

А. И. Баранчиков
П. А. Баранчиков
А. Н. Пылькин

Алгоритмы и модели ограничения доступа к записям баз данных



А. И. Баранчиков
П. А. Баранчиков
А. Н. Пылькин

Алгоритмы и модели ограничения доступа к записям баз данных

Москва
Горячая линия - Телеком
2023

УДК 621:391.
ББК 007:519.876
Б24

Рецензенты:

доктор техн. наук, профессор *Е. А. Саксонов*; кафедра «Вычислительные системы и сети» Московского государственного института электроники и математики (технический университет);

доктор техн. наук, профессор, *С. В. Скворцов*; кафедра «Систем автоматизированного проектирования вычислительных средств» Рязанского государственного радиотехнического университета.

Баранчиков А. И., Баранчиков П. А., Пылькин А. Н.

Б74 Алгоритмы и модели ограничения доступа к записям БД. – М.: Горячая линия – Телеком, 2023. – 182 с.: ил.

ISBN 978-5-9912-0203-9.

Рассмотрены вопросы проектирования защищенных баз данных с использованием ограничения доступа к отдельным записям. Рассмотрено как ограничение несанкционированного доступа к записям, так и предоставление ложной маскировочной информации вместо запрашиваемой.

Для специалистов и научных работников в области разработки информационных систем и защиты информации, квалифицированных программистов, будет полезна студентам и аспирантам.

ББК 007:519.876

Адрес издательства в Интернет WWW.TECHBOOK.RU

Научное издание

**Баранчиков Алексей Иванович, Баранчиков Павел Алексеевич,
Пылькин Александр Николаевич**

Алгоритмы и модели ограничения доступа к записям БД

Монография

Компьютерная верстка И. А. Благодаровой

Обложка художника В. Г. Ситникова

Подписано в печать 17.01.20123 Печать офсетная. Формат 60×88/16. Уч. изд. л. 11,35.

Тираж 500 экз. (4-й завод – 50 экз.)

ISBN 978-5-9912-0203-9

© А. И. Баранчиков, П. А. Баранчиков,
А. Н. Пылькин, 2011, 2023

© Издательство «Горячая линиям – Телеком», 2023

Оглавление

Введение.....	3
Глава 1. Современное ограничение доступа к информации в БД	4
1.1. Проектирование схем БД	4
1.1.1. Ограничение целостности данных.....	4
1.1.2. Уникальность ключей	5
1.1.3. Восстановление данных.....	6
1.1.4. Кластеры.....	7
1.1.5. Аномалия удаления	8
1.1.6. Борьба с аномалиями	8
1.1.7. БД реального времени.....	9
1.2. Современные разработки по ограничению доступа в БД	9
1.2.1. Гибкий доступ к БД.....	10
1.2.2. Тестирование ограничений доступа	12
1.2.3. Практические разработки для ограничения доступа к записям	14
1.2.4. Oracle RLS	14
1.2.5. Правила перезаписи запросов в PostgreSQL.....	15
1.2.6. Метки доступа в Linter	15
1.3. Модели ограничения доступа.....	17
1.3.1. Мандатная модель ограничения доступа.....	17
1.3.2. Дискреционная модель ограничения доступа	19
1.3.3. Ролевая модель ограничения доступа.....	19
1.3.4. Функциональная модель доступа	20
1.3.5. Кластеризационная модель ограничения доступа.....	21
1.4. Способы организации ограничения доступа	22
1.4.1. Использование сервера приложений	24
1.4.2. Использование интерфейса между клиентом и сервером	25
1.4.3. Создание отдельной таблицы для каждого класса записей сущности	25
1.4.4. Создание отдельного представления для каждого класса записей.....	28
1.4.4.1. Создание «динамического» представления пользователя.....	29
1.4.4.2. Выбор конкретного способа доступа на основе специфики задачи.....	32

1.5. Выводы.....	33
Глава 2. Ограничение доступа к записям таблиц БД.....	34
2.1. Конфликт ключей отношения	36
2.1.1. Блокировка изменений.....	40
2.1.2. Изменение доступа к записи	42
2.2. Ограничение доступа при использовании кластеризационной модели	46
2.3. Ограничение доступа при использовании мандатной модели	50
2.3.1. Изменения в дочерних отношениях.....	54
2.4. Ограничение доступа при использовании дискреционно-ролевой модели.....	57
2.4.1. Хранение привилегий в защищаемом отношении.....	60
2.4.2. Хранение привилегий в отдельном отношении.....	63
2.5. Ограничение доступа при функциональной модели	65
2.6. Выводы	69
Глава 3. Маскировка записей в таблицах БД.....	71
3.1. Применение маскировки данных	72
Проблема раскрытия маскировки	72
Области применения	74
3.2. Организация хранения истинной и ложной информации	76
3.2.1. Организация хранения ложной информации.....	79
3.2.2. Операции над незасекреченными данными.....	83
3.2.3. Декомпозиция отношения по принципу секретности	84
3.2.4. Хранение истинных и ложных записей в различных отношениях	86
3.2.5. Изменения дочерних отношений	90
3.3. Мандатный доступ.....	92
3.3.1. Ключи.....	96
3.3.2. Внешние ключи.....	96
3.4. Функциональный доступ	100
3.4.1. Маскировка атрибутов	104
3.4.2. Организация хранения	107
3.4.3. Реализация предиката определения доступа	110
Использование побитной карты.....	111
3.5. Синхронизация данных	112
3.5.1. Точки входа в алгоритм	113
3.5.2. Алгоритм проверки «лишних» записей	114

3.5.3. Алгоритм добавления «недостающих» ложных записей ...	115
3.5.4. Мандатная модель доступа	116
3.5.5. Ролевая модель доступа	118
3.5.6. Функциональная модель доступа	119
3.5.7. Автоматическая генерация ложных записей	121
3.6. Выводы.....	125
Глава 4. Практическая реализация предложенных алгоритмов и моделей	126
4.1. Испытания.....	126
4.1.1. ПО для тестирования запросов	129
4.1.2. Разработка хранимых процедур для различных СУБД.....	130
Имя пользователя	130
Мандат пользователя.....	131
4.2. Реализация дискреционно-ролевого доступа.....	132
4.2.1. Символьные идентификаторы владельца и группы (роли)	133
4.2.2. Числовые идентификаторы	135
4.2.3. Отношение с привилегиями.....	137
4.2.4. Тестовое отношение.....	139
4.2.5. Статистическая обработка	140
4.3. Реализация мандатного доступа.....	143
4.3.1. Ограничение доступа	145
4.3.2. Маскировка данных	149
4.4. Реализация функционального доступа	153
4.4.1. Ограничение доступа	154
4.4.2. Маскировка данных	163
4.5. Выводы.....	170
Заключение.....	171
Список использованных источников.....	173