Смирнов С. Н.

Безопасность систем баз данных. — М.: Гелиос АРВ, 2007. —352 с., ил.

В учебном пособии систематически изложены вопросы информационной безопасности систем баз данных. Представлена постановка задачи обеспечения информационной безопасности баз данных: классифицированы основные угрозы, отражена специфика, характерная для баз данных. Рассмотрены основные модели разграничения доступа. Наряду с классическими методами аутентификации, обеспечения целостности баз данных также обсуждаются вопросы шифрования элементов баз данных, реализации ролевой и мандатной модели доступа, технология избирательного аудита. Теоретические положения проиллюстрированы большим количеством примеров на основе СУБД Oracle.

Для студентов, обучающихся по специальностям группы «информационная безопасность» и направлениям подготовки, связанным с вычислительной техникой, аспирантов и специалистов, интересующихся технологиями обеспечения безопасности баз данных.

Оглавление

Защита информационных ресурсов России — стратегическая задача ... 3

Предисловие ... 6

Введение ... 9

1. Постановка задачи обеспечения информационной безопасности баз данных ... 17

1.1. Этапы научного формирования проблемы обеспечения информационной безопасности баз данных ... 17

1.2. Критерии качества баз данных ... 23

1.3. Сущность понятия безопасности баз данных ... 28

1.4. Основные подходы к методам построения защищенных информационных систем ... 30

1.5. Архитектура систем управления базами данных ... 35

1.6. Структура свойства информационной безопасности баз данных ... 41

2. Угрозы информационной безопасности баз данных ... 46

2.1. Источники угроз информации баз данных ... 48

2.2. Классификация угроз информационной безопасности баз данных ... 50

2.3. Угрозы, специфичные для систем управления базами данных ... 58

2.4. Объекты и субъекты моделей информационной безопасности баз данных на примере СУБД Oracle 62

Вопросы для самопроверки ... 68

3. Политика безопасности ... 71

3.1. Сущность политики безопасности ... 71

3.2. Цель формализации политики безопасности ... 71

3.3. Принципы построения защищенных систем баз данных 74
3.4. Стратегия применения средств обеспечения информационной безопасности 78
Вопросы для самопроверки 82
4. Атаки, специфические для баз данных 84
4.1. Подбор и манипуляция с паролями как метод реализации несанкционированных прав 84
4.2. Нецелевое расходование вычислительных ресурсов сервера 88
4.3. Использование триггеров для выполнения незапланированных функций 95
4.4. Использование SQL-инъекции для нештатного использования процедур и функций 97
Вопросы для самопроверки 104
5. Анализ методов аутентификации участников взаимодействия в процессе обработки баз данных.... ……105
5.1. Аутентификация, основанная на знании и защита от компрометации паролей 108
5.2. Аутентификация, основанная на наличии, и защита от компрометации 114
5.3. Аутентификация, основанная на биометрических характеристиках 117
5.4. Аутентификация пользователей в Oracle 121
5.5. Внешняя аутентификация пользователей Oracle 129
5.6. Аутентификация на основе инфраструктуры сертификатов 131
Вопросы для самопроверки 134
6. Методы дискреционного разграничения доступа 136
6.1. Реализация модели дискреционного управления

доступом в Oracle 137
6.2. Базовое понятие системы разграничения доступа — привилегии 139
6.3. Предоставление системных привилегий..... 141
6.4. Предоставление привилегий доступа к объекту 167
6.5. Отмена привилегий 171
Вопросы для самопроверки..... 173
7. Роли и разграничение доступа на основе ролей..... 175
7.1. Базовая ролевая модель разграничения доступа 177
7.2. Расширенные ролевые модели 182
7.3. Управление привилегиями с помощью ролей в СУБД Oracle 192
7.4. Управление допустимостью использования ролей……..196
7.5. Технология обеспечения конфиденциальности системы распределенных баз данных на основе ролевой модели доступа 199
Вопросы для самопроверки 203
8. Реализация мандатной модели доступа в СУБД Oracle 204
Вопросы для самопроверки 222
9. Шифрование элементов баз данных 224
9.1. Шифрование данных с неявным заданием ключа……224
9.2. Шифрование данных с явным заданием ключа..... 229
Вопросы для самопроверки 237
10. Статическая и динамическая проверка ограничений целостности 238
Вопросы для самопроверки 254
11. Обеспечение согласованности данных в многопользовательском режиме обработки 255
11.1.Понятие транзакции..... 255

11.2.Параллельная обработка данных
и уровни изоляции 261
11.3.Типы блокировок 267
Вопросы для самопроверки 269
12. Анализ включающей инфраструктуры 271
12.1.Архитектура сервера с позиций администратора
безопасности 271
12.2.Управление прослушивающим процессом 273
12.3.Управление доступностью табличных областей.....275
Вопросы для самопроверки..... 279
13. Аудит систем баз данных 281
13.1.Причины проведения аудита..... 281
13.2.Общая характеристика средств аудита СУБД 281
13.3.Аудит системных событий в Oracle..... 286
13.4.Аудит событий, связанных с доступом к объекту ……...291
13.5.Обработка данных аудита 294
13.6.Прекращение регистрации событий 297
13.7.Возможности избирательного аудита в Oracle..... 299
Вопросы для самопроверки 320
Заключение..... 322
Приложения 325
1.Перечень российских и международных стандартов в
области информационной безопасности 325
Российские и отраслевые стандарты..... 325
Безопасность информационных технологий..... 327
Алгоритмы идентификации и аутентификации 333
Пластиковые карты как инструмент идентификации
и аутентификации..... 333
Другие документы..... 337
2.Литература и источники в Интернет..... 338