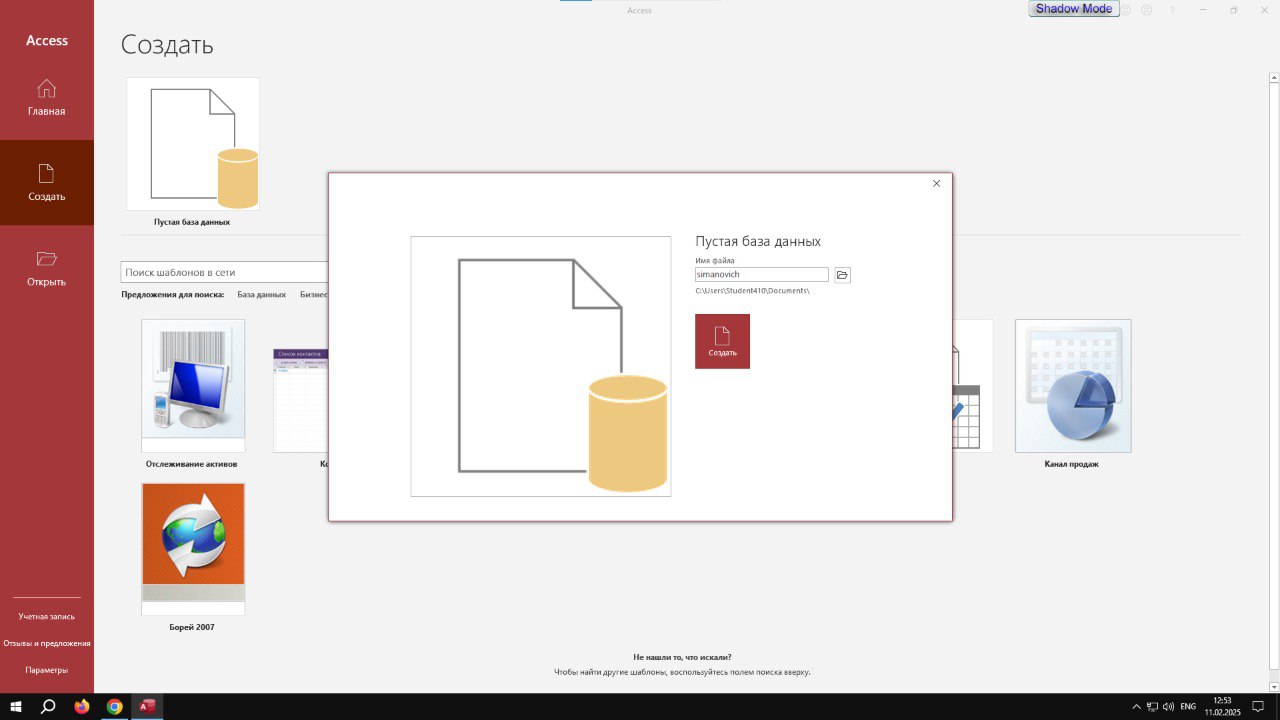
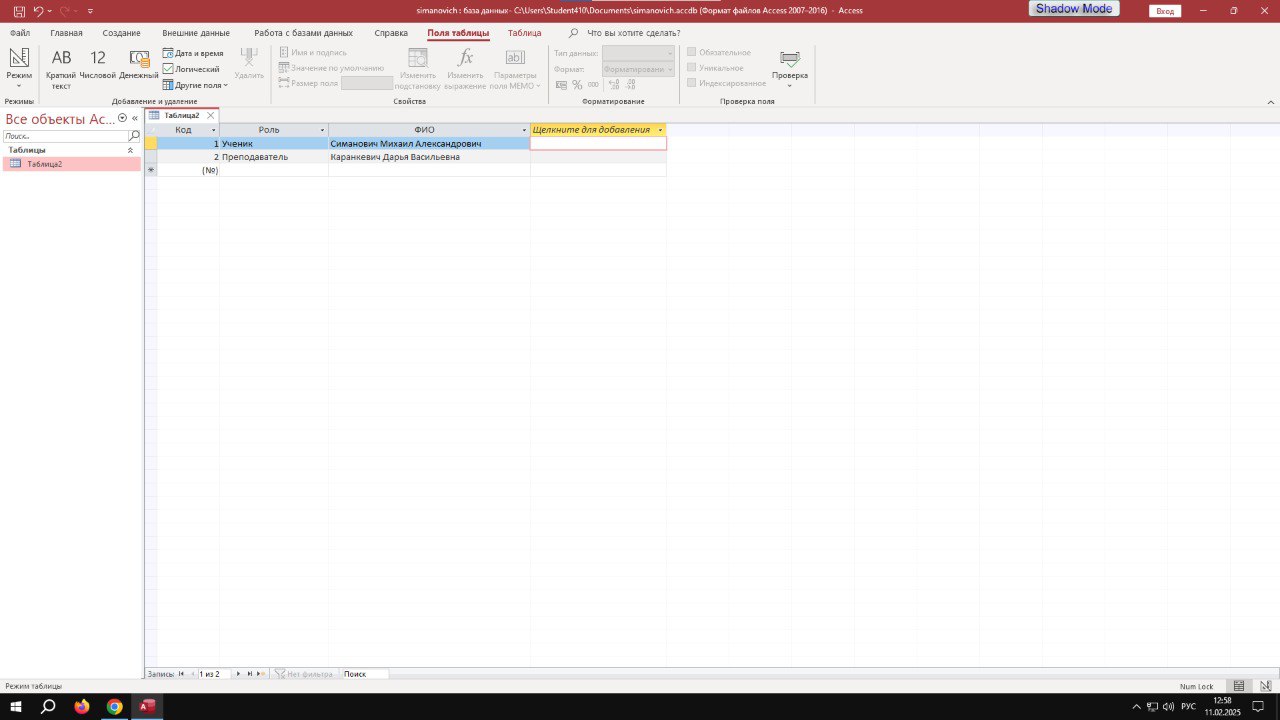
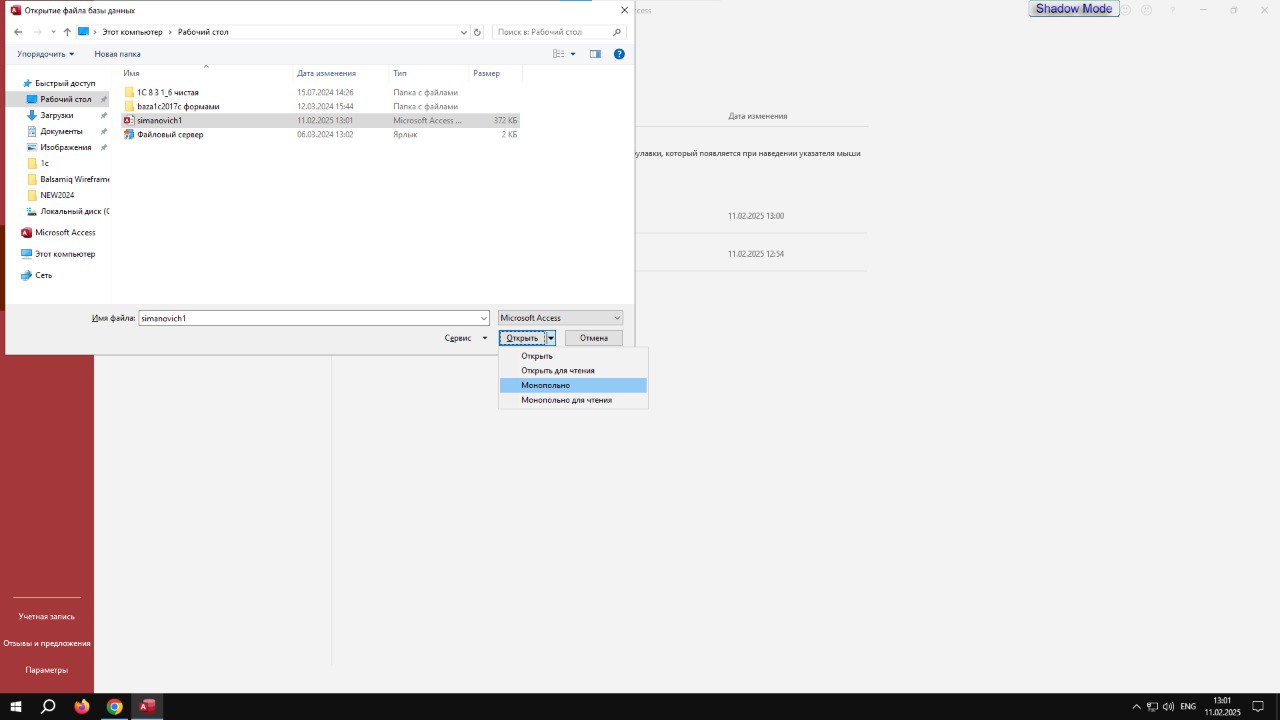
**Отчет по Лабораторной работе 11**

# 1.Создаем базу данных

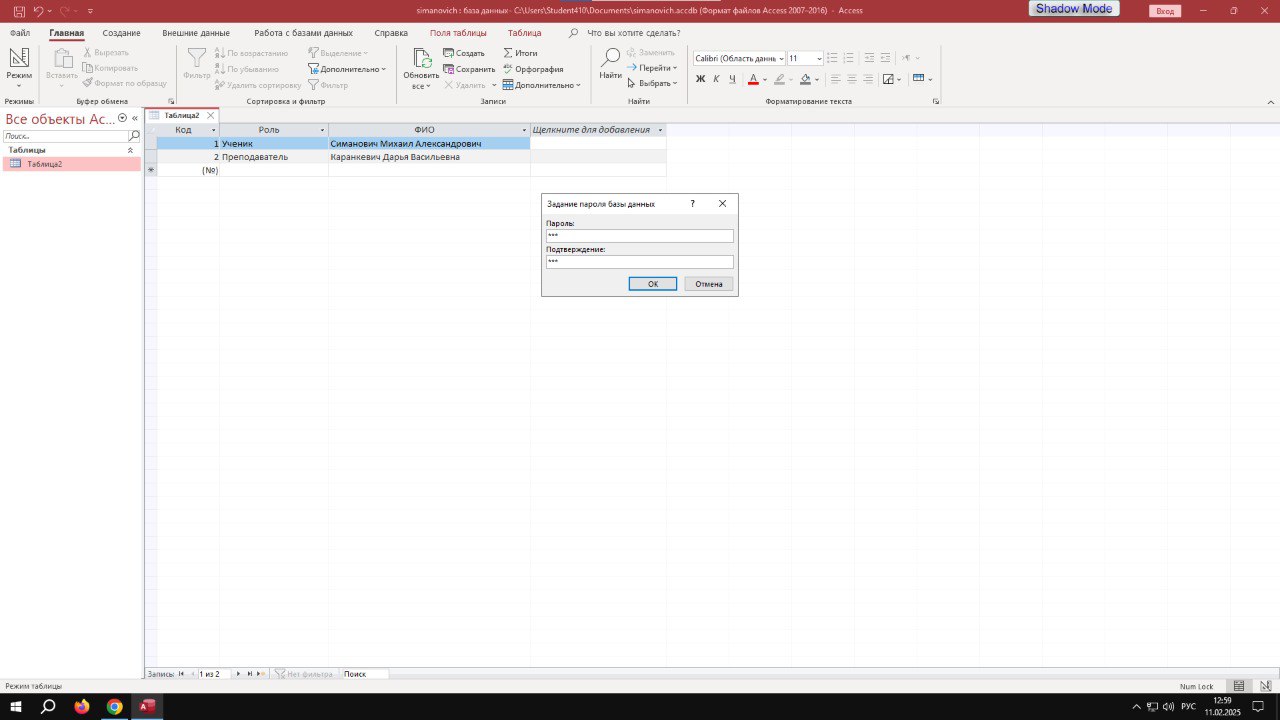




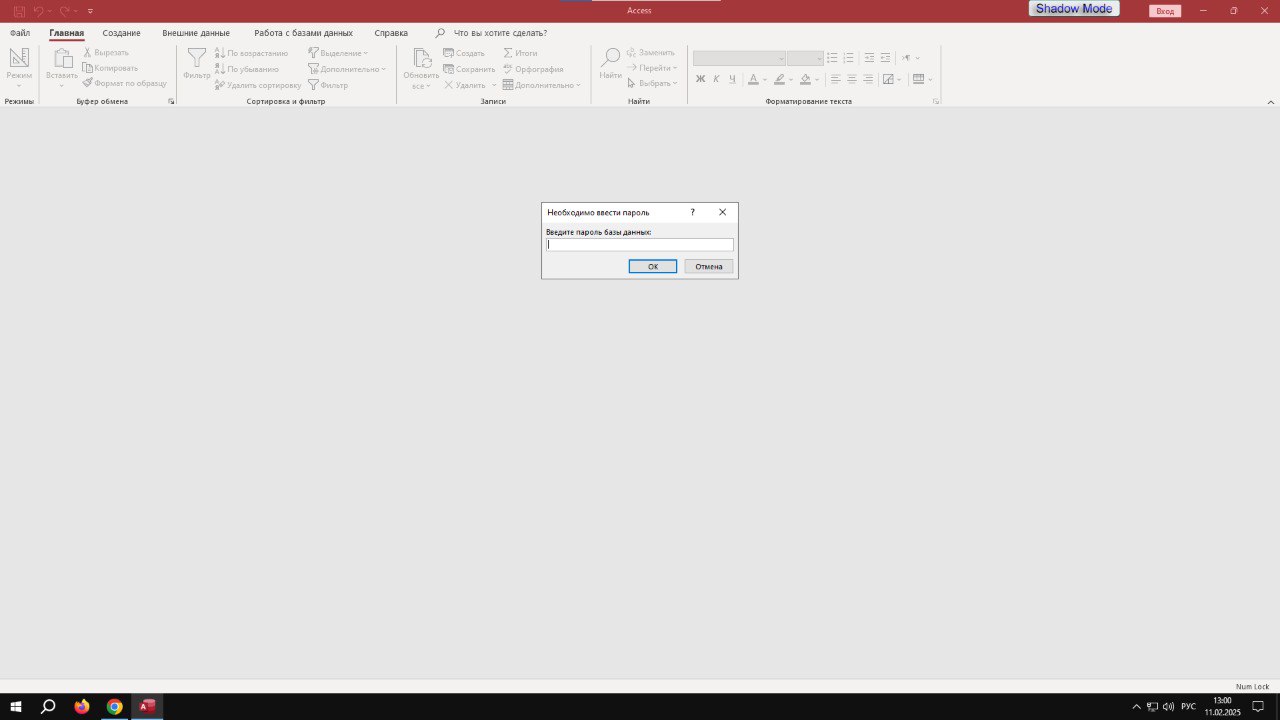
# 2.Сохраняем и открываем монопольно



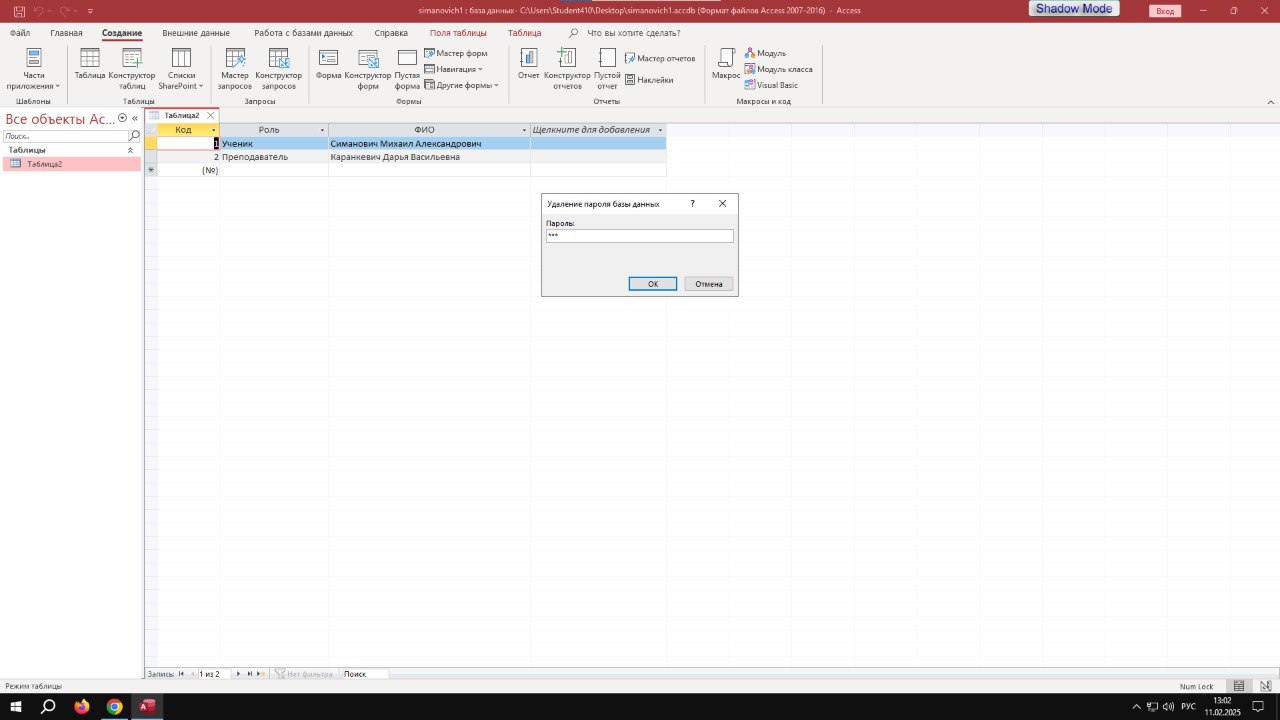
# 3. Задаем пароль



# 4.Результат задачи пароля



# 5. Удаляем пароль



**Контрольные вопросы**

**1. Способы защиты данных в Microsoft Access**

Для обеспечения безопасности базы данных Access применяются следующие методы:

* **Парольная защита** – установка пароля для открытия базы данных.
* **Рабочая группа безопасности** – использование файла рабочей группы (.mdw) для управления правами пользователей.
* **Ограничение доступа** – настройка прав на просмотр, редактирование, удаление и создание объектов.
* **Шифрование** – встроенные механизмы защиты для предотвращения несанкционированного доступа.
* **Форматы MDE/ACCDE** – преобразование базы в формат, защищающий код VBA от изменений.
* **Внешняя защита** – использование системы NTFS для управления доступом на уровне операционной системы.

**2. Пользователи, группы и файл рабочей группы в Access**

* **Пользователи** – каждый пользователь обладает определенным уровнем доступа (администратор, стандартный пользователь, гость).
* **Группы** – объединения пользователей с одинаковыми правами (например, стандартные группы *Admins* и *Users*).
* **Файл рабочей группы (.mdw)** – содержит информацию о пользователях, группах и их правах, применяется для многоуровневой защиты данных.

**3. Основные объекты базы данных Access и управление доступом**

**Объекты базы данных:**

* **Таблицы**
* **Запросы**
* **Формы**
* **Отчеты**
* **Макросы**
* **Модули**

**Уровни прав доступа:**

* **Чтение** – просмотр данных.
* **Редактирование** – внесение изменений.
* **Удаление** – удаление данных или объектов.
* **Полный контроль** – полный доступ с возможностью изменения прав других пользователей.

**Владелец объекта** – пользователь или группа, создавшая объект. Только владелец может изменять права доступа или передавать их другим.

**4. Основные шаги по защите базы данных Access**

1. **Определение стратегии безопасности** – назначение ролей и прав пользователей.
2. **Создание файла рабочей группы** – настройка .mdw с добавлением пользователей и групп.
3. **Установка пароля администратора** – защита учетной записи Admin надежным паролем.
4. **Добавление пользователей и групп** – распределение ролей среди пользователей.
5. **Настройка доступа к объектам** – ограничение прав для минимизации рисков.
6. **Шифрование базы** – использование встроенных средств защиты.
7. **Резервное копирование** – регулярное создание копий базы данных.
8. **Проверка безопасности** – тестирование настроенных ограничений и доступа.

4o