

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ

АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

ВОЕННЫЙ УЧЕБНЫЙ ЦЕНТР

РЕФЕРАТ

**Тема: «Предназначение, состав и особенности реализации механизмов защиты , встроенных в СУБД»**

**Выполнил:**

Студент 1810 взвода

Ю.Л. Попов

17 мая 2020 г.

**Проверил:**

преподаватель военно-учебного центра

А. П. Поляков

«\_\_» \_\_\_\_\_\_\_ 2020 г.

Москва 2020

Содержание

[Введение 3](#__RefHeading___Toc371_1084908452)

[Немного о СУБД 4](#__RefHeading___Toc483_1084908452)

[Средства обеспечения безопасности доступа, используемые в известных СУБД 7](#__RefHeading___Toc589_1084908452)

[Почему невозможно обеспечить информацию только средствами ОС? 8](#__RefHeading___Toc375_1084908452)

# Введение

Основной целью данной работы является введение в само понятие СУБД, обзор реализаций механизмов защиты встроенных в СУБД и получение ответа на вопрос: «Почему для обеспечения безопасности СУБД недостаточно средств защиты ОС?»

# Немного о СУБД

Давайте разберёмся с терминами и понятиями баз данных:

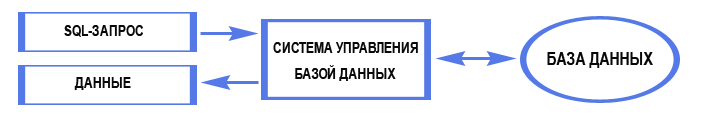
***База данных*** - набор сведений, хранящихся некоторым упорядоченным способом.

Можно сравнить базу данных со шкафом, в котором хранятся документы. Иными словами, база данных - это хранилище данных. Сами по себе базы данных не представляли бы интереса, если бы не было систем управления базами данных (СУБД).

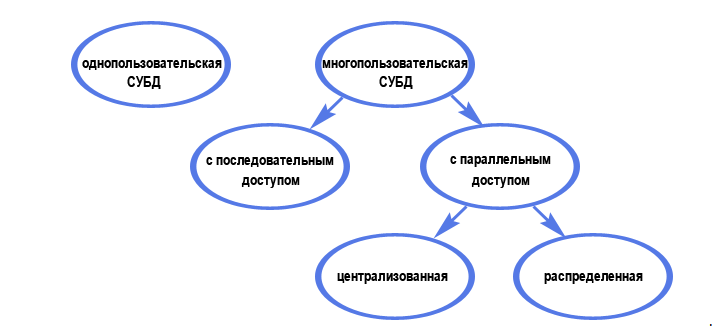
***Система управления базами данных(СУБД)*** - это совокупность языковых и программных средств, которая осуществляет доступ к данным, позволяет их создавать, менять и удалять, обеспечивает безопасность данных и т. д.

В общем СУБД - это система, позволяющая создавать базы данных и манипулировать сведениями из них. А осуществляет этот доступ к данным СУБД посредством специального языка — SQL.

***SQL*** - язык структурированных запросов, основной задачей которого является предоставление простого способа считывания и записи информации в базу данных.  
  
Итак, простейшая схема работы с базой данных выглядит примерно так:



По характеру использования СУБД делят на однопользовательские (предназначенные для создания и использования БД на персональном компьютере) и многопользовательские (предназначенные для работы с единой БД нескольких компьютеров, объединённых в локальные сети).



Нас интересуют многопользовательские БД. Самый распространённый тип БД — реляционной

Именно о нем мы и поговорим

Реляционные базы данных состоят из таблиц. Каждая таблица состоит из столбцов и строк Таблицы в реляционных базах данных обладают рядом свойств. Основными являются следующие:

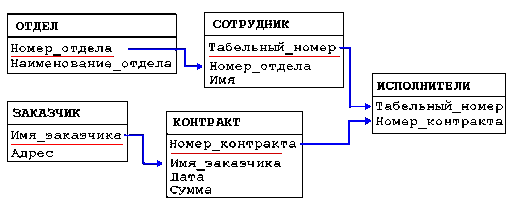
* В таблице не может быть двух одинаковых строк.
* Столбцы располагаются в определённом порядке, который создаётся при создании таблицы. В таблице может не быть ни одной строки, но обязательно должен быть хотя бы один столбец.
* У каждого столбца есть уникальное имя (в пределах таблицы), и все значения в одном столбце имеют один тип (число, текст, дата...).
* На пересечении каждого столбца и строки может находиться только значение

Рассмотрим, как хранится в памяти простейшая БД:

Как уже говорилось раньше, БД — это набор таблиц и связи между ними. Например, нам нужно хранить информацию об исполнителе: табельный номер и номер контракта. Но нам также необходимо знать, что это за сотрудник и в каком отделе он работает. Вопрос как же тогда хранить столько связей?

Для этого придумали создавать несколько таблиц, где каждая ячейка может указывать на ещё одну таблицу. Итак, у нас итоговая таблица по исполнителю, которая хранит его табельный номер и номер контракта. Если мы хотим узнать более подробно, про табельный номер, мы можем перейти в таблицу, где такой номер есть и посмотреть кому он принадлежит. В нашем случае, мы попадём в таблицу «Сотрудник», и узнаем его имя и номер отдела. А если в нашей организации много отделов и мы не помним у какого отдела какой номер? Не проблема! Для этого сделаем ещё одну таблицу «Отдел», в котором будет сопоставляться номер отдела и его наименование.

Таким образом, наша БД, представляет собой множество таблиц, и ссылки, по которым мы можем переходить и получать более подробную информацию.



# Средства обеспечения безопасности доступа, используемые в известных СУБД

Существенным аспектом СУБД является защита данных. В современных СУБД поддерживается как избирательный, так и обязательный подходы к обеспечению безопасности данных. В случае избирательного управления, некий пользователь обладает различными правами, или привилегиями, и полномочиями при работе с различными объектами. В случае обязательного управления, каждому объекту присваивается некий квалификационный уровень, а каждому пользователю предоставляются права доступа к тому или иному уровню.

Как правило, для идентификации и проверки подлинности пользователя применяется либо соответствующий механизм операционной системы, либо функциональные возможности SQL-оператора «connect».

В момент начала сеанса работы с сервером базы данных пользователь идентифицируется под своим логином, а средством аутентификации служит пароль. Все операции над базой данных, которые будут выполнены после этого, СУБД связывает с конкретным пользователем, который запустил приложение.

Одна из проблем защиты данных возникает по той причине, что при работе с базами данных инициируются процессы, которые могут запускаться как пользователями, так и прикладными программами. Одно из решений проблемы заключается в том, чтобы прикладной программе также были предоставлены некоторые привилегии доступа к объектам базы данных. В этом случае пользователь, не обладающий специальными привилегиями доступа к некоторым объектам базы данных, может запустить прикладную программу, которая имеет такие же привилегии. В СУБД «Oracle» решение данной проблемы обеспечивается использованием механизма ролей. Роль представляет собой именованный объект, хранящийся в базе данных, и связывается с конкретной прикладной программой для придания последней привилегий доступа к базам данных, таблицам, представлениям и процедурам базы данных. Роль создаётся и удаляется администратором базы данных, ей может быть придан определённый пароль. Как только роль создана, ей можно предоставить привилегии доступа к объектам базы данных.

Ещё одним эффективным способом обеспечения безопасности является шифрование данных.

Современные СУБД включают резервное копирование и аудит как непременные составляющие системы безопасности.

# Почему невозможно обеспечить информацию только средствами ОС?

Чтобы обеспечить безопасность СУБД, для начала нужно ответить на вопрос: кто в компании вообще пользуется базой данных и имеет к ней доступ?

Существует три большие группы пользователей СУБД, которых условно можно назвать **операторами; аналитиками; администраторами**.

* *Операторы - это*  те, кто либо заполняет базу данных (вводят туда вручную информацию о клиентах, товарах и т. п.), либо выполняют задачи, связанные с обработкой информации: кладовщики, отмечающие перемещение товара, продавцы, выписывающие счета и т. п.
* *Аналитики — это*  те, ради кого, собственно, создаётся эта база данных: логистики, маркетологи, финансовые аналитики и прочие. Эти люди по роду своей работы получают обширнейшие отчеты по собранной информации.
* Администраторы - Эта категория людей может только в общих чертах представлять, что хранится и обрабатывается в хранилище данных. Но они решают ряд важнейших задач, связанных с жизнеобеспечением системы, ее отказо- и катастрофоустойчивости.

Но различные роли по отношению к обрабатываемой информации - не единственный критерий. Указанные группы различаются еще и по способу взаимодействия с СУБД

Операторы чаще всего работают с информацией через различные приложения. Для данные группы пользователей безопасность необходимо обеспечивать встроенными средствами СУБД. И чаще всего о безопасности СУБД судят только по этому критерию. Но это неправильно! Беда в том, что основные проблемы с безопасностью приходятся на две оставшиеся категории пользователей.

Проблема с аналитиками заключается в том, что они работают с СУБД на уровне ядра. Они должны иметь возможность задавать и получать всевозможные выборки информации из всех хранящихся там таблиц. Вот тут как раз необходимы средства защиты ОС!

С администраторами дело обстоит ненамного лучше. Начиная с того, что в крупных информационных системах их число сопоставимо с числом аналитиков. И хотя абсолютно полными правами на СУБД наделены лишь два-три человека, администраторы, решающие узкие проблемы (например резервное копирование данных), все равно имеют доступ ко всей информации, хранящейся в СУБД. А для обеспечения безопасности от этой группы пользователей необходим комплексный подход: средства СУБД + средства ОС

БД отличается от обычного файла на локальном компьютере тем, что БД хранится на удалённом сервере и каждый, желающих получить доступ к БД должен подключиться к этому серверу.

Подводя итог, если говорить простыми словами, то на стороне сервера безопасность обеспечивается средствами защиты СУБД, а на стороне клиента безопасность обеспечивается средствами защиты ОС.