Безопасность баз данных

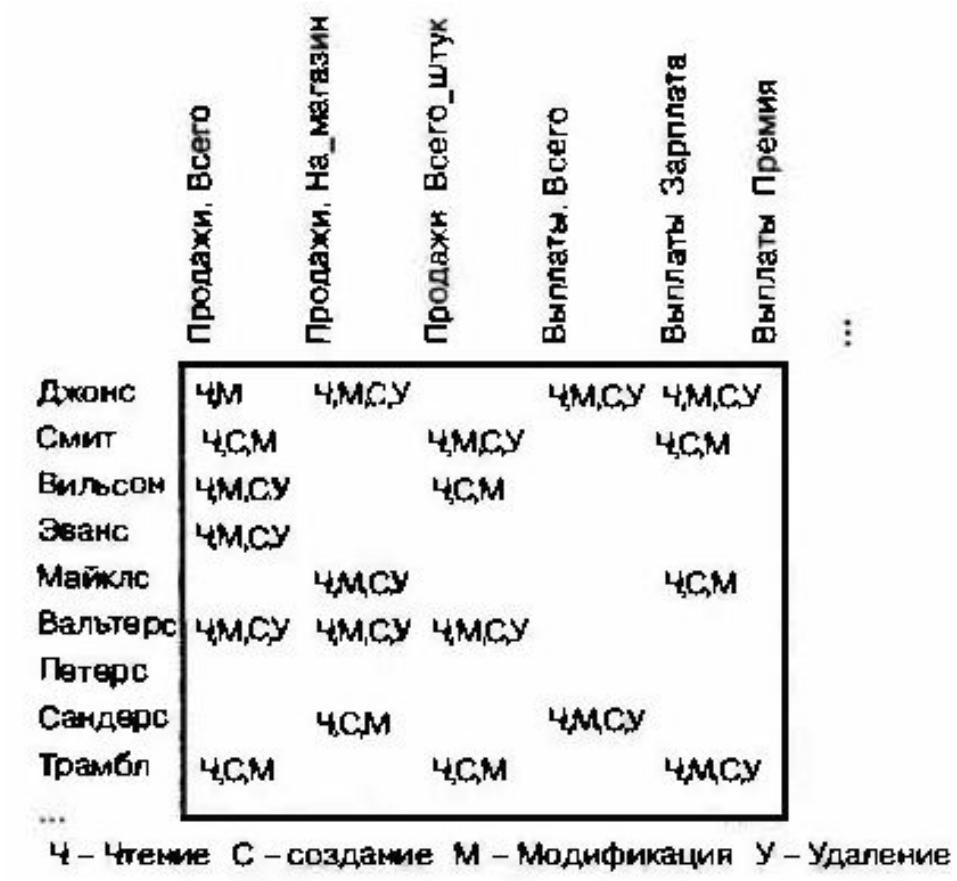
Распределённые базы данных и хранилища данных

Модели безопасности баз данных

- Простейшая модель безопасности баз данных:
- Проверка полномочий;
- Проверка подлинности.
- Модель многоуровневой безопасности баз данных.

Проверка полномочий

- Простая модель проверки полномочий

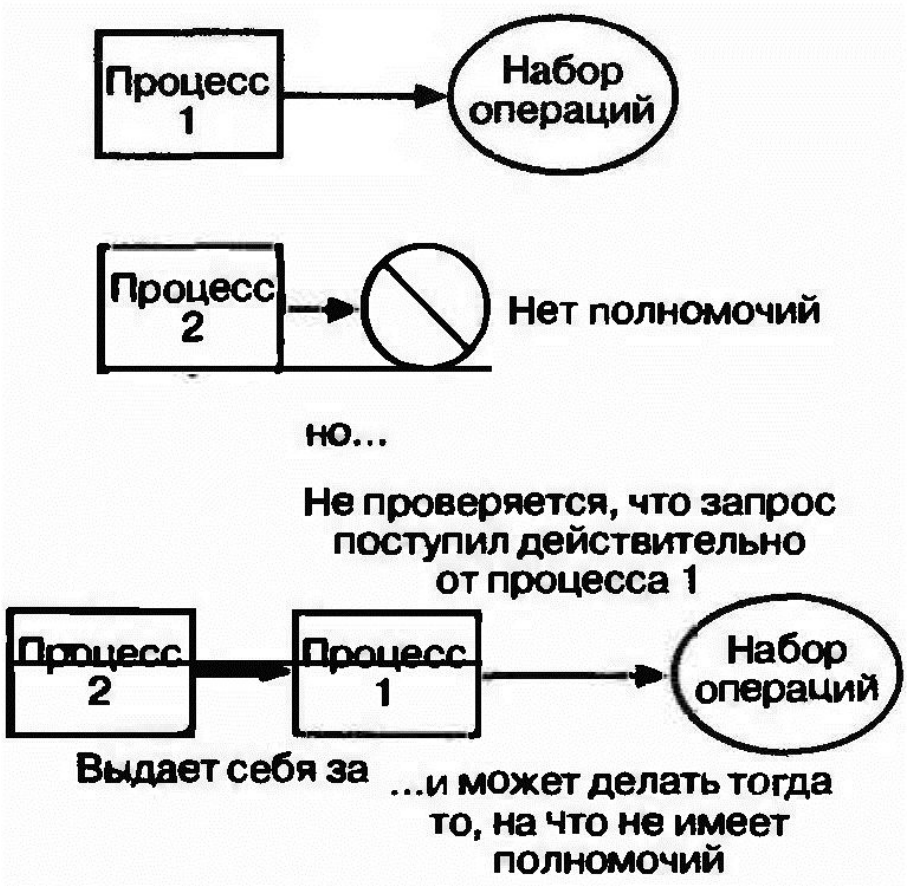


	Продажи. Всего	Продажи. На_магазин	Продажи Всего_штук	Выплаты. Всего	Выплаты Зарплата	Выплаты Премия	...
Джонс	Ч,М	Ч,М,С,У		Ч,М,С,У	Ч,М,С,У		
Смит	Ч,С,М		Ч,М,С,У		Ч,С,М		
Вильсон	Ч,М,С,У		Ч,С,М				
Эванс	Ч,М,С,У						
Майкле		Ч,М,С,У			Ч,С,М		
Вальтерс	Ч,М,С,У	Ч,М,С,У	Ч,М,С,У				
Петерс							
Сандерс		Ч,С,М		Ч,М,С,У			
Трамбл	Ч,С,М		Ч,С,М		Ч,М,С,У		
...							

Ч – Чтение С – создание М – Модификация У – Удаление

Проверка подлинности

- Необходимость проверки подлинности



Модель многоуровневой безопасности

Многоуровневая безопасность:

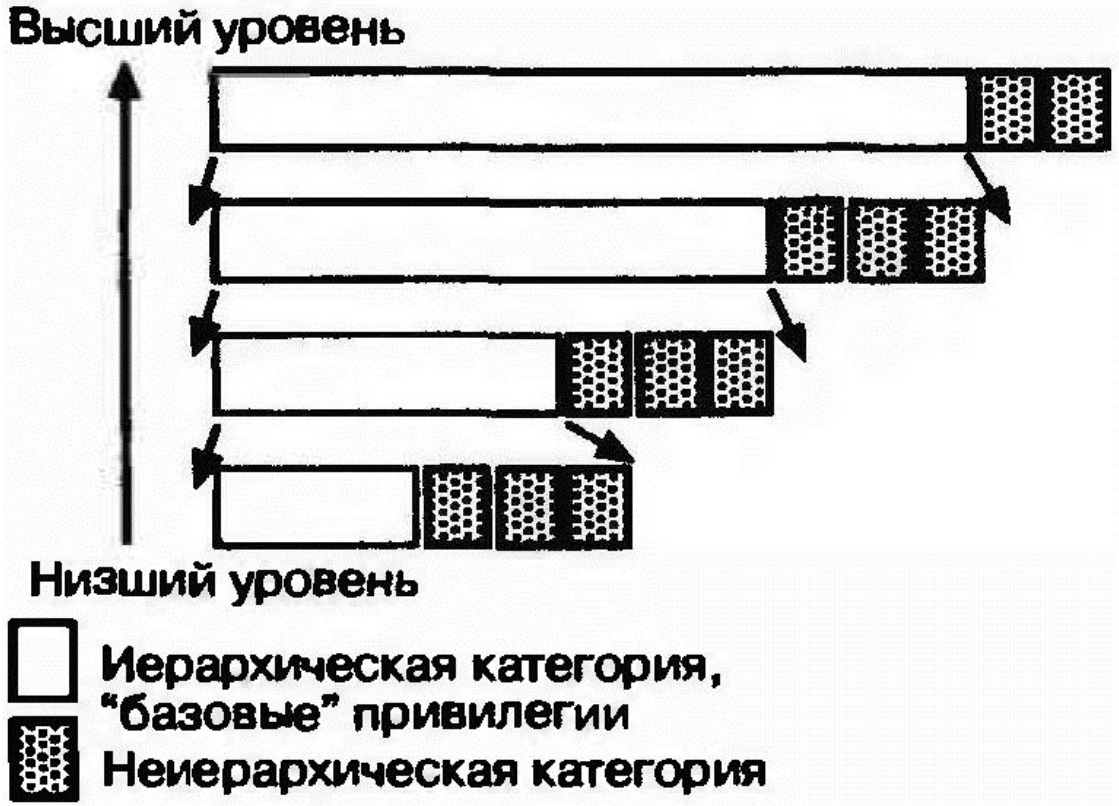
- в вычислительной системе хранится информация, относящаяся к разным классам безопасности;
- часть пользователей не имеет доступа к информации, относящейся к высшему классу безопасности.

Модель Белла-ЛаПадула:

- управления субъектами, т.е. активными процессами, запрашивающими доступ к информации;
- управление объектами, т.е. файлами, представлениями, записями, полями или другими сущностями информационной модели.

Модель Белла-ЛаПадула

- Решетка классов доступа

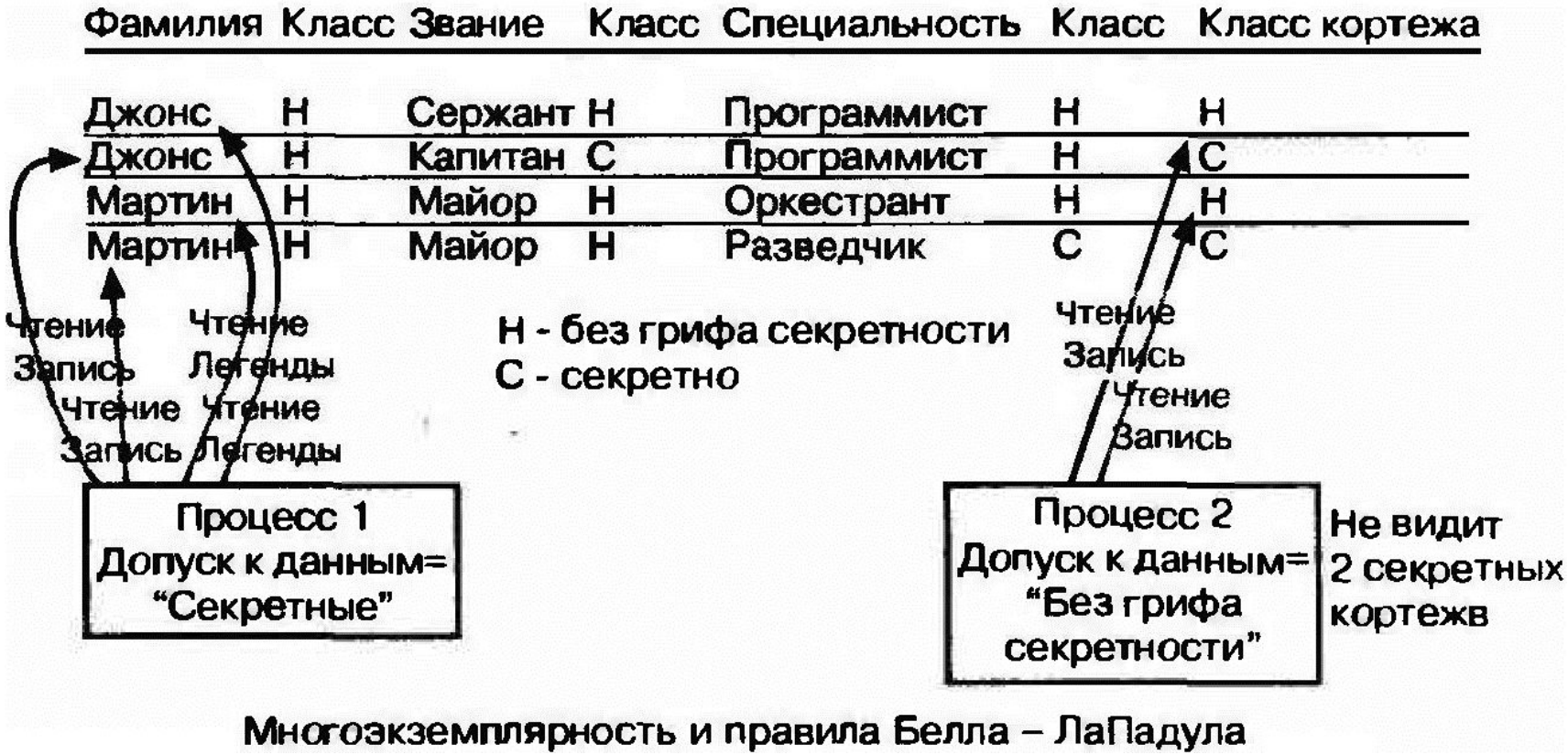


Модель Белла-ЛаПадула

- Пример применения правил доступа

Многоэкземплярность

- В рамках одного отношения может существовать множество кортежей с одним и тем же значением первичного ключа



Тайные каналы

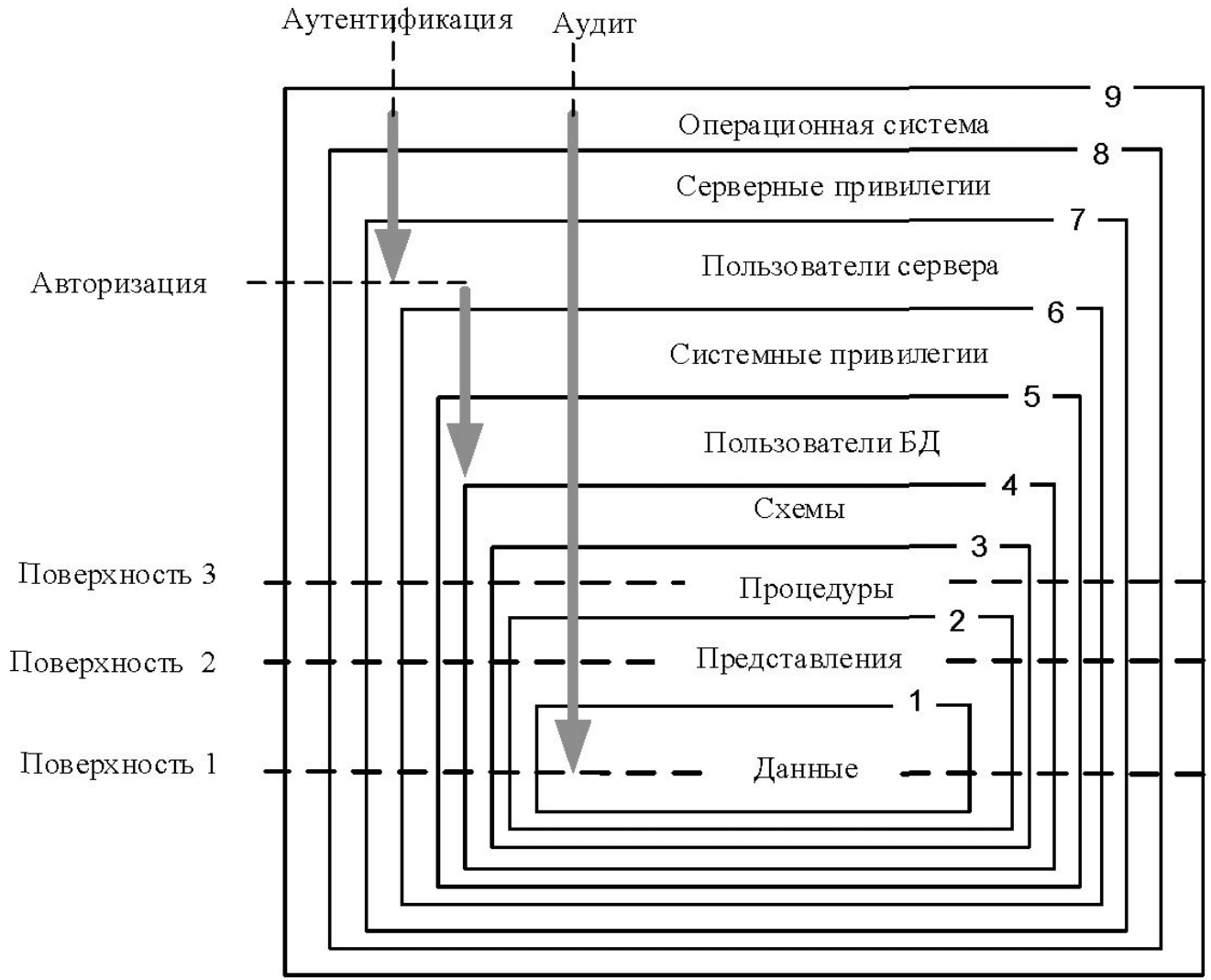
Типы тайных каналов:

- Тайные каналы памяти: некоторая область памяти прямо или косвенно используется как средство несанкционированного раскрытия конфиденциальной информации;
- Тайные каналы хронометража: измеряя время, необходимое процессу с низким уровнем допуска для передачи данных известного объема, и сравнивая эти данные с временем передачи конфиденциальной информации можно оценить объем передаваемых секретных данных.

Безопасная распределенная база данных

- Псевдомногоуровневый внутренний интерфейс для архитектуры безопасной распределенной СУБД

Обобщенная модель информационной безопасности СУБД



Обобщенная модель информационной безопасности СУБД

1. Уровень данных. Собственными объектами уровня являются реляционные таблицы базы данных.
2. Уровень представления. Собственными объектами уровня выступают представления, являющиеся поименованными и хранящимися в базе данных SELECT-запросами.
3. Уровень процедур. Объекты уровня представляют собой программные структуры: процедуры, функции, триггеры, пакеты процедур, функций и пользовательские типы.
4. Уровень схем. Схема – это поименованная совокупность объектов базы данных. С точки зрения информационной безопасности схема может определять группу объектов, доступных пользователю для выполнения заданного перечня операций.
5. Уровень пользователей базы данных. Основными объектами уровня являются пользователи базы данных, объектные привилегии и роли уровня базы данных.
6. Уровень системных привилегий. Системная привилегия – это элементарное разрешение, связанное с элементарной операцией для типа объекта. Системные привилегии назначает привилегированный пользователь – администратор базы данных.
7. Уровень пользователей сервера. Возможности серверного пользователя определяются назначенными ему серверными привилегиями.
8. Уровень серверных привилегий. Собственными объектами уровня являются серверные роли и профили безопасности.
9. Уровень операционной системы. На этом уровне база данных представляет собой набор файлов. Доступ к файлам данных и памяти процессов регулируется средствами операционной системы.

Подходы к безопасности

- Полный доступ всех пользователей к серверу базы данных;
- Разделение пользователей на доверенных и частично доверенных средствами СУБД;
- Введение системы аудита (логов действий пользователей) средствами СУБД;
- Введение шифрования данных; вынос средств аутентификации за пределы СУБД в операционные системы и промежуточное программное обеспечение; отказ от полностью доверенного администратора данных.

Проблемы обеспечения безопасности

- Проблемами безопасности серьезно занимаются только крупные производители прежде всего в ведущих продуктах линеек для хранения данных;
- Программисты баз данных, прикладные программисты и администраторы баз данных не уделяют должного внимания вопросам безопасности;
- Разные масштабы и виды хранимых данных требуют разных подходов к безопасности;
- Различные СУБД используют разные языковые диалекты для доступа к данным, организованным на основе одной и той же модели;
- Появляются новые виды и модели хранения данных.

Особенности систем баз данных как объекта защиты

- Система баз данных включает в себя два компонента: хранимые данные (собственно базы данных) и программы управления (СУБД).
- Уязвимости и вопросы безопасности СУБД можно разделить на две категории: зависимые от данных и независимые от данных.
- Архитектура применяемых языков и наборов функций напрямую связаны с моделью данных, применяемой для хранения информации. Модель определяет особенности языка, а особенности языка – наличие в нем уязвимостей.

Требования к безопасности

Независимые от данных:

- Функционирование в доверенной среде.
- Организация физической безопасности файлов данных.
- Организация безопасной и актуальной настройки СУБД.

Зависимые от данных:

- Безопасность пользовательского программного обеспечения.
- Безопасная организация данных и манипулирование ими.

Пути создания защищенных баз данных

- Разработка комплексных методик обеспечения безопасности хранилищ данных.
- Оценка и классификация угроз и уязвимостей СУБД.
- Разработка стандартных механизмов обеспечения безопасности.
- Разработка теоретической базы информационной защиты систем хранения и манипулирования данными.