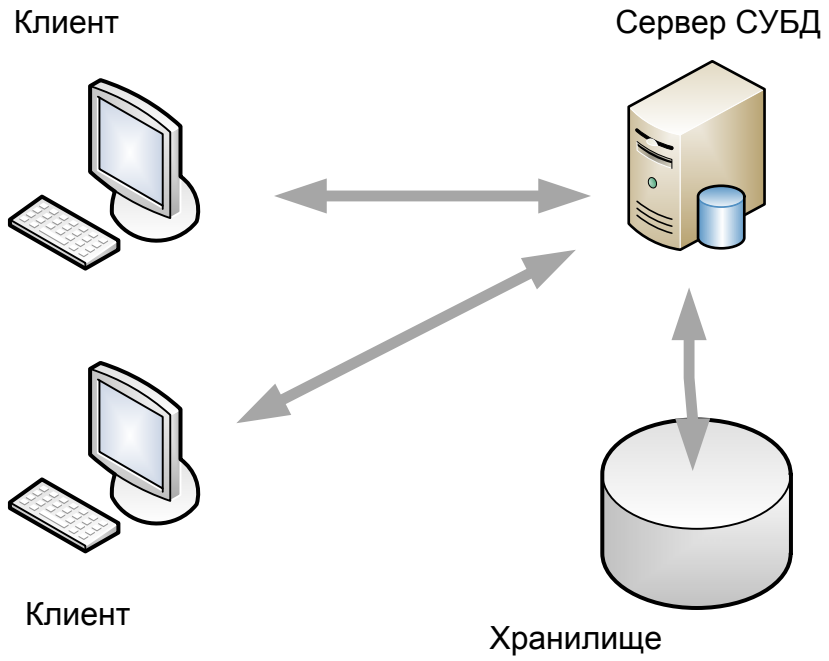

Рис. 2.1. Архитектура клиент-сервер современных СУБД

В соответствии с клиент-серверной архитектурой программное обеспечение СУБД тоже включает две составляющие: клиентское и серверной программное обеспечение.

Клиентское программное обеспечение предназначено для подключения к серверу, формирования и отправки запросов на языке SQL, а также приема и обработки ответа сервера.

Серверное программное обеспечение предназначено для выполнения аутентификации и авторизации клиентского подключения, обработки и выполнения SQL-запросов клиента, формирования и оправки клиенту ответа.

Обмен сообщениями между клиентом и сервером осуществляется в соответствии с сетевым протоколом СУБД прикладного уровня. Протокол СУБД работает над сетевым стеком протоколов TCP/IP и/или стандартными IPC-протоколами.

Клиентское программное обеспечение для доступа к серверу применяет стандартные программные интерфейсы, такие как ODBC, JDBC, OLEDB, ADO.NET и пр.

Схемы, отражающие архитектуру системы безопасности Microsoft SQL Server 2008 и Oracle 11.2g, представлены на рис. 2.2 и 2.3. При дальнейшем описании схем используется термин «привилегия», отражающий возможность выполнить те или иные операции с объектами сервера (в этом случае говорится о серверной привилегии) или с объектами базы данных (в этом случае говорится о привилегиях уровня базы данных). Для системы Oracle в русскоязычной литературе это термин используется (он является прямым переводом английского слова Privilege, принятого в оригинальной документации). Для Microsoft SQL Server в оригинальной документации применяется термин «Permission», который в русскоязычной литературе чаще всего переводят как «разрешение».

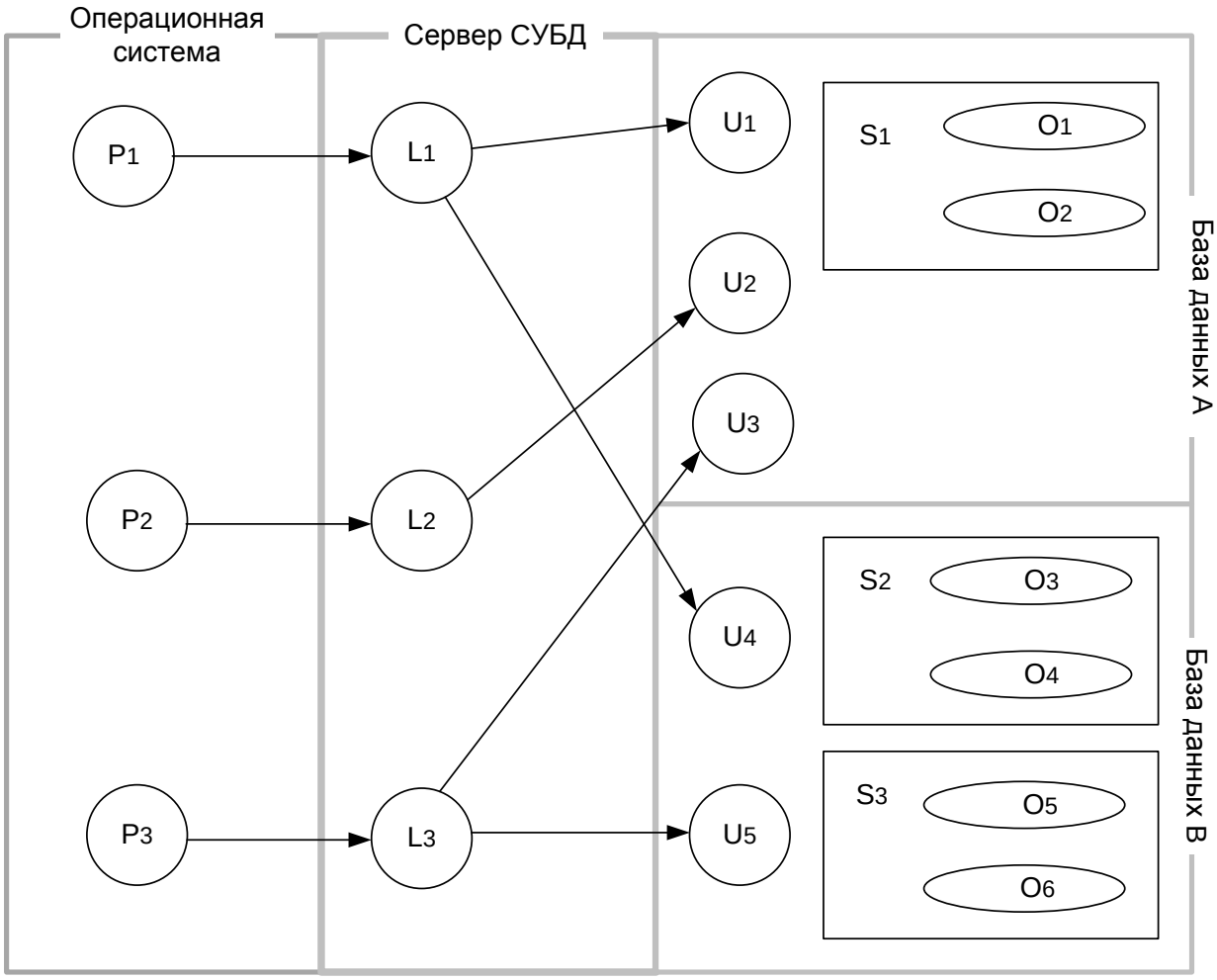

Рис. 2.2. Архитектура безопасности СУБД Microsoft SQL Server 2008

Архитектура СУБД Microsoft SQL Server 2008 безопасности имеет явную трехзвенную структуру: операционная система, сервер СУБД, база данных. Один сервер обеспечивает работу нескольких баз данных. Все базы данных

делятся на два типа: системные и пользовательские. Системные базы (master, msdb, tempdb, model, resource) данных необходимы для работы сервера СУБД.

Подключение к серверу СУБД Microsoft SQL Server 2008 осуществляет пользователь операционной системы (на рис. 2.2 обозначены как P_1, P_2, P_3). В рамках сервера Microsoft SQL Server 2008 пользователя операционной системы представляет серверный объект LOGIN (на рис. 2.2 обозначены как L_1, L_2, L_3). Объекту LOGIN могут назначаться серверные привилегии, определяющие его возможности на уровне сервера.

В каждой базе данных LOGIN представляет объект базы данных USER (на рис. 2.2 обозначены как U_1, U_2, U_3). Объекту USER могут быть назначены привилегии уровня базы данных.

Следует отметить, что установка соединения клиента с сервером в Microsoft SQL Server возможна двумя способами.

В первом случае, Windows-пользователь интегрирован с серверным объектом LOGIN и поэтому пользователю операционной системы не требуется проходить дополнительную процедуру аутентификации на сервере СУБД. Такой способ соединения с сервером называется Windows-аутентификацией.

Во втором случае, пользователь операционной системы при соединении с сервером вводит пароль и имя, т. е. проходит процедуру аутентификации. Такой способ соединения называется смешанной (в оригинале mixed) аутентификацией, подразумевая, что пользователь проходит эту процедуру дважды – сначала при входе в Windows, затем при подключении к серверу СУБД.

От имени объекта USER, при наличии у него соответствующих привилегий могут, выполняться операции с объектами базы данных (на рис. 2.2 обозначены как O_1, O_2, O_3, O_4, O_5, O_6).

Объекты базы данных могут быть объединены в рамках схем базы данных (на рис. 2.2 обозначены как S_1, S_2, S_3), которые представляют собой поименованные контейнеры объектов. Любой объект базы данных (таблица, представление, процедура, функция и пр.) может являться элементом только одной схемы.

Архитектура безопасности Oracle 11.2g несколько иная и не имеет явную трехзвенную структуру как в Microsoft SQL Server 2008.

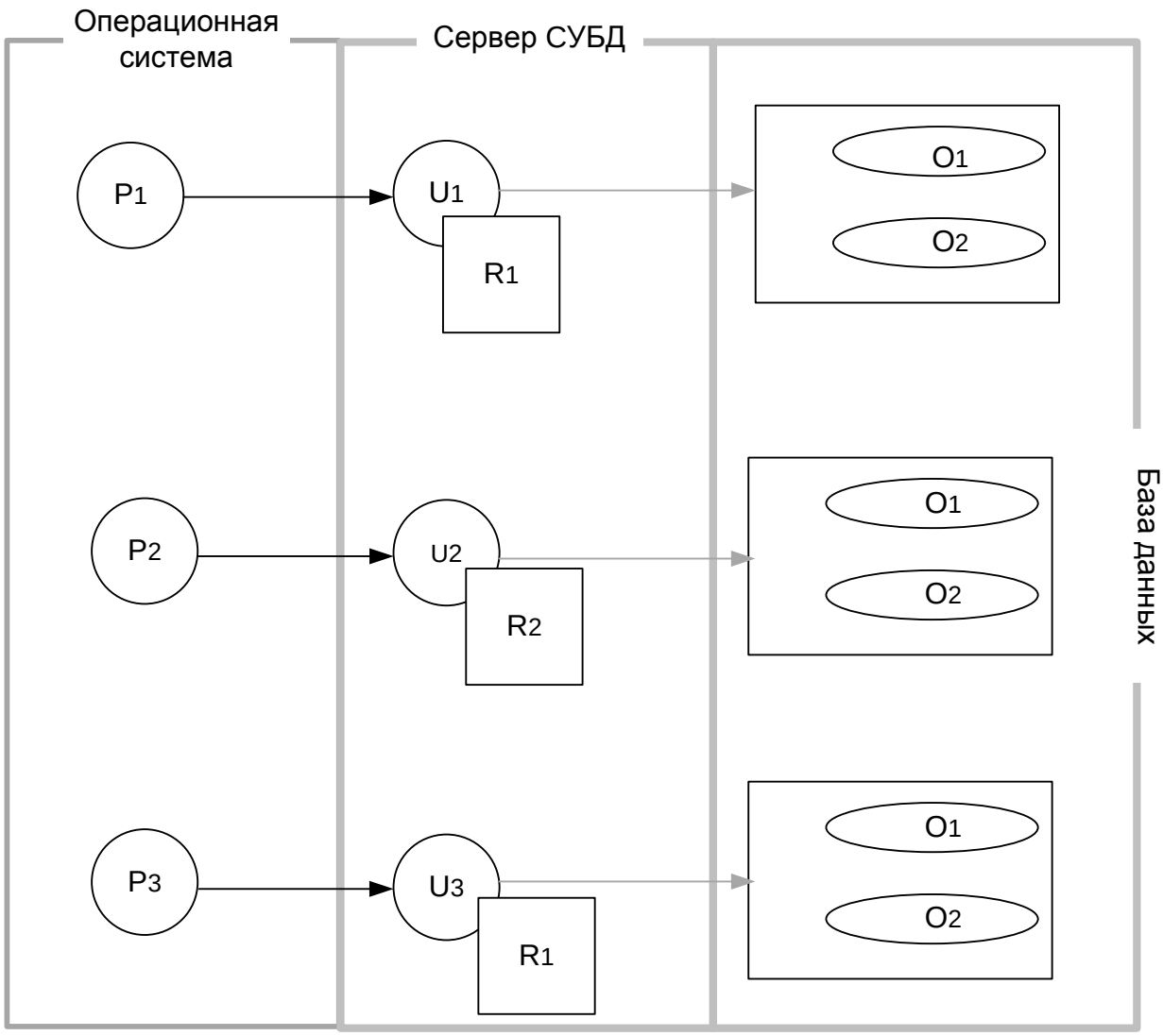

Рис. 2.3. Архитектура безопасности СУБД Oracle 11.2g

Подключение к серверу СУБД Oracle 11.2g осуществляет пользователь операционной системы (на рис. 2.3 обозначены как P_1, P_2, P_3). Сервер обеспечивает работу только с одной базой данных.

В рамках сервера СУБД Oracle 11.2g пользователя операционной системы представляет объект USER (на рис. 2.3 обозначены как U_1, U_2, U_3). Ему могут быть назначены привилегии, как серверного уровня, так и уровня базы данных. Помимо привилегий, возможности объекта USER на уровне сервера определены специальным объектом PROFILE (на рис. 2.3 обозначены как R_1, R_2, R_3). Если с экземпляром USER не связана объект типа PROFILE, то возможности объекта типа USER на уровне сервера определены специальным PROFILE-объектом с именем DEFAULT.

Все операции с объектами базы данных выполняются от имени объекта USER. Множество объектов, созданных от имени экземпляра объекта USER,

представляют собой схему базы данных. Имя схемы базы данных Oracle 11.2g совпадает с именем пользователя-владельца схемы.

2.2. Соединение с сервером СУБД

Для соединение клиентского приложения с сервером СУБД, необходимо выполнить процедуру аутентификации, основная задача которой идентифицировать субъекта, подключающегося к серверу. В современных СУБД процедура аутентификации сводится к передаче при подключении серверу двух значений: имени и пароля. После проверки корректности этих значений все дальнейшие действия в рамках данного подключения с сервером будут выполняться от имени специального объекта безопасности.

В случае Microsoft SQL Server таким объектом является LOGIN. На рис. 2.4 представлен пример создания (SQL оператор CREATE) объекта LOGIN, который применяется для смешанной аутентификации клиента.

```
CREATE LOGIN smw                        -- имя
       WITH PASSWORD=N'smwpassword',    -- пароль
       DEFAULT_DATABASE=Magister,       -- база данных по умолчанию
       CHECK_POLICY=OFF                 -- политика безопасности на пароль
```

Рис. 2.4. Microsoft SQL Server 2008: создание объекта LOGIN для смешанной аутентификации

Значение, следующий сразу за ключевым словом LOGIN задает имя объекта LOGIN (оно должно совпадать с тем именем которое указывается в процедуре аутентификации). С помощью ключевого слова PASSWORD задается пароль. При этом параметр CHECK_POLICY указывает на применение к паролю политики безопасности операционной системы (длина пароля, его сложность и пр.).

На рис. 2.5 представлен пример создания объекта LOGIN, который применяется для Windows-аутентификации клиента (на это указывает фраза FROM WINDOWS). В качестве имени используется имя пользователя операционной системы, а пароль в этом случае не задается, т.к. он уже определен при создании Windows-пользователя.

```
CREATE LOGIN [WIN-FPSVQQ7K4B3\Administrator] FROM WINDOWS
       WITH DEFAULT_DATABASE=Magister
```

Рис. 2.5. Microsoft SQL Server 2008: создание объекта LOGIN для Windows- аутентификации

На уровне базы данных все операции выполняются от имени экземпляра объекта USER. Каждый экземпляр объекта USER связан с единственным объектом LOGIN. При создании объекта USER базы данных Microsoft SQL Server с помощью ключевого выражения FOR LOGIN указывается имя объекта LOGIN, который проецируется на USER [19].

```
USE [Magister]
GO
CREATE USER magister_smw          -- имя
       FOR LOGIN smw              -- LOGIN-имя
```

Рис. 2.6. Microsoft SQL Server 2008: создание объекта USER

В СУБД Oracle 11.2g все операции на уровне сервера и на уровне базы данных выполняются от имени объекта USER [20].

```
CREATE USER smw                     -- имя
       IDENTIFIED BY smwpassword;   -- пароль
```

Рис. 2.7. Oracle 11.2g: создание объекта USER

Большинство свойства соединения в СУБД Oracle 11.2g может быть установлено с помощью объекта PROFILE. На рис. 2.8 представлен пример его создания.

```
CREATE PROFILE pfsmw LIMIT    -- профиль
       PASSWORD_LIFE_TIME     180  -- кол. дней жизни пароля
       SESSIONS_PER_USER      3    -- макс. кол. сессий пользователя
       FAILED_LOGIN_ATTEMPTS  7    -- кол. ошибок при вводе пароля
       PASSWORD_LOCK_TIME     1    -- кол. дней блокировки
       CONNECT_TIME           180  -- макс. минут соединения
       IDLE_TIME              30   -- макс. минут простоя
```

Рис. 2.8. Oracle 11.2g: создание объекта PROFILE

Для того, чтобы связать экземпляр объекта USER с экземпляром объектом PROFILE необходимо выполнить следующий оператор (рис.2. 9).

```
ALTER USER smw PROFILE pfsmw;
```

Рис. 2.9. Oracle 11.2g: изменение свойств объекта USER

2.3. Серверные привилегии

Любые привилегии могут быть назначены с помощью оператора GRANT и отобраны с помощью оператора REVOKE. Microsoft SQL Server поддерживает еще один оператор – DENY, позволяющий запретить выданную привилегию.

Microsoft SQL Server 2008 поддерживает привилегии двух уровней: серверные привилегии и привилегии уровня базы данных. Управление привилегиями осуществляется с помощью DCL-операторов.

Привилегии уровня сервера назначаются экземпляру объекта LOGIN. В табл. 2.1 перечислены основные серверные привилегии [19].

Таблица 2.1. Основные серверные привилегии Microsoft SQL Server 2008

Привилегии (Permission)	Описание
CONTROL SERVER	Позволяет выполнять любые действия на уровне сервера
CONNECT	Позволяет установить соединение с сервером
ALTER SERVER STATE	Позволяет изменять состояние сервера
VIEW SERVER STATE	Позволяет просмотреть состояние сервера
CREATE ANY DATABASE	Позволяет создавать базу данных
ALTER ANY DATABASE	Позволяет изменять любую базу данных
VIEW ANY DATABASE	Позволяет просмотреть любую базу данных
VIEW ANY DEFENITION	Позволяет просмотреть определение любого объекта базы данных
BACKUP DATABASE	Позволяет выполнять резервное копирование базы данных
BACKUP LOG	Позволяет выполнять резервное копирование журнала транзакций базы данных
SHUTDOWN	Позволяет остановить сервер

Для назначения привилегии экземпляру объекта LOGIN используется DCL-оператор GRANT. На рис. 2.10 приведен пример, демонстрирующий назначение экземпляру LOGIN-объекта с именем smw привилегии CONTROL SERVER, разрешающей выполнять любые операции на уровне сервера.

```
GRANT CONTROL SERVER TO smw;
```

Рис. 2.10. Microsoft SQL Server 2008: назначение серверной привилегии

СУБД Oracle не выделяет явно привилегии уровня сервера. Это связано с архитектурой СУБД, которая не разделяет сервер и базу данных.

2.4. Привилегии уровня базы данных

На уровне базы данных привилегии, поддерживаемые Microsoft SQL Server 2008, условно можно разбить на две группы: системные и объектные привилегии. Оба типа привилегий назначаются экземпляру объекта USER с помощью DCL-оператора GRANT. В табл. 2.2 приведены примеры привилегий уровня базы данных [19].

Таблица 2.2. Примеры системных привилегии Microsoft SQL Server 2008 уровня базы данных

Привилегии (Permission)	Описание
CONNECT	Позволяет создавать соединение с базой данных
CONTROL	Позволяет выполнять все операции в рамках базы данных (административные права)
CREATE TABLE	Позволяет создавать, удалять и изменять таблицы
CREATE VIEW	Позволяет создавать, удалять и изменять представления
CREATE FUNCTION	Позволяет создавать, удалять и изменять функции
CREATE PROCEDURE	Позволяет создавать, удалять и изменять процедуры
VIEW DEFINITION	Позволяет просматривать исходный код процедур, функций, триггеров, представлений и других программных объектов

Системные привилегии, как правило, назначает пользователь (экземпляр объекта USER) обладающий административными правами. На рис. 2.11 представлен пример назначения системных привилегий пользователю базы данных с именем magister_smw.

```
GRANT CONNECT, CREATE TABLE, CREATE VIEW TO magister_smw;
```

Рис. 2.11. Microsoft SQL Server 2008: назначение системных привилегий уровня базы данных

В СУБД Oracle тоже применяются два вида привилегий: системные и объектные. Примеры нескольких системных привилегий представлены в табл. 2.3.

Таблица 2.3. Примеры системных привилегии Oracle 11.2g

Привилегии (Permission)	Описание
CREATE SESSION	Позволяет создавать соединение с базой данных
CREATE USER	Позволяет создавать пользователей базы данных
DROP USER	Позволяет удалять пользователей базы данных
CREATE PROFILE	Позволяет создавать профиль безопасности
DROP PROFILE	Позволяет удалять профиль безопасности
CREATE TABLE	Позволяет создавать, удалять и изменять таблицы
CREATE VIEW	Позволяет создавать, удалять и изменять представления
CREATE PROCEDURE	Позволяет создавать, удалять и изменять процедуры и функции
VIEW DEFINITION	Позволяет просматривать исходный код процедур, функций, триггеров, представлений и других программных объектов

На рис. 2.12 представлен пример назначения системных привилегий пользователю с именем smw.

```
GRANT CREATE SESSION, CREATE TABLE, CREATE VIEW to smw;
```

Рис. 2.12. Oracle 11.2.g: назначение системных привилегий

Объектные привилегии, как правило, назначает владелец объекта (экземпляр объекта USER, олицетворяющий субъекта-пользователя базы данных, создавшего объект) в пользу другого пользователя базы данных.

За небольшим исключением объектные привилегии, поддерживаемые СУБД Microsoft SQL Server 2008 и СУБД Oracle совпадают. Перечень основных объектных привилегий приведен в табл. 2.4 [19] [20].

Таблица 2.4. Примеры объектных привилегий

Привилегии (Permission)	Описание
SELECT	Позволяет выполнять DML-оператор SELECT
INSERT	Позволяет выполнять DML-оператор INSERT
DELETE	Позволяет выполнять DML-оператор DELETE
UPDATE	Позволяет выполнять DML-оператор UPDATE
EXECUTE	Позволяет вызвать функцию, процедуру или применять пользовательский тип
REFERENCE	Позволяет ссылаться на PRIMARY KEY при создании констрейнта FOREIGN KEY

Пример на рис. 2.13 демонстрирует назначение пользователю magister_smw уровня базы данных следующих привилегий:

- выполнение DML-оператора SELECT для таблицы dbo.Person;
- выполнение DML-оператора UPDATE для столбца Name таблицы dbo.Person;
- вызов скалярной функции dbo.Add2.

```
GRANT SELECT  on dbo.Person to magister_smw;
GRANT UPDATE  on dbo.Person(Name) to magister_smw;
GRANT EXECUTE on dbo.Add2   to magister_smw;
```

Рис. 2.13. Назначение объектных привилегий

2.5. Роли

Принципал – это объект сервера или базы данных, которому может быть назначена привилегия.

Роль – это принципал, представляющий собой поименованный набор привилегий. Роль может быть назначена другому принципалу, при этом весь набор привилегий роли распространяется на этот принципал. Одному пользователю может быть назначено несколько ролей. В этом случае он приобретает привилегии всех назначенных ему ролей.

СУБД Microsoft SQL Server 2008, поддерживает роли двух типов: фиксированные и пользовательские.

Фиксированные серверные роли Microsoft SQL Server 2008 – предопределенные роли с фиксированным набором привилегий. В табл. 2.5 представлен набор фиксированных ролей уровня сервера [19].

Таблица 2.5. Фиксированные серверные роли Microsoft SQL Server 2008

Роли	Описание
SYSADMIN	Выполнение любых операций
DBCREATER	Создание и изменение базы данных
DISKADMIN	Управление дисковым пространством
SERVERADMIN	Конфигурирование на уровне сервера
SECURITYADMIN	Управление и аудит объектов LOGIN
PROCESSADMIN	Управление серверными процессами
BUKLADMIN	Выполнение оператора BULK INSERT
SETUPADMIN	Конфигурировать репликацию и подключаемые серверы

Для назначение фиксированной серверной роли заданному экземпляру объекта LOGIN применяется системная процедура sp_addsrvrolemember (рис. 2.14).

```
EXEC master..sp_addsrvrolemember
              @loginame = N'smw',            -- LOGIN
              @rolename = N'securityadmin'   -- серверная роль
```

Рис. 2.14. Microsoft SQL Server 2008: назначение серверной роли

Следует отметить, что все фиксированные роли, кроме SYSADMIN, представляют собой просто совокупность привилегий, и создав пользовательские роли, всегда можно получить аналогичные. Иначе обстоит с SYSADMIN: помимо совокупности привилегий, эта роль предоставляет некоторые возможности, которые не могут быть заданы привилегиями.

На уровне базы данных СУБД Microsoft SQL Server 2008 обеспечивает свой набор фиксированных ролей (табл. 2.6) [19].

Таблица 2.6. Фиксированные роли уровня базы данных Microsoft SQL Server 2008

Роли	Описание
DB_OWNER	Выполнение любых операций в базе данных
DB_SECURITYADMIN	Изменение пользовательских ролей и управление привилегиями
DB_ACCESSADMIN	Запрет или разрешение доступа к данным для LOGIN
DB_BACKUPOPERATOR	Выполнение резервного копирования
DB_DDLADMIN	Выполнение любого DDL-оператора
DB_DATAWRITER	Добавление, удаление и изменение данных во всех пользовательских таблицах
DB_DATAREADER	Чтение данных во всех пользовательских таблицах
DB_DENYDATAWRITER	Запрет на добавления, удаления и изменения данных во всех пользовательских таблицах
DB_DENYDATAREADER	Запрет чтения данных во всех пользовательских таблицах

Для назначение фиксированной серверной роли уровня базы данных заданному экземпляру объекта USER применяется системная процедура sp_addrolemember (рис. 2.15).

```
EXEC sp_addrolemember
     N'db_owner',      -- фиксированая роль БД
     N'magister_smw'   -- USER
```

Рис. 2.15. Microsoft SQL Server 2008: назначение фиксированной роли уровня базы данных

На уровне базы данных допускается создавать пользовательские роли. На рис. 2.16 представлен пример оператора CREATE ROLE, создающего роль с именем rlsmw.

```
CREATE ROLE rlsmw   -- создание пользовательской роли БД
```

Рис. 2.16. Microsoft SQL Server 2008: создание пользовательской роли

Для того, чтобы связать созданную роль с привилегией необходимо их назначить роли. На рис. 2.17 представлен пример, в котором пользовательской роли с именем rlsmw назначаются две объектные привилегии позволяющие выполнять оператор SELECT для таблицы dbo.Person и выполнять скалярную функцию dbo.Add2.

```
GRANT SELECT  ON dbo.Person TO rlsmw
GRANT EXECUTE ON dbo.ADD2   TO rlsmw
```

Рис. 2.17. Microsoft SQL Server 2008: назначение привилегий пользовательской роли уровня базы данных

Если необходимо назначить пользовательскую роль экземпляру объекта USER, следует воспользоваться уже применяемой ранее (рис. 2.12) системной процедурой sp_addrolemember (рис. 2.18).

```
EXEC sp_addrolemember N'rlsmw',          --пользовательская роль БД
                      N'magister_smw'    -- экземляр объекта USER
```

Рис. 2.18. Microsoft SQL Server 2008: назначение роли пользователю базы данных

СУБД Oracle 11.2g поддерживает роли только уровня базы данных (уровень сервера в Oracle не выделяется). Фиксированных ролей нет, но есть роли предустановленные. Состав привилегий, входящих в предустановленные роли, может быть изменен. Из предустановленных роль, наиболее часто используется роль DBA, позволяющая назначить пользователю административные права [20]. На рис. 2.19 представлен пример, демонстрирующий назначение предустановленной роли DBA пользователю с именем smw.

```
GRANT DBA to smw;
```

Рис. 2.19. Oracle 11.2.g: назначение роли DBA пользователю smw

Пользовательская роль в СУБД Oracle 11.2g создается с помощью оператора CREATE ROLE (рис. 2.20).

```
CREATE ROLE rlsmw;
```

Рис. 2.20. Oracle 11.2.g: создание роли smw

Связать созданную роль с набором привилегий можно с помощью оператора GRANT. На рис. 2.21 представлен пример, демонстрирующий назначение привилегий роли rlsmw;

```
GRANT CREATE SESSION,          -- выполнить соединение
      CREATE TABLE,            -- создать таблицу
      CREATE VIEW,             -- создать предствление
      EXECUTE ANY PROCEDURE    -- вызвать любые процедуры и функции
      TO rlsmw;
```

Рис. 2.21. Oracle 11.2.g: создание роли с именем rlsmw

Назначить роль пользователю можно тоже с помощью DC оператора GRANT (рис. 2.22).

```
GRANT rlsmw to smw;
```

Рис. 2.22. Oracle 11.2.g: назначение роли rlsmw пользователю smw

2.6. Имперсонизация

Имперсонизация – механизм, позволяющий выполнить одному пользователю операции в базе данных от имени другого пользователя, обладающего, как правило, большим набором привилегий.

Рис. 2.20 поясняет механизм имперсонизации. На рисунке изображены два экземпляра объекта USER: A и B. Пусть пользователю A назначена привилегия, позволяющая ему выполнять операцию UPDATE над таблицей TABLE. Кроме того, пользователь A создал процедуру PROCEDURE, которая выполняет операцию UPDATE и назначил объектную привилегию EXECUTE (допускает выполнение процедуры) пользователю B. Пользователь B вызывая процедуру выполняет операцию UPDATE. Другими словами, пользователь B выполняет операцию UPDATE над таблицей TABLE, хотя напрямую он не

имеет соответствующую привилегию. Механизм имперсонизации позволяет пользователю получить доступ к объектам базы данных через программные объекты: процедуры, функции, (Oracle 11.2g) пакеты или (Microsoft SQL Server 2008) представления.

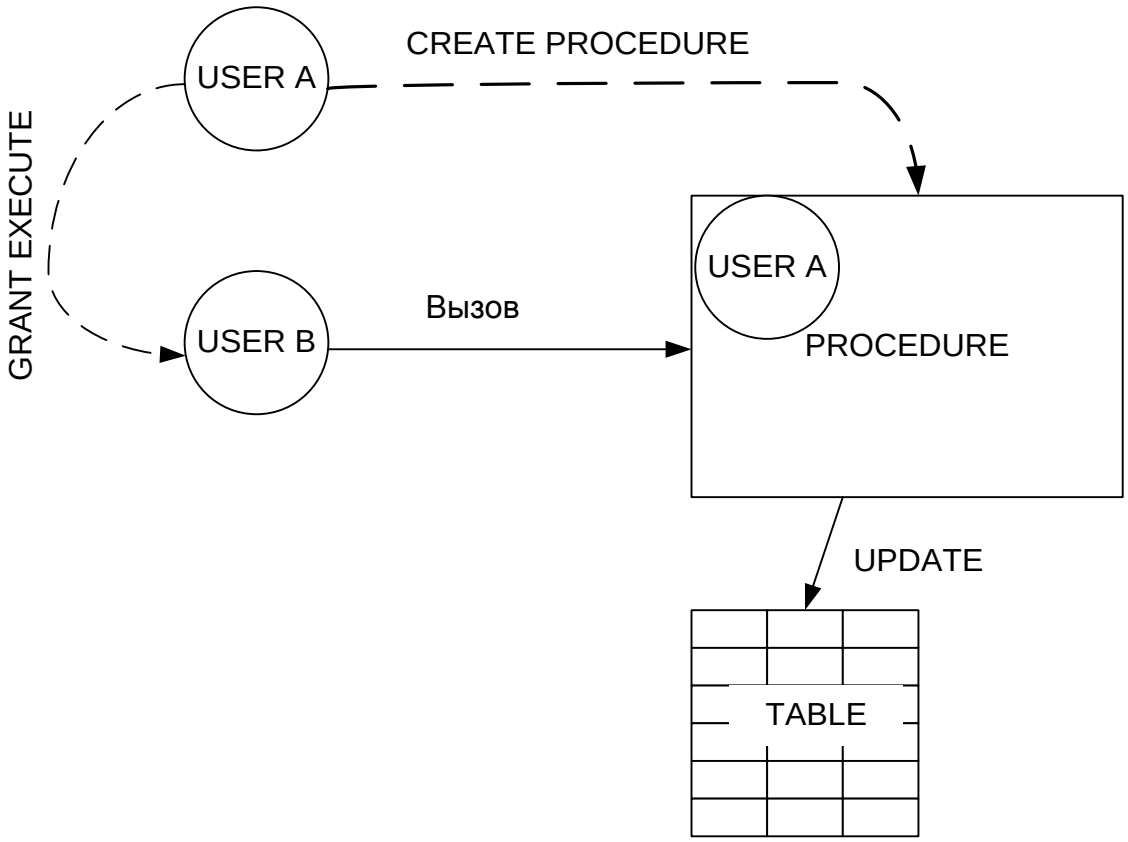

Рис. 2.23. Схема, поясняющая механизм имперсонизации

На рис. 2.24 представлен пример процедуры, которая будет работать от имени пользователя magister_smw (конструкция WITH EXECUTE AS).

```
CREATE PROCEDURE INSPERSON
@k int, @n VARCHAR
WITH EXECUTE AS 'magister_smw'
AS BEGIN
  INSERT INTO dbo.Person(id, name)VALUES(@k,@n);
END;
```

Рис. 2.24. Microsoft SQL Server 2008: процедура, выполняющая от имени пользователя magister_smw

На рис. 2.25 представлен пример, в котором пользователю назначается привилегию, позволяющую вызывать процедуру INPERSON.

```
GRANT EXECUTE ON DBO.INSPERSON TO magister_simpl;
```

Рис. 2.25. Microsoft SQL Server 2008: назначение привилегии EXECUTE

На рис. 2.26 представлен пример функции СУБД Oracle, которая будет работать от имени создателя (конструкция AUTHID DEFINER).

```
CREATE OR REPLACE FUNCTION INPERSON(pid INT, pn VARCHAR2) RETURN INT
       AUTHID DEFINER
       AS BEGIN
       INSERT INTO PERSON(ID, NAME) VALUES (pid, pn);
EXCEPTION
    WHEN OTHERS THEN RETURN 0;
END INPERSON;
```

Рис. 2.26. Oracle 11.2.g: процедура выполняющаяся от имени создателя

В обеих СУБД при создании представления (VIEW), автоматически осуществляется имперсонизация – в рамках представления действуют привилегии создателя представления.

2.7. Заключение

1. Один сервер Microsoft SQL Server 2008 может обслуживать несколько баз данных.
2. Система безопасности Microsoft SQL Server 2008 является двухуровневой: уровень сервера и уровень базы данных.
3. Привилегии Microsoft SQL Server 2008 разделены на две группы: серверные привилегии, привилегии уровня базы данных.
4. На уровне сервера Microsoft SQL Server 2008 для представления пользователя операционной системы используется специальный объект – LOGIN. Серверные привилегии назначаются экземпляру объекта LOGIN.
5. Система безопасности Microsoft SQL Server 2008 уровня может быть интегрирована с системой безопасности операционной системы Windows.
6. Экземпляр объекта LOGIN проецируется на экземпляры объектов USER.

7. На уровне базы данных пользователь представлен экземпляром объекта USER, которому назначаются привилегии уровня базы данных.
8. На уровне сервера Microsoft SQL Server 2008 поддерживает 2008 поддерживает только фиксированные серверные роли
9. На уровне базы данных Microsoft SQL Server поддерживает фиксированные, серверные и роли приложений.
10. На уровне базы данных Microsoft SQL Server поддерживает привилегии двух типов: системные и объектные. Системные привилегии назначает системный администратор, объектные – владелец объекта.
11. В рамках СУБД Microsoft SQL Server обеспечивается имперсонизация с помощью процедур, функций и представлений.
12. СУБД Microsoft SQL Server поддерживает независимые от пользователя схемы объектов базы данных.
13. В рамках одного сервера Oracle 11.2g может существовать только одна база данных.
14. Система безопасности Oracle 11.2g является одноуровневой: серверный уровень и уровень базы данных совмещен.
15. Все привилегии Oracle 11.2g находятся на уровне базы данных.
16. Система безопасности Oracle 11.2g является не зависит от программной платформы и не интегрируется с операционной системой.
17. В базе данных СУБД Oracle 11.2g пользователь представлен экземпляром объекта USER.
18. Все привилегии в СУБД Oracle 11.2g назначаются экземпляру объекта USER.
19. СУБД Oracle 11.2g поддерживает привилегии двух типов: системные и объектные. Системные привилегии назначает системный администратор, объектные – владелец объекта.
20. СУБД Oracle 11.2g поддерживает только пользовательские роли.
21. СУБД Oracle 11.2g предоставляет десять предопределенных ролей.
22. В СУБД Oracle 11.2g схема базы данных – множество объектов одного пользователя. Имя схемы совпадает с именем пользователя.
23. В рамках СУБД Oracle 11.2g обеспечивается имперсонизация с помощью процедур, функций, представлений и типов.

3. ОБОБЩЕННАЯ МОДЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СУБД

3.1. Структура модели

На рис. 3.1 представлена обобщенная модель информационной безопасности современной СУБД. Модель построена на основе анализа двух СУБД: Oracle 11g, IBM DB/2 и Microsoft SQL Server 2008. 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.

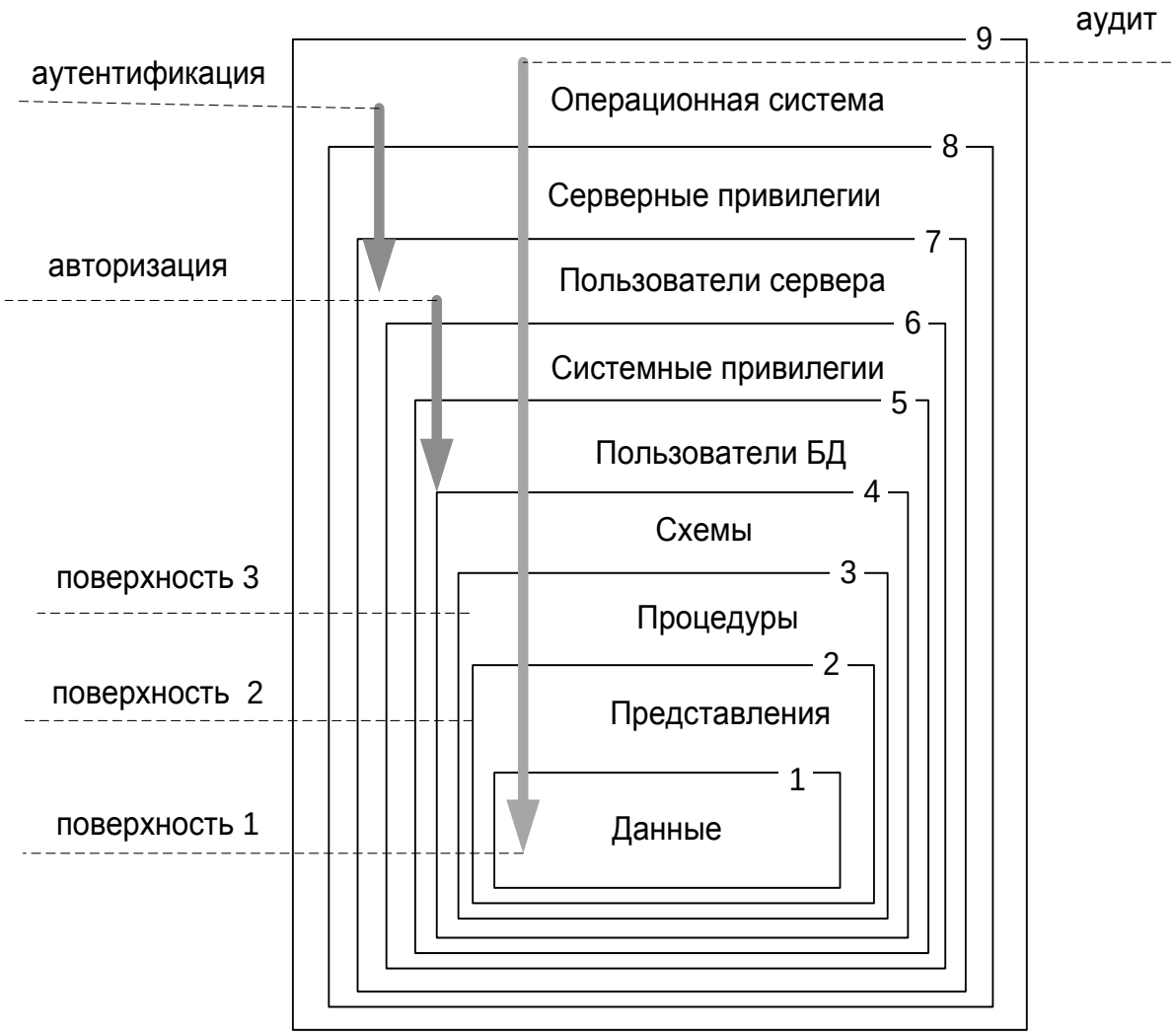

Рис. 3.1. Обобщенная модель информационной безопасности

Модель представляет собой девять взаимодействующих пронумерованных компонент. 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.

В дальнейшем говорится об уровнях модели. Каждый уровень соответствует компоненте с тем же номером. При этом уровень содержит собственные объекты соответствующей компоненты.

3.2. 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.

3.3. Уровень представлений

Собственными объектами этого уровня являются представления (view), являющиеся поименованными и хранящимися в базе данных SELECT-запросами. Некоторые СУБД поддерживают DML-операции INSERT, DELETE, UPDATE для простых приложений (например, Oracle 11.2g и Microsoft SQL Server).

С точки зрения информационной безопасности представления являются механизмом позволяющим создать промежуточный слой (рис. 3.2) между пользователем (пятый уровень) и таблицами данных (первый уровень).

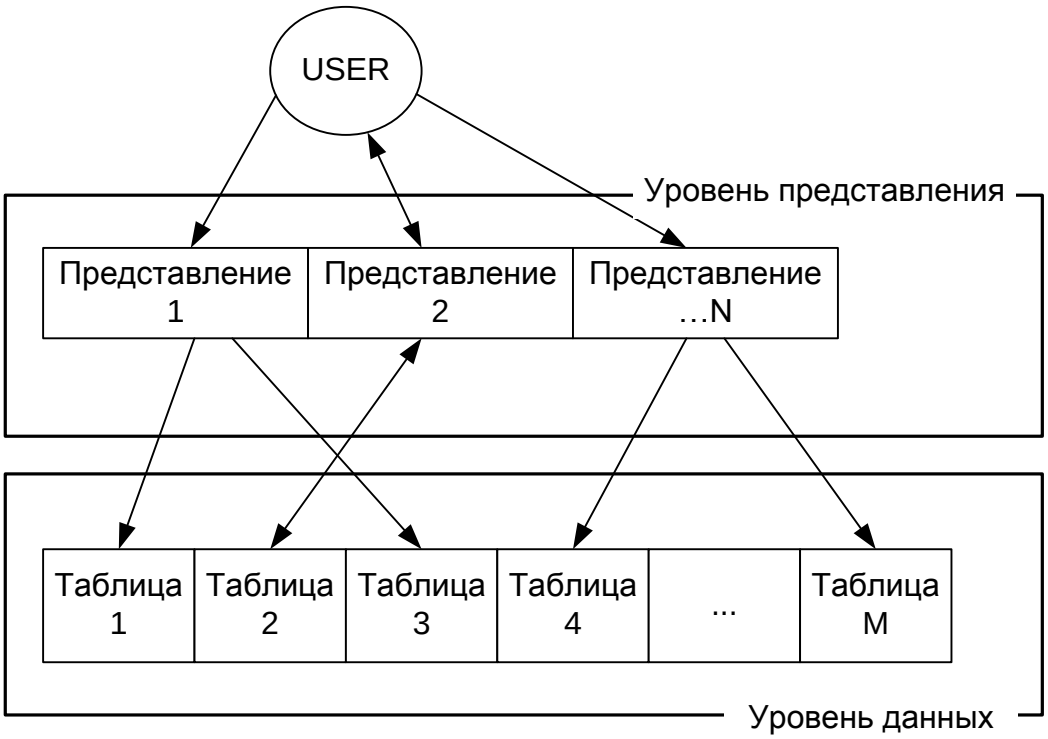

Рис. 3.2. Взаимодействие уровней данных и представлений

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. В последнем случае применяются триггеры замещения (тип INSTEAD OF), определенные на уровне процедур (уровень 3).

Некоторые СУБД позволяют осуществлять шифрование текста SELECT-запроса. Как правило, шифрование, применяемое в СУБД к представлениям не представляет механизм дешифрования (не позволяет восстановить исходный код SELECT-запроса по зашифрованному тексту).

Доступ к представлениям регулируется таким же образом, как и таблицам. Уровень представления может быть использован в качестве поверхности базы данных.

3.4. Уровень процедур

Для создания собственных 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.

К уровню процедур относятся DML-триггеры. DML-триггеры представляют собой особый вид процедур, вызываемых сервером СУБД автоматически при возникновении DML-события (выполнения SQL-операторов, изменяющих таблицу базы данных). DML-триггеры всегда связаны с конкретной таблицей и реагируют только на DML-события именно этой таблицы. СУБД может поддерживать несколько типов триггеров: before (триггеры, выполняющиеся до операции модификации), after (триггеры, выполняющиеся после операции модификации), instead of (триггеры замещения). Кроме того, триггеры могут разных уровней: уровня строки (реагирующих на модификацию строки) или оператора (выполняющихся только один раз для оператора модифицирующего таблицу базы данных). В системах безопасности СУБД DML-триггеры применяются для аудита и шифрования данных. Триггеры замещения вместе с представлениями, позволяют скрыть о пользователя логическую структуру базы данных.

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

3. 5. Уровень схем

Схемы представляют собой поименованную совокупность объектов базы данных. При этом каждый объект, всегда принадлежит ровно одной группе. Схему можно рассматривать, как пространство имен для объектов низших уровней модели. У каждой схемы есть владелец – пользователь базы данных. Схема может быть назначена пользователю базы данных в качестве схемы по умолчанию.

Наличие механизма схем, позволяет создавать в разных схемах объекты с одинаковыми именами, однако при ссылке на эти объекты требуется применять двухкомпонентное имя. В тех случаях, когда схема для пользователя, является схемой по умолчанию, применение двухкомпонентных имен не является обязательнвм.

С точки зрения информационной безопасности схема представляет собой группу объектов базы данных (таблицы, представления, процедуры, функции и пр.), доступ к которым может регулироваться одновременно. Другими

словами СУБД предоставляет возможность назначить привилегию пользователю сразу на все объекты, входящие в эту схему. Например, можно разрешить выполнять оператор INSERT для всех таблиц схемы, или можно разрешить выполнять все процедуры и функции входящие в некоторую схему базы данных.

3. 6. Уровень пользователей базы данных

Основными объектами этого уровня являются пользователи базы данных (экземпляры объектов USER), 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. Основное назначение пользователя базы данных – олицетворять, подключившегося к базе данных субъекта.

Объектные привилегии – набор элементарных разрешений, которые может выдать пользователь-владелец объекта другому пользователю для его использования. Объектные привилегии могут быть назначены на объект или схему объектов.

Роль базы данных – это принципал, представляющий собой поименованный набор привилегий, который может быть назначен пользователю или другой роли. Роль позволяет создавать категории пользователей, обладающих одинаковым набором привилегий.

Одному пользователю может быть назначено несколько ролей. В этом случае пользователь будут обладать объединением всех привилегий, назначенных ролям.

Роль может быть назначена другой роли. Такая возможность позволяет создавать иерархии ролей.

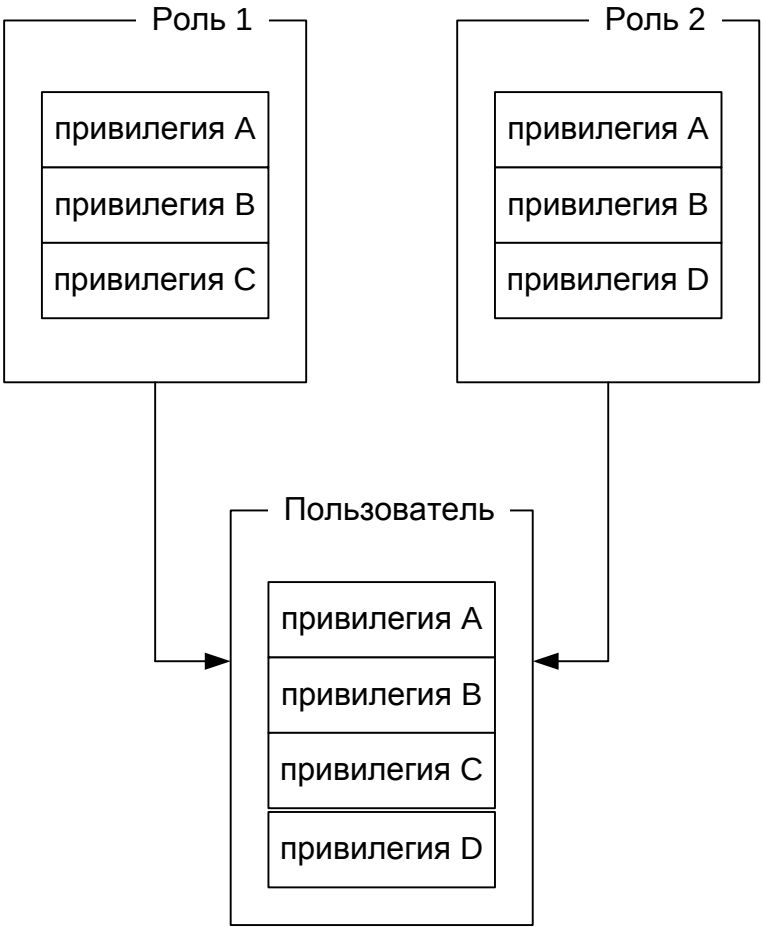

Рис. 3.3. Наследование привилегий нескольких ролей пользователем базы данных

Как правило, на уровне базы данных всегда предопределены два обязательных пользователя: один – с максимальными системными привилегиями, другой – с минимальными. Пароли этим пользователям, как правило задаются при инсталляции СУБД или имеют стартовые значения описанные в документации. Первый является владельцем базы данных (всех ее объектов) и предназначен для выполнения административных функций (создание других пользователей, ролей, назначение привилегий), второй предназначен для подключения к базе данных незарегистрированных пользователей (как правило, называется GUEST).

Каждый пользователь базы данных связываются с пользователем сервера, определенном на седьмом уровне модели.

3. 7. Уровень системных привилегий

Системная привилегия – это элементарное разрешение, которое связано с типом объекта (например, привилегия на создание или удаление таблиц), но не с экземпляром типа. Рассматриваемые на этом уровне модели системные

привилегии действуют на уровне базы данных и назначаются пользователю или роли базы данных. Как правило, системные привилегии назначает привилегированный пользователь базы данных, выполняющий роль администратора. Таким образом, пользователь или роль базы данных может обладать одновременно объектными и системными привилегиями.

На уровне системных привилегий могут существовать предопределенные фиксированные роли.

Как правило, среди предопределенных ролей этого уровня существует специальная роль (обычно она имеет имя PUBLIC), олицетворяющая минимальный набор привилегий, которыми обладает любой пользователь базы данных. Другими словами, пользователь уровня сервера, который соединился с сервером СУБД, даже если он не проецируется на пользователя базы данных, будет обладать набором системных привилегий в этой базе данных.

3. 8. 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. В некоторых СУБД (например, Oracle) пользователь сервера и пользователь базы могут быть совмещены.

Уровень пользователей сервера отделяет процесс аутентификации пользователя от процесса авторизации на уровне базы данных.

3. 9. Уровень серверных привилегий

Собственными объектами уровня серверных привилегий являются серверные роли (фиксированные и пользовательские) и профили безопасности.

Серверная роль – поименованная совокупность серверных привилегий, действующих на уровне сервера. Другими словами серверные привилегии определяют возможности доступа серверного пользователя к объектам сервера СУБД.

На этом уровне могут быть фиксированные и пользовательские серверные роли . Фиксированные 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 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 баз данных и сервера.

3. 10. 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.

3. 11. Поверхности базы данных

Поверхность базы данных – совокупность объектов базы данных, доступных пользователю. В модели выделены три поверхности: на уровнях данных, представлений и процедур.

На рис. 3.4 изображена схема, поясняющая понятие поверхности базы данных.

Поверхности базы данных на рисунке отображаются горизонтальными линиями помеченные цифрами 1, 2 и 3. Пользователи базы данных изображены в виде окружностей, помеченных символом USER. Кроме того, на схеме отображены объекты базы данных: таблицы, представления и процедуры – все они помечены соответствующими символами. Сплошные двухконечные стрелки, соединяющие изображение пользователя с линией поверхности и помеченные символом DML, обозначают возможность применения пользователем DML-операторов к объектам поверхности. Двухконечная стрелка, помеченная символом EXECUTE, обозначает возможность вызова процедурных объектов (процедур, функций). Штриховые линии, помеченные символом GRANT и соединяющие обозначения пользователей, обозначают назначение одним пользователем (начало стрелки) привилегий другому (конец стрелки).

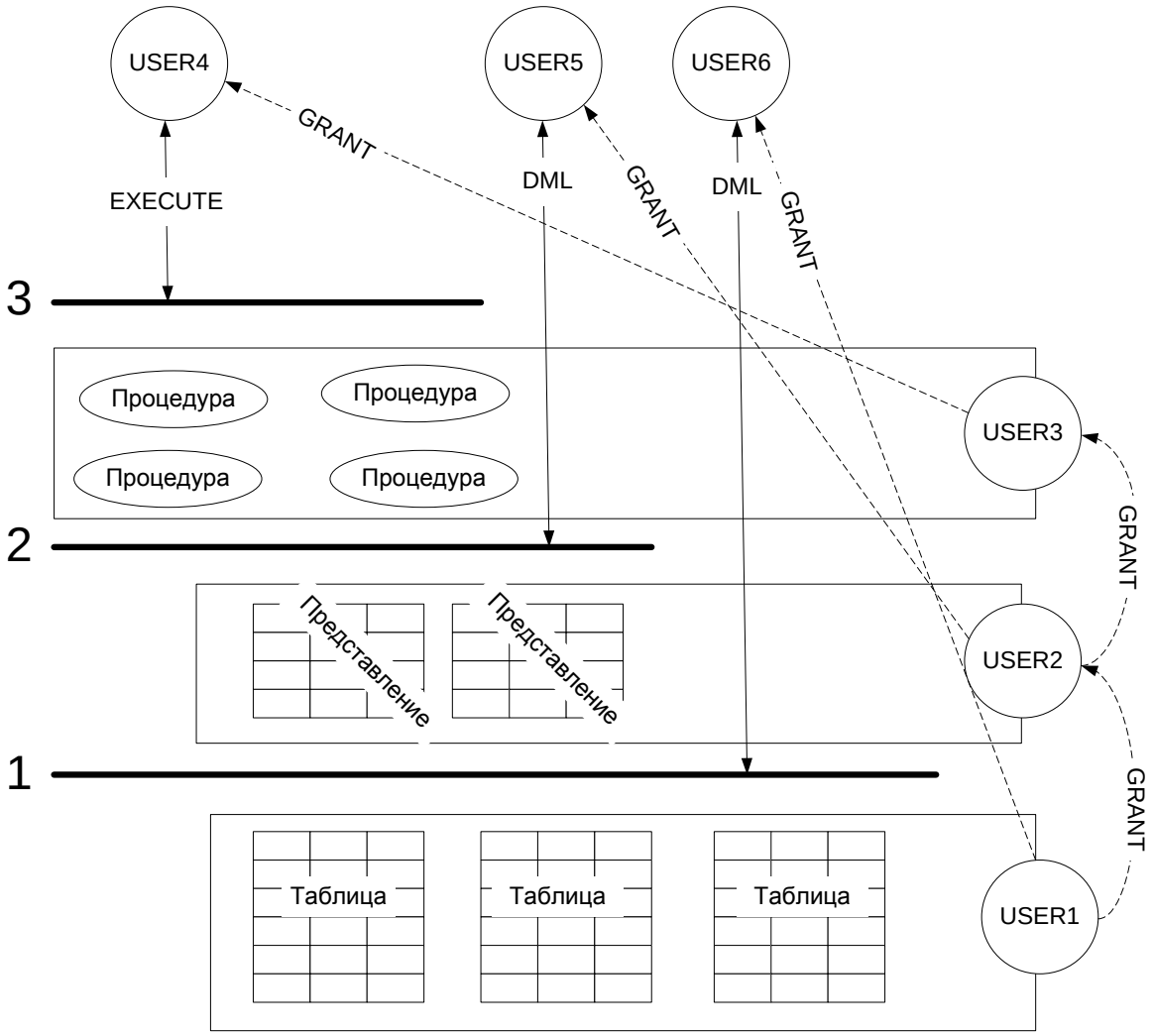

Рис. 3.4.Поверхности базы данных

Поверхность 1 представляет пользователю USER6 DML-доступ непосредственно к таблицам базы данных. Владельцем таблиц является USER1. Он обладает полным набором объектных и системных привилегий на объекты своего уровня с административными возможностями (может назначать эти привилегии другим пользователям). Он должен наделить пользователя USER6 соответствующими объектными привилегиями. Привилегии могут быть назначены посредством соответствующей роли (что является более рациональным) или непосредственно пользователю.

Поверхность 2 представляет пользователю USER5 DML-доступ к представлениям (при этом не разрешает доступ к таблицам), владельцем которых является USER2. Операции модификации над представлениями, транслируются в операции над соответствующими таблицами поверхности 1. Трансляция может осуществляться с помощью стандартных средств СУБД или с помощью триггеров, реагирующих на события модификации представлений. При этом не обязательно взаимно-однозначное соответствие

между представлениями и таблицами. Модификация одного представления, может повлечь модификацию более одной таблицы. Некоторые представления могут быть только для чтения. Возможности пользователя USER2 регулируются привилегиями назначенные ему пользователем USER1, а возможности пользователя USER5 привилегиями назначенные ему пользователем USER2. Пользователю USER5 база данных представляется как набор представлений.

Владельцем процедур поверхности 3 является USER3. При этом он обладает набором привилегий, назначенных ему пользователем USER2. Пользователю USER4 предоставлены необходимые для выполнения процедур привилегии пользователем USER3. Процедуры поверхности обеспечивают полную функциональность работы с базой данных. Другими словами пользователю USER4 база данных представляется как набор процедур.

Приведенная на рис. 3.4 схема, отображает классический вид взаимодействия поверхностей между собой и применения их пользователями USER4, USER5, USER6. Кроме этого модель допускает отклонения от классического вида взаимодействия. Например, процедуры могут напрямую работать с таблицами, не создавая промежуточный слой представлений поверхности 2. Или, например, может быть пользователь, работающий одновременно с несколькими поверхностями: может напрямую читать представление, но модификацию базы данных осуществлять с помощью процедур поверхности 3.

3. 12. Процессы аутентификации и авторизации

Процесс аутентификации охватывает три уровня модели (рис. 3.5). Задачей этого процесса является идентификация, подключающегося к серверу субъекта.

Процесс начинается с аутентификации пользователя операционной системы (на схеме OS-USER) в рамках уровня 9 (операционной системы) модели.

После этого осуществляется проецирование пользователя операционной системы на пользователя сервера СУБД (на схеме SERVER-USER). В некоторых случаях, если отсутствует или запрещен механизм прямого проецирования, может потребоваться ввод имени и пароля пользователя СУБД.

После того, как на уровне 7 (пользователи сервера) создан экземпляр серверного пользователя, процесс аутентификации завершается.

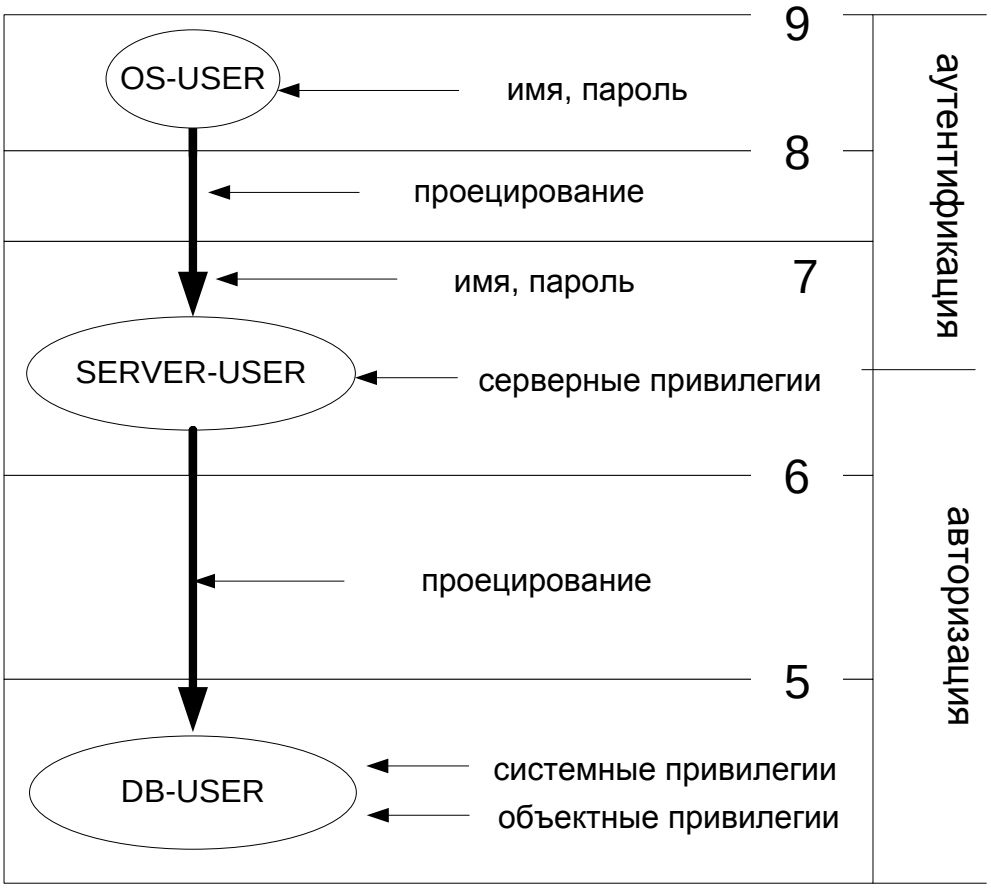

Рис. 3.5. Схема процессов аутентификации и авторизации

Если процесс аутентификации завершился успешно, в рамках уровня 7 инициируется процесс авторизации, который начинается с наделения созданного экземпляра серверного пользователя серверными привилегиями.

Задачей процесса авторизации является наделения пользователей сервера и базы данных соответствующими привилегиями.

После создания серверного пользователя привилегиями (уровень 7), он проецируется на пользователя базы данных (на схеме DB-USER), которому назначаются системные и объектные привилегии. Процесс авторизации завершился.

3. 13. Процесс аудита

Процесс аудита охватывает все уровни модели. В модели выделяются две задачи аудита: аудит операций, аудит привилегий.

Назначение первой задачи: фиксация в журнале аудита всех операций осуществляемых в сервере и базе данных.

Назначение второй задачи: выявить неиспользуемые (лишние) привилегии, назначенные пользователям.

3. 14. Заключение

1. Предлагаемая модель системы безопасности СУБД не зависит от реализации СУБД.
2. Модель содержит девять уровней, на каждом уровне рассматривается собственный перечень объектов сервера СУБД или базы данных.
3. В модели рассматриваются следующие принципалы: пользователи операционной системы, пользователи сервера, пользователи базы данных, фиксированные серверные роли, фиксированные роли базы данных, пользовательские серверные роли, пользовательские роли базы данных.
4. В модели рассматриваются следующие объекты: серверные привилегии, привилегии базы данных, реляционные таблицы, представления, программные объекты.
5. В модели рассматриваются следующие операции: DML-операции, DCL-операции, DDL-операции.
6. В модели введено понятие поверхности базы данных, описывающее способы представления базы данных пользователем. Описывается три поверхности, определяющих доступ к базе данных на уроне таблиц, представлений или программных объектов.
7. В модели рассматриваются три процесса: процесс аутентификации, процесс авторизации и процесс аудита.
8. Модель описывает аспекты внутренней реализации системы безопасности СУБД.
9. С помощью модели можно описать системы безопасности СУБД Oracle 11.2g и Microsoft SQL Server 2008.

4. СРАВНИТЕЛЬНАЯ ОЦЕНКА СИСТЕМ БЕЗОПАСНОСТИ СУБД ORACLE 11.2G И MICROSOFT SQL SERVER 2008

4.1. Принципы оценки систем безопасности

В соответствии с оценочным стандартом TCSEC системы безопасности обеих СУБД (Oracle 11.2g и Microsoft SQL Server 2008) относят к уровню C2.

Предлагаемая стандартом TCSEC оценка применяется к информационным системам в независимости от их назначения. При оценке TCSEC применяет общий подход для операционных систем, серверов приложений, СУБД и других компонентов информационных систем. Более того, с помощью TCSEC можно оценить уровень безопасности всей информационной системы. При этом, практически не учитывается внутреннее устройство предмета оценки.

Проведенный во второй главе анализ продемонстрировал значительные отличия внутреннего устройства систем безопасности СУБД Oracle 11.2g и Microsoft SQL Server 2008. Очевидно, что одномерная оценка не может в полной мере отражать разницу систем безопасности этих СУБД.

В третьей главе работы построена и описана обобщенная модель информационной безопасности СУБД. Модель позволяет в соответствии с общими принципами структурно описать систему безопасности любой СУБД.

В основе предлагаемого здесь подхода к оценке систем безопасности СУБД лежит структура обобщенной модели информационной безопасности. На каждом уровне модели выделяются метрики, значения которых отражают оценку элементов системы безопасности СУБД. Значения метрик устанавливаются на основе экспертной оценки и могут варьировать от 0 до 3.

Оценки для каждой метрики определяются по следующему принципу: сначала выбирается СУБД у которой оцениваемые метрикой возможности реализованы лучше и выставляется 3 балла, оценка другой СУБД выставляется относительно первой. При этом 0 означает, что эта возможность не реализована, 1, как правило, указывает на то, что для ее реализации требуется разработка дополнительного кода, 2 – реализация качественно или количественно хуже.

Комплексная оценка вычисляется для каждого уровня путем усреднения оценок метрик, относящихся к данному уровню. Таким образом, окончательная оценка представляется в виде вектора, содержащего 9 (по количеству уровней модели) числовых компонент, значение которых находится в пределах от 0 до 3.

4.2. Метрики системы безопасности СУБД

4.2.1.Уровень данных

На уровне данных рассматриваются три метрики:

1) шифрование на уровне столбца: определяет возможность шифровать данные в столбце таблицы при выполнении DML-операторов INSERT, UPDATE и расшифровывать при выполнении SELECT;
2) поддержка специального столбца для версии строки: определяет встроенные механизмы, позволяющие определить либо версию (число, позволяющее определить хронологию операций в базе данных) либо штамп времени;
3) разграничение доступа на уровне строк таблиц: определяет встроенные механизмы позволяющие определить возможность разграничение доступа пользователей к строкам таблиц;

4.2.2.Уровень представлений

На уровне представлений рассматриваются четыре метрики:

4) поддержка CHECK OPTION: определяет наличие специальной опции у представления, которая позволяет задать дополнительное ограничение целостности в секции WHERE;
5) обфускация SELECT-запроса: определяет возможность скрыть текст SELECT-запроса представления;
6) имперсонизация: определяет возможность назначить представлению определенные привилегии;
7) связывание со схемой: определяет возможность запретить удаление или модификацию таблиц, если существует представление, построенное на основе SELECT-запроса к ним.

4.2.3.Уровень процедур

На уровне процедур рассматриваются шесть метрик:

8) обфускация процедур: определяет возможность скрыть текст процедур и функций;
9) поддержка спецификаций процедур: определяет возможность отделить спецификацию процедур и функций (разместить в отдельном объекте их сигнатуры) от их реализации;
10) имперсонизация: определяет возможность назначить процедуре и/или функции определенные привилегии;
11) триггеры таблиц: определяет возможность создать DML-триггеры;

12) управление уровнем изолированности транзакций: возможность устанавливать в процедурах уровень изолированности транзакций;
13) контроль безопасности встроенного кода: наличие средств, контролирующих безопасность (внешний доступ, доступ к памяти и пр.) встроенного в СУБД кода.

4.2.4. Уровень схем

На уровне схем рассматриваются две метрики:

14) поддержка схем: определяет возможность создавать схемы и управлять привилегиями уровня схем;
15) стандартные схемы: определяет наличие стандартных схем – схем, содержащих системные объекты;

4.2.5. Уровень пользователей базы данных

На уровне пользователей базы данных рассматриваются четыре метрики:

16) объектные привилегии: определяет наличие, количество, уровень назначения (пользователю, роли, на схему) объектных привилегий;
17) фиксированная роль уровня базы данных: определяет наличие фиксированных полей;
18) пользовательская роль уровня базы данных: определяет возможность создания пользовательской роли уровня базы данных;
19) роль приложения: определяет наличие ролей уровня приложений;
20) связь с пользователем операционной системы: определяет возможность совмещения пользователей операционной системы и сервера базы данных;

4.2.6. Уровень системных привилегий

На уровне системных привилегий рассматриваются четыре метрики:

21) уровень детализации системных привилегий: определяет степень детализации возможностей, определяемых привилегиями;
22) разграничение системных привилегий сервера и базы данных: определяет возможность пользователей сервера, которым не доступны привилегии пользователя базы данных;
23) профиль безопасности: определяет наличие отдельного объекта сервера, содержащего ограничения пользовательского севнса;
24) системные триггеры: определяет наличие триггеров, реагирующих на DDL-события, старт или остановку сервера, подключение или отключение клиента и пр.

4.2.7. Уровень пользователей сервера

На уровне пользователей сервера рассматриваются три метрики:

25) серверные пользователи: определяет возможность создавать отдельно пользователей сервера и пользователей базы данных;
26) прокси-пользователи: определяет возможность создавать на уровне сервера объекты, представляющие пользователей операционной системы, от имени которых можно выполнять внешние по, отношению к серверу СУБД, операции;
27) хранение учетных данных: определяет наличие специальных объектов, предназначенных для хранения учетных записей внешних пользователей.

4.2.8. Уровень серверных привилегий

На уровне серверных привилегий рассматриваются три метрики:

28) системный каталог: определяет наличие системного каталога и степень его защищенности;
29) фиксирование серверные роли: наличие фиксированных ролей уровня сервера;
30) пользовательские серверные роли: определяет возможность создавать серверные роли;
31) DDL-триггеры: определяет возможность создавать триггеры, реагирующие на изменение привилегий.

4.2.9. Уровень операционной системы

32) защита файлов операционной системы: определяет возможность защитить файлы базы данных средствами СУБД;
33) защита процессов операционной системы: определяет возможность защитить процессы СУБД средствами СУБД;
34) интеграция с операционной системой: определяет степень интеграции с операционной системой.

4.3. Результаты экспертной оценки

Результаты экспертной оценки систем безопасности СУБД Oracle 11.2g и Microsoft SQL Server 2008 сведены в табл. 4.1.

Таблица 4.1. Сравнительная оценка систем безопасности

Метрики информационной безопасности	Оценка (0 – 3)	
	Oracle 11.2g	Microsoft SQL Server 2008
I. Уровень данных		
1. Шифрование данных на уровне столбца	3	2
2.Поддержка специального столбца для версии строки	2	3
3.Разграничение доступа на уровне строк таблиц	3	1
II. Уровень представлений		
4. Поддержка CHECK OPTION	3	3
5. Обфускация SELECT-запроса	3	0
6. Имперсонизация	3	3
7. Связывание со схемой	2	3
III. Уровень процедур		
8. Обфускация процедур	3	3
9. Поддержка спецификаций процедур	3	0
10. Имперсонизация	2	3
11. Триггеры таблиц	3	1
12. Управление уровнем изолированности транзакций	2	3
13. Контроль безопасности встроенного кода	1	3
IV. Уровень схем		
14. Поддержка схемы	2	3
15. Стандартные схемы	3	3
V. Уровень пользователей базы данных		
16. Объектные привилегии	2	3
17.Фиксированная роль уровня базы данных	3	0
18. Пользовательская роль уровня базы данных	3	3
19. Роль приложения	1	3
20. Связь с пользователем ОС	1	3

VI. Уровень системных привилегий		
21. Уровень детализации системных привилегий	3	2
22.Разграничение системных привилегий сервера и базы данных	2	3
23. Профиль безопасности	٣	٠
24. Системные триггеры	٣	٢
VII. Уровень пользователей сервера		
25. Серверные пользователи	3	1
26. Прокси-пользователи	١	٣
27. Хранение учетных данных	2	3
VIII. Уровень серверных привилегий		
28.Системный каталог	3	3
29.Фиксирование серверные роли	0	3
30.Пользовательские серверные роли	2	1
31. DDL-триггеры	٢	٢
IX. Уровень операционной системы		
32.Защита файлов ОС	1	1
33.Защита процессов ОС	1	1
34.Интеграция с ОС	1	3

Усредненные экспертные оценки (табл. 4.2) для каждого уровня модели информационной безопасности СУБД сведены в табл. 4.2

Таблица 4.2. Средние значения оценок для каждого уровня модели

Уровни модели информационной безопасности СУБД	Средние оценки	
	Oracle 11.2g	Microsoft SQL Server 2008
I. Уровень данных	2.7	2
II. Уровень представлений	2.75	2.25
III. Уровень процедур	2.3	2.17
IV. Уровень схем	2.5	3
V. Уровень пользователей базы данных	2	2,4
VI. Уровень системных привилегий	2.75	1.75
VII. Уровень пользователей сервера	2	2.3
VIII. Уровень серверных привилегий	1.75	2.25
IX. Уровень операционной системы	1	1.6
Сумма	19.75	19.72

На рис. 4.1 результаты из табл.4.2 представлены в виде диаграммы. На диаграмме изображены девять осей, соответствующие девяти уровням модели.

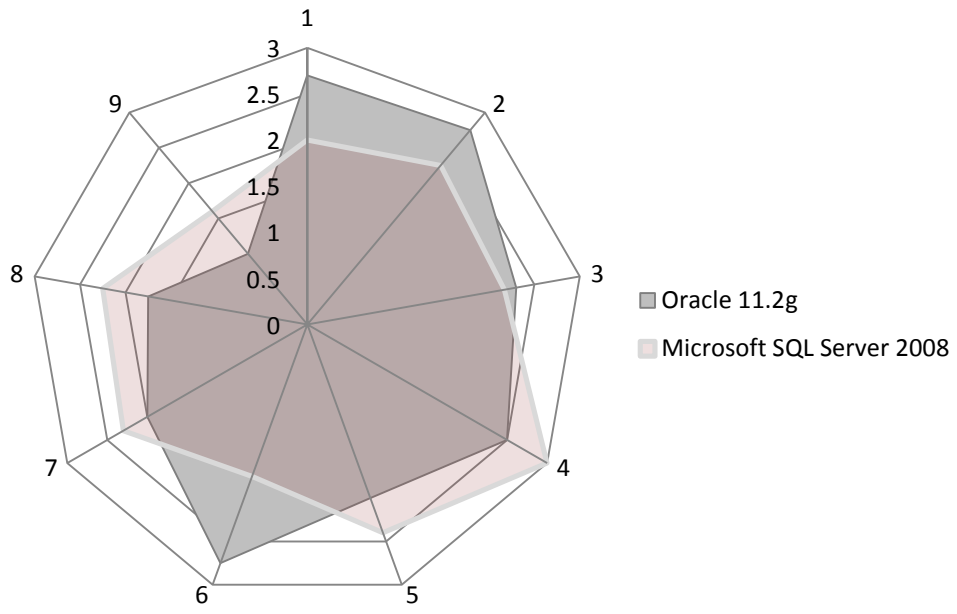

Рис.4.1. Диаграмма средних значений

На диаграмме ясно видно, что ни одна из рассматриваемых систем безопасности явно не преобладает над другой. В тоже время оценка Microsoft SQL Server 2008 выше на тех уровнях модели, которые относятся к реализации сервера и его интеграции с операционной системой (уровни 8 и 9), у СУБД Oracle 11.2g оценка преобладает на первых трех уровнях модели и на уровне системных привилегий (уровень 6).

ЗАКЛЮЧЕНИЕ

1. Для оценки системы информационной безопасности СУБД обычно применяется стандарт TCSEC (Trusted Computer Systems Security Evaluation Criteria – Критерии оценки безопасности доверенных компьютерных систем).В соответствии с классификацией TCSEC СУБД Microsoft SQL Server 2008 и Oracle 11.2g имеют системы безопасности категории C2.
2. Исследования, проведенные в главе 2 работы, показывают, что оценка TCSEC является интегрированной, не учитывающей внутренних механизмов системы безопасности. Для более детальной оценки уровня системы безопасности в рамках диссертационной работы (глава 3) разработана обобщенная модель информационной безопасности СУБД.
3. Обобщенная модель системы безопасности СУБД содержит девять уровней. Каждый уровень характеризуется наличием собственных объектов (базы данных, сервера базы данных, операционной системы), свойства безопасности которых, определяются объектами уровней, находящихся выше.
4. Для сравнительной оценки систем безопасности СУБД Microsoft SQL Server 2008 и Oracle 11.2g использовалось 34 метрики, распределенных по 9 уровням обобщенной модели безопасности. Каждая метрика получила экспертную оценку в диапазоне от 0 до 3. Для каждого уровня модели были вычислены средние значения метрик.
5. Анализ показал, что ни одна из рассматриваемых систем безопасности СУБД явно не преобладает над другой, а суммы усредненных по каждому уровню метрик примерно равны.
6. Оценка систем безопасности СУБД Microsoft SQL Server 2008 выше на тех уровнях модели, которые относятся к реализации сервера СУБД и интеграции с операционной системой. Это объясняется следующими конструктивными особенностям СУБД Microsoft SQL Server 2008: в структуре СУБД явно выделены два уровня: уровень сервера и уровень базы данных; один сервер может обслуживать несколько баз данных;

   СУБД предназначена для работы только в операционной системе Windows и как следствие – сильно интегрирована с этой операционной системой.
7. Оценка систем безопасности СУБД Oracle 11.2g выше на первых трех уровнях модели – уровнях соответствующих реализации базы данных, а также уровне системных привилегий. Это объясняется, тем что в сервер СУБД Oracle 11.2g поддерживает только одну базу данных и все средства обеспечения безопасности сосредоточены на этих четырех уровнях.

СПИСОК ЛИТЕРАТУРЫ

1. Группы доступности AlwaysOn (SQL Server) [Электронный ресурс] / Microsoft Corporation, 2015. – Режим доступа: http://msdn.microsoft.com/ru-ru/library/hh510230.aspx – Дата доступа: 09.03.2015.
2. Стандарт информационной безопасности: курс лекций: учебное пособие/ Второе издание / В.А. Галатенко. Под редакцией академика РАН В.Б. Бетелина/ –М: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2006, –254с.
3. Oracle Database 11.2g Enterprise Edition [Электронный ресурс] / Oracle Corporation, 2015. – Режим доступа: http://oracle.com/database. – Дата доступа: 09.03.2015.
4. Microsoft SQL Server 2008 [Электронный ресурс] / Microsoft Corporation, 2015. – Режим доступа: http://www.microsoft.com/sqlserve/2008/ru/ru/overview.aspx – Дата доступа: 09.03.2015.
5. Дейт, К., Дж. Введение в системы баз данных / К. Дж. Дейт. – М.: Вильямс, 2005. –1316 с.
6. Язык описания данных КОДАСИЛ/ М. Когаловский, Г. Столяров. – М.: Статистика, 1981. – 183с.
7. IBM DB2 database software [Электронный ресурс] / IBM Corporation, 2015. – Режим доступа: http://www-01.ibm.com/software/data/db2 – Дата доступа: 09.03.2015.
8. Gartner 2014 Magic Quadrant for Operational Database Management System [Электронный ресурс] / ODBMS. – Режим доступа: http://www.odbms,org/2014/11/gartner-2014-magic-qudrant-operational-database-management-systems-2/– Дата доступа: 09.03.2015.
9. ITU-T Recommendations. ITU-T X.500 [Электронный ресурс] / ITU-T, 2015. – Режим доступа: http://www.itu.int/ITU-T /recommendations/rec.aspx?rec=X.500 – Дата доступа: 09.03.2015.
10. Таненбаум Э. Компьютерные сети/ Э. Таненбаум. – СПб.: Питер, 2009. –992 с.
11. Описание протоколов SSL/TSL [Электронный ресурс] / Крипто-Про , 2002.Режим доступа: http://www.cryptopro.ru/sites/default/ files/ docs/ TLS_description.pdf – Дата доступа: 09.03.2015
12. Common Vulnerability and Exposure [Электронный ресурс] / Mitre , 2015. Режим доступа: http://cve.mitre.org – Дата доступа: 09.03.2015

13. Common Vulnerability and Exposure [Электронный ресурс] / NIST , 2015. Режим доступа: http://web.nvd.nist.gov – Дата доступа: 15.06.2015.
14. ISACA [Электронный ресурс] / ISACA , 2015. Режим доступа: http://www.isaca.org – Дата доступа: 15.06.2015.
15. PCI Security Standards Council [Электронный ресурс] / PCI Security Standards Council , 2015. Режим доступа: http://www.pcisecuritystandards.org – Дата доступа: 15.06.2015.
16. ISO/IEC 27002 [Электронный ресурс] / ISO/IEC 27002:2005 , 2007. Режим доступа: http://pgm-online.com/accets/files/lib/std/iso_iec_27002-2005.pdf – Дата доступа: 15.06.2015.
17. Security and Privacy Controls for Federal Information Systems and Organizations [Электронный ресурс] / NIST , 2013. Режим доступа: http://nvlpubs.nist.gov/nistpubs/SpetialPublications/NIST.SP.800-53r4.pdf – Дата доступа: 15.06.2015.
18. Закон Республики Беларусь «Об информации, информатизации и защите информации» № 455-4 от 10.11.2008[Электронный ресурс] Национальный правовой интернет-портал Республики Беларусь. Режим доступа: http://www.pravo.by/main.aspx?guid=3871&p0=h1080045&p2={NRPA} – Дата доступа: 15.06.2015.
19 Найт, Б. Microsoft SQL Server 2008: руководство администратора для профессионалов / Б. Найт, К. Пэтел, В. Снайдер, Р. Лоффорт, С. Уорт – М.: Вильямс, 2010. – 944 с.
20 Алапати, С. Р. Oracle 11g. Руководство администратора баз данных/ С. Р. Алапати – М.: Вильямс, 2015. – 1440 с.

ПРИЛОЖЕНИЕ 1.Глоссарий терминов

Англійский	Русский	Арабский
Audit: - is systematic measurable technical assessment of a system or application. Performing security vulnerability scans, reviewing application and operating system access controls, and analyzing physical access to the systems. Automated assessments, include system generated audit reports or using software to monitor and report changes to files and settings on a system. Systems can include personal computers, servers, mainframes, network routers, switches. Applications can include Web Services, Microsoft Project Central, Oracle Database	**Аудит:-** систематическое измеримы техническая оценка системы или приложения. выполнения сканирования уязвимостей безопасности, рассматривая приложения и операционной системы контроля доступа и анализа физического доступа к системам. Автоматизированные оценки, включают в себя системы генерируется аудиторские отчеты или с помощью программного обеспечения для мониторинга и отчетности изменения в файлах и настройках в системе. Системы могут включать в себя персональные компьютеры, серверы, мэйнфреймы, сетевые маршрутизаторы, коммутаторы. Приложения могут включать в себя веб-служб, Microsoft Project Central, Oracle Database	**التدقيق:-** هو التقييم الفني للقياس المنهجي لنظام أو تطبيق. القيام بمسح ثغرة أمنية، ومراجعة تطبيق وتشغيل التحكم بالوصول للنظام، وتحليل الوصول الفعلي إلى النظم. تقييم الآلي، وتتضمن تقارير مراجعة نظم ولدت أو باستخدام برنامج لرصد والإبلاغ عن التغييرات إلى الملفات والإعدادات على النظام. ويمكن أن تشمل أنظمة أجهزة الكمبيوتر الشخصية والخوادم والحاسبات وأجهزة التوجيه الشبكة والمحولات. تطبيقات يمكن أن تشمل خدمات ويب ، المركزية، قاعدة Microsoft. بيانات أوراكل Project
Authentication: - is the act of confirming the truth of an attribute of a single piece of data (datum) or entity. In contrast with identification which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually confirming that identity. It might involve confirming the identity of a person by validating their identity	**Аутентификация:-** В информатике безопасности система, при которой признается для прокси-сервера к системе или пользователям доступ к информации. Это делается в одном из средств аутентификации известны: кто вы есть (отпечатков пальцев, например), поэтому есть (корпоративная карта,	**المصادقة:-** في علم أمن الحاسوب هو اجراء يقر النظام بمقتضاه ولوج الوكيل إلى النظام أو وصول المستخدِم إلى المعلومات. يتم ذلك باحدى وسائل الاستيقان المعروفة: من أنت (البصمة مثلا), ماذا تملك (بطاقة اعتبارية مثلا), أو ماذا تعرف (اسم المستخدِم وكلمة المرور وذلك بأن تقارن بمحتوى قائمة المسموح لهم مثلا لمعرفة إن كان هناك تطابق). اذا تم الاستيقان بنجاح يمنح المستخدم حق النفاذ إلى

documents, verifying the validity of a Website with a digital certificate, tracing the age of an artifact by carbon dating, or ensuring that a product is what its packaging and labeling claim to be. In other words, authentication often involves verifying the validity of at least one form of identification.	например), или то, что вы знаете (имя пользователя и пароль, так что сравнение содержания перечня позволило им увидеть, например, если есть совпадение). Если аутентификация прошла успешно дает пользователю право на доступ к указанному уровню в списке своих полномочий.	المستوى المحدَّد له في قائمة الصلاحيات.
Authorization: - is the function of specifying access rights to resources related to information security and computer security in general and to access control in particular. More formally, "to authorize" is to define an access policy.	**Авторизация:-** это функция определения прав доступа к ресурсам, связанным с информационной безопасностью и компьютерной безопасности в целом и контроля доступа, в частности.Более формально, "для авторизации" является определение политики доступа.	**ترخيص:-** هي وظيفة من تحديد حقوق الوصول إلى الموارد المتعلقة بأمن المعلومات وأمن الكمبيوتر بشكل عام، والوصول إلى السيطرة على وجه الخصوص. بشكل رسمي، "أن تأذن" هو تعريف نهج الوصول .
DBMS (database management system) is a collection of programs that enables you to store, modify, and extract information from a database. There are many different types of database management systems, ranging from small systems that run on personal computers to huge systems that run on mainframes.	**СУБД (Система управления базами данных)** представляет собой набор программ, который позволяет хранить, изменять и извлекать информацию из базы данных. Есть много различных типов систем управления базами данных, начиная от небольших систем, которые работают на персональных компьютерах в огромных	**نظم إدارة قواعد البيانات:-** هي عبارة عن مجموعة من البرامج التي تمكنك من تخزين وتعديل واستخراج المعلومات من قاعدة بيانات. هناك العديد من أنواع مختلفة من أنظمة إدارة قواعد البيانات، بدءا من الأنظمة الصغيرة التي تعمل على أجهزة الكمبيوتر الشخصية بأنظمة الضخمة التي تعمل على الحاسبات.

	систем, которые работают на ЭВМ.	
Object: - In computer science is a location in memory having a value and possibly referenced by an identifier. An object can be a variable, a data structure, or a function. In the class-based object-oriented programming paradigm, "object" refers to a particular instance of a class where the object can be a combination of variables, functions, and data structures. In relational database management, an object can be a table or column, or an association between data and a database entity	**Объект: -** В информатика расположение в памяти, имеющий значение и, возможно, на который ссылается идентификатор.Объект может быть переменная, структура данных, или функция. В классе на основе объектно-ориентированного программирования парадигмы, "объект" относится к конкретному экземпляру класса, где объект может быть комбинация переменных, функций и структур данных. В управлении реляционных баз данных, объект может быть таблицы или столбца, или связь между данными и организация базы данных	**الكائن:-** في علم الحاسوب هو موقع في الذاكرة لها قيمة، وربما المشار إليه بواسطة معرف. كائن يمكن أن يكون متغير، بنية بيانات، أو وظيفة. على أساس طبقي للكائن المنحى لنمط برمجته، "كائن" يشير إلى حالة معينة من فئة حيث الكائن يمكن أن يكون مزيجا من المتغيرات، وظائف، وهياكل البيانات. في إدارة قواعد البيانات العلائقية، ويمكن أن يكون كائن جدول أو عمود، أو وجود ارتباط بين البيانات وكيان قاعدة البيانات
Oracle Corporation: - is a multinational computer technology corporation headquartered in Redwood City, California, United States. The company specializes in developing and marketing computer hardware systems and enterprise software products – particularly its own brands of database management systems.	**Корпорация Oracle:-** является многонациональным компьютерные технологии корпорация со штаб-квартирой в городе Редвуд-Сити, Калифорния, США.Компания специализируется на разработке и маркетинге компьютерная аппаратных систем и программных продуктов предприятий - в частности, его собственные бренды систем управления базами данных.	**شركة أوراكل:-** هي شركة التكنولوجيا الكمبيوتر متعددة الجنسيات مقرها في ريدوود سيتي، كاليفورنيا، الولايات المتحدة الأمريكية. وتتخصص الشركة في تطوير وتسويق أنظمة أجهزة الكمبيوتر ومنتجات البرمجيات للشركات - وخاصة العلامات التجارية الخاصة بها من أنظمة إدارة قواعد البيانات .

OSI Model (Open Systems Interconnection model):- is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard of their underlying internal structure and technology. Its goal is the interoperability of diverse communication systems with standard protocols. The model partitions a communication system into abstraction layers. The original version of the model defined seven layers.	**Модель OSI (Взаимосвязь открытых систем модель):-** является концептуальная модель, которая характеризует и стандартизирует связи функции телекоммуникационной системы или вычислительной без учета их основной внутренней структуры и технологии. Его целью является совместимость различных систем связи со стандартными протоколами.Модель разделяет систему связи в абстракции слоев.Оригинальная версия модели определили семь слоев.	**-:OSI (ترابط النظم المفتوحة نموذجا)** هو النموذج المفاهيمي الذي يميز وتوحد وظائف الاتصالات من نظام الاتصالات السلكية واللاسلكية أو الحوسبة دون اعتبار لبنيتها الداخلية الكامنة والتكنولوجيا. هدفها هو التشغيل البيني للأنظمة الاتصالات المختلفة مع البروتوكولات القياسية. نموذج تقسيم نظام الاتصالات في طبقات التجريد. النسخة الأصلية من طراز تعريف سبع طبقات .
Procedures: - is a group of PL/SQL statements that you can call by name. A call specification (sometimes called call spec) declares a Java method or a third-generation language (3GL) routine so that it can be called from SQL and PL/SQL. The call spec tells Oracle Database which Java method to invoke when a call is made. It also tells the database what type conversions to make for the arguments and return value.	**Процедур :-** группа PL отчетности / SQL, что вы можете позвонить по имени.Спецификация вызовов (иногда называется вызов спецификации) объявляет метод Java или языка третьего поколения (3GL) рутину так, что она может быть вызвана из SQL и PL / SQL.Вызов спец говорит Oracle Database, какой метод Java, который будет вызван вызова. Это также говорит, что базу данных преобразования типов, чтобы сделать для аргументов и возвращаемого значения.	**الإجراءات:-** هو مجموعة من البيانات التي يمكنك PL / SQL مواصفات A .الاتصال بالاسم المكالمة (تسمى أحيانا الدعوة المواصفات) تعلن طريقة جافا أو لغة روتين بحيث (٣GL) الجيل الثالث PL / و SQL يمكن استدعاؤها من المواصفات الدعوة تحكي SQL. قاعدة بيانات أوراكل التي جافا طريقة لاستدعاء عند إجراء المكالمة. ويحكي أيضا قاعدة البيانات ما نوع التحويلات لجعل لحجج وقيمة الإرجاع.

Server: - is a running instance of an application (software) capable of accepting requests from the client and giving responses accordingly. Servers can run on any computer including dedicated computers, which individually are also often referred to as "the server".	**Сервер:-** экземпляр (программное обеспечение) приложения способны принимать запросы от клиента и давать ответы соответствующим образом. Серверы могут работать на любом компьютере, включая выделенных компьютеров, которые по отдельности, также часто называют "сервером".	**الخادم:-** هو عبارة عن مثيل قيد التشغيل من تطبيق (برنامج) قادرة على قبول الطلبات من العميل وتقديم ردود وفقا لذلك. يمكن ملقمات تشغيلها على أي جهاز كمبيوتر بما في ذلك أجهزة الكمبيوتر المخصصة مما فردي كما غالبا ما يشار إليها باسم "الخادم ".
SQL (Structured Query Language):- is a special-purpose programming language designed for managing data held in a relational database management system (RDBMS), or for stream processing in a relational data stream management system (RDSMS)	**SQL (язык структурированных запросов):-** это язык программирования специального назначения предназначены для управления данных, хранящихся в системе управления реляционными базами данных (СУБД), или для обработки потока в системе управления реляционными базами поток данных (RDSMS)	**SQL(لغة الاستعلام الهيكلية):-** هي لغة برمجة لأغراض خاصة مصممة لإدارة البيانات الموجودة في نظام إدارة قواعد البيانات العلائقية (RDBMS) ، أو للتجهيز تيار في نظام إدارة تدفق البيانات العلائقية. (RDSMS)
Transaction symbolizes a unit of work performed within a database management system (or similar system) against a database, and treated in a coherent and reliable way independent of other transactions. A transaction generally represents any change in database.	**Транзакции:-** символизирует единицу выполненной работы в системе управления базами данных (или аналогичной системы) с базой данных, и обработанной в последовательной и надежный способ, независимо от других операций.Сделки в общем случае представляет каких-либо изменений в базу данных.	**المعاملات:-** ترمز إلى وحدة العمل المنجز في إطار نظام إدارة قواعد البيانات (أو نظام مماثل) ضد قاعدة بيانات، ويعامل بطريقة متماسكة وموثوق بها مستقلة عن غيرها من المعاملات. معاملة يمثل عموما أي تغيير في قاعدة البيانات.
User: - is a person who uses a computer or network service. Users generally use a system or a	**Пользователь:-** это человек, который использует компьютер или	**المستخدم:-** هو الشخص الذي يستخدم خدمة الكمبيوتر أو الشبكة. المستخدمين عموما استخدام نظام أو

software product without the technical expertise required to fully understand it. Power users use advanced features of programs, though they are not necessarily capable of computer programming and system administration.	сетевой службы. Пользователи обычно используют систему или программный продукт без технических знаний, необходимых для полного понимания его. Опытные пользователи используют расширенные функции программы, хотя они не обязательно способны программирования и системного администрирования.	منتج البرنامج دون الخبرة التقنية اللازمة لفهم بشكل كامل. للمستخدمين المتمرسين استخدام ميزات متقدمة من البرامج، على الرغم من أنها ليست قادرة بالضرورة برمجة الكمبيوتر وإدارة النظام.