

УДК 004.056.5(075)
ББК А68я7
А235

Рецензенты: д-р техн. наук, доц. С. Б. П о п о в,
д-р техн. наук, проф. В. А. Ф у р с о в

Агафонов, Антон Александрович
А235 **Безопасность систем баз данных:** учебное пособие /
А.А. Агафонов, А.С. Юмаганов. – Самара: Издательство
Самарского университета, 2023. – 272 с.

ISBN 978-5-7883-1916-2

Учебное пособие посвящено основам безопасности систем баз данных. В пособии рассматриваются задачи построения защищенной базы данных, которая обеспечивает конфиденциальность, доступность и целостность данных пользователя. Для решения задачи построения защищенной базы данных рассматриваются вопросы, связанные с ограничением доступа к данным, вопросы управления доступом к данным, создания учетных записей и настройки процедуры аутентификации, управления привилегиями. Также рассматриваются вопросы обеспечения доступности данных, создание резервных копий баз данных, настройка репликации данных, балансировки нагрузки, секционирования и сегментирования данных, мониторинга доступности баз данных. Отдельные разделы посвящены аудиту и шифрованию данных, а также SQL-инъекциям. Рассматриваются вопросы обеспечения целостности данных с использованием механизма транзакций и встроенных средств СУБД. Для иллюстрации примеров решения данных задач используются СУБД MySQL, PostgreSQL и MongoDB.

Предназначено для студентов института информатики и кибернетики, обучающихся по специальности 10.05.03 Информационная безопасность автоматизированных систем.

УДК 004.056.5(075)
ББК А68я7

ISBN 978-5-7883-1916-2

© Самарский университет, 2023

ОГЛАВЛЕНИЕ

Введение	9
1 Введение в безопасность систем баз данных.....	10
1.1 Понятие защищенной базы данных	10
1.2 Угроза информационной безопасности.....	13
1.3 Основные принципы обеспечения безопасности	17
1.3.1 Принцип системности.....	17
1.3.2 Принцип комплексности	18
1.3.3 Принцип непрерывности защиты	18
1.3.4 Принцип разумной достаточности	19
1.3.5 Принцип гибкости системы защиты.....	19
1.3.6 Принцип открытости алгоритмов и механизмов защиты	20
1.3.7 Принцип простоты применения средств защиты.....	20
1.4 Особенности систем баз данных как объекта защиты.....	21
1.4.1 Угрозы безопасности баз данных	23
1.4.2 Администрирование СУБД	24
2 Управление доступом к данным	29
2.1 Основные понятия.....	29
2.2 Модель управления доступом	31
2.2.1 Дискреционная модель управление доступом.....	32
2.2.2 Мандатная модель управления доступом	35
2.2.3 Ролевая модель управления доступом	37
2.2.4 Смешанная модель управления доступом	39
2.3 Управление привилегиями средствами языка SQL.....	39
3 Учетные записи. Аутентификация.....	46
3.1 Аутентификация в MySQL	47
3.2 Аутентификация в PostgreSQL.....	51
3.3 Аутентификация в MongoDB	59
4 Управление привилегиями	63
4.1 Привилегии MySQL	65

4.2 Привилегии PostgreSQL.....	70
4.3 Привилегии MongoDB	79
5 Резервное копирование	84
5.1 Основные понятия. Типы резервного копирования	84
5.1.1 Классификация резервного копирования по резервируемым данным	85
5.1.2 Классификация резервного копирования по способу создания	86
5.1.3 Классификация резервного копирования по доступности сервера	89
5.2 Факторы планирования резервного копирования	90
5.2.1 Показатели RTO и RPO	90
5.2.2 Возможность тестирования резервных копий	91
5.2.3 Характеристики базы данных	92
5.2.4 Ограничения на ресурсы	92
5.3 Стратегии резервного копирования	92
5.4 Общие рекомендации по резервированию данных	94
5.5 Резервное копирование в MySQL	96
5.5.1 Логическое резервное копирование в MySQL	98
5.5.2 Инкрементное резервное копирование в MySQL	101
5.6 Резервное копирование в PostgreSQL	102
5.6.1 Логическое резервное копирование в PostgreSQL	103
5.6.2 Резервное копирование на уровне файлов в PostgreSQL	106
5.6.3 Непрерывное архивирование в PostgreSQL	107
5.7 Резервное копирование в MongoDB	113
5.7.1 Физическое резервное копирование в MongoDB	114
5.7.2 Логическое резервное копирование в MongoDB	115
6 Репликация. Балансировка нагрузки	117
6.1 Понятие репликации	117
6.2 Типы репликации	118

6.3	Виды топологии репликации.....	120
6.3.1	Репликация с одним ведущим сервером	120
6.3.2	Репликация с несколькими ведущими серверами.....	122
6.3.3	Репликация без ведущих серверов	124
6.4	Балансировка нагрузки	126
6.5	Механизмы репликации в MySQL.....	128
6.5.1	MySQL. Репликация двоичных журналов	128
6.5.2	MySQL. Пример настройки репликации.....	131
6.6	Механизмы репликации в PostgreSQL	132
6.6.1	Физическая репликация в PostgreSQL.....	133
6.6.2	Логическая репликация в PostgreSQL	135
6.6.3	PostgreSQL. Пример настройки физической репликации.....	138
6.7	Репликация в MongoDB	139
6.7.1	MongoDB. Пример настройки репликации.....	140
7	Секционирование. Сегментирование	142
7.1	Основные понятия	142
7.2	Секционирование	143
7.2.1	Секционирование в MySQL	145
7.2.2	Секционирование в PostgreSQL.....	150
7.3	Сегментирование	153
7.3.1	Сегментирование в MongoDB.....	155
8	Аудит	167
8.1	Задачи аудита.....	167
8.2	Журнал аудита	168
8.3	Проблемы аудита.....	169
8.4	Методы аудита.....	169
8.4.1	Трассировка	169
8.4.2	Анализ журнала транзакций.....	170
8.4.3	Использование темпоральных данных.....	171
8.4.4	Аудиторские следы в данных.....	172

8.4.5 Мониторинг сетевого трафика сервера БД	172
8.4.6 Мониторинг сервера БД	173
8.5 Общие рекомендации	173
8.6 Возможности аудита в MySQL	174
8.6.1 Плагины аудита	175
8.6.2 Анализ серверных журналов	176
8.6.3. Анализ производительности	177
8.7 Возможности аудита в PostgreSQL	178
8.7.1 Протоколирование	178
8.7.2 Расширение PGAudit	181
8.8 Возможности аудита в MongoDB	181
8.8.1 Гарантия аудита	182
8.8.2 Настройка аудита	183
8.8.3 Настройка фильтрации	183
8.8.4 Сообщения аудита	186
9 Мониторинг	187
9.1 Мониторинг инфраструктуры	187
9.1.1 Уровни системы мониторинга	188
9.2 Мониторинг баз данных	190
9.3 Иерархия мониторинга	191
9.4 Мониторинг хранилища данных	192
9.4.1 Мониторинг соединения с хранилищем данных	192
9.4.2 Мониторинг процессов внутри базы данных	193
9.4.3 Мониторинг объектов базы данных	194
9.4.4 Мониторинг запросов к базе данных	195
9.5 Мониторинга в PostgreSQL	195
9.5.1 Примеры просмотра статистики	199
9.6. Системы мониторинга	201
9.6.1 Zabbix	201
9.6.2 Prometheus	205
10 Шифрование	210

10.1 Основные определения	210
10.2 Виды шифрования БД	212
10.2.1 Шифрование на уровне хранилища	212
10.2.2 Шифрование на уровне базы данных	213
10.2.3 Шифрование на уровне приложения	214
10.3 Риски шифрования данных	214
10.4 Шифрование подвижных данных	215
10.4.1 Использование шифрованного соединения	216
10.4.2 Использование защищённых туннелей	217
10.5 Шифрование в MySQL	218
10.5.1 Шифрование на уровне данных	218
10.5.2 Прозрачное шифрование данных	220
10.5.3 Защита соединений в MySQL	221
10.6 Шифрование в PostgreSQL	222
10.6.1 Шифрование на уровне полей данных	222
10.6.2 Защита соединений в PostgreSQL	225
10.7 Шифрование в MongoDB	226
11 SQL-инъекции	228
11.1 Основные понятия	228
11.2 Основные приёмы внедрения SQL кода	230
11.3 Типы SQL-инъекций	231
11.3.1 Классические SQL-инъекции	232
11.3.2 Слепые SQL-инъекции	236
11.4 База данных INFORMATION_SCHEMA	240
11.5 Противодействие SQL-инъекциям	242
11.5.1 Настройка прав доступа к учетным записям	242
11.5.2 Выдача клиентскому приложению «неинформативных» сообщений об ошибках	242
11.5.3 Фильтрация пользовательского ввода	242
11.6 Подготовленные выражения	245
12 Целостность данных	249

12.1 Основные понятия	249
12.2 Транзакции	252
12.2.1 Свойства транзакций.....	252
12.2.2 Блокировки.....	254
12.2.3 Проблемы совместного доступа к данным	255
12.2.4 Уровни изоляции транзакций.....	256
12.2.5 «Мертвые» блокировки	259
12.2.6 MVCC	260
12.3 Защита данных встроенными средствами СУБД	261
12.3.1 Представления	261
12.3.2 Хранимые процедуры и функции	264
12.3.3 Триггеры.....	266
Заключение.....	269
Библиографический список	270