В рамках цієї методики для кількісної оцінки якості експертів використовуються такі методи:

- евристичні, при використанні яких значення оцінок визначаються людиною. Методи евристичної оцінки засновані на тому, що подання, яке склалося про даного експерта у оточуючих (або у нього самого), досить правильно відображає його дійсну якість. Евристичні оцінки включають: самооцінку, оцінку колективу, оцінку експерта членами робочої групи;
- статистичні, при використанні яких значення оцінок визначаються в результаті обробки судження експертів про оцінювану продукцію;
- тестові, при використанні яких значення оцінок визначаються в результаті спеціальних випробувань, заснованих на вирішенні спеціально підібраних тестових завдань;
- документальні, при використанні яких значення оцінок визначаються на основі аналізу документальних даних про експертів;
- комбіновані, при використанні яких значення оцінок визначаються за допомогою будь-якої сукупності перерахованих вище методів.

Розробка автоматизованої методики формування груп експертів є складною аналітично-дослідницькою роботою, але дозволяє внести позитивні якості у діяльність експертної служби, покращити якість та результати при формуванні групи або команди, зменшити часові витрати на формування груп експертів для проведення експертиз.

Панферова И.Ю.

ВЫБОР МОДЕЛИ БАЗЫ ДАННЫХ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Исследованы характеристики основных моделей баз данных, проведена сравнительная качественная оценка основных моделей баз данных и их характеристик. Выявлены критерии оценки модели данных для выбора оптимальной модели.

Для обеспечения эффективной работы информационной системы необходимо правильно выбрать модель организации хранения данных. В настоящее время традиционная реляционная модель данных по-прежнему занимает господствующее положение. Несмотря на большие ограничения в формировании и управлении данными, реляционные базы данных сохраняют широкие возможности по настройке и предлагают довольно большой функционал. В случае если проектируется распределенная система, SQL СУБД не обеспечивают высокую производительность, т.к. затрачивают значительные системные ресурсы на обслуживание буферного пула, ведение журнала и обеспечение блокировок. NoSQL базы данных предлагают более простые способы горизонтального масштабирования (т.е. создание кластера из нескольких машин).

NoSQL убирает все ограничения реляционной модели (недостаточная производительность, трудоёмкое горизонтальное масштабирование, недостаточная производительность в кластере) и облегчает средства хранения и доступа к данным. Такие БД используют неструктурированный подход (создание структуры на лету), тем самым снимая ограничения жестких связей и предлагая различные типы доступа к специфическим данным. Такие бессхемные решения снимают ограничения с формирования сущностей и допускают хранения данных в виде ключ-значение.

Однако, если в системе важны надежность, сохранность данных и гарантии выполнения транзакций, предпочтение отдается SQL базам данных. Кроме того, при возникновении проблем, все же гораздо проще найти ответ, если дело касается реляционных систем, чем NoSQL.

Для решения проблем масштабируемости без отказа от ACID-транзакций и языка SQL разработан ряд новых систем и подходов, которые можно объединить под общим названием NewSQL.

Концепция NewSQL объединяет преимущества реляционных баз данных с распределенной архитектурой. Эти системы поддерживают SQL и ACID-транзакций, но отличаются от реляционных систем поддерживаемой функциональностью, имеют особенности проектирования схемы и доступа к данным. В информационных системах, где требуется обработка большого потока коротких транзакций, NewSQL-системы могут обеспечить гораздо более высокую производительность и масштабируемость.

Многие NewSQL базы данных хранят все данные в оперативной памяти, при этом ведется журнал операций и периодически скидывают снимки данных на диск. Эти системы позволяют достичь производительности, сравнимой с NoSQL-решениями, гарантируя согласованность данных. NewSQL-системы имеют новые архитектуры, повышают производительность за счет оптимизации скорости доступа к данным.

Существующее сегодня большое разнообразие систем и подходов к построению модели базы данных позволяет информационной системе наилучшим образом учитывать особенности предметной области, выбирать решения, обусловленные спецификой решаемого класса задач.

Погребняк К.А, Повтарев Д.В.

КРИТЕРИИ БЕЗОПАСНОСТИ ПУБЛИЧНЫХ ОБЛАЧНЫХ ХРАНИЛИЩ

В настоящее время существует большое разнообразие сервисов хранения данных в публичном облаке, количество которых постоянно возрастает. При использовании подобных сервисов информация пользователя копируется или перемещается на физические носители провайдера услуги. Определенные гарантии безопасного хранения данных и их использование в структуре информационных сетей организации, предоставляющей сервис хранения, становятся все более и более критичными для широкого круга пользователей. В то же время все еще не существует международных стандартов и технических спецификаций, регулирующих общие подходы к обеспечению информационной безопасности и определяющих рекомендованные безопасные протоколы передачи и хранения данных. Ввиду этого на данном этапе развития этого направления сервисов каждый провайдер разрабатывает и использует свои решения к общим подходам обеспечения безопасности хранения информации. Это приводит к тому, что конечный пользователь должен самостоятельно оценивать качество услуг с точки зрения защиты его личных данных. Часто выбор между сервисами является высокоприоритетной и рискованной задачей ввиду ценности информации. Поэтому актуальной задачей является разработка критериев безопасности для анализа существующих сервисов хранения информации в публичном облаке.

В ходе работы были определены следующие критерии сравнения относительно существенных характеристик безопасности:

1. Вход в систему и регистрация (ограничение на длину пароля; защита от атаки перебора пароля; двухфакторная аутентификация; механизм восстановления пароля).
2. Защищенный канал связи (протокол формирования защищенного канала связи; алгоритм аутентификации сообщений; алгоритм согласования ключей).
3. Безопасность хранения данных (алгоритм шифрования данных; владение ключом шифрования).
4. Безопасный обмен хранящимися файлами.
5. Дедупликация файлов
6. Безопасное использование нескольких устройств для доступа к информации.
7. Использование функций обновления программного обеспечения.