Министерство образования и науки Челябинской области ГБПОУ «Копейский политехнический колледж имени С.В. Хохрякова»

Администрирование базы данных для информационной системы "Патрульно-постовая служба"

Пояснительная записка к курсовому проекту

КПК.23.02.07.001-02ПЗ

Руководитель проекта

\_\_\_\_\_\_\_\_ Абдулвалеева З.В.

Выполнил

Обучающийся гр. 1ИСиП-18

\_\_\_\_\_\_\_\_Давлетов Д.Н.

Копейск 2022

|  |
| --- |
| КУРСОВОЙ ПРОЕКТ  по МДК.07.01  УПРАВЛЕНИЕ И АВТОМАТИЗАЦИЯ БАЗ ДАННЫХ  Копейск 2022 |

Содержание

|  |  |
| --- | --- |
| Введение | 3 |
| 1. Характеристика состава автоматизированной системы | 4 |
| 2. Программная и эксплуатационная документация | 8 |
| 3. Установка и настройка SQL – сервера | 10 |
| 4. Проектирование структуры базы данных | 13 |
| 5. Работа с журналом аудита базы данных. Мониторинг нагрузки сервера | 16 |
| 6. Настройки политики безопасности | 19 |
| 7. Обеспечение восстановления базы данных | 22 |
| Заключение | 26 |
| Библиография | 27 |

Введение.

Администрирование базам данных предусматривает выполнение функций, направленных на обеспечение надежного и эффективного функционирования системы баз данных, адекватности содержания базы данных информационным потребностям пользователей, отображения в базе данных актуального состояния предметной области.

Необходимость персонала, обеспечивающего администрирование данными в системе БД в процессе функционирования, является следствием централизованного характера управления данными в таких системах, постоянно требующего поиска компромисса между противоречивыми требованиями к системе в социальной пользовательской среде. Хотя такая необходимость и признавалась на ранних стадиях развития технологии баз, данных, четкое понимание и структуризация функций персонала, занятого администрированием, сложилось только вместе с признанием многоуровневой архитектуры СУБД.

1.Харакетристика состава автоматизированной системы

Автоматизированная информационная система (Automated information system, AIS) - это совокупность программных и аппаратных средств, предназначенных для хранения и (или) управления данными и информацией, а также для производства вычислений.

Основная цель АИС – хранение, обеспечение эффективного поиска и передачи информации по соответствующим запросам для наиболее полного удовлетворения информационных запросов большого числа пользователей.

К основным принципам автоматизации информационных процессов относят: окупаемость, надежность, гибкость, безопасность, дружественность, соответствие стандартам.

Окупаемость означает затрату меньших средств, на получение эффективной, надёжной, производительной системы, возможностью быстрого решения поставленных задач.

- Надежность достигается использованием надёжных программных и технических средств, использования современных технологий.

- Гибкость означает легкую адаптацию системы к изменению требований к ней, к вводимым новым функциям. Это обычно достигается созданием модульной системы.

- Безопасность означает обеспечение сохранности информации, регламентация работы с системой, использование специального оборудования и шифров.

- Дружественность заключается в том, что система должна быть простой, удобной для освоения и использования (меню, подсказки, система исправления ошибок и др.).

Выделяются четыре типа АИС:

1.Охватывающий один процесс (операцию) в одной организации.

2.Объединяющий несколько процессов в одной организации.

3.Обеспечивающий функционирование одного процесса в масштабе нескольких взаимодействующих организаций.

Реализующий работу нескольких процессов или систем в масштабе нескольких организаций.

АИС можно представить, как комплекс автоматизированных информационных технологий, составляющих информационную систему, предназначенную для информационного обслуживания потребителей.

Основное назначение автоматизированных информационных систем не просто собрать и сохранить электронные информационные ресурсы, но и обеспечить к ним доступ пользователей. Одной из важнейших особенностей АИС является организация поиска данных в их информационных массивах (базах данных). Поэтому АИС практически являются автоматизированными информационно-поисковыми системами (АИПС)

Автоматизированная информационно-поисковая система - программный продукт, предназначенный для реализации процессов ввода, обработки, хранения, поиска, представления данных т.п.

- АИПС бывают фактографическими и документальными.

- Фактографические АИПС обычно используют табличные реляционные БД с фиксированной структурой данных (записей).

- Документальные АИПС отличаются неопределённостью или переменной структурой данных (документов). Для их разработки обычно применяются оболочки АИС.

В качестве предметной области выбрано образовательное учреждение «Патрульно-Постовая служба», которое занимается патрулирование населенных пунктов. Информационная система (ИС) данной службы деятельность заключается в том, чтобы следить за нормальной жизнью и в случае появления проблем их разрешать.

Для осуществления работы патрульно-постовой службы между сотрудником, и гражданином необходима следующая информация:

Персональные данные сотрудника;

Персональные и контактные данные ученика.

Информация, хранящаяся в разрабатываемой системе, не будет носить строго конфиденциального характера и для обеспечения функционирования программы "Патрульно-постовой службы" произведено разграничение прав доступа с помощью пароля. После ввода пароля разрешается доступ к базе данных, а без ввода пароля база данных не доступна. Таким образом, необходимо реализовать ввод, хранение и изменение информации в базе данных:

Персональные и контактные данные гражданина (ФИО, паспортные данные, ИНН, адрес, телефон);

Персональные и контактные данные сотрудника (ФИО, возраст, образование, стаж, телефон, орден);

Конечный продукт должен выполнять следующие функции:

Ввод, изменение и удаление данных во всех таблицах;

Печать списка сотрудников;

Печать списка гражданина;

Для реализации вышеперечисленных функций конечный продукт должен содержать следующие формы:

Главную (начальную) форму выбора действий, из которых должны запускаться остальные формы, реализующие все функции;

Форма редактирования группы, сопряженная с выбором сотрудника и гражданина;

Форма редактирования гражданина;

Патрульно-постовая служба выполняет следующие задачи:

Ведет учет гражданина, их количество.

Ведет учёт нарушений гражданина.

Составляет нарушение, согласует с гражданином и обеспечивает явку в пункт.

Привязывает к определенному пункту определенного сотрудника.

Оформляет списки для дальнейшего дела в участковом пункте.

Обеспечивает выполнение требований государственного стандарта для гражданина.

Предоставляет различную справочную информацию.

2. Программная и эксплуатационная документация

Требования к программному обеспечению:

ОС: Windows 7 or 10.

Процессор: 2ух ядерный, частота 1.7 Ггц.

Оперативная память: 4 GB ОЗУ

Место на диске: 500 MB.

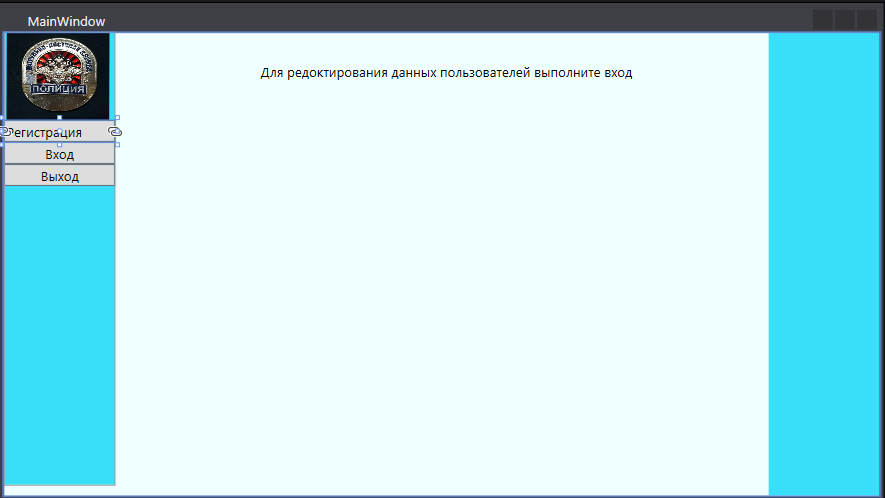
Установка:

Установка приложения выполняется с диска или по ссылке в интернете.

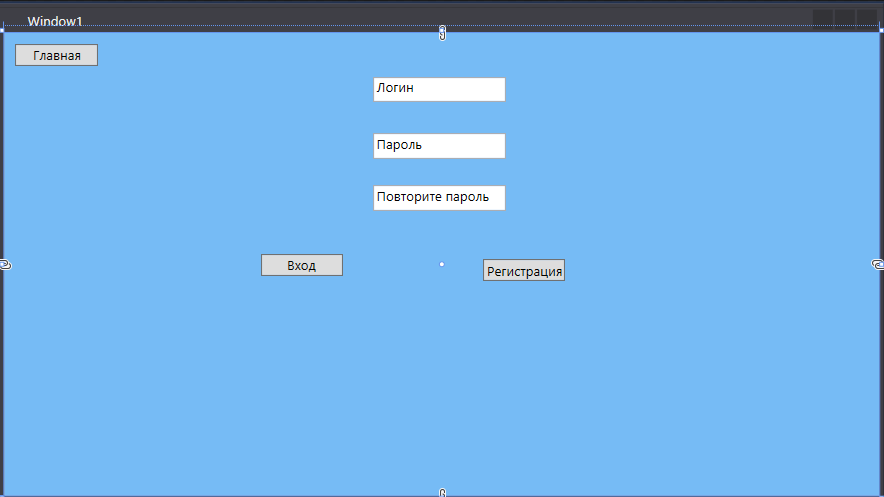
Запуск приложения:

Для запуска приложения необходимо два раза нажать на ярлык самого приложения, далее нужно подождать пару секунд и приложение откроется.

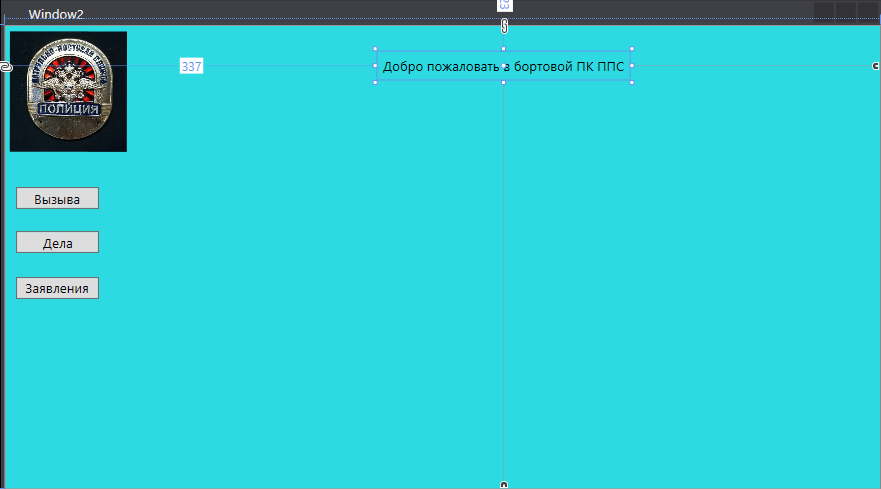
Интерфейс приложения:

При запуске приложения появляется главное окно, где можно увидеть три кнопки «Вход», «Регистрация», «Выход».

Для использования приложения необходимо зарегистрироваться, перейдя в окно регистрации вводим свои данные и, если регистрация прошла успешно далее выполняем вход.



После авторизации пользователь попадает в личный кабинет, где должен заполнить свои личные данные, чтобы использовать весь функционал приложения.



После того как пользователь ввёл свои данные он может использовать функционал бортового ПК, просматривать вызова и заполнять заявление от граждан.

3.Установка и настройка SQL сервера

Первое, что нужно сделать - это скачать сам дистрибутив. Скачать его можно с официального сайта.

Необходимо открыть дистрибутив и запустить установку. В меню слева нужно нажать "Installation" => New SQL Server stand-alone installation.

В новом открывшемся окне вас запросят выбрать бесплатную версию установки, к примеру "Ознакомительные", то есть Evaluation, либо если у вас есть ключ активации, для SQL Server, или любой другой полнофункциональный ключ, то вводите его.

Приобрести ключ активации SQL Server можно на официальном сайте программы.

Читаем и соглашаемся с лицензионным соглашением.

Соглашаемся на загрузку обновлений при наличии доступа в интернет. (либо можете отказаться, тут опционально).

В следующем окне нам предлагают выбрать компоненты MS SQL Server, которые Вы хотите установить. Выбираете нужные компоненты под Ваши задачи и идем далее.

Теперь нужно установить экземпляр. Если на вашем сервере, или виртуальной машине еще не установлен никакой SQL Server, то можете выбрать "Default instance", если уже SQL Server был установлен ранее, и вы поверх его ставите еще один экземпляр, то Вам нужно выбрать "Named instance" и дать ему имя.

SQL Server Agent, SQL Server Database, SQL Server Browser. По умолчанию используются персонализированные учетные записи.

Но вы можете выбрать учетную запись Вашего домена, если Ваша сеть работает на домене (сервер включен в домен).

Не забываем выбрать то, как будут стартовать службы, автоматически, вручную, либо вообще будут отключены, если они не нужны под Ваши задачи.

 Следующим пунктом нам предлагают выбрать серверную конфигурацию. Здесь предлагают выбрать, что вы сможете подключиться только с Windows логинами к SQL Серверу, либо Mixed, что вы сможете еще подключиться внутренними учетными записями SQL Server, создав их в SQL Server.

После на данном этапе имеет смысл нажать кнопку "Add Current User" и добавить текущего пользователя, а также Вы можете добавить учетную запись Вашего домена.

В том же окне переходим во вкладку "Data Directories". В этом пункте Вы можете выбрать Root директорию, директорию куда будут по умолчанию создаваться базы данных, директорию лог файлов и директорию для бекасов. Соответственно желательно, чтобы все директории были на разных жестких дисках.

В следующей вкладке переходим к настройкам базы TempDB. Это системная база, которая используется для хранения временных объектов.

Количество файлов прописано по умолчанию от кол-ва ядер.

Инициализационный размер в мегабайтах - здесь имеет смысл прибавить размер хотя бы до 16, или 32 мб.

Autogrowth MB - Это то кол-во мегабайт, которое будет приращиваться, если файл будет заполнен на 100%. Выбираем на свое усмотрение, в зависимости от Ваших задач и размер БД, по умолчанию средний размер 64мб, но лучше, чтобы было не более 1гб, дабы не страдала производительность. Если не знаете какая будет нагрузка на Вашу базу, то оставьте как есть.

Директория для временных файлов в идеале должна быть отдельным диском.

Следующая вкладка — это настройки Filestream - это настройка, которая позволяет хранить файлы в файловой системе NTFS, она может быть, как активирована, так и нет, опционально.

В разделе Ready to Install Вы можете наблюдать все те настройки, которые ранее прописали.

Нажимаем Next и ждем пока все установится.

Если все установилось успешно, то в конце все компоненты будут "Succeeded".

4.Проектирование структуры БД

Проектирование программного обеспечения — процесс создания проекта программного обеспечения (ПО), а также дисциплина, изучающая методы проектирования. Проектирование ПО является частным случаем проектирования продуктов и процессов.

Целью проектирования является определение внутренних свойств системы и детализации её внешних (видимых) свойств на основе выданных заказчиком требований к ПО (исходные условия задачи). Эти требования подвергаются анализу.

Проектирование ПО включает следующие основные виды деятельности:

выбор метода и стратегии решения;

выбор представления внутренних данных;

разработка основного алгоритма;

документирование ПО;

тестирование и подбор тестов;

выбор представления входных данных.

Первоначально программа рассматривается как чёрный ящик. Ход процесса проектирования и его результаты зависят не только от состава требований, но и выбранной модели процесса, опыта проектировщика.

Модель предметной области накладывает ограничения на бизнес-логику и структуры данных.

В зависимости от класса, создаваемого ПО, процесс проектирования может обеспечиваться как «ручным» проектированием, так и различными средствами его автоматизации. В процессе проектирования ПО для выражения его характеристик используются различные нотации — блок-схемы, ER-диаграммы, UML-диаграммы, DFD-диаграммы, а также макеты.

Проектированию обычно подлежат:

Архитектура ПО;

Устройство компонентов ПО;

База данных «Патрульно-постовая служба» состоит из 8 таблиц:

1.Автомобили

2.Группы

3.Категории

4.Пользователи

5.Программа обучения

6.Тип коробки передач

7.Учебные классы

8.Занятия

Также в данных таблицах существуют столбцы:

1.Автомобили (Наименование, Гос. Номер, Категория, Тип коробки передач, Инструктор)

2.Группы (Наименование)

3.Категории (Наименование)

4.Пользователи (Логин, Пароль, id)

5.Программа обучения (Наименование, Стоимость, Категории, Количество часов теории, Количество теории практики)

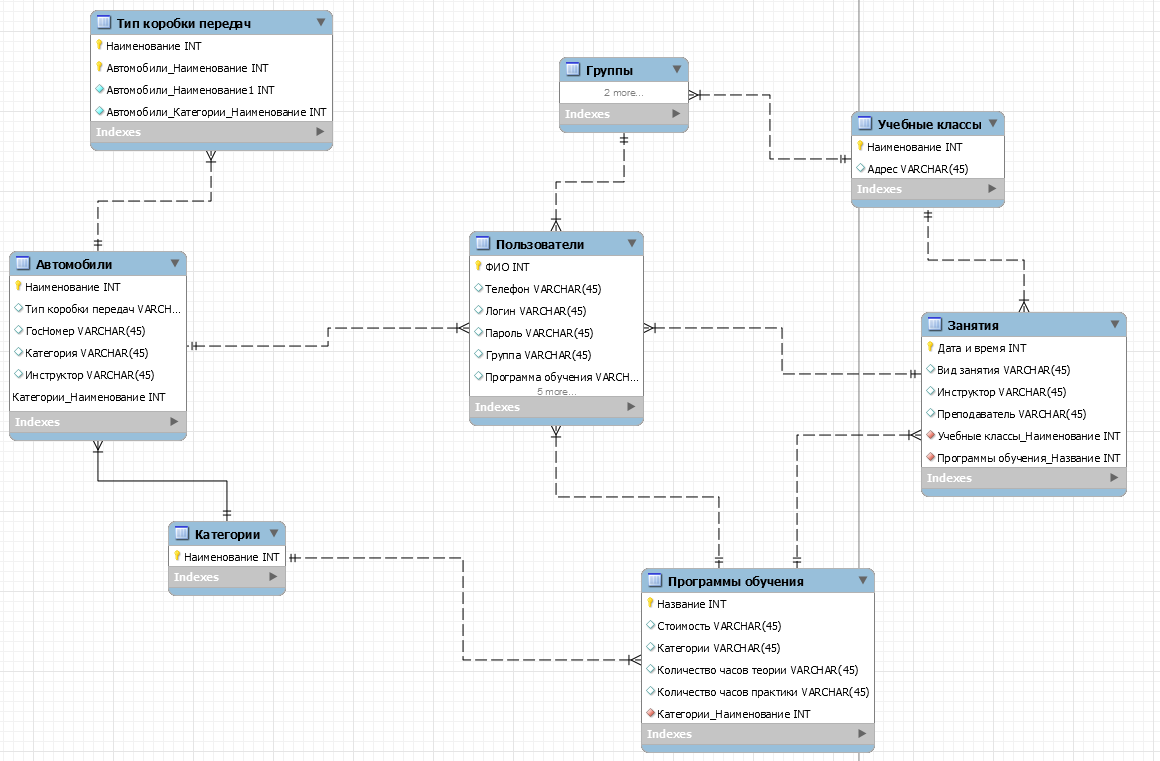
6.Тип коробки передач (Наименование, Наименование автомобиля)

7.Учебные классы (Наименование, Адрес)

8.Занятия (Дата и время, Вид занятия, Инструктор, Преподаватель)

Также модель БД представлена и в виде ER-Диаграммы.

ER -модель представляет собой схему, составными элементами которой являются: Сущность — это реальный, либо воображаемый объект, информацию о котором необходимо хранить в базе данных. На диаграмме ER-модели сущность изображается в виде прямоугольника, содержащего имя сущности.



5.Работа с журналом аудита БД. Мониторинг нагрузки сервера.

Аудит баз данных

Иногда необходимо регистрировать информацию об операциях, выполняемых в системе баз данных. Это насыпается аудитом (***audit***). Например, может потребоваться статистика о том, какие действия в системе выполняют пользователи. Аудит можно применять также для слежения за базой данных с целью обнаружения потенциальных нарушении ее защиты.

Избирательный аудит

Средство аудита SQL можно включать и выключать. При включении аудита требуется определенный расход ресурсов, необходимый для гене­рации записей аудита. Чтобы свести к минимумуработу, выполняемую SQL для аудита базы данных, нужно точно определить, для чего нужен аудит:

- Можно выполнять аудит конкретных SQL-операторов безотноси­тельно к конкретным объектам. Например, можно просить SQL генерировать запись аудита всякий раз, когда какой-либо пользователь выполняет оператор DROPTABLE, и не учитывать, к какой таблице относится этот оператор.

- Можно выполнять аудит использования мощных системных привилегий. Например, просить SQL генерировать запись аудита всякий раз, когда какой-либо пользователь применяет системную привилегию SELECTANYTABLE для запроса к таблице базы данных.

- Можно выполнять аудит определенных SQL-операторов для конкретных объектов базы данных. Например, просить SQL генерировать запись аудита всякий раз, когда какой-либо пользователь удаляет запись из таблицы SALES.CUSTOMERS.

- Для каждой разрешенной опции аудита можно просить SQL генерировать запись аудита для успешного, неуспешного или любого выполнения операторов. Более того, можно установить каждую разрешенную опцию аудита для всех либо для некоторых пользователей базы данных.

Объект Спецификация аудита базы данных также принадлежит подсистеме аудита SQL Server. Для каждого аудита каждой базы данных SQL Server можно создать одну спецификацию аудита базы данных.

Спецификация аудита базы данных включает действия аудита уровня базы данных, вызываемые компонентом расширенных событий. В спецификацию аудита базы данных можно добавлять либо группы действий аудита, либо события аудита. События аудита — это атомарные события, аудит которых может производиться ядром SQL Server. Группы действий аудита — это стандартные группы действий. Они расположены в области базы данных SQL Server. Эти действия передаются аудиту, который регистрирует их в целевом объекте. Не включайте объекты области сервера, такие как системные представления, в пользовательскую спецификацию аудита базы данных.

Спецификации аудита базы данных являются незащищаемыми объектами, которые находятся в определенной базе данных. После создания спецификация аудита базы данных находится в отключенном состоянии.

Если спецификация аудита базы данных создается или изменяется в пользовательской базе данных, не включайте действия аудита для объектов области сервера, таких как системные представления. Если вы включаете объекты области сервера, аудит будет создан, но объекты области сервера не будут включены и при этом не будет возвращаться ошибка.

Существует несколько вариантов диагностики нагрузки на сервер в виртуальном хостинге:

1.Изучение лог-файлов – помогает определить, к каким страницам идет наибольшее обращение. Это придется делать вручную. Чтобы понять, какие изменения происходят, достаточно сравнить участки логов с нормальной и максимальной нагрузкой;

2.Аудит кода – проводится для выявления слабых участков кода. Некоторые из них могут вообще впустую расходовать ресурсы. После того как неоптимальные участки найдены, необходимо заняться их устранением или улучшением;

3.Профилирование – исследование времени реализации маленьких участков кода. Благодаря профилированию можно узнать, какие части скрипта в первую очередь нуждаются в оптимизации.

Если вы хотите уменьшить нагрузку на сервер, для начала стоит определить, какие именно места вызывают наибольшую нагрузку. После этого можно приступать к оптимизации. Проанализируйте работу плагинов и виджетов – как правило, некоторые из них попусту нагружают ЦПУ. Если много ресурсов уходит на генерацию страниц, необходимо задуматься о кэшировании страниц.

Существует много способов уменьшения нагрузки на сервер, но делать все вручную очень долго и сложно. Для автоматизации процессов в сети лучше выбрать специальные инструменты для мониторинга сервера. Это могут быть платные или бесплатные программы, которые подходят для создания и управления сценариями мониторинга.

Использование панели мониторинга для наблюдения за нагрузкой сервера удаленного доступа:

1.В диспетчере серверов щелкните Средства и выберите пункт Управление удаленным доступом.

2.Щелкните на “ПАНЕЛЬ МОНИТОРИНГА”, чтобы открыть Панель удаленного доступа в Консоли управления удаленным доступом.

3.На панели мониторинга мониторинга обратите внимание на плитку состояния удаленного клиента на плитке состояния сервера. На этой плитке перечислены статистические данные, такие как общее число подключенных удаленных клиентов, общее количество подключенных клиентов DirectAccess и максимальное число пользователей, подключившихся за последние 24 часа.

4.Вы можете нажать кнопку “Обновить” в разделе задачи на правой панели, чтобы перезагрузить состояние работоспособности. Чтобы изменить интервал обновления по умолчанию, щелкните настроить интервал обновления в разделе задачи.

На рисунке 5 можно увидеть нагрузку увеличивается, когда отправляются запросы.

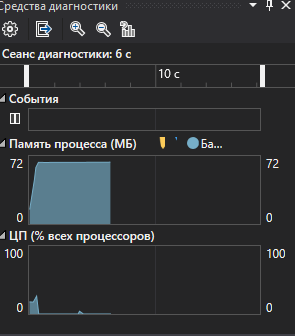


Рисунок - 5 “Нагрузка на сервер”

6. Настройки политики безопасности

Мероприятия охватывают целый ряд аспектов законодательного, организационного и программно-технического характера. Для каждого из них формулируется ряд задач, выполнение которых необходимо для защиты информации. Перечислим самые общие из них.

В нормативно-законодательном аспекте необходимо решение следующих задач:

1.определение круга нормативных документов международного, федерального и отраслевого уровня, применение которых требуется при проектировании и реализации системы информационной безопасности;

2.определение на основе нормативных документов требований по категорированию информации;

3.определения на основе нормативных документов базовых требований к системе информационной безопасности и ее компонентам.

В организационном аспекте:

1.определение соответствия структурируемой и защищаемой информации подсистемам и ресурсам информационной системы, в которых производится хранение, обработка и передача информации конечному пользователю (должно быть организовано ведение реестра ресурсов, содержащих информацию, значимую по критериям конфиденциальности, целостности и доступности);

2.определения набора служб, обеспечивающих доступ к информационным ресурсам системы (необходима выработка и согласование типовых профилей пользователей, ведение реестра таких профилей);

3.формирования политики безопасности, включающей описание границ и способов контроля безопасного состояния системы, условия и правила доступа различных пользователей к ресурсам системы, мониторинга деятельности пользователей.

В процедурном аспекте:

1. Организация физической защиты помещений и компонентов информационной системы, включая сети и телекоммуникационные устройства;

2. Обеспечение решения задач информационной безопасности при управлении персоналом;

3. Формирование, утверждение и реализация плана реагирования на нарушения режима безопасности;

4. Внесение дополнений, связанных со спецификой ликвидации последствий несанкционированного доступа, в план восстановительных работ.

В программно-техническом аспекте:

1. Обеспечение архитектурной и инфраструктурной полноты решений, связанных с хранением, обработкой и передачей конфиденциальной информации;

2. Обеспечение проектной и реализационной непротиворечивости механизмов безопасности по отношению к функционированию информационной системы в целом;

3. Выработка и реализация проектных и программно-аппаратных решений по механизмам безопасности.

Правила политики безопасности:

В информационной системе «Магазин автозапчастей» хранение, обработка и передача конфиденциальной информации осуществляется в рамках информационной системы самим пользователем.

Запрещается раскрывать конфиденциальную информацию в связи с возможной потерей аккаунта и данных, а также от взлома злоумышленников.

Запрещается передавать личную информацию (логин, пароль) другим лицам.

Администратор базы данных обязан держать в тайне информацию о пользователях информационной системы.

Запрос и ответы баз данных осуществляется только между пользователем и базой данных без участия иных лиц.

Для защиты личной информации пользователя используется шифрование.

Запрещается пользоваться информационной системой на других устройствах с сохранением своей личной информации.

Как видно на рисунке 8 при вводе пароля строка отображается в виде «кружков», это сделано для конфиденциальности, чтобы при записи экрана либо если вы работаете в офисе посторонние люди не смогли увидеть ваши данные.

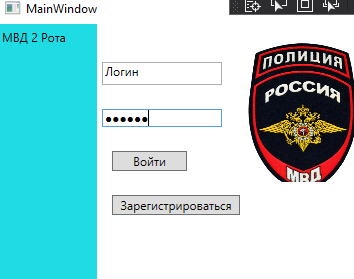


Рисунок - 6 Окно “Вход”

1. Обеспечение восстановления базы данных

Восстановление базы данных – это функция, которая приводит базу данных в актуальное и консистентное состояние. В случае логического отказа или сигнала отката одной транзакции журнал изменений сканируется в обратном направлении, и все записи отменяемой транзакции извлекаются из журнала вплоть до отметки начала транзакции. Согласно извлеченной информации выполняются действия, отменяющие действия транзакции.

Формы восстановления размещаются по щелчку правой кнопкой мыши на базе данных, которую вы хотите восстановить. Далее перемещайтесь по последующим всплывающим меню, пока не дойдете до разных типов восстановления, которые можете использовать

Восстановление базы данных осуществляется путём нажатия на необходимую базу данных правой кнопкой мыши. Далее необходимо навести на пункт Tasks, Restore, после чего нажать «Database…». Восстановление базы данных

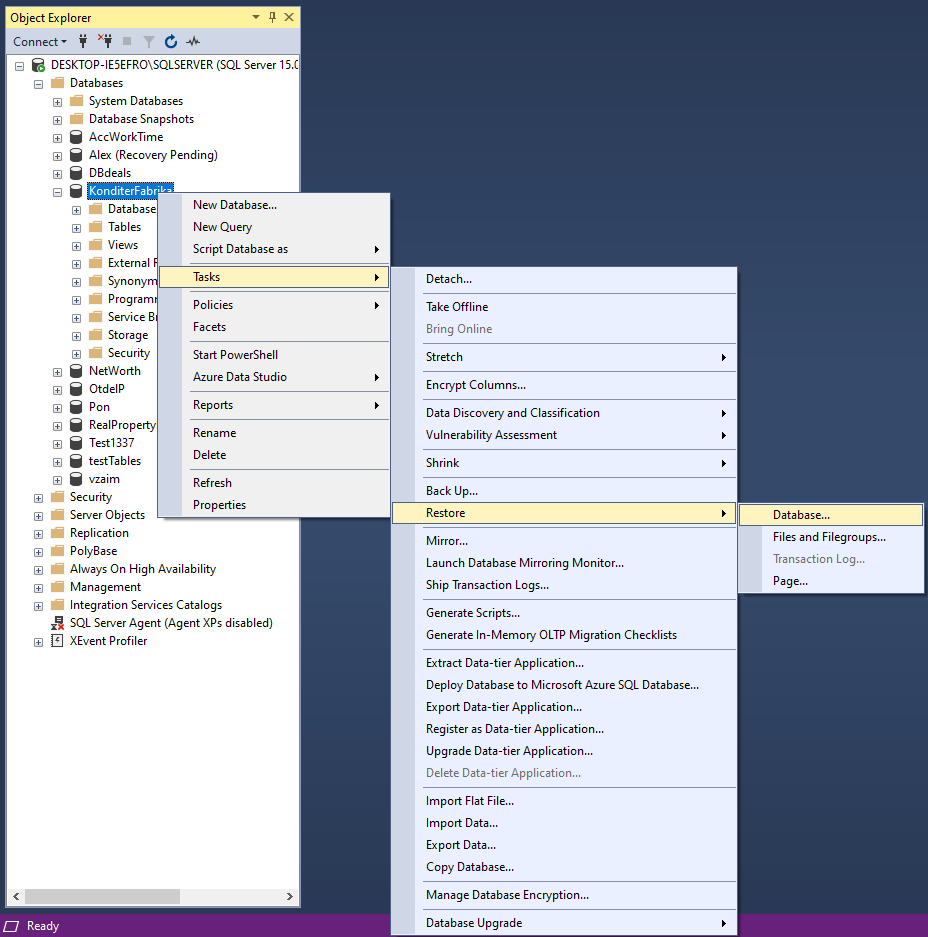


Рисунок 2 – Восстановление базы данных

После данных действий открывается окно Восстановление базы данных. В данном окне будут заполнены необходимые значения. Необходимо начать с последней полной резервной копии, последней разностной копии, сформированной до момента, который SQL Server считает вашей точкой восстановления — последним моментом времени, до которого возможно восстановление; далее следуют журналы регистрации транзакций.

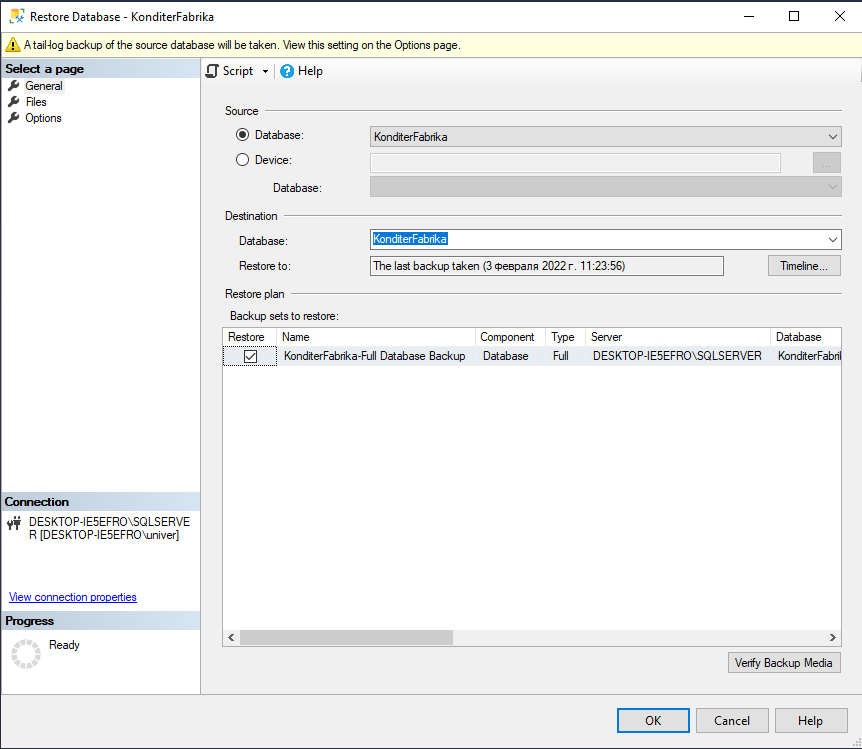


Рисунок 3 – Окно восстановление базы данных

Чтобы восстановить базу данных к состоянию на последний из возможных моментов времени необходимо перейти на страницы Файлы и Параметры. На странице Файлы вносить изменения нет необходимости. Далее переходим на страницу Параметры. На данной странице нам предоставляют выбор способа восстановления базы данных:

- Перезаписать существующую базу данных (WITH REPLACE)

- Сохранить настройки репликации (WITH KEEP\_REPLICATION)

- Ограничить доступ к восстанавливаемой базе данных (WITH RESTRICTED\_USER)

В Состоянии восстановлении необходимо выбрать RESTORE WITH RECOVERY. Нужно это для того, чтобы вновь подключить базу данных к сети. Почти во всех диалоговых окнах SQL Server Management Studio предусмотрена возможность в фоновом режиме записывать в виде сценария выполняемые действия в новое окно запроса, в буфер обмена или в задание агента SQL Server, с тем чтобы выполнить их позднее.

Выполнение процесса восстановления:

USE [master]

-Переводим базу данных в режим Single\_User:

ALTER DATABASE [SQL\_Cruise] SET SINGLE\_USER WITH ROLLBACK IMMEDIATE

- Формируем резервную копию хвоста журнала

BACKUP LOG [SQL\_Cruise]

TO  DISK = N'C:\Data\MSSQL12.MSSQLSERVER\MSSQL\Backup\SQL\_Cruise\_LogBackup\_2016-08-30\_20-37-27.bak'

WITH NOFORMAT, NOINIT,  NAME = N'SQL\_Cruise\_LogBackup\_2016-08-30\_20-37-27', NOSKIP, NOREWIND, NOUNLOAD,  STATS = 5

- Восстановление первой полной резервной копии

RESTORE DATABASE [SQL\_Cruise]

FROM  DISK = N'C:\temp\SQL\_Cruise\_FULL.bak'

WITH  FILE = 1,  NORECOVERY,  NOUNLOAD,  REPLACE,  STATS = 5

-Восстановление поздней последней резервной копии из возможных:

RESTORE DATABASE [SQL\_Cruise]

FROM  DISK = N'C:\temp\SQL\_Cruise\_DIFF\_3.bak'

WITH  FILE = 1,  NORECOVERY,  NOUNLOAD,  STATS = 5

-Восстановление полной резервные копии журнала регистрации транзакций в порядке:

RESTORE LOG [SQL\_Cruise]

FROM  DISK = N'C:\temp\SQL\_Cruise\_log\_03.trn'

WITH  FILE = 1,  NORECOVERY,  NOUNLOAD,  STATS = 5

RESTORE LOG [SQL\_Cruise]

FROM  DISK = N'C:\temp\SQL\_Cruise\_log\_04.trn'

WITH  FILE = 1,  NORECOVERY,  NOUNLOAD,  STATS = 5

-Восстановление последней резервной копии журнала регистрации транзакций:

RESTORE LOG [SQL\_Cruise]

FROM  DISK = N'C:\temp\SQL\_Cruise\_log\_05.trn'

WITH  FILE = 1,  RECOVERY, NOUNLOAD,  STATS = 5,

        STOPAT = N’2016-08-30T20:26:00’-Выводим базу данных из режима single\_user:ALTER DATABASE [SQL\_Cruise] SET MULTI\_USERGO

Заключение

На основании проведенного мной исследования, можно сделать следующие выводы, что поставленные задачи были решены в полном объеме. Таким образом, база данных информационной системы патрульно-постовой службы является автоматизированной. Для реализации вышеуказанных целей было выполнены следующие задачи: обеспечивает безопасность информационной системы, обеспечивают безопасность хранения личной информации пользователей, ведение учет пользователей, их количество, ведение учет делав, ведет учет новых гражданина.

Поставленная цель администрирование базы данных патрульно-постовая служба была достигнута, однако требуется усовершенствование безопасности, например, разработка дополнительных параметров защиты (CAPTCHA), работа с журналом аудита базы данных. Мониторингом нагрузки сервера. Спроектирована структура базы данных.

Библиография

1. ГОСТ 2.105-95. Единая система конструкторской документации. Общие требования к текстовым документам. - Введен в действие постановлением Госстандарта РФ от 8 августа

2. ГОСТ 7.80-2000. Библиографическая запись. Заголовок. Общие требования и правила составления. - Введение. 2000-01-07. - М.: Изд-во стандартов, - (Система стандартов по информации, библиотечному и издательскому делу).

3. Васильков А. В. Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков. - М.: Форум,

4. Гвоздева В. А. Информатика, автоматизированные информационные технологии и системы / В.А. Гвоздева. - М.: Форум, Инфра-М, 2018. - 544 c.

5. Голицына, Максимов, Попов: Информационные системы. Учебное пособие

6. Ивлев В. А. Информационные системы на основе действий / В.А. Ивлев, Т.В. Попова. - М.: 1С-Паблишинг, 2018.

7. Исаев Г.Н., Роганов А.А. Управление информационными системами. (Бакалавриат). Учебное пособие.

8. Киселев Г. М. Информационные технологии в педагогическом образовании // Бочкова Р.В. – 2018 – С.

9. Троелсен Э., Джепикс Ф. - Язык программирования C# 7 и платформы .NET и .NET Core – 2018.