|  |  |
| --- | --- |
|  | **Министерство науки и высшего образования Российской Федерации**  **Федеральное государственное бюджетное образовательное учреждение**  **высшего образования**  **«Московский государственный технический университет**  **имени Н.Э. Баумана**  **(национальный исследовательский университет)»**  **(МГТУ им. Н.Э. Баумана)** |

ФАКУЛЬТЕТ Информатика и системы управления

КАФЕДРА Информационная безопасность

**РАСЧЕТНО-ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

***К КУРСОВОЙ РАБОТЕ***

***НА ТЕМУ:***

***Разработка защищенной БД информационной системы «Поликлиника»***

Студент \_\_\_ИУ8-85\_\_\_\_\_ **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_**

(Группа) (Подпись, дата) (И.О.Фамилия)

Руководитель курсовой работы **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** Е. В. Глинская

(Подпись, дата) (И.О.Фамилия)

Москва, 2021 г.

**Министерство науки и высшего образования Российской Федерации**

**Федеральное государственное бюджетное образовательное учреждение**

**высшего образования**

**«Московский государственный технический университет имени Н.Э. Баумана**

**(национальный исследовательский университет)»**

**(МГТУ им. Н.Э. Баумана)**

УТВЕРЖДАЮ

Заведующий кафедрой ИУ8

(Индекс)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_М.А.Басараб

(И.О.Фамилия)

« \_\_\_\_\_ » \_\_февраля\_\_ 2021 г.

**ЗАДАНИЕ**

**на выполнение курсовой работы**

по дисциплине \_\_Безопасность систем баз данных\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Студент группы \_ИУ8-85\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Романчук Юрий Владиславович\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Фамилия, имя, отчество)

Тема курсовой работы: Разработка защищенной БД информационной системы «*Поликлиника*».

Направленность КР (учебная, исследовательская, практическая, производственная, др.)

\_\_\_учебно-практическая\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Источник тематики (кафедра, предприятие, НИР) \_кафедра ИУ8 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

График выполнения КР: 25% к \_4\_ нед., 50% к \_7\_ нед., 75% к \_12\_ нед., 100% к \_15\_ нед.

Техническое задание: Проанализировать существующую проблему информационной безопасности и защиты информации в базах данных информационной системы «Поликлиника». Представить решение проблемы информационной безопасности и защиты информации в базах данных информационной системы « Поликлиника».\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

***Оформление курсовой работы:***

Расчетно-пояснительная записка на 33 листах формата А4.

Перечень графического (иллюстративного) материала (чертежи, плакаты, слайды и т.п.)

\_\_Презентация\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_Флешка\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Дата выдачи задания «\_12\_\_» \_февраля\_ 2021 г.

**Руководитель курсовой работы**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е. В. Глинская

(Подпись, дата) (И.О.Фамилия)

**Студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** Ю. В. Романчук

(Подпись, дата) (И.О.Фамилия)

Оглавление

[**Введение** 4](#_Toc69927517)

[Основная часть 5](#_Toc69927518)

[Анализ предметной области 5](#_Toc69927519)

[Проектирование базы данных 6](#_Toc69927520)

[Подход к проектированию 6](#_Toc69927521)

[Построение инфологической (концептуальной) модели предметной области 6](#_Toc69927522)

[Ограничение целостности 10](#_Toc69927523)

[Физическая реализация базы данных 11](#_Toc69927524)

[Разработка средств защиты 27](#_Toc69927525)

[Аутентификация 27](#_Toc69927526)

[Форма регистрации сотрудника в системе 27](#_Toc69927527)

[Средства защиты от НСД и разграничение доступа 28](#_Toc69927528)

[Резервное копирование 28](#_Toc69927529)

[Заключение 32](#_Toc69927530)

[Список использованных источников 33](#_Toc69927531)

**Введение**

База данных - совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимая от прикладных программ. Иначе говоря, база данных – это электронное хранилище информации, которая имеет свою определённую функциональную структуру. В настоящее время почти любая большая компания, организация или предприятие использует электронные базы данных для хранения большого количества информации. Такие базы предоставляют высокую скорость работы с большим количеством данных и её безопасное хранение. В частности, безопасности баз данных уделяется большое значение: система должна обладать таким набором программных и аппаратных средств, чтобы обеспечивалась целостность, конфиденциальность и доступность информации.

Для создания базы данных и работы с ними существуют различные системы управления базами данных (СУБД) – комплекс программ, позволяющих создать базу данных и манипулировать данными. Такие программные средства предоставляют возможность реализовывать информационные системы, которые будут использовать структурированную информацию из базы данных, которая будет предоставляться на основе описанных разработчиком правил.

В настоящее время существует необходимость реализовывать информационные системы для различных сфер жизни, которые используют базы данных: интернет-магазины, различные веб-сайты и приложения. В частности, существуют приложения, которые используются для учета сотрудников, пациентов и кабинетов в различных медицинских учреждениях, а также составления расписания приема пациентов в данных учреждениях.

Целью данной работы является проектирования и разработка базы данных для удобного учета сотрудников, пациентов и оказанных им услуг. А также для удобного составления расписания приема врачей и специального персонала.

# Основная часть

## Анализ предметной области

При выполнении работы была выбрана следующая задача: Информационная система «Апгрейд ПК». В рамках этой задачи необходимо разработать БД, которая автоматизировала бы процесс учета сотрудников и клиентов, а также заказов и их транспортировки.

Для корректной работы и сохранения целостности, конфиденциальности данных необходима реализация процесса администрирования и авторизации: введение пользователя с соответствующими правами и реализация возможности авторизации с помощью логина и пароля. Доступ к системе в течение сессии будет осуществляться при помощи JWT, который будет генерироваться при успешной авторизации. Также необходимо обеспечить непрерывный доступ к системе, т.е. обеспечить резервное копирование данных.

Необходимо обеспечить разграничение доступа, так как администраторы, сотрудники и клиенты должны обладать разными уровнями прав доступа к системе. В рамках реализации системы администратор должен обладать правами для добавления и редактирования информации о сотрудниках, клиентах, заказах, а также приемных пунктах. Сотрудник должен иметь доступ только к связанным с ним заказам. Клиент также должен иметь доступ к своим заказам, но, в отличие от сотрудника, не должен иметь права изменять информацию.

Знакомство с теорией построения баз данных было произведено с помощью источника [1].

## Проектирование базы данных

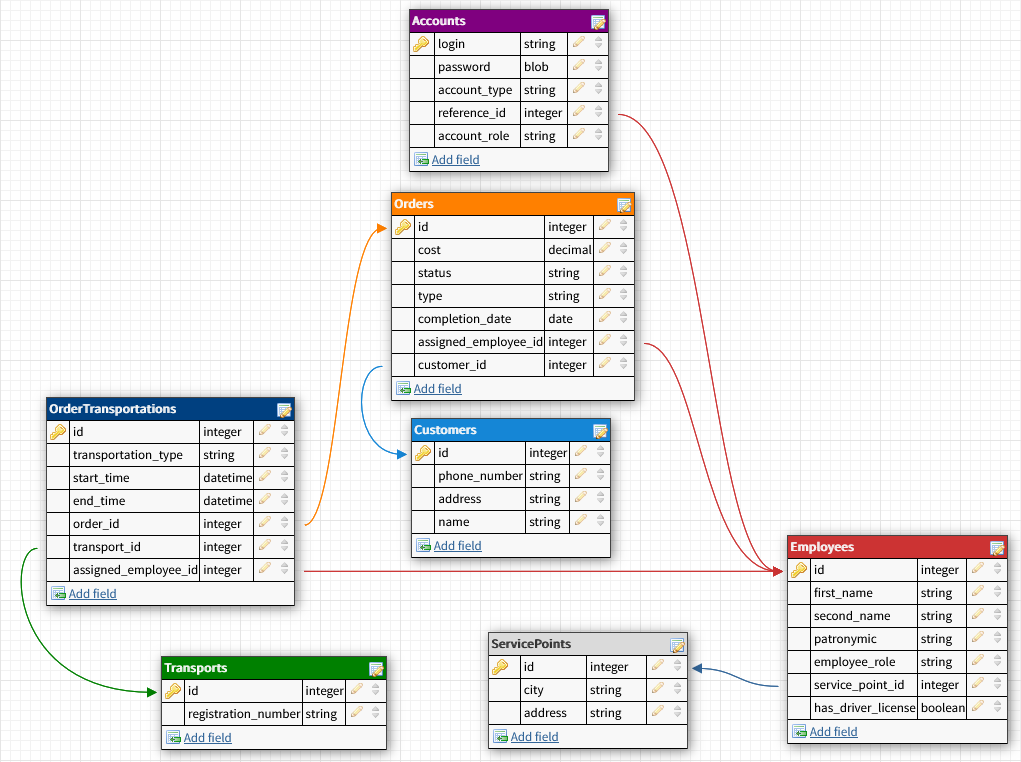
### Подход к проектированию

Для системы «Апгрейд ПК» необходима база данных, которая будет обеспечивать конфиденциальность, целостность, доступность данных, а также будет быстро функционировать, не требуя большого объема занимаемой памяти. Важным критерием является простота использования и реализации.

В качестве СУБД была взята PostgreSQL, а для обеспечения возможности авторизации и реализации разграничения прав доступа использован веб-сервис, написанный на языке программирования Java. Система удовлетворяет описанным выше требованиям [2].

### Построение инфологической (концептуальной) модели предметной области

На рисунке 1 изображена схема базы данных и установленные связи между сущностями:



**Рис.** 1 – схема БД

В каждой таблице имеется уникальное поле id, которое является первичным ключом таблицы (primary key).

В базе данных имеются следующие таблицы и поля:

* ServicePoints – приемные пункты.
  + City – город, в котором расположен приемный пункт
  + Address – адрес приемного пункта
* Employees – сотрудники.
  + First\_name – имя сотрудника
  + Second\_name – фамилия сотрудника
  + Patronymic – отчество сотрудника
  + Employee\_role – специализация сотрудника (категория его прав и обязанностей)
  + Service\_point\_id – идентификатор приемного пункта
  + Has\_driver\_license – флаг, обозначающий, имеет ли данный сотрудник водительские права для доставки/сбора аппаратуры у клиентов, а также перемещения аппаратуры между приемными пунктами и стационарным цехом
* Transports – транспортные средства, которые используются для перевозки аппаратуры.
  + Registration\_number – регистрационный номер транспортного средства.
* Customers – клиенты.
  + Phone\_number – телефонный номер клиента для связи
  + Address – адрес клиента, необходимый для доставки аппаратуры или осуществления заказов на дому.
  + Name – имя клиента
* Orders – заказы.
  + Cost – стоимость заказа
  + Status – статус готовности заказа
  + Type – тип заказа (срочный, стандартный, на дому)
  + Completion\_date – ожидаемое время выполнения заказа.
  + Assigned\_employee\_id – идентификатор сотрудника, который выполняет данный заказ
  + Customer\_id – идентификатор клиента, осуществившего заказ
* OrderTransportations – информация о перемещении заказа (между приемными пунктами и стационарным цехом или заказчиком).
  + Transportation\_type – тип перемещения заказа (между приемными пунктами и стационарным цехом или заказчиком)
  + Start\_time – ожидаемое время начала транспортировки
  + End\_time – ожидаемое время окончания транспортировки (для распределения и отслеживания свободных транспортных средств для доставки)
  + Order\_id – идентификатор заказа, который перевозится
  + Transport\_id – идентификатор транспортного средства, на котором осуществляется перевозка
  + Assigned\_employee\_id – идентификатор сотрудника, осуществляющего перевозку.
* Accounts – учетные записи администраторов, сотрудников и клиентов.
  + Login – уникальный логин учетной записи
  + Password – пароль (зашифрованный при помощи средств базы данных)
  + Account\_type – тип аккаунта (сотрудник или клиент)
  + Account\_role – права, которыми обладает владелец аккаунта.
  + Reference\_id – идентификатор сотрудника или клиента в зависимости от типа аккаунта

Целостность данных обеспечена наличием внешних ключей. Связи, образованные внешними ключами, изображены на рисунке 1.

### Ограничение целостности

Целостность – это актуальность и непротиворечивость информации; защищенность от разрушения и несанкционированного изменения.

Ограничение целостности – это набор специальных предложений, описывающих допустимые значения отдельных информационных единиц и связей между ними. Нарушение ограничений целостности может происходить по нескольким причинам: ошибки, преднамеренное нарушение, вирусы, сбои. Поэтому необходимо контролировать ограничения целостности.

Для данной предметной области можно выделить следующие ограничения целостности:

* + Ключевые поля каждой таблицы должны иметь непустые и уникальные значения;
  + Поле Login в таблице «Accounts» должно быть уникальным;
  + Поле Registration\_number в таблице «Transports» должно быть уникальным.
  + Значение поля Reference\_id в таблице «Accounts» должно присутствовать либо в таблице «Employees», либо в таблице «Customers».

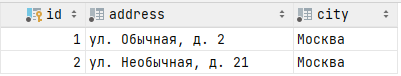
Для обеспечения целостности таблиц также будут использоваться дополнительные меры защиты информации, такие как авторизация, аутентификация и разграничение доступа.

### Физическая реализация базы данных

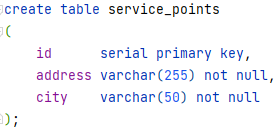
#### Таблицы

Для реализации информационной системы были реализованы 7 таблиц.

##### Таблица service\_points

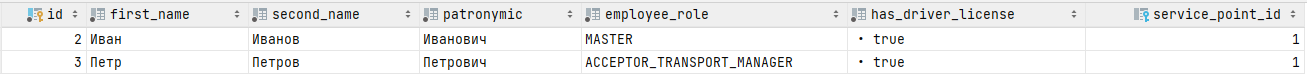


**Рис. 2.** Таблица service\_points.

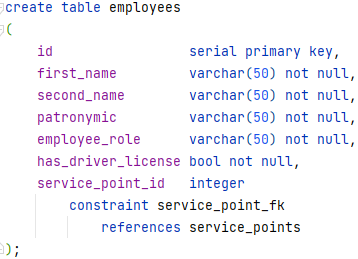


**Рис. 3.** Скрипт для создания таблицы service\_points.

##### Таблица employees

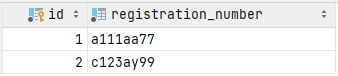


**Рис. 4.** Таблица employees.

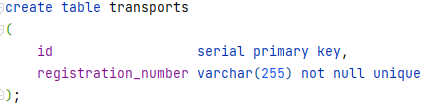


**Рис. 5.** Скрипт для создания таблицы employees.

##### Таблица transports

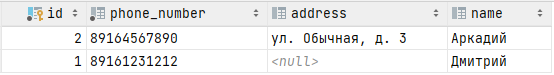


**Рис. 6.** Таблица transports.

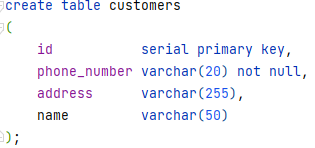


**Рис. 7.** Скрипт для создания таблицы transports.

##### Таблица customers

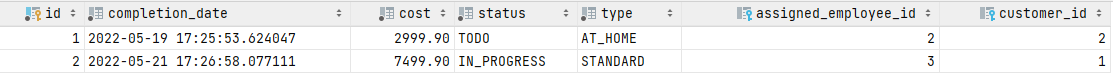


**Рис. 8.** Таблица customers.

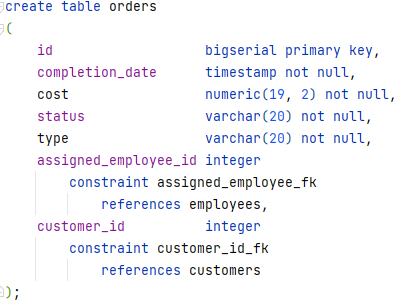


**Рис. 9.** Скрипт для создания таблицы customers.

##### Таблица orders



**Рис. 10.** Таблица orders.

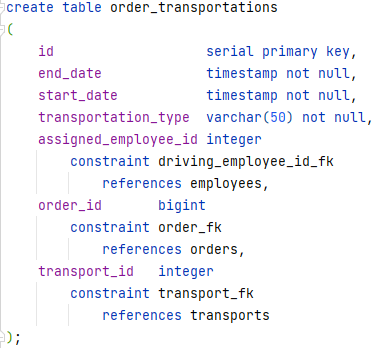


**Рис. 11.** Скрипт для создания таблицы orders.

##### Таблица order\_transportations

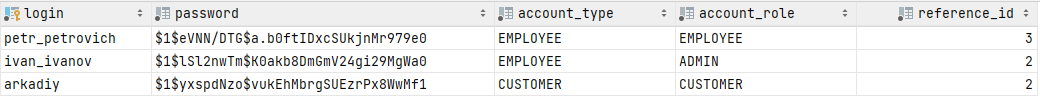


**Рис. 12.** Таблица order\_transportations.

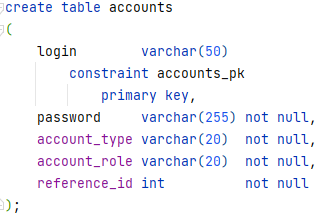


**Рис. 13.** Скрипт для создания таблицы order\_transportations.

##### Таблица accounts



**Рис. 14.** Таблица accounts.



**Рис. 15.** Скрипт для создания таблицы accounts.

#### Запросы

На втором этапе разработки физической модели были созданы запросы [3]. В базе данных есть следующие запросы:

1. Запрос авторизации
2. Список приемных пунктов для заданного города
3. Данные заказа по его номеру (идентификатору)
4. Список заказов заданного клиента
5. Время освобождения заданного автобуса от транспортировки
6. Данные клиента по номеру заказа
7. Список заказов, исполняемых заданным сотрудником
8. Отчет по заказам клиента

##### Запрос авторизации

Запрос авторизации позволяет найти аккаунт пользователя по данному логину и паролю. При сохранении в базу данных пароль хешируется при помощи функций crypt и gen\_salt пакета pgcrypto. Запрос на добавление аккаунта:



**Рис. 16.** Запрос на добавление аккаунта.

При использовании запроса на добавление аккаунта, приведенного на рисунке 16, запрос авторизации выглядит следующим образом:

**Рис. 17.** Запрос авторизации.

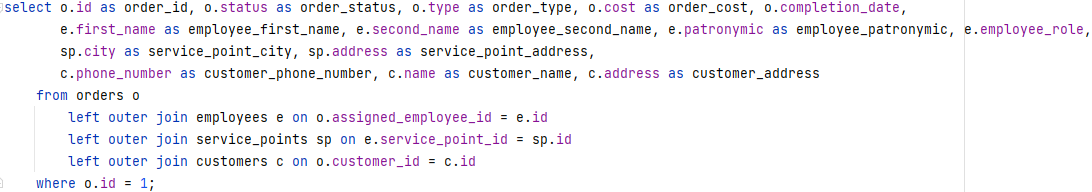
##### Запрос списка приемных пунктов для заданного города



**Рис. 18.** Запрос списка приемных пунктов для заданного города.

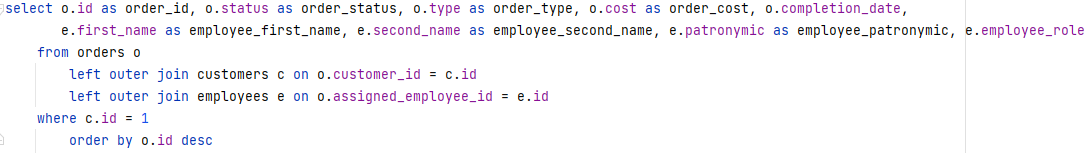
1. *Данные заказа по его номеру (идентификатору)*

Запрос Данные заказа по его номеру (идентификатору) позволяет получить информацию, связанную с заказом, а также о том, какой сотрудник исполняет заказ и о клиенте, создавшем заказ.



**Рис. 19.** Данные заказа по его номеру (идентификатору).

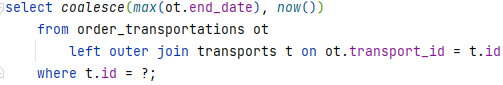
1. *Список заказов заданного клиента*



**Рис. 20.** Список заказов заданного клиента.

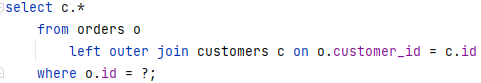
##### Время освобождения заданного автобуса от транспортировки

Запрос Время освобождения заданного автобуса от транспортировки позволяет получить время, когда данный автобус может начинать следующую транспортировку.



**Рис. 21.** Время освобождения заданного автобуса от транспортировки.

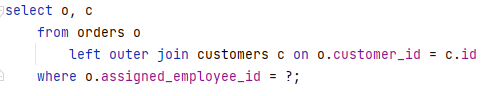
##### Данные клиента по номеру заказа

****

**Рис. 33.** Данные клиента по номеру заказа.

##### Список заказов, исполняемых заданным сотрудником

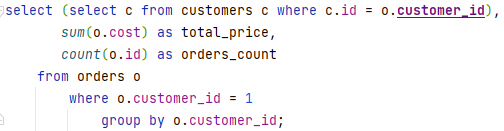
Результат данного запроса также содержит данные клиента, который оформлял заказы.



**Рис. 35.** Список заказов, исполняемых заданным сотрудником.

1. *Отчет по заказам клиента*

Результат данного запроса содержит число заказов, оформленных заданным клиентом и их общую стоимость.



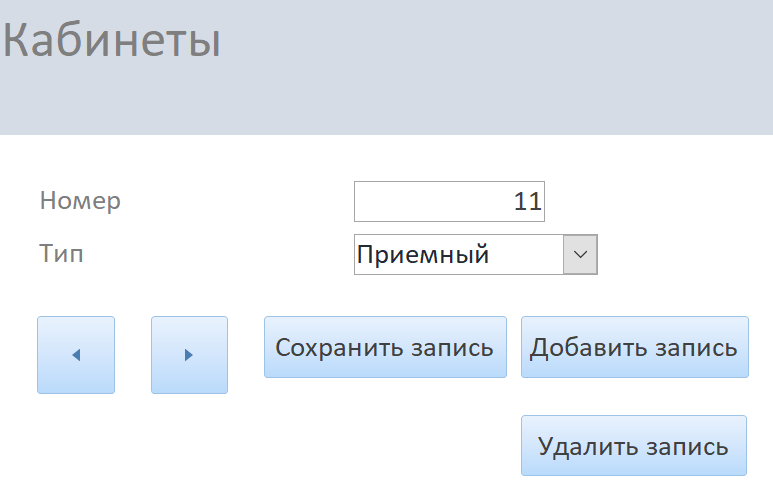
**Рис. 35.** Список заказов, исполняемых заданным сотрудником.

#### Формы

Для реализации стандартных операций добавления, обновления и удаления записей из таблиц был выбран встроенный в Microsoft Access инструмент – формы.

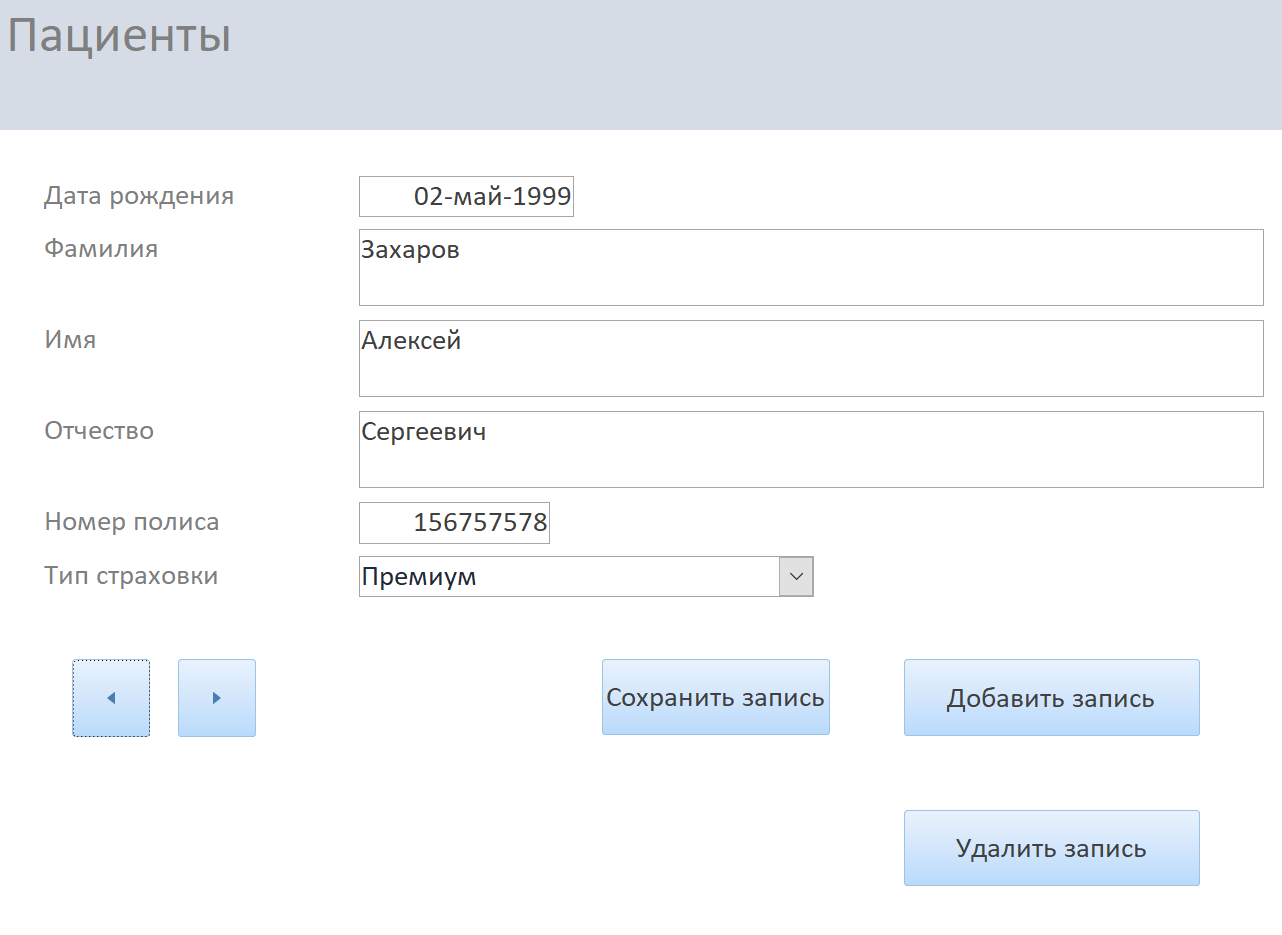
Каждая форма позволяет по нажатию кнопки совершить одно из вышеописанных действий: удалить, сохранить или добавить новую запись.

##### Форма Кабинеты



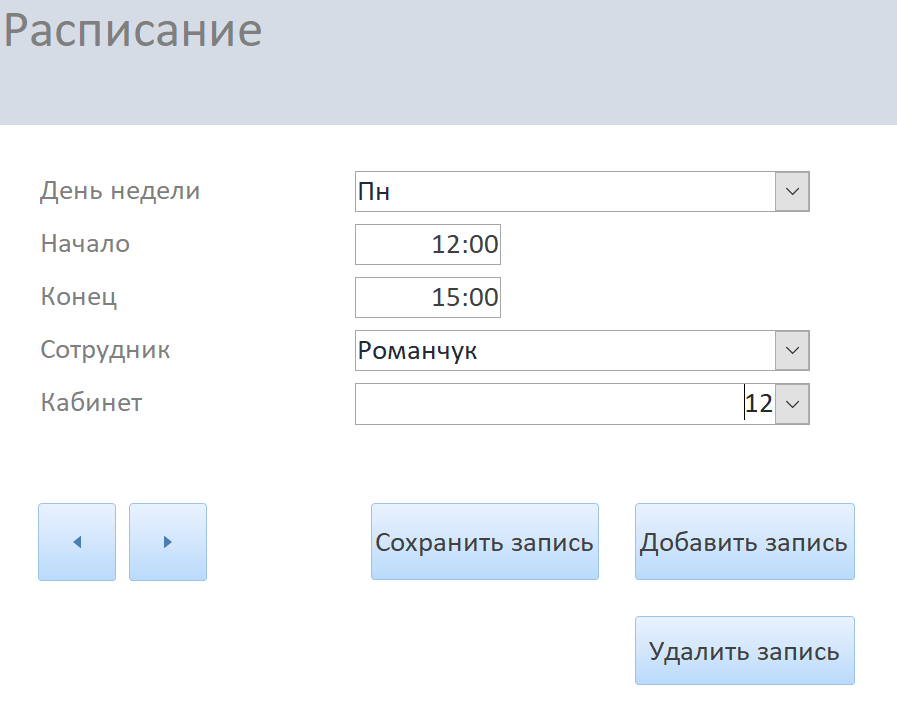
**Рис. 39.** Форма Кабинеты.

##### Форма Пациенты



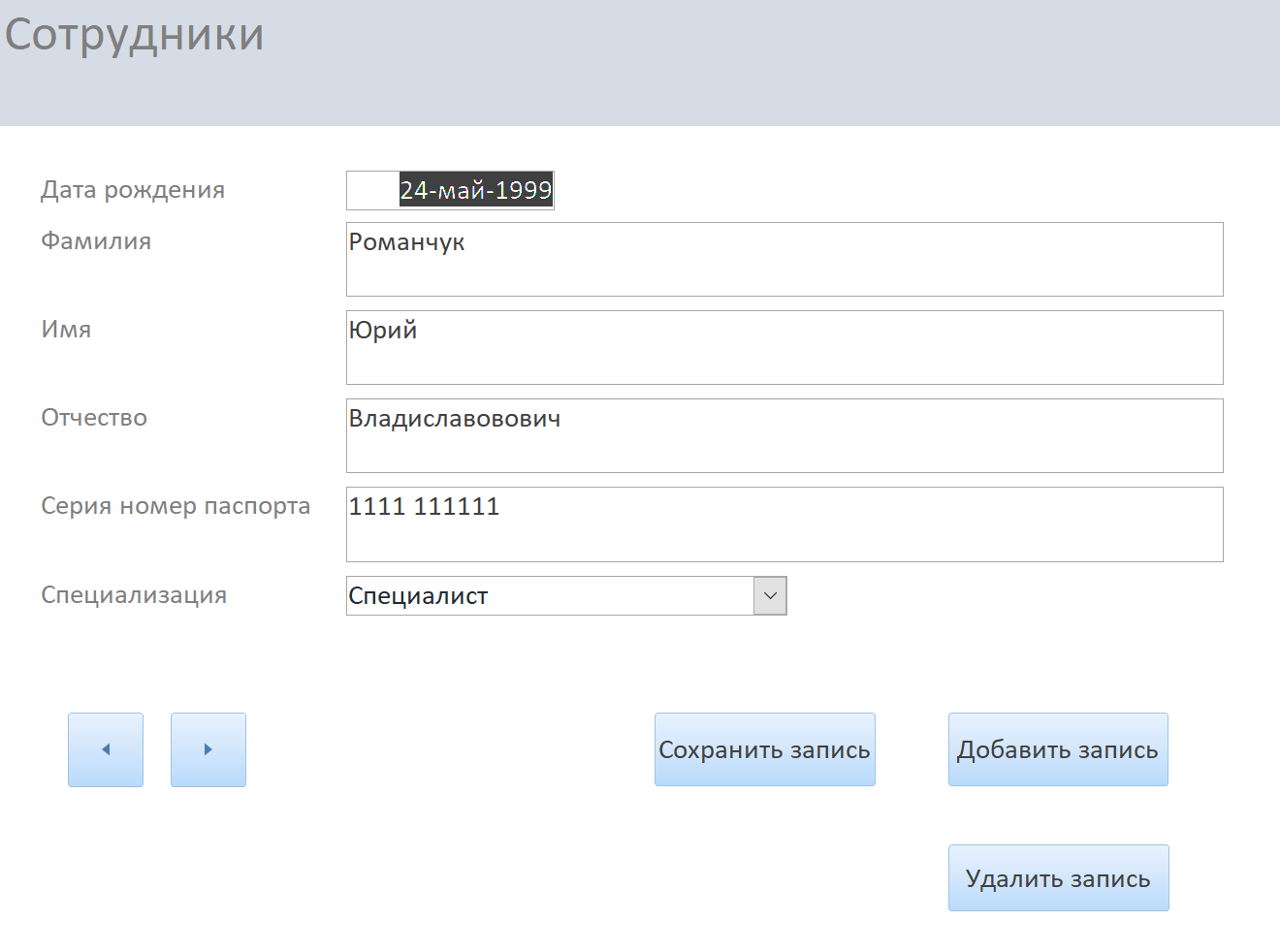
**Рис. 40.** Форма Пациенты.

##### Форма Расписание



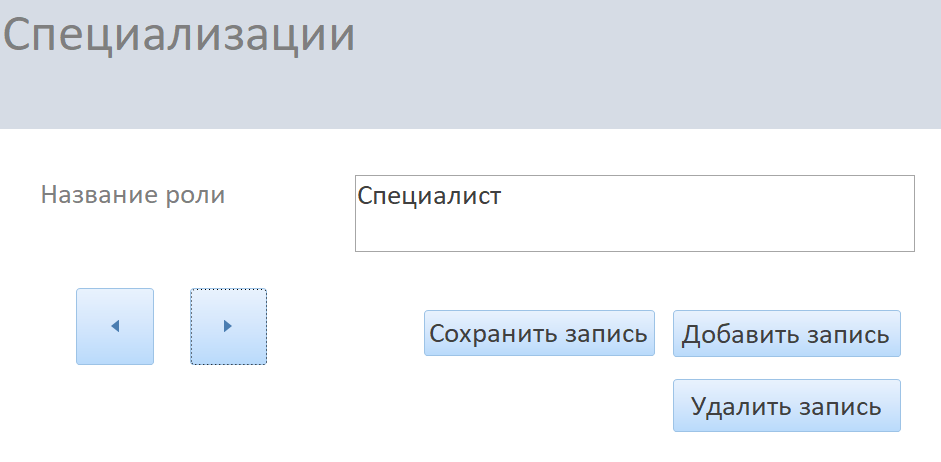
**Рис. 41.** Форма Расписание.

##### Форма Сотрудники



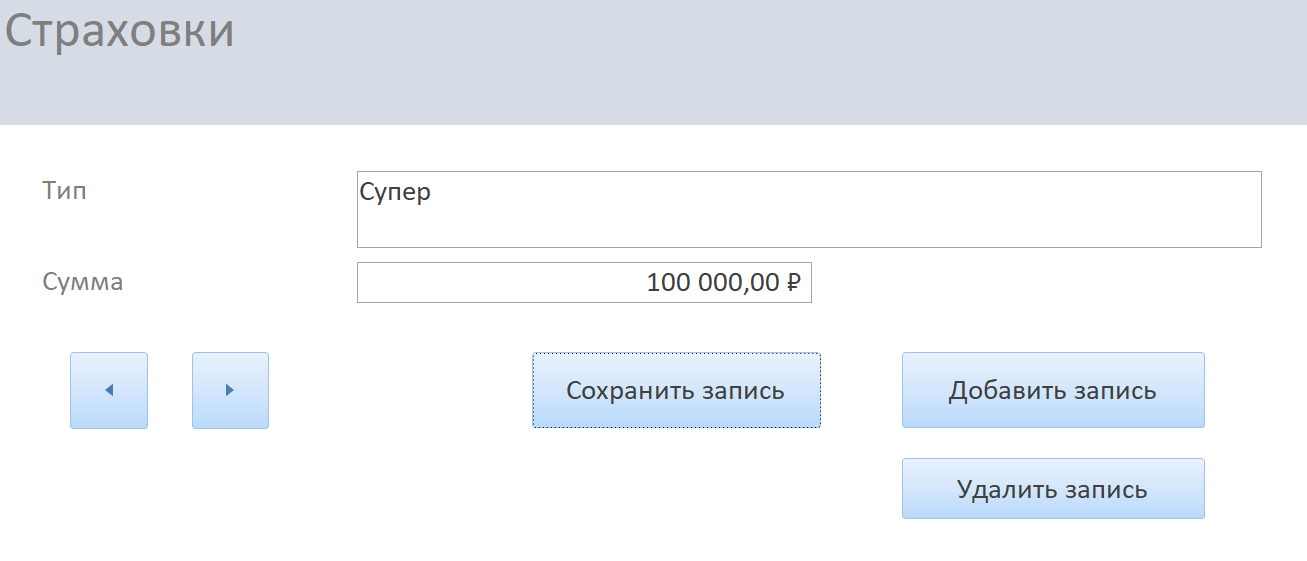
**Рис. 42.** Форма Сотрудники.

##### Форма Специализации



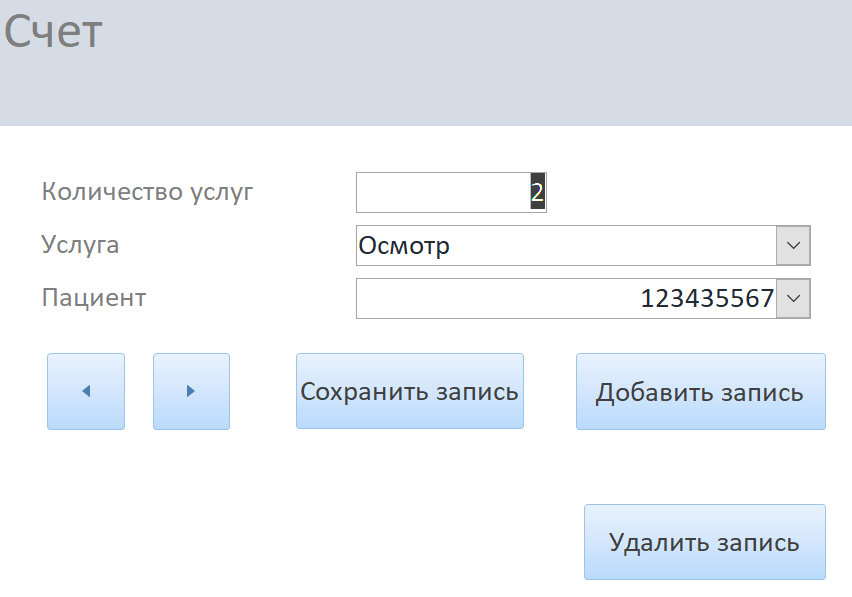
**Рис. 43.** Форма Специализации.

##### Форма Страховки



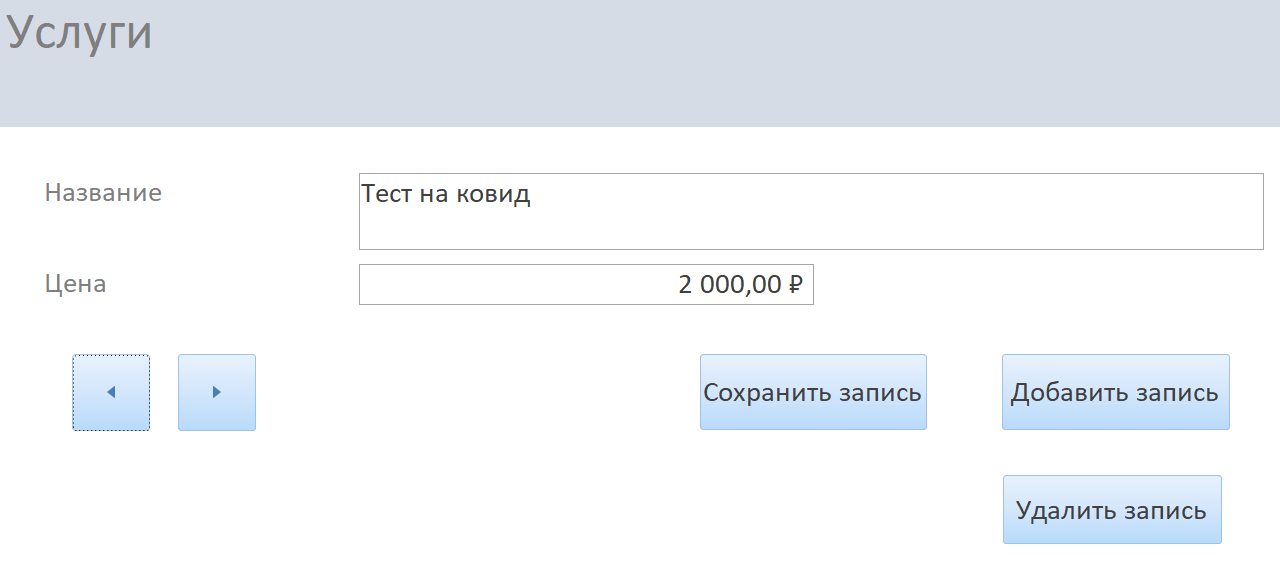
**Рис. 44.** Форма Страховки.

##### Форма Счет



**Рис. 45.** Форма Счет.

##### Форма Услугу



**Рис. 46.** Форма Счет.

# Разработка средств защиты

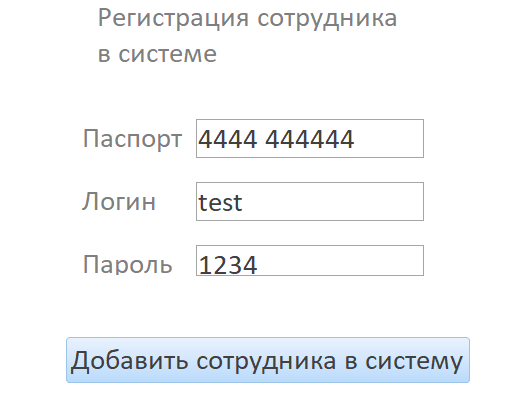
В источнике [5] приведены сведения о методах обеспечения защиты информации, были выбраны несколько из них. Для обеспечения защиты информации системы «Меломан» были реализованы следующие средства:

1. Авторизация по логину и паролю;
2. Разграничение прав пользователей;
3. Защита он некорректного ввода;
4. Резервное копирование.

## Аутентификация

### Форма регистрации сотрудника в системе

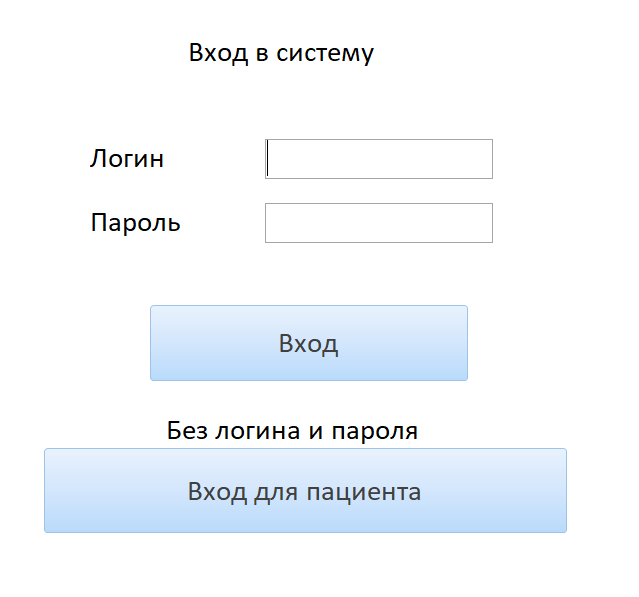
Так как пароли необходимо хранить в захешированном виде, то форма регистрации сотрудников в системе была реализована отдельно. Для хеширования встроенными средствами Microsoft Access, а именно на языке VBA, была реализована функция SHA256. Для оформления внешнего интерфейса данного функционала также был использован инструмент Форма.



**Рис. 47.** Форма Зарегистрировать сотрудника.

### Средства защиты от НСД и разграничение доступа

Организована парольная защита данной базы средствами Microsoft Access. При попытке открыть базу, будет предложено ввести логин и пароль. Или же войти в систему без логина и пароля. В данном случае будет доступен только просмотр расписания.



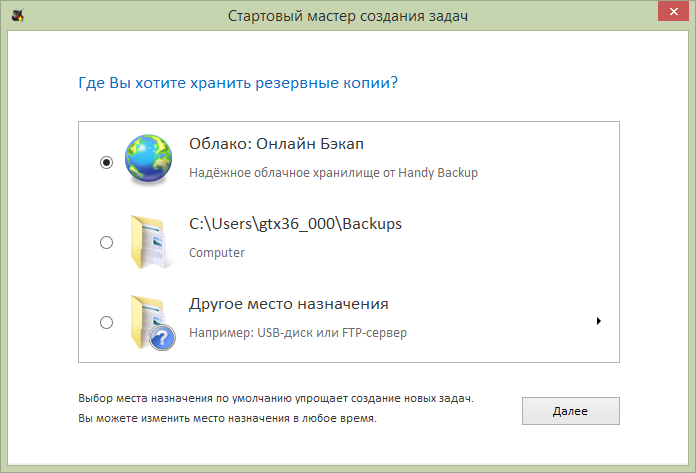
**Рис. 48.** Вход в базу данных.

При введении неверного пароля будет выдана ошибка и будет повторно предложено ввести пароль. При успешном входе в систему будет доступен полный функционал системы.

### Резервное копирование

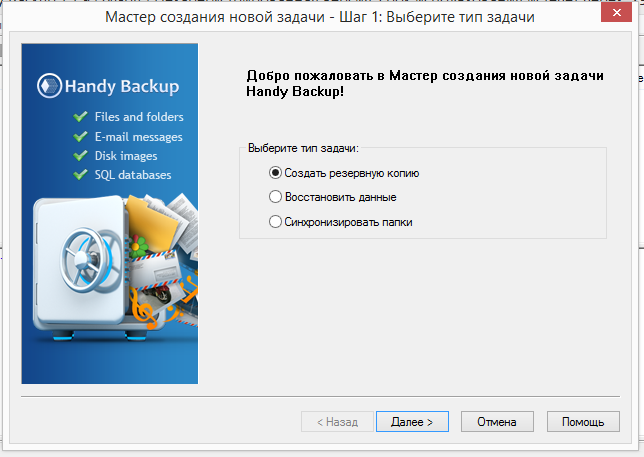
Для организации резервного копирования была использована сторонняя программа Handy Backup.

Данная программа может хранить данные (в том числе и нашу БД) в разных местах по выбору – облако, папка на компьютере, флеш–накопители или сервера.

****

**Рис. 49.** Выбор места хранения резервной копии

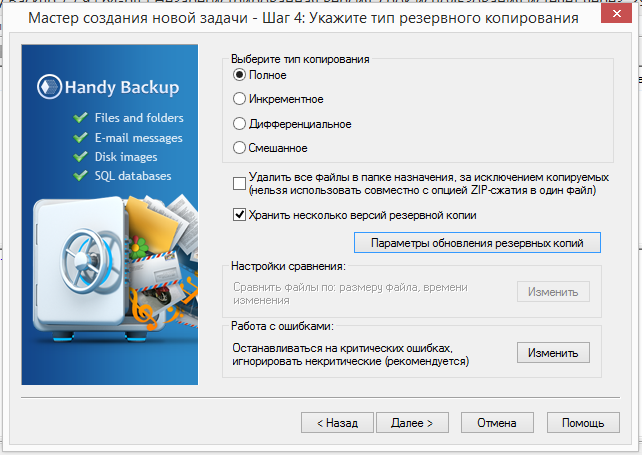
Программа может как создавать резервные копии, так и восстанавливать данные из данных копий.



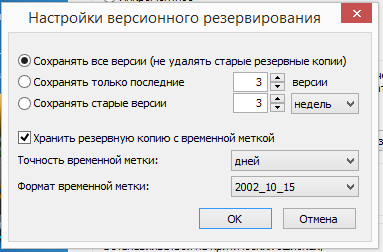
**Рис. 50.** Выбор задачи

Выбираем копирование базы данных, а затем место, куда будет сохраняться резервная копия.

Следующим шагом мы выбираем тип копирования – полное, инкрементное, дифференциальное либо смешанное. Также мы можем выбрать, будет ли хранимая резервная копия единственной, или же будет храниться несколько резервных копий разных дат. Можно выбрать также длительность хранения старых версий. Так как зачастую базы весят немало, хранить множество их резервных копий слишком затратно в плане объемов памяти.

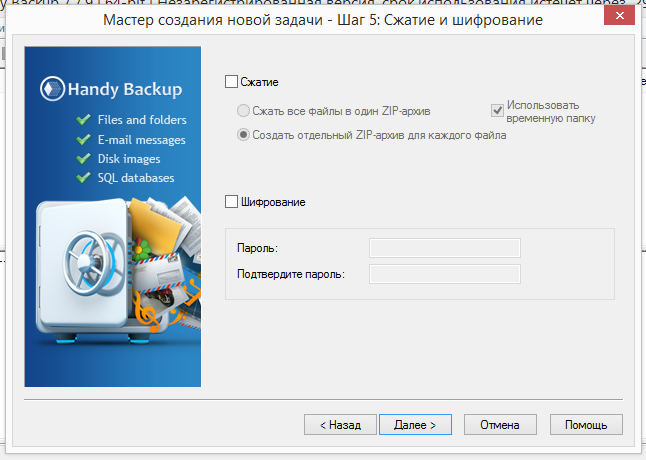
****

**Рис. 51.** Выбор типа копирования.

****

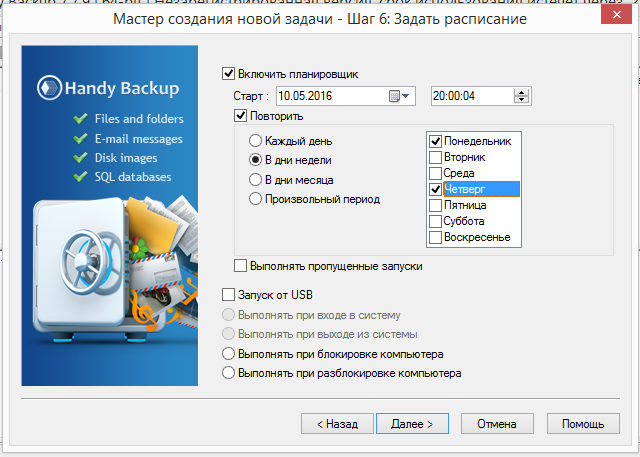
**Рис. 52.** Хранение различных версий копий.

При больших объемах файл может быть сжат, а также дополнительно зашифрован паролем, чтобы злоумышленник не мог получить доступа к копиям.

****

**Рис. 53.**  Сжатие и шифрование.

Одним из главных преимуществ данной программы является автоматическое резервное копирование. Можно установить расписание, по которому база будет копироваться, что будет являться защитой от человеческого фактора во время ручного копирования базы – администратор может просто забыть сделать вовремя резервную копию базы.

****

**Рис. 54.** Расписание копирования

Еще один плюс программы – она может сделать копию вне зависимости, работаем ли мы сейчас с базой данных или нет ("Горячее копирование").

# Заключение

Работа Поликлиники связана с большими объемами информации, которые необходимо обрабатывать. Поэтому для эффективной организации работы необходимо использование баз данных. Это позволяет упростить работу с большими объемами информации, ускорить поиск данных, фильтровать ввод информации, удобно и быстро добавлять, а также редактировать данные.

В первой части курсовой работы была спроектирована модель базы данных, а именно, проанализирована предметная область, разработан подход к проектированию базы данных и выбраны средства разработки.

Во второй части была разработана база данных: созданы и заполнены таблицы, реализованы формы для работы пользователей с базой данных, а также запросы и отчеты.

В третьей части описаны средства защиты от несанкционированного доступа и средства защиты от сбоев.

Таким образом, в данной работе спроектирована и разработана реляционная база данных «Поликлиника» и средства защиты от несанкционированного доступа (разграничение доступа к базе данных) и от сбоев (фильтрация ввода, обеспечение целостности данных).

# Список использованных источников

1. Базы данных / под ред. проф. А.Д. Хомоненко. – М.: КОРОНА-Век, 2011.
2. Брешенков, А.В. Проектирование объектов баз данных в среде Access : учеб. пособие / А.М. Губарь, А.В. Брешенков. – М. : Изд-во МГТУ им. Н.Э. Баумана, 2006..
3. Белоус, В.В. Основы реляционных баз данных. Практикум по SQL [Электрон. ресурс] : метод. указ. к лаб. работам по курсу "Базы данных" / В.В. Белоус, Н.В. Пивоварова. – М. : Изд-во МГТУ им. Н. Э. Баумана, 2014.
4. Туманов, В.Е. Основы проектирования реляционных баз данных / В.Е. Туманов. – М.: Бином-Пресс, 2012. – 420 c.
5. Цирлов. В.Л. Основы информационной безопасности автоматизированных систем – М.: Феникс, 2006. 256 с.