ТИТУЛЬНИК (будет напечатан отдельно вместо с отчетом, т.к. он сохранен как отдельный лист в формате PDF)

СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 3](#_Toc1466880762)

[1 ОБЩАЯ ХАРАКТЕРИСТИКА ООО “МАЛЛЕНОМ СИСТЕМС” 3](#_Toc1725279117)

[1.1 Организационная структура предприятия 3](#_Toc1600382551)

[1.2 Внутренний распорядок работы предприятия, охрана труда ИТ-специалистов 4](#_Toc71552217)

[1.3 Должностные инструкции ИТ-специалистов предприятия 4](#_Toc828193802)

# ВВЕДЕНИЕ

# 1 ОБЩАЯ ХАРАКТЕРИСТИКА ООО “МАЛЛЕНОМ СИСТЕМС”

# 1.1 Организационная структура предприятия

Организационная структура: Линейная, есть отделы компании и в них есть руководители.

1. Центр по развитию интеллектуальных систем, отдел разработки ПО. Проектирование, разработка, оптимизация ПО для клиентов компании.
2. Производственно-технический отдел. Отдел с инженерами, которые проводят пусконаладочные работы на предприятиях, проектируют местонахождение оборудования на предприятии и устанавливают его.
3. АУП (Административно-управленческий персонал). Руководство компании, которое формирует стратегии развития, управляет отделами, планирует деятельность предприятия, обеспечивает внешние коммуникации компании на выставках, в СМИ.
4. Группа Маркетинга. Формирование маркетинговой стратегии компании, внутренний и внешний PR-компании, продвижение бренда и продуктов на рынке.
5. Коммерческий отдел. Продажа продуктов компании заказчикам, поиск новых клиентов, участие в PR-продвижении компании.
6. Отдел технической поддержки и контроля качества. Техническая поддержка пользователей и тестировка ПО на выявление ошибок и проблем.
7. Отдел акселерационных и образовательных программ. Разработка и проведение обучающих курсов по машинному зрению и языку программирования, PR компании на рынке образовательных учреждений.
8. Отдел кадров. Управление персоналом компании, поиск, подбор, адаптация сотрудников, ведение кадрового документооборота, разработка стратегия развития персоналом предприятия.
9. Юридический отдел. Обработка всех документов в компании в соответствии с законодательством, взаимодействие с заказчиками и менеджерами по договорным обязательствам.
10. Бухгалтерия. Ведение экономической деятельности предприятия, бухгалтерского учета, формирование бюджетов компании.
11. ОХР (общественно-хозяйственные рабочие). Поддержание чистоты, порядка на рабочих местах, ремонт, уборка служебных помещений.

# 1.2 Внутренний распорядок работы предприятия, охрана труда ИТ-специалистов

Внутренний распорядок работы сотрудников Малленом Системс регламентируется внутренними документами организации, такими как положение о внутреннем распорядке и правила охраны труда.

Основные положения внутреннего трудового распорядка включают:

- Режим рабочего времени (обычно пятидневная рабочая неделя с понедельника по пятницу с восьмичасовым рабочим днем).

- Порядок учета рабочего времени (фиксирование прихода и ухода сотрудников через систему электронного пропускного контроля).

- Обеспечение соблюдения трудовой дисциплины (ответственность за нарушение внутренних норм и правил).

Охрана труда осуществляется в соответствии с действующими законодательными актами Российской Федерации. Основные меры по охране труда включают:

- Проведение инструктажей по технике безопасности перед началом работ.

- Регулярное обучение сотрудников правилам безопасной эксплуатации техники и инструментов.

- Оснащение рабочих мест средствами индивидуальной защиты (например, защитными очками и спецодеждой).

- Организация медицинского осмотра сотрудников и проведение профилактических мероприятий.

Особое внимание уделяется вопросам информационной безопасности, защите персональных данных и предотвращению утечек конфиденциальной информации.

# 1.3 Должностные инструкции ИТ-специалистов предприятия

Должностная инструкция

Техник

1. Общие положения

1.1 Техник должен знать и уметь:

– Писать программный код процедур проверки работоспособности программного обеспечения на выбранном языке программирования под руководством наставника;

– Использовать выбранную среду программирования для разработки процедур проверки работоспособности программного обеспечения на выбранном языке программирования;

– Применять методы и средства проверки работоспособности программного обеспечения;

– Анализировать значения полученных характеристик программного обеспечения;

– Документировать результаты проверки работоспособности программного обеспечения;

– Применять методы, средства для рефакторинга и оптимизации;

– Публиковать результаты рефакторинга и оптимизации в коллективной базе знаний в виде лучших практик;

– Использовать систему контроля версий для регистрации произведенных изменений;

– Применять методы и приемы отладки дефектного программного кода;

– Интерпретировать сообщения об ошибках, предупреждения, записи технологических журналов, возникающих при выполнении дефектного кода.

2. Должностные обязанности

Техник выполняет следующие должностные обязанности:

2.1 Выполняет работу по проведению необходимых технических расчетов;

2.2 Осуществляет наладку, настройку, регулировку и опытную проверку оборудования и систем, следит за его исправным состоянием;

2.3 Принимает участие в проведение экспериментов и испытаний;

2.4 Принимает участие в разработке программ, инструкций и другой технической документации, в изготовлении макетов, а также в испытаниях и экспериментальных работах;

2.5 Выполняет работу по сбору, обработке и накоплению исходных материалов, данных статистической отчетности, научно-технической информации;

2.6 Составляет описания проводимых работ, необходимые спецификации, диаграммы, таблицы, графики и другую техническую документацию;

2.7 Выполняет работу по оформлению плановой и отчетной документации, вносит необходимые изменения и исправления в техническую документацию в соответствии с решениями, принятыми при рассмотрении и обсуждении выполняемой работы;

2.8 Систематизирует, обрабатывает и подготавливает данные для составления отчетов о работе;

2.9 Принимает необходимые меры по использованию в работе современных технических средств.

3. Обязанности и ответственность

Техник обязан:

3.1 Соблюдать локально-нормативные акты Общества.

3.2 Не разглашать информацию и сведения, являющиеся коммерческой тайной.

3.3 Использовать только принятые в Обществе программные инструменты и технологию разработки программного обеспечения.

3.4 Соблюдать трудовую и производственную дисциплину, правила и нормы охраны труда, требования производственной санитарии и гигиены, требования противопожарной безопасности.

Ведущий программист привлекается к ответственности:

3.5 За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией, в порядке, установленном действующим трудовым законодательством Российской Федерации;

3.6 За правонарушения и преступления, совершенные в процессе своей деятельности, в порядке, установленном действующим административным, уголовным и гражданским законодательством Российской Федерации;

3.7 За причинение ущерба организации в порядке, установленном действующим трудовым законодательством Российской Федерации.

# 2 ОСНОВНЫЕ НАПРАВЛЕНИЯ АДМИНИСТРИРОВАНИЯ БАЗ ДАННЫХ И СЕРВЕРОВ

# 2.1 Технические проблемы, возникающие в процессе эксплуатации баз данных

Эксплуатация баз данных связана с рядом технических проблем, среди которых наиболее распространенными являются:

1. Потери данных: Могут возникать вследствие неправильных действий администраторов, случайного удаления важных записей или аппаратных сбоев.
2. Перегрузки и снижение производительности: Избыточное количество одновременных обращений к данным, неоптимальные запросы и неэффективные алгоритмы приводят к замедлению работы всей системы.
3. Технические неисправности: Выход из строя дисков, оперативной памяти, процессора или сетевых интерфейсов негативно сказывается на работе базы данных.
4. Безопасность: Постоянная угроза взлома, вредоносных программ и несанкционированного доступа требует регулярных проверок уровня защиты и устранения уязвимостей.
5. Неправильная конфигурация: Ошибочные настройки хранения, индексации или репликации могут привести к некорректному функционированию базы данных.
6. Отказ оборудования: Например, выход из строя жесткого диска или блока питания приведет к полной остановке работы системы.

# 2.2 Администрирование отдельных компонент серверов

1. Администрирование серверов подразумевает выполнение ряда функций для поддержания стабильной и безопасной работы систем:
2. Установка и настройка: Включает установку операционной системы, драйверов, необходимых сервисов и программного обеспечения.
3. Мониторинг состояния: Постоянный контроль ресурсов сервера (процессор, память, дисковая подсистема), состояние служб и протоколов.
4. Обновление и патчинг: Своевременное применение обновлений безопасности и исправлений критичных багов в системах и приложениях.
5. Резервное копирование: Создание периодических копий важной информации и разработка стратегии быстрого восстановления после потерь данных.
6. Управление доступом: Контроль и ограничение доступа пользователей к ресурсам сервера, назначение ролей и привилегий.
7. Оптимизация производительности: Настройка SQL-запросов, создание индексов, улучшение архитектуры приложения для повышения скорости отклика.
8. Поддержка бесперебойной работы: Предупреждение и устранение потенциальных причин отказов и деградации качества обслуживания.

# 2.3 Требования, предъявляемые к конфигурации локальных компьютерных сетей и серверного оборудования

Для надежной и эффективной работы сети и серверов важно учитывать ряд требований:

1. Производительность: Система должна справляться с нагрузкой, обеспечивая необходимую производительность даже при пиковых нагрузках.
2. Доступность: Локальная сеть и серверы должны поддерживать высокий уровень готовности, исключая длительные простои.
3. Масштабируемость: Возможность увеличения объема обрабатываемых данных и числа пользователей без потери стабильности.
4. Совместимость: Серверное оборудование должно взаимодействовать с используемым программным обеспечением и поддерживаться производителями ПО.
5. Безотказность: Использование дублирующих решений (резервные каналы, RAID-массивы, кластеры) для минимизации последствий выхода из строя оборудования.
6. Информационная безопасность: Средства защиты от внешнего проникновения, проверка подлинности пользователей, механизмы шифрования данных.
7. Простота управления: Удобные инструменты мониторинга и диагностики, автоматизация рутинных процессов.

# 2.4 Аудит систем безопасности баз данных и серверов

Аудит направлен на оценку текущего уровня безопасности системы и выявления слабых мест:

1. Анализ текущих настроек безопасности: Проверяется правильность конфигурирования брандмауэра, учетных записей, разрешений и шифрования.
2. Тестирование на наличие уязвимостей: Используются специальные программы и методики тестирования на проникновение для обнаружения возможных точек входа злоумышленника.
3. Оценка соблюдения внутренних стандартов безопасности: Соответствие корпоративным стандартам и законодательным нормам в области защиты информации.
4. Реакция на инциденты: Оцениваются планы реагирования на возможные угрозы, эффективность используемых инструментов слежения и предупреждения атак.
5. Контроль журналов активности: Анализируются журналы попыток входа, изменения данных и прочие события, позволяющие выявить подозрительную активность.

# 2.5 Регламенты по защите информации баз данных

Для защиты данных разработаны строгие правила и инструкции, обязательные для исполнения всеми пользователями и подразделениями организации:

1. Классификация данных: Определение уровней конфиденциальности информации, разделение её на категории согласно важности и риску ущерба.
2. Физическая безопасность: Ограничение физического доступа к серверам и помещениям, содержащим важные данные.
3. Логический доступ: Назначение индивидуальных учетных записей пользователям, управление ролями и разрешениями, двухфакторная аутентификация.
4. Шифрование: Обязательное использование криптографических методов для защиты передаваемых и хранимых данных.
5. Архивирование и резервное копирование: Регулярное создание архивных копий данных, хранение резервных копий вне основной площадки.
6. Регулярные проверки: Проведение аудитов и стресс-тестов для оценки надежности и безопасности системы.
7. Подготовка сотрудников: Повышение осведомленности сотрудников о правилах информационной безопасности, обучение правильному обращению с информацией.

# 3 ВЫПОЛНЯЕМЫЕ ЗАДАНИЯ

Задание 1

1) Выбор предметной области:

База данных для хранения результатов автоматического контроля качества металлопроката.

Данная база данных имеет название “MetalDB”. В ней созданы таблицы с помощью SQL-запросов. Таблицы изображены на Рисунке 1.

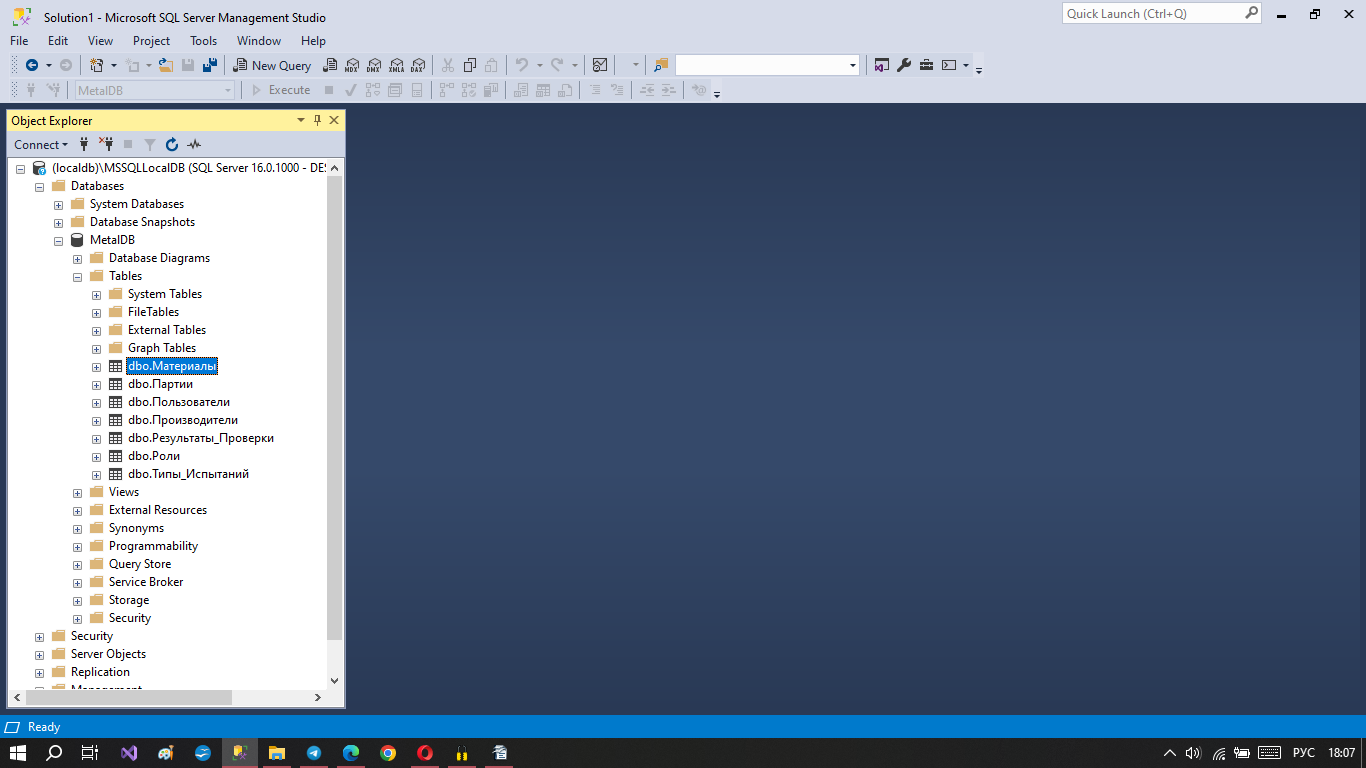


Рисунок 1 - Таблицы в БД “MetalDB”

Таблица “Материалы” представлена на Рисунке 2.

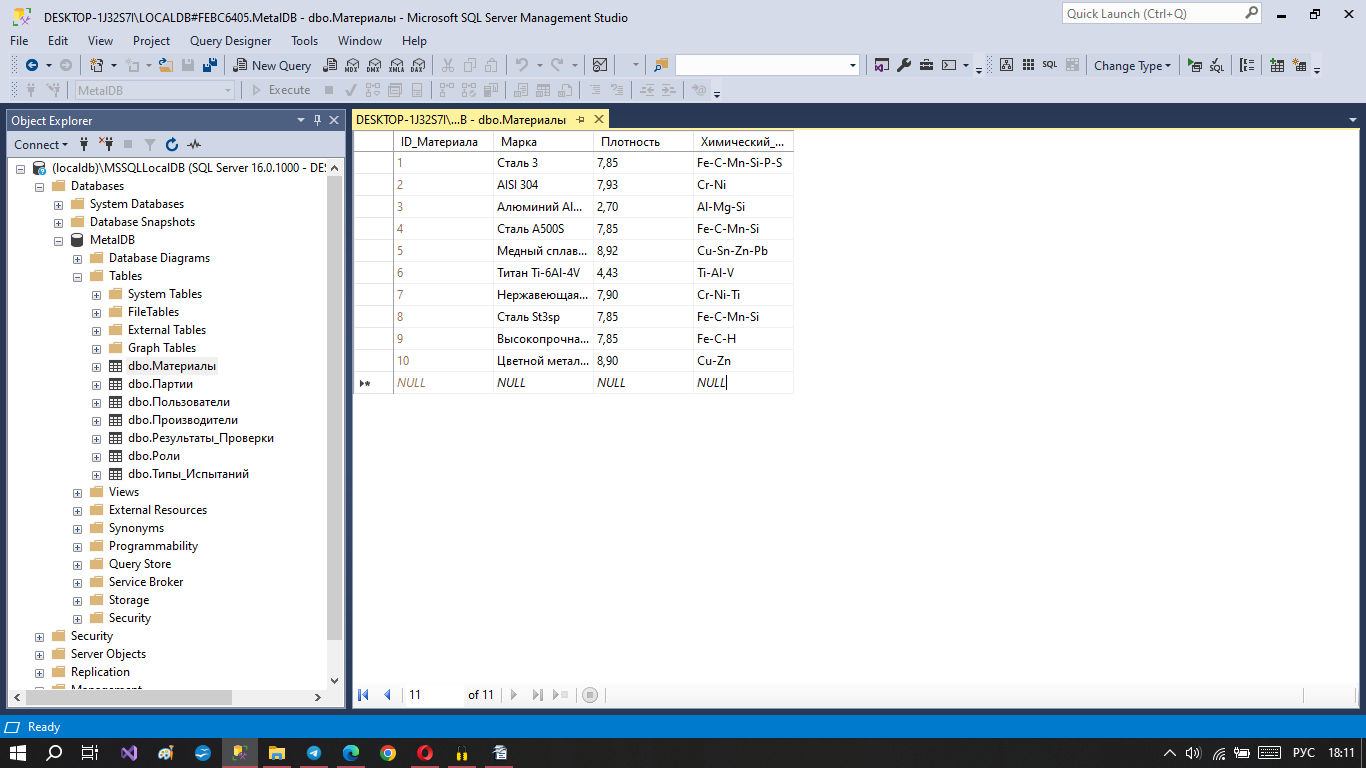


Рисунок 2 - Таблица “Материалы”

Таблица “Партии” представлена на Рисунке 3.

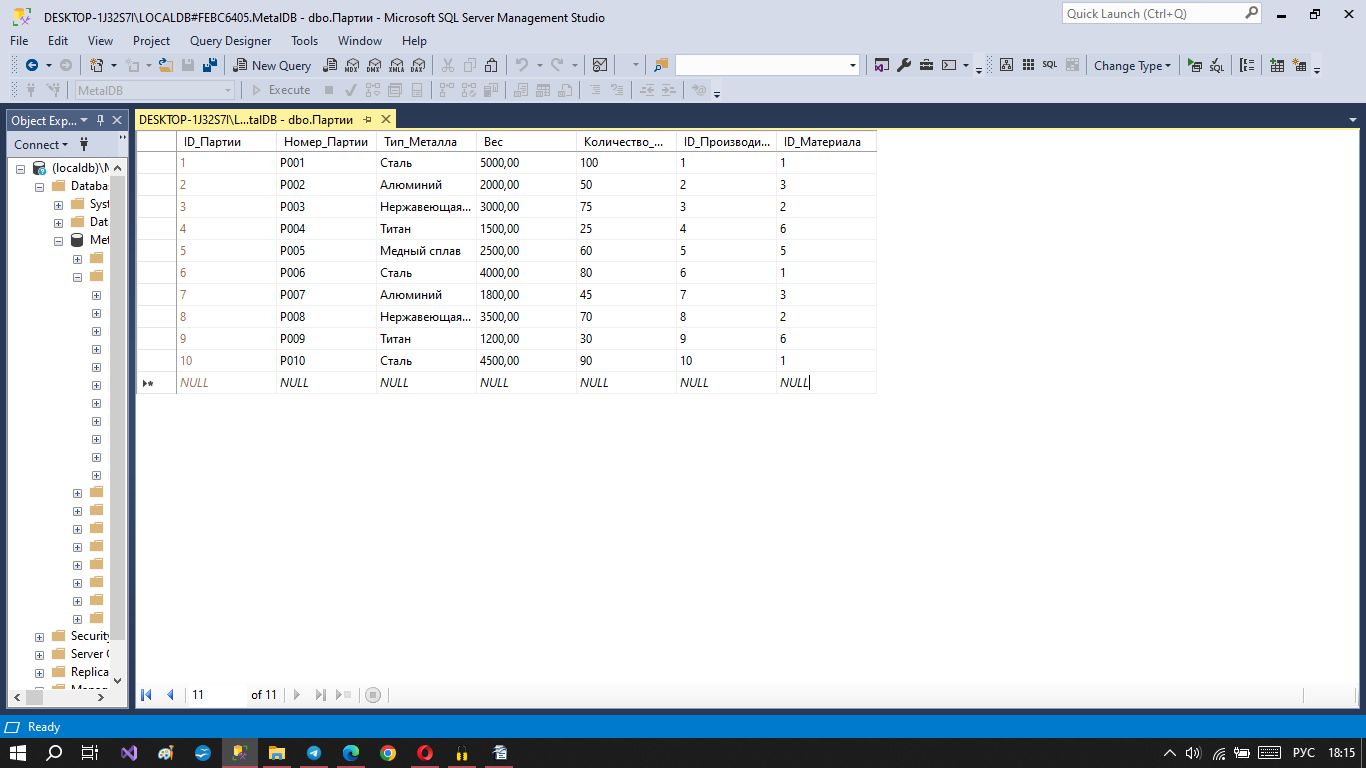


Рисунок 3 - Таблица “Партии”

Таблица “Пользователи” представлена на Рисунке 4.

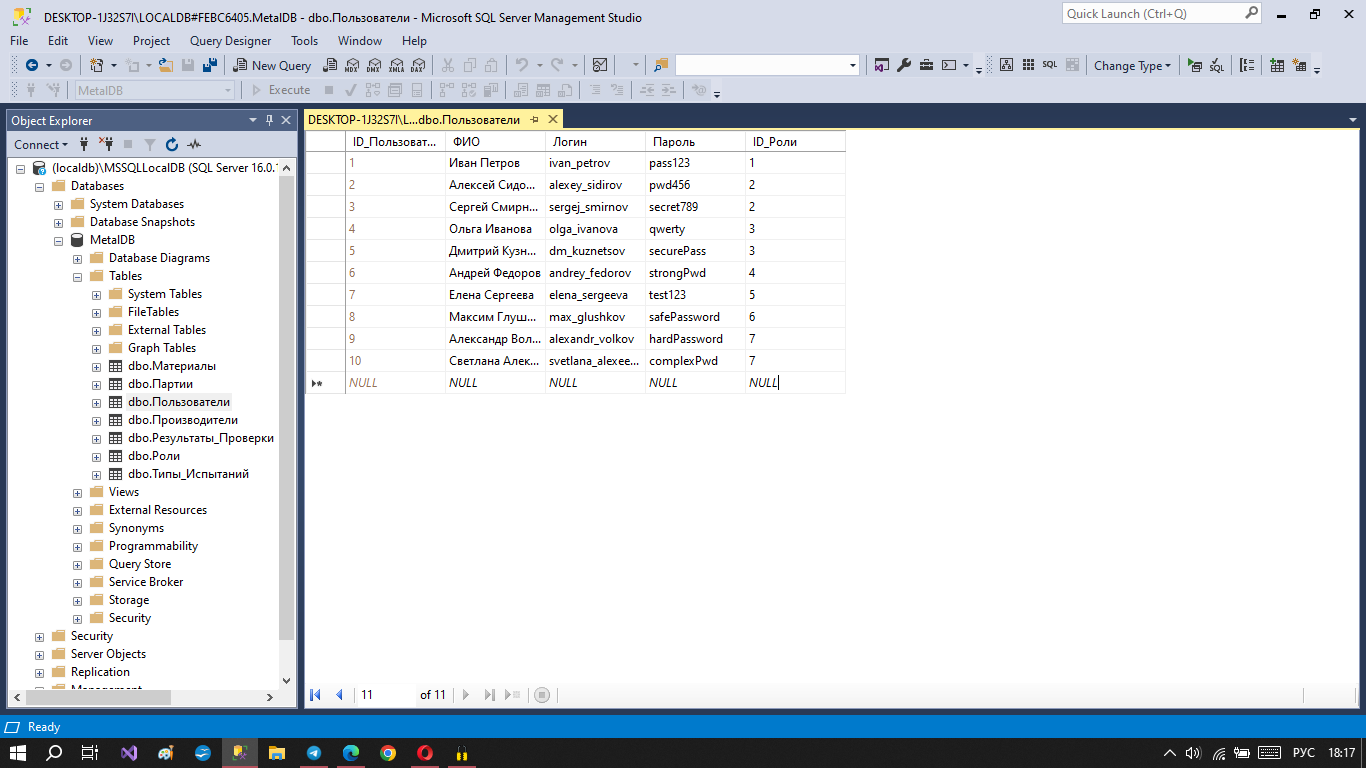


Рисунок 4 - Таблица “Пользователи”

Таблица “Производители” представлена на Рисунке 5.

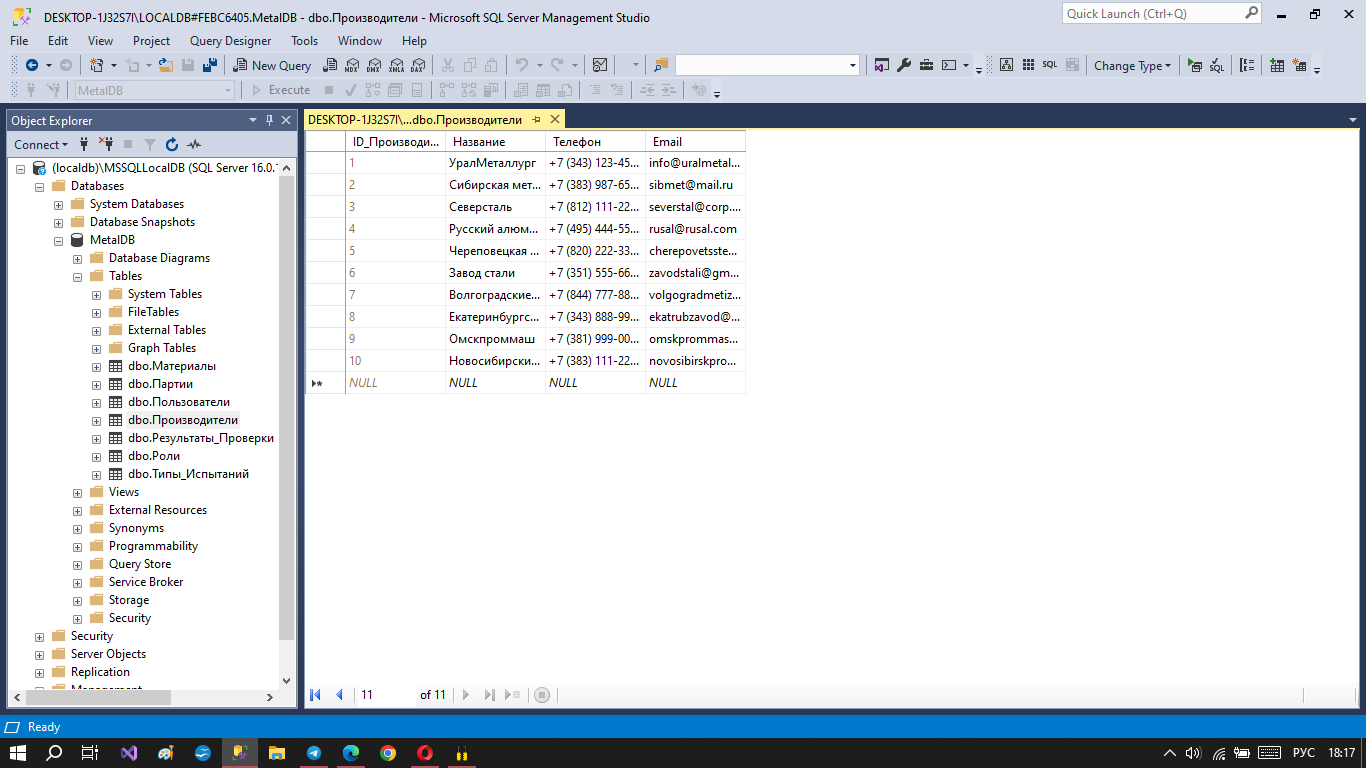


Рисунок 5 - Таблица “Производители”

Таблица “Результаты\_Проверки” представлена на Рисунке 6.

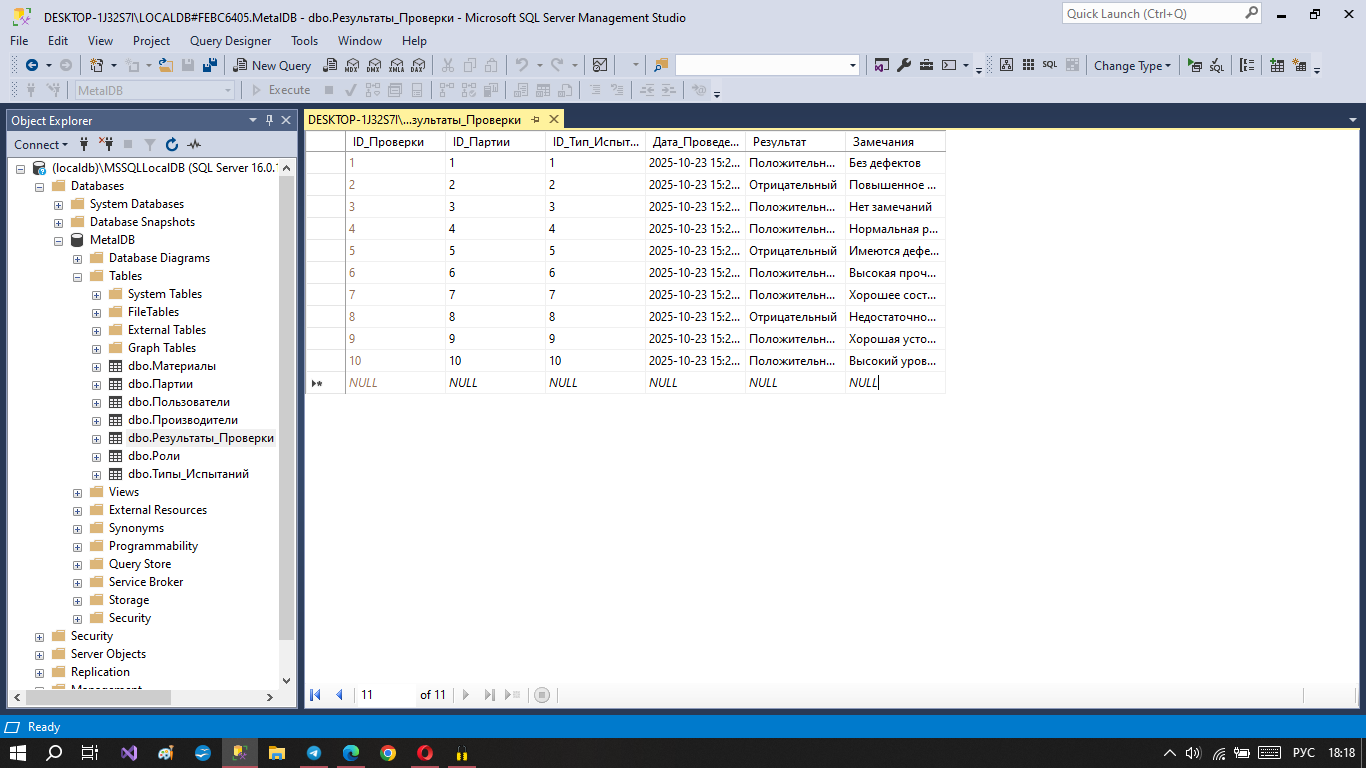


Рисунок 6 - Таблица “Результаты\_Проверки”

Таблица “Роли” представлена на Рисунке 7.

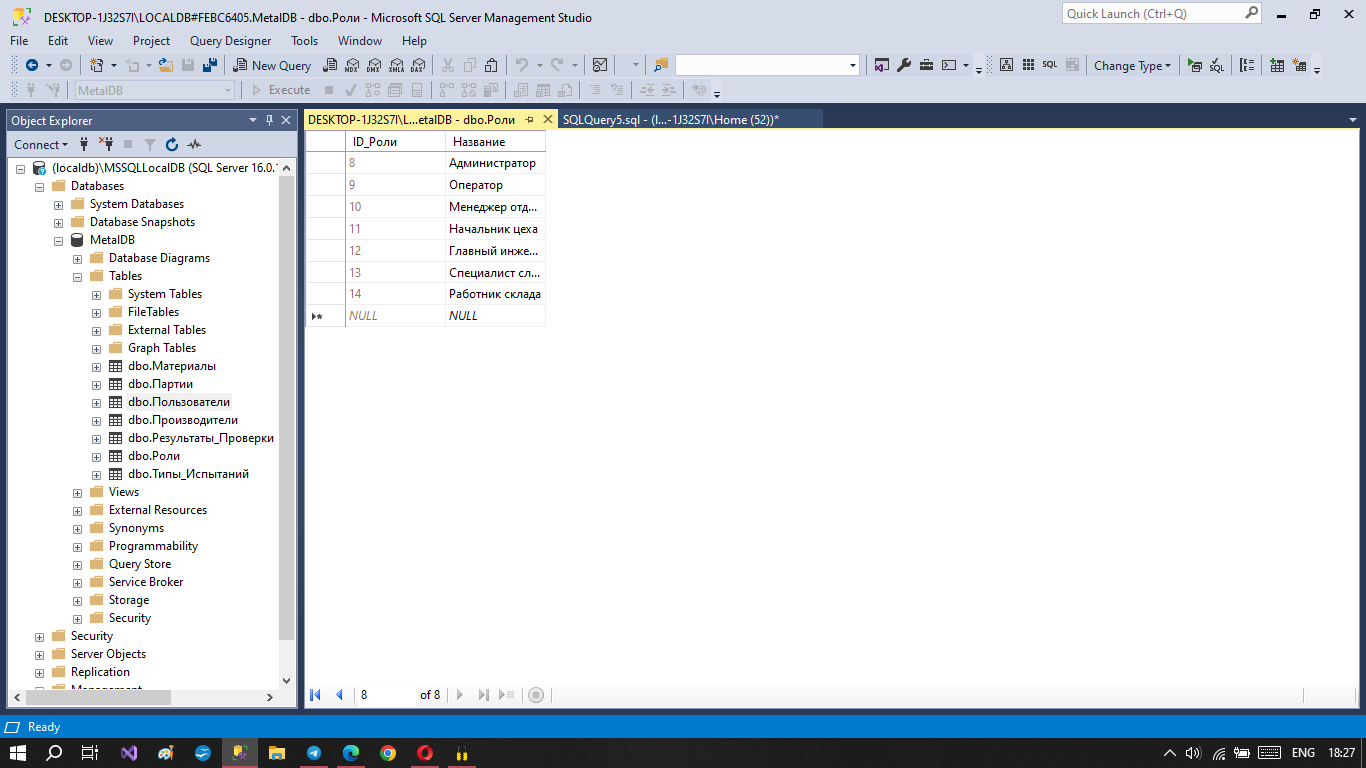


Рисунок 7 - Таблица “Роли”

Таблица “Типы\_Испытаний” представлена на Рисунке 8.

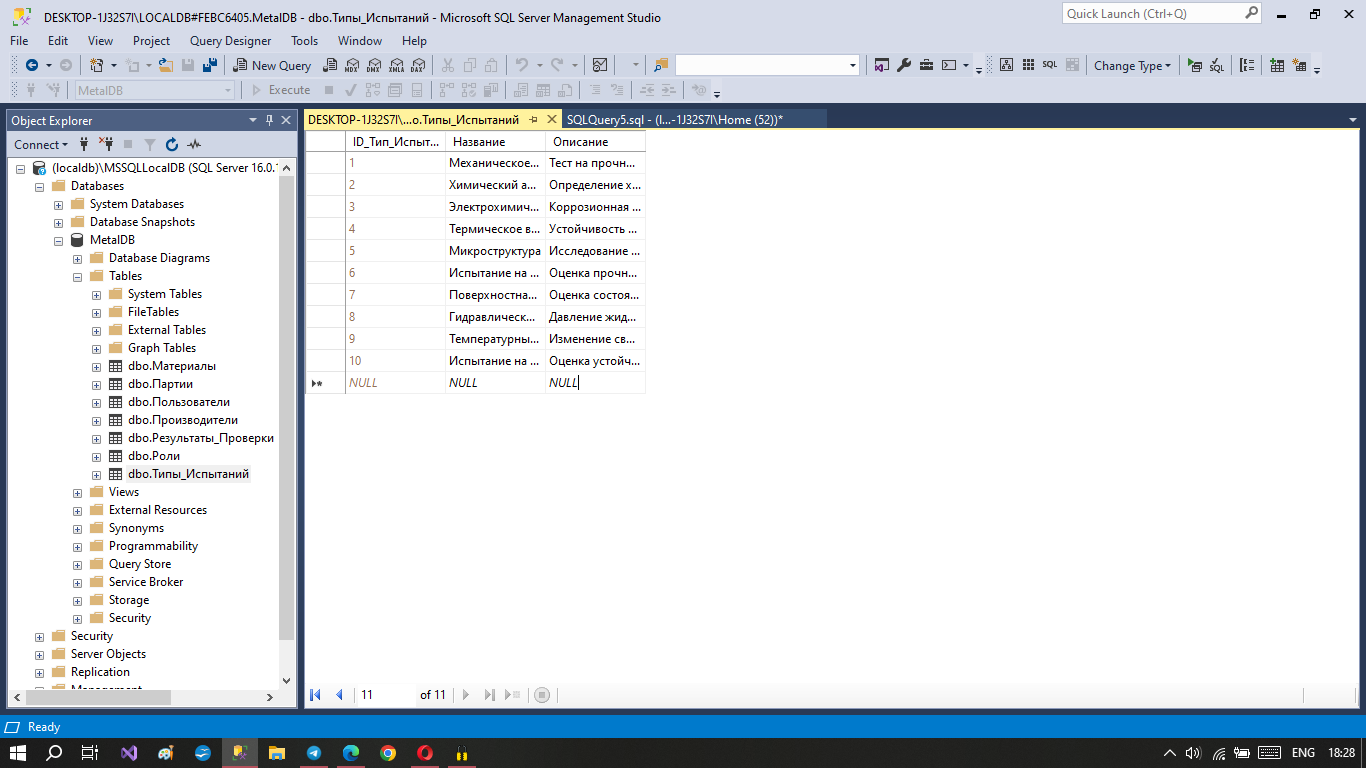


Рисунок 8 - Таблица “Типы\_Испытаний”

Задание 2

1) Необходимо для выбранной темы разработать программное приложение (ПП) для работы с базой данных (БД), с графическим интерфейсом.

ПП должно содержать:

a. Выбор базы данных и подключение к ней.

b. Работа с каждой существующей в этой базе данных таблицей (добавление, изменение и удаление записей).

c. Администрирование ролей и пользователей БД для данных баз данных. Добавление, Изменение и Удаление происходят в диалоговых окнах.

2) Требования к технологиям для разработки на C#:

a. Платформа: .NET 9 (C#)

b. Для реализации базы данных: MS SQL.SERVER

c. Для взаимодействия с базой данных: EntityFramework

d. Для реализации UI: WinForms