Разграничение доступа к базам данных в сервис-ориентированных приложениях

Быков Д.В., Лукьянов В.С., Прохоров И.В., Скакунов А.В.

В статье анализируются существующие подходы к аутентификации и разграничению доступа к базам данных при организации трехстороннего взаимодействия: тонкий клиент (web-браузер) – сервер приложений – система управления базами данных (СУБД).

В последнее время все более явно прослеживается ориентация разработчиков программного обеспечения на сервис-ориентированную архитектуру приложений (Service-Oriented Architecture или SOA), и технологию тонких клиентов, накладывающую минимальные требования к оконечному обеспечению пользователей информационных систем.

Это связано с повсеместным глубоким проникновением Интернет-технологий и необходимостью единой платформы, строящейся по конструкционному принципу, как набор необходимых пользователям сервисов.

Сами сервисы реализуются при помощи трехуровневой схемы: тонкий клиент – сервер приложений – система управления базами данных (Рисунок 1).

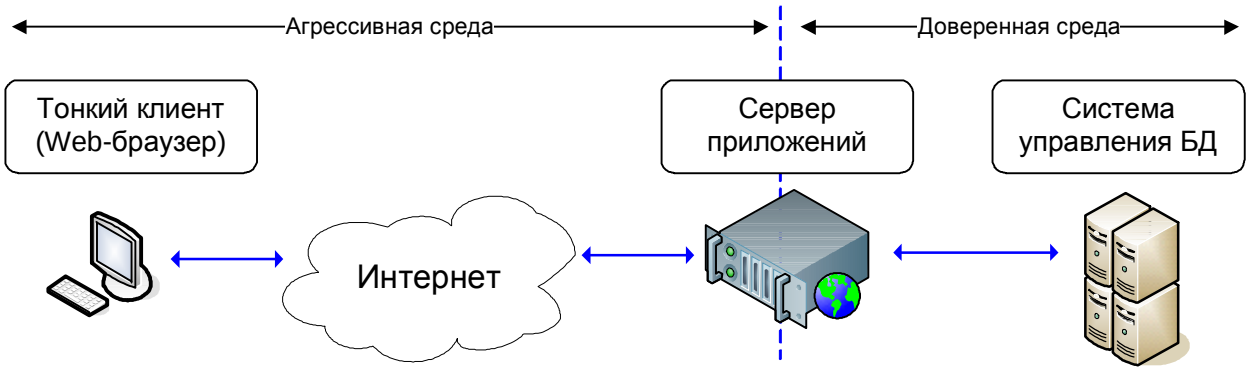

Рисунок 1. Трехуровневая архитектура Web-сервисов

Перенесение в Интранет и в Интернет информации ограниченного доступа требует реализации надежных механизмов аутентификации пользователей и разграничения доступа к данным.

В качестве наиболее распространенных способов организации такого доступа следует выделить следующие:

1) разграничение доступа средствами приложения при аутентификации самого приложения по единственной учетной записи СУБД;
2) разграничение доступа внутренними средствами СУБД.

Второй способ во многом зависит от выбранной в информационной системе СУБД. В качестве анализируемых решений рассматривались следующие распространенные системы управления базами данных: MS SQL, Oracle, PostgreSQL.

Применялись следующие критериев оценки:

- Реализация политики управления доступом при помощи СУБД:
  - шифрование отдельных элементов баз данных (строк и столбцов таблиц);
  - проверка прав на доступ к отдельным элементам баз данных;
  - встроенный механизм аутентификации пользователей СУБД;
  - защита транзакций;
  - протоколирование;
- Реализация политики управления доступом средствами приложения:
  - способы аутентификации;
  - защита соединений;
  - разграничение доступа.

По результатам проведенных исследований была составлена следующая таблица:

Реализация политики управления доступом средствами приложения		Реализация политики управления доступом при помощи СУБД	
Достоинства	Недостатки	Достоинства	Недостатки
Аутентификация			
• методы и средства аутентификации ограничены только сложностью приложения; • возможность проведения многофакторной аутентификации; • внедрение нестандартных решений.	• аутентификация не сквозная и не обеспечивает автоматический доступ к БД; • зачастую сами приложения аутентифицируются в БД под административной записью.	• позволяет использовать механизмы разграничения доступа СУБД; • определяет права пользователя при доступе непосредственно к БД	• требует знания учетных записей БД на стороне тонкого клиента;
Защита данных			
• позволяет шифровать трафик на сетевом и транспортном уровне • позволяет использовать любые криптографические алгоритмы	• операции по защите отдельных транзакций и обращений к БД трудоемки и малоэффективны	• позволяет применять механизм защиты отдельных транзакций;	• средства защиты транзакций и шифрования канала ограничены возможностями конкретной СУБД
Разграничение доступа			
• формирование бизнес-логики приложения напрямую отражено в политике доступа к его функциям и данным; • приложение абстрагировано от механизмов СУБД;	• высока вероятность ошибки при проектировании политики разграничения доступа при усложнении логики информационного сервиса	• готовые решения по разграничению доступа на уровне отдельных полей БД и формализованный механизм их интеграции в приложение	• зависимость информационного сервиса от конкретных механизмов разграничения доступа, применяемого в СУБД.

В результате анализа указанных способов и программных продуктов их реализующих, нельзя дать однозначное предпочтение одному из них. Наиболее предпочтительным является комбинированных подход, использующий достоинства обоих вариантов, и позволяющий избегать свойственные им недостатки.

Ниже представлена схема управления доступом к функциям и данным, на которой обозначены описанные методы:

- под цифрой 1 - реализация политики управления доступом средствами приложения
- под цифрой 2 - реализация политики управления доступом при помощи СУБД
- под цифрой 3 - реализация политики управления доступом комбинированным способом.

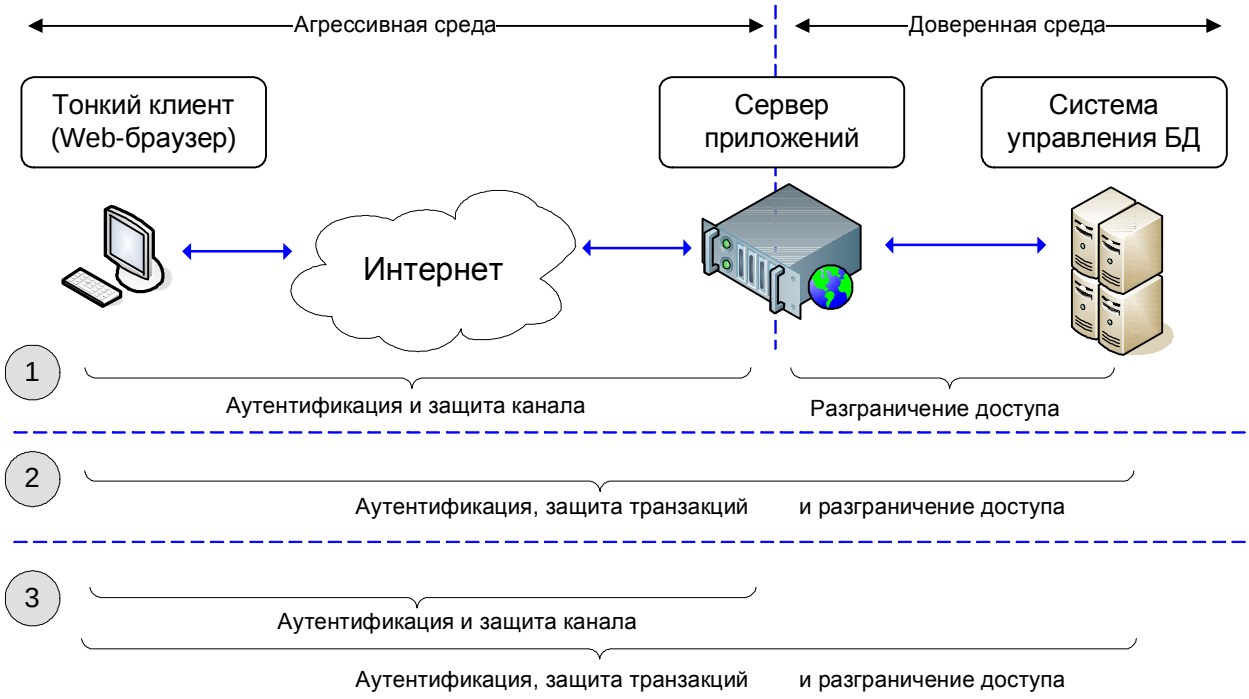

Рисунок 2. Сравнение способов управления доступом