

1. Проанализируем ЛВС

Анализ существующей в организации ЛВС показал, что технический ее уровень удовлетворяет требованиям сервера баз данных. А вот организационный требует доработок по каждому пункту.

Следующим группам пользователей необходимо разрешить подключение и аутентификацию на сервере БД:

- Бухгалтера (группа Accounting);
- Менеджеры по продажам (группа Sales);
- Логисты (группа Logistics);

А также, используя инструментальное средство администрирования СУБД, создать необходимые учетные записи для этих групп, и определить права доступа.

Также, этим группам пользователей необходимо разрешить следующие действия в разрабатываемой БД:

- Бухгалтера (группа Accounting) – просмотр всех таблиц;
- Менеджеры по продажам (группа Sales) – просмотр всех таблиц;
- Логисты (группа Logistics) – просмотр всех таблиц, вставка и редактирование следующих таблиц:

- Журнал операций;
- Объекты хранения;
- Склады;
- Места хранения;
- Единицы измерения;
- Типы операций.

Политика безопасности доступа к серверу баз данных включает в себя следующие требования:

1. Не осуществлять доступ к серверу баз данных с личных и общественных компьютеров, планшетов, смартфонов.

2. Не осуществлять доступ к серверу баз данных посредством домашних и общественных сетей передачи данных – публичные Wi-Fi сети и т.п.

3. Не сообщать свои учетные данные другим сотрудникам или третьим лицам, кроме как по письменному распоряжению директора по информационной безопасности.

4. Не реже, чем раз в три месяца, менять пароль от корпоративной учетной записи.

Мероприятия по обслуживанию сервера БД включают в себя:

- Процедура установки сервера MySQL.
- Процедура выгрузки базы данных в дамп базы данных.
- Процедура восстановления базы данных из дампа на сервере MySQL.
- Процедура создания новой учетной записи пользователя БД и делегирования ему прав доступа к базе данных или отдельным ее таблицам.
- Процедура резервного копирования базы данных.
- Процедура восстановления базы данных из резервной копии.
- Процедура мониторинга нагрузки на сервер БД.
- Процедура работы с журналом аудита базы данных.

Учетные записи на сервере MySQL могут быть созданы при помощи инструментального средства phpMyAdmin 5.2.1. На рисунке 1 показан процесс создания учетной записи для главного бухгалтера.

Сервер: 127.0.0.1:3306

Базы данных SQL Состояние Учетные записи пользователей Экспорт Импорт

Добавить учетную запись пользователя

Информация учётной записи

Имя пользователя: Использовать текстов SeniorAccountant

Имя хоста: Любой хост % ?

Пароль: Использовать текстов Стойкость: Сложный

Подтверждение:

Плагин аутентификации: Собственная проверка подлинности MySQL

Создать пароль: Генерировать 5h(qA)c_j)Op@/gW

База данных для учетных записей пользователей

Создать базу данных с таким же именем и предоставить на неё все привилегии.

Предоставить все привилегии на то, что подпадает под шаблон (имя пользователя_%).

Предоставить все привилегии в базе данных warehousing.

Рисунок 1. Создание учетной записи в phpMyAdmin.

На рисунке 2 показана процедура добавления прав на просмотр всех таблиц в БД пользователю «Главный бухгалтер» (SeniorAccountant).

Редактирование привилегий: Учетная запись пользователя 'SeniorAccountant'@'%' - База данных *warehousing*

Привилегии уровня базы данных Отметить все

Примечание: типы привилегий MySQL отображаются по-английски.

Данные

SELECT

INSERT

UPDATE

DELETE

Структура

CREATE

ALTER

INDEX

DROP

CREATE TEMPORARY TABLES

SHOW VIEW

CREATE ROUTINE

ALTER ROUTINE

EXECUTE

CREATE VIEW

EVENT

TRIGGER

Администрирование

GRANT

LOCK TABLES

REFERENCES

Вперёд

Рисунок 2. Редактирование привилегий учетной записи в phpMyAdmin.

На рисунках 3-4 показана процедура добавления прав на просмотр всех таблиц в БД пользователю «Младший логист» (JuniorLogistic).

