

## Тема: Система безопасности Microsoft Access

Цель работы: ознакомление с основными возможностями системы безопасности Microsoft Access.

Время выполнения – 4 часа.

### 1. Постановка задачи

Отработать вопросы, связанные с обеспечением безопасности данных своей спроектированной БД в Microsoft Access версий старше 2007.

1. Предоставление доверия базе данных в текущем сеансе работы.
2. Создание доверенного места размещения БД.
3. Перемещение базы данных в доверенное место расположения.
4. Создание собственного сертификата.
5. Создание подписанного пакета.
6. Извлечение и использование подписанного пакета.
7. Включение отключенного содержимого базы данных при ее открытии.
8. Зашифрование и расшифрование данных БД.

### 2. Отработка вопросов лабораторной работы.

Основные методические указания выполнения лабораторной работы с конкретными примерами приведены ниже.

Каждый студент в соответствии с данными методическими указаниями выполняет работу для своей спроектированной базы данных и представляет свой индивидуальный отчет.

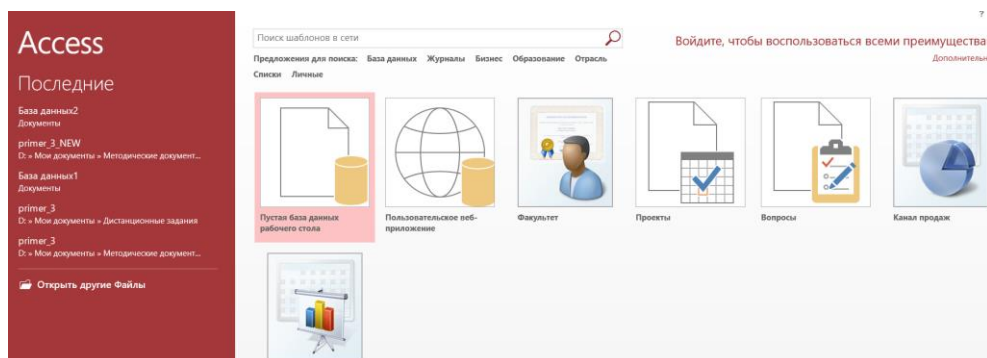
Последовательность выполняемых действий для отработки 1 вопроса задания.

#### Предоставление доверия базе данных в текущем сеансе работы

#### Пример для Microsoft Access 2007

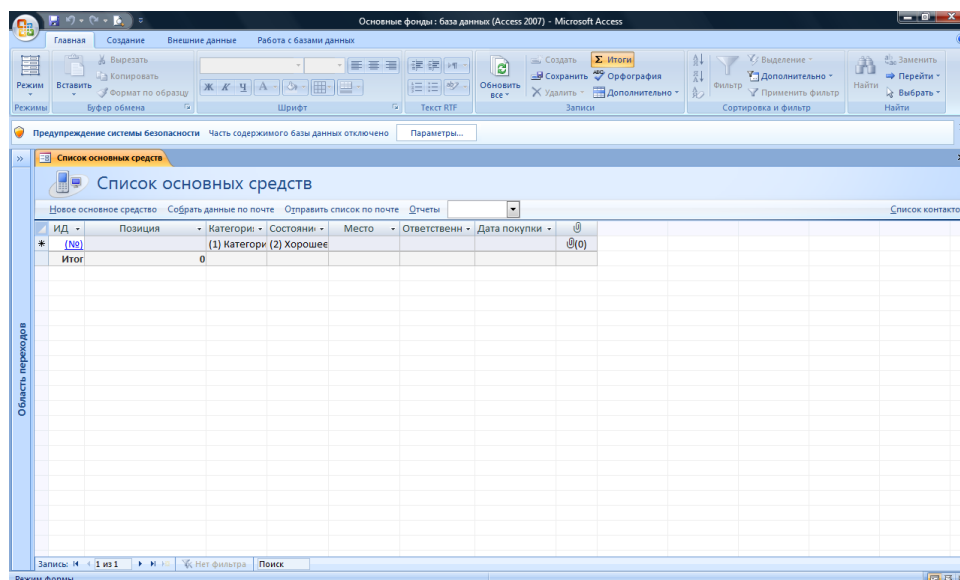
1. Запустите Office Access и на странице *Приступая к работе с Microsoft Office Access* в разделе *Шаблоны из Интернета*, щелкните значение *Основные фонды*, чтобы открыть шаблон «Основные фонды».

*Примечание: можно выбрать любой шаблон (см. рисунок ниже для Access 2013)*



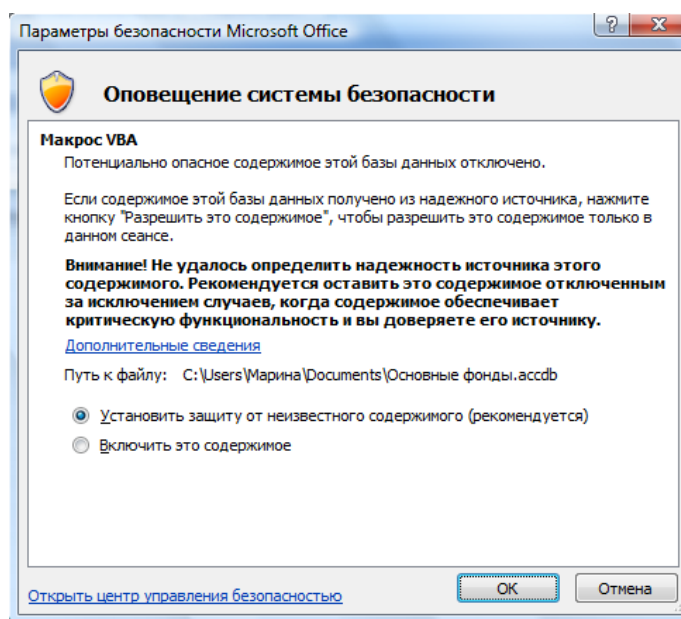
2. В поле *Имя файла* введите имя новой базы данных и нажмите кнопку *Загрузка*.

Будет загружен шаблон базы данных и создана новая база данных, при этом появится панель сообщений.



3. На панели сообщений щелкните *Параметры*.

Откроется диалоговое окно *Параметры безопасности Microsoft Office*.



4. Щелкните *Включить это содержимое* и нажмите кнопку *OK*.

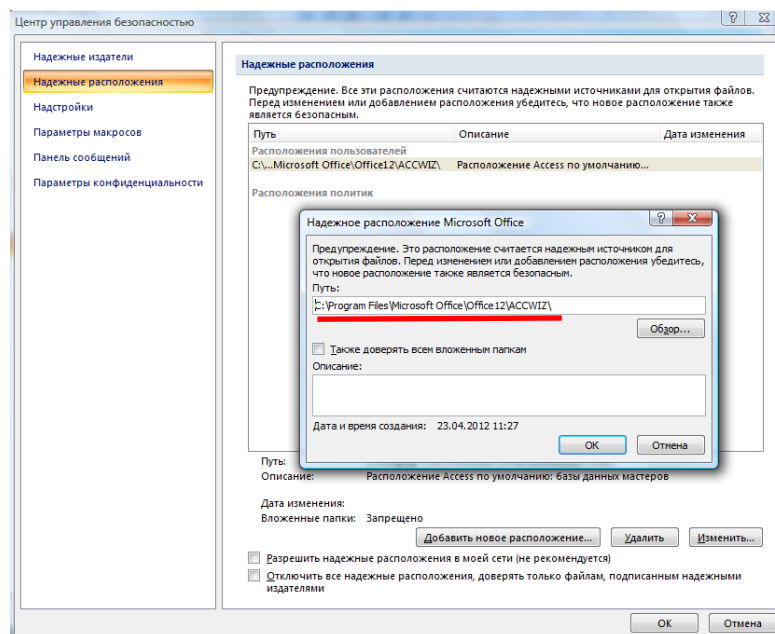
**ПРИМЕЧАНИЕ.** Если при открытии базы данных выводится панель сообщений, можно перейти непосредственно к шагу 3.

Последовательность выполняемых действий для отработки 2 вопроса задания.

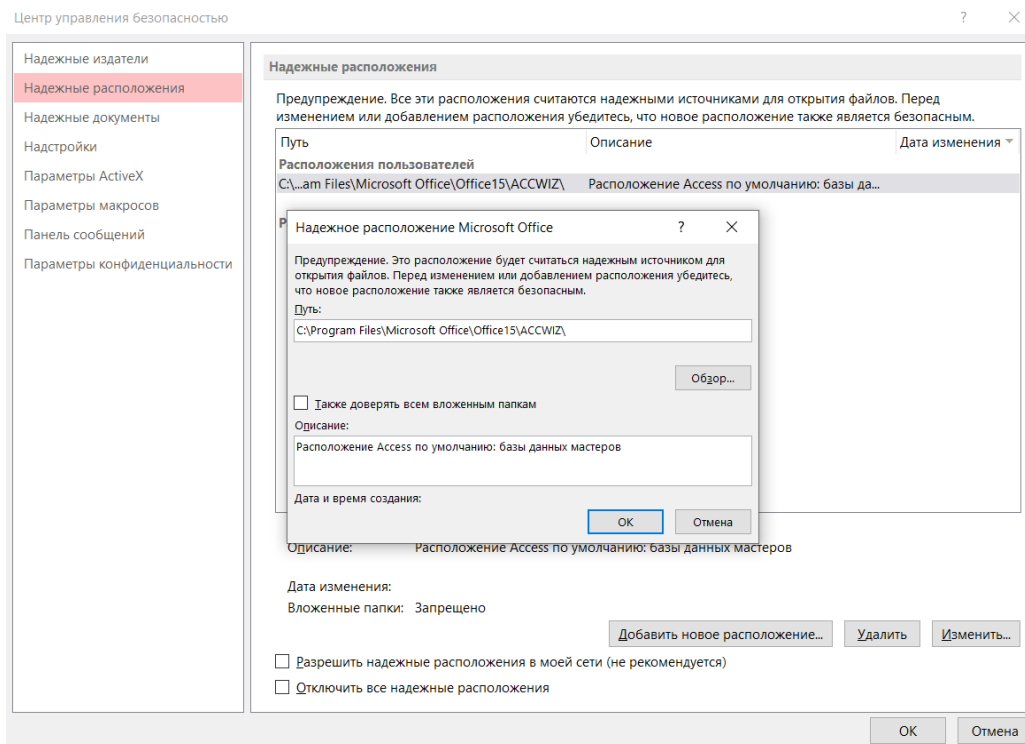
#### *Создание доверенного места*

1. Запустите Office Access версий старше 2007 (для выполнения этих шагов не нужно открывать базу данных).

2. Нажмите кнопку *Microsoft Office* и выберите команду *Параметры Access*.  
Откроется диалоговое окно *Параметры Access*.
3. В левой области этого диалогового окна нажмите кнопку *Центр управления безопасностью*, а затем в правой области щелкните *Параметры центра управления безопасностью*.  
Откроется диалоговое окно *Центр управления безопасностью*.
4. В левой области нажмите *Надежные расположения*.
5. Щелкните кнопку *Добавить новое расположение*.  
Откроется диалоговое окно *Надежное расположение Microsoft Office*.



## Access 2007



## Access 2013

6. В поле *Путь* введите путь к файлу и имя папки для места, которое нужно сделать доверенным источником, либо нажмите кнопку *Обзор* и перейдите к этой папке. По умолчанию такая папка должна находиться на локальном диске.

**ПРИМЕЧАНИЕ.** Если требуется указать доверенные сетевые папки, в диалоговом окне *Центр управления безопасностью* отметьте флажок (рис. 1) *Разрешить надежные расположения в моей сети* (не рекомендуется).


7. Нажмите кнопку *ОК*, чтобы закрыть все диалоговые окна.

**ПРИМЕЧАНИЕ.** Чтобы завершить процедуру и предоставить базе данных доверие на постоянной основе, необходимо переместить эту базу данных в доверенное место. В следующих шагах объясняются некоторые из наиболее распространенных способов перемещения базы данных.

Последовательность выполняемых действий для отработки 3 вопроса задания.

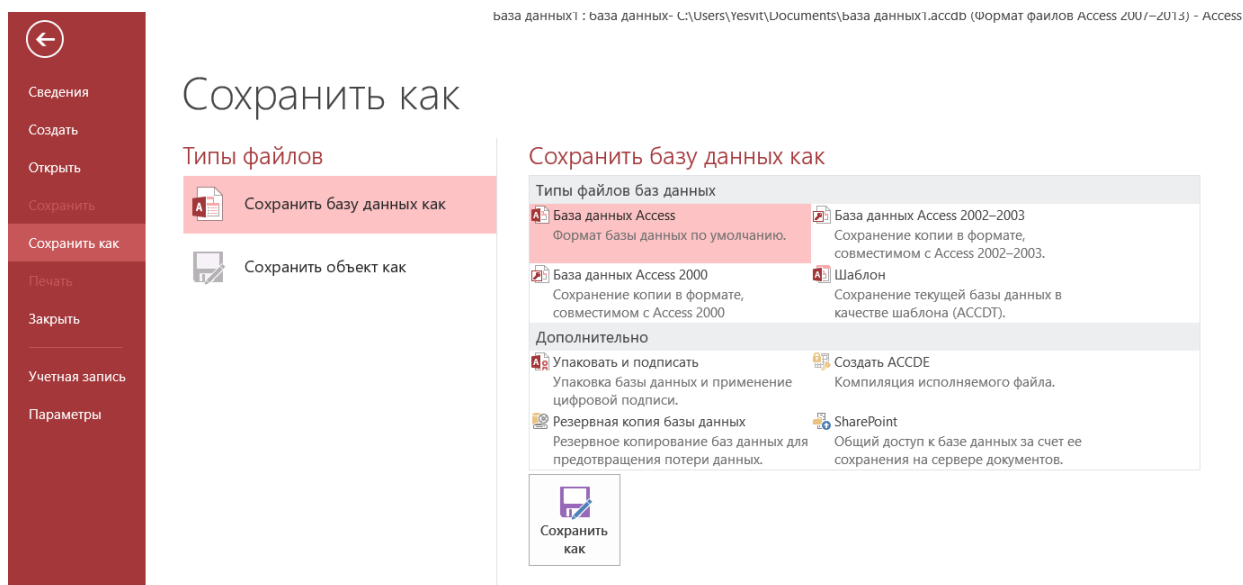
### *Перемещение базы данных в доверенное место*

#### *Если база данных открыта*

1. Нажмите кнопку *Microsoft Office* .
2. Выделите команду *Сохранить как* и в разделе *Сохранить базу данных в другом формате* выберите один из доступных параметров.
3. В диалоговом окне *Сохранение* перейдите к доверенному месту, а затем нажмите кнопку *Сохранить*.

#### *Если база данных не открыта*

1. Запустите проводник Windows. Для этого нажмите кнопку *Пуск* и последовательно выберите команды *Все программы*, *Стандартные* и *Проводник Windows*.
2. Найдите и скопируйте базу данных. Для этого щелкните файл правой кнопкой мыши и выберите в контекстном меню команду *Копировать*.  
-или-  
*Клавиши быстрого доступа*. Выберите (выделите) файл и нажмите сочетание клавиш CTRL+C.
3. Создайте доверенную папку, откройте ее, щелкните в ней правой кнопкой мыши и выберите в контекстном меню команду *Вставить*.  
-или-  
*Клавиши быстрого доступа*. Нажмите сочетание клавиш CTRL+V, чтобы вставить базу данных в новое место.



### Access 2013

Последовательность выполняемых действий для отработки 4 вопроса задания.

#### Создание собственного сертификата

1. Нажмите кнопку *Пуск* и последовательно выберите пункты *Все программы*, *Microsoft Office*, *Средства Microsoft Office* и *Цифровой сертификат для проектов VBA*.

-или-

Перейдите к папке, содержащей программные файлы Office Профессиональный. Например, для версии *Microsoft Office 2007* По умолчанию используется папка *Диск:\Program Files\Microsoft Office\Office12*. В этой папке найдите и дважды щелкните файл *SelfCert.exe*.


Будет открыто диалоговое окно *Создание цифрового сертификата*.

2. В поле *Название сертификата* введите имя нового сертификата.
3. Два раза нажмите кнопку *ОК*.

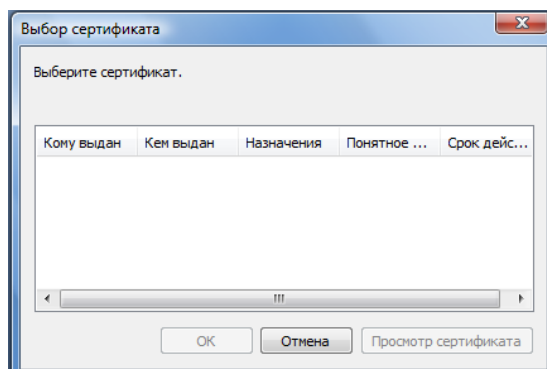
**ПРИМЕЧАНИЕ.** Если команда *Цифровой сертификат для проектов VBA* недоступна или не удастся найти файл *SelfCert.exe*, возможно, требуется установить средство *SelfCert*.

Последовательность выполняемых действий для отработки 5 вопроса задания.

#### Создание подписанного пакета

1. Откройте базу данных, для которой требуется создать пакет и подписать его (база данных должна иметь новый формат: **.accdb**, **.accde**, но не **.mdb**).
2. Нажмите кнопку *Microsoft Office* , выберите команду *Опубликовать*, а затем команду *Упаковать и подписать*.


Откроется диалоговое окно *Выбор сертификата*.

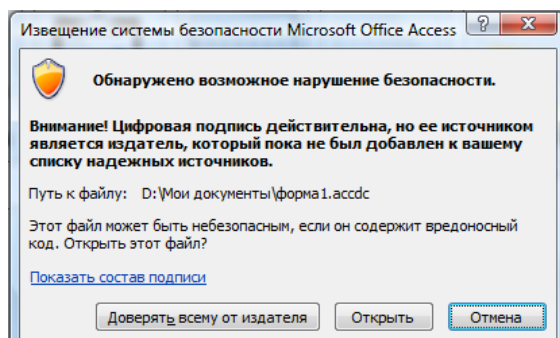


3. Выберите цифровой сертификат, а затем нажмите кнопку *ОК*.  
Откроется диалоговое окно *Создать подписанный пакет Microsoft Office Access*.
4. В списке *Сохранить в* выберите расположение для подписанного пакета базы данных.
5. В поле *Имя файла* введите имя для подписанного пакета, а затем нажмите кнопку *Создать*.  
Access создаст ACCDC-файл и поместит его в выбранное расположение.

Последовательность выполняемых действий для отработки 6 вопроса задания.

#### *Извлечение и использование подписанного пакета*

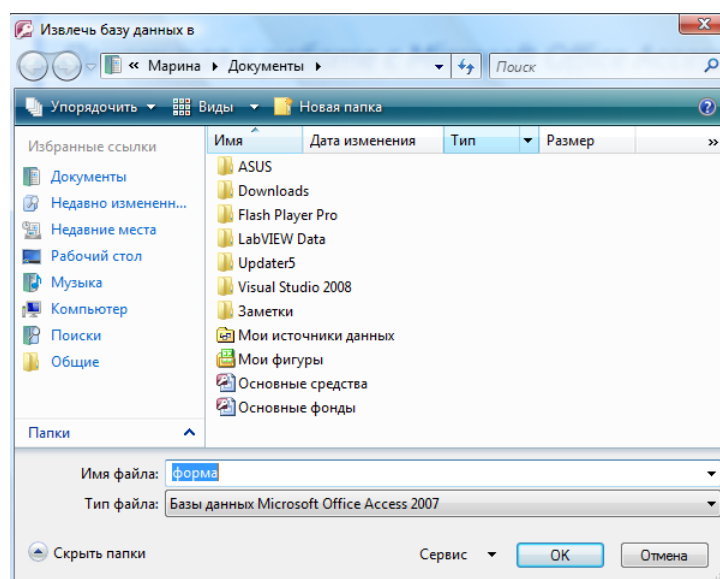
1. Щелкните значок *Кнопка Microsoft Office* , а затем выберите команду *Открыть*.  
Откроется диалоговое окно *Открыть*.
2. В списке *Тип файлов* выберите вариант *Подписанные пакеты Microsoft Office Access (\*.accdc)*.
3. Воспользуйтесь списком *Папка*, чтобы найти папку, содержащую ACCDC-файл, выделите этот файл и нажмите кнопку *Открыть*.
4. Выполните одно из следующих действий.
  - Если выбран параметр доверия к цифровому сертификату, примененному к развернутому пакету, появится диалоговое окно *Извлечь базу данных в*. Перейдите к следующему этапу.
  - Если параметр доверия к цифровому сертификату еще не выбран, появится предупреждение.



Если вы доверяете базе данных, нажмите кнопку *Открыть*. Если вы доверяете всем сертификатам этого поставщика, нажмите кнопку



*Доверять всему от издателя.* Откроется диалоговое окно *Извлечь базу данных в*.



5. В списке *Сохранить в* можно выбрать расположение для извлекаемой базы данных, а в поле *Имя файла* – ввести для нее другое имя.
6. Нажмите кнопку *ОК*.

Если вы сомневаетесь в том, можно ли считать сертификат надежным, ниже приведены основные сведения о проверке дат и других элементов сертификата для установления его подлинности.

#### *Определение надежности цифровой подписи*

Цифровые подписи играют решающую роль в подтверждении безопасности программного обеспечения.

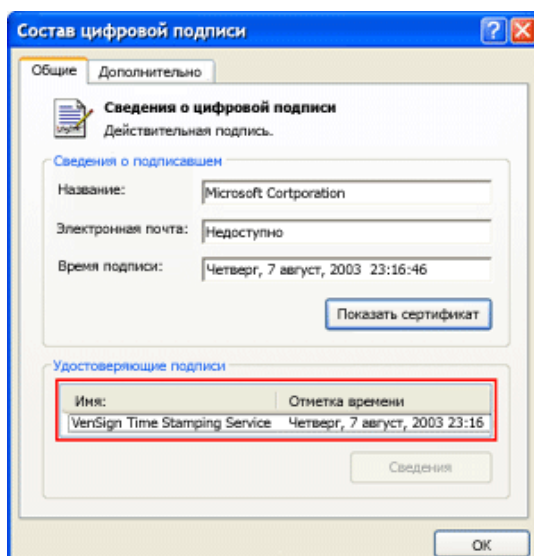
Требования к цифровой подписи:

- цифровая подпись должна быть *действительной*. Характеризует статус сертификата, проверка которого по базе данных центра сертификации показала, что он является законным, действующим, не был просрочен или отозван. Документы, подписанные действительным сертификатом и не изменявшиеся с момента их подписания, считаются *действительными*;
- сертификат, связанный с данной цифровой подписью, должен быть действующим (не просроченным);
- лицо (или организация), поставившее цифровую подпись и именуемое издателем, должно быть надежным. *Доверенный издатель*. Разработчик макроса, которому пользователь доверяет и разрешает выполняться на своем компьютере. Доверенный издатель определяется по сертификату, который используется им для подписывания макроса цифровой подписью. Также известен как *надежный источник*;
- сертификат цифровой подписи должен быть выдан подписывающему издателю заслуживающим доверия центром сертификации (*центр сертификации* – ЦС – коммерческая организация, выпускающая цифровые сертификаты, отслеживающая, кому они были назначены,

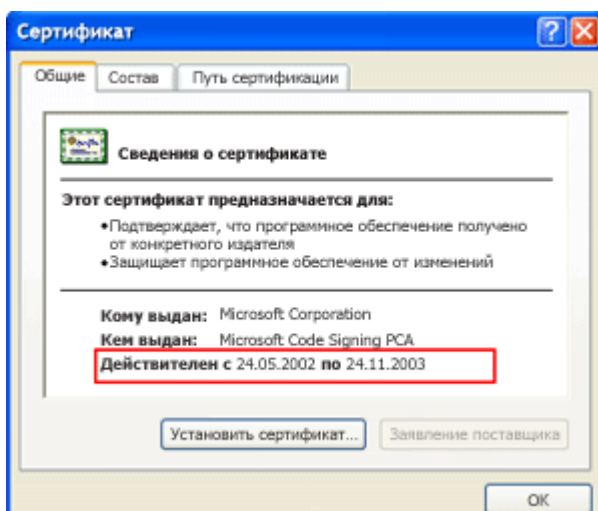
подписывающая сертификаты для удостоверения их подлинности и следящая за истечением срока действия выпущенных сертификатов и их отзывом).

Приложения выпуска 2007 и старше системы Microsoft Office проверяют эти требования и предупреждают о наличии проблем с цифровой подписью.

Если цифровая подпись действительна, в верхней части диалогового окна *Сведения о цифровой подписи* появляется сообщение, подтверждающее, что это действительно так. Следует также обратить внимание на сведения штампа времени в разделе *Подписи других сторон*. Штамп времени показывает, что центр сертификации – в данном случае VeriSign – проверил и утвердил цифровую подпись.



Дата в штампе времени – в данном случае 7 августа 2003 года – должна находиться в границах диапазона дат сертификата *Действителен с*. Чтобы увидеть диапазон дат в цифровой подписи, нажмите кнопку *Просмотреть сертификат*.



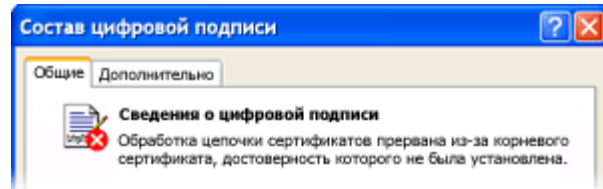
Издатель, в данном случае – корпорация Майкрософт, по умолчанию должен быть установлен как надежный издатель на компьютерах, работающих под управлением операционной системы Microsoft Windows.



Сертификаты для Майкрософт находятся в хранилище надежных корневых центров сертификации. Если данный издатель не установлен как надежный по умолчанию, необходимо задать это явно. В противном случае содержимое, подписанное этим издателем, не пройдет проверку на безопасность программного обеспечения.

*Проверка цифровой подписи, помеченной красным крестом*

Цифровая подпись, вызывающая проблемы, помечается красным крестом.



Красный крест появляется в следующих случаях:

- цифровая подпись по каким-либо причинам недействительна (например, содержимое документа изменялось после добавления цифровой подписи);
- срок действия цифровой подписи истек;
- сертификат, связанный с данной цифровой подписью, не был выдан центром сертификации. Например, сертификат может иметь цифровую подпись, созданную при помощи программы *Selfcert.exe*;
- издатель не является надежным.

*Предполагаемые действия при наличии проблем с цифровой подписью*

Если возникли проблемы с цифровой подписью, в зависимости от ситуации можно выполнить одно из действий, перечисленных ниже.

- Обратиться к источнику подписанного содержимого и сообщить ему о возникновении проблемы с цифровой подписью.
- Обратиться к системному администратору, ответственному за безопасность инфраструктуры организации.
- Если предполагается, что макрос или другое активное содержимое данного документа заслуживает доверия, следует сохранить этот документ в надежном расположении. Документы из надежного расположения можно открывать без проверки системой безопасности Центра обеспечения безопасности. Рекомендуется использовать надежные расположения вместо изменения настроек на более низкий уровень безопасности для всех макросов.
- Можно в явном виде включить данного издателя в число надежных.

Последовательность выполняемых действий для отработки 7 вопроса задания.

*Включение отключенного содержимого при открытии базы данных*

По умолчанию Access отключает все выполняемое содержимое в базе данных, если она не имеет состояния доверенной или не размещена в надежном расположении. При открытии такой базы данных Access отключает это содержимое и отображает панель сообщений.



В отличие от Access 2003 в Office Access 2007 и более старших версий при открытии базы данных не отображается набор модальных диалоговых окон (это диалоговые окна, в которых необходимо принять какое-либо решение для того, чтобы продолжить работу). Однако при необходимости можно добавить ключ реестра, чтобы в Office Access 2007 и более старших версий отображались прежние модальные диалоговые окна.

#### *Добавление ключа реестра для отображения модальных диалоговых окон*

**Внимание!** Неверное изменение параметров реестра может привести к существенному повреждению операционной системы с необходимостью ее переустановки.

1. Нажмите кнопку *Пуск* и выберите команду *Выполнить*.
2. В поле *Открыть* введите *regedit*, а затем нажмите клавишу ВВОД. Запустится редактор реестра.
3. Разверните папку `HKEY_CURRENT_USER` и укажите следующий раздел реестра:  
`Software\Microsoft\Office\12.0\Access\Security`
4. В правой области редактора реестра щелкните правой кнопкой мыши пустое место, выберите команду *Создать*, а затем выберите вариант *Параметр DWORD*. Появится новый пустой параметр типа *DWORD*.
5. Введите следующее имя параметра: *ModalTrustDecisionOnly*.
6. Дважды щелкните новый параметр. Откроется диалоговое окно *Изменение параметра DWORD*.
7. В поле *Значение* поменяйте значение *0* на *1*, а затем нажмите кнопку *ОК*.
8. Закройте редактор реестра.


Теперь при открытии базы данных, включающей небезопасное содержимое, вместо панели сообщений будет отображаться ряд диалоговых окон. Чтобы вернуться к исходному варианту, повторите эти действия и поменяйте значение *1* на *0*.

Последовательность выполняемых действий для отработки 8 вопроса задания.

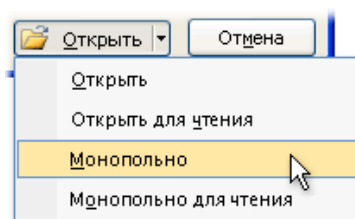
#### *Зашифрование и расшифрование базы данных*

##### *Шифрование с использованием пароля базы данных*

###### **Access 2007**

1. Откройте в монопольном режиме базу данных, которую требуется зашифровать, для чего:
  - 1) Щелкните значок *Кнопка Microsoft Office* , а затем выберите команду *Открыть*.
  - 2) В диалоговом окне *Открыть* найдите файл, который нужно открыть, и выделите его.

- 3) Щелкните стрелку рядом с кнопкой *Открыть* и выберите команду *Монопольно*.



2. На вкладке *Работа с базами данных* в группе *Работа с базами данных* щелкните *Зашифровать паролем*.

Откроется диалоговое окно *Задание пароля базы данных*.

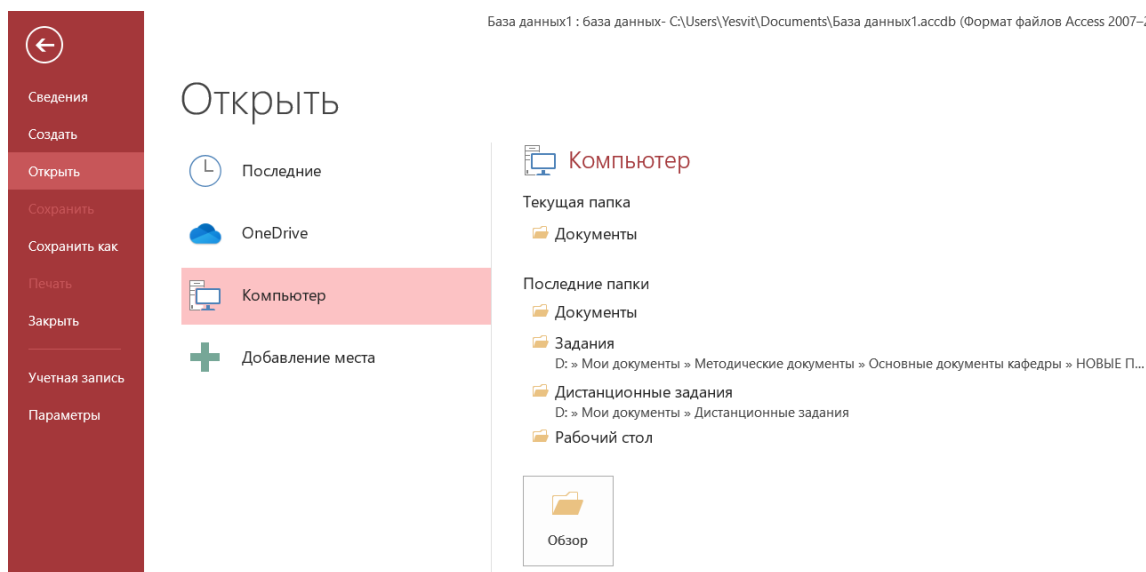
3. Введите пароль в поле *Пароль*, а затем повторите его в поле *Подтверждение*.

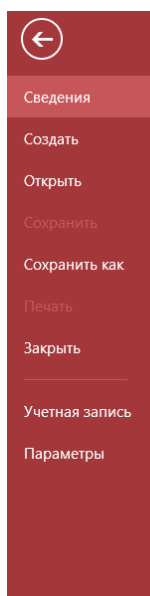
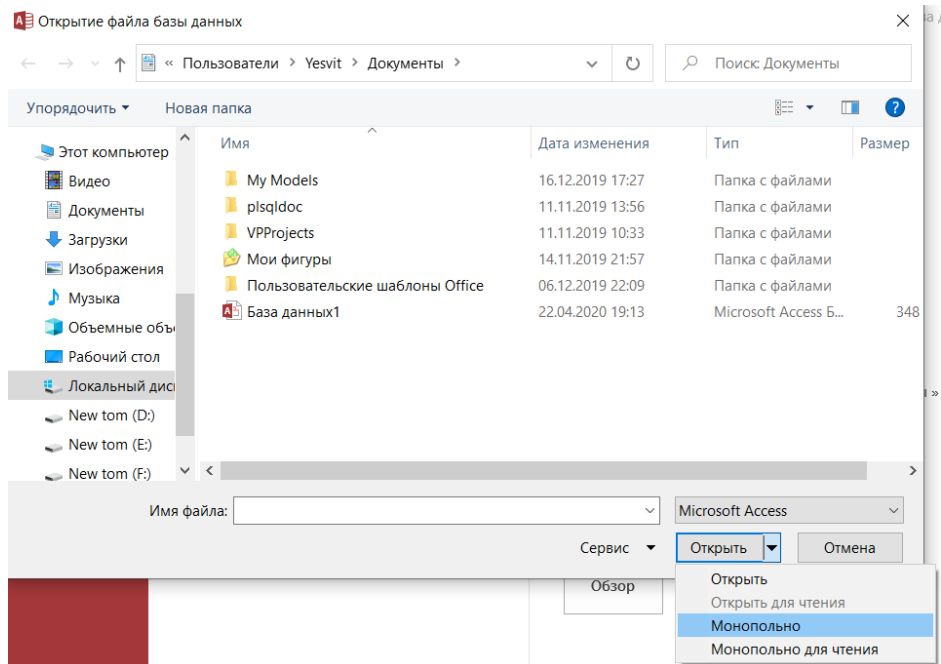
Используйте надежные пароли, представляющие собой сочетание прописных и строчных букв, цифр и символов. Пароли, не содержащие набор таких элементов, являются ненадежными. Надежный пароль: Y6dh!et5. Ненадежный пароль: House27. Пароли должны состоять не менее чем из 8 символов. Рекомендуется использовать фразу-пароль, состоящую из 14 или более символов. Важно помнить свой пароль. Если вы забыли пароль, восстановить его невозможно.

4. Нажмите кнопку *OK*.

### **Access 2013...**

База данных1 : база данных- C:\Users\Yesvit\Documents\База данных1.accdb (Формат файлов Access 2007–2013) - Access

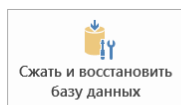




## Сведения

primer\_3\_NEW

D: » Мои документы »



### Сжать и восстановить

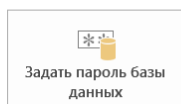
Предотвращение и устранение проблем с файлом базы данных при помощи средства сжатия и восстановления.

[Просмотр и изменение свойств базы данных](#)



### Управление пользователями и разрешениями

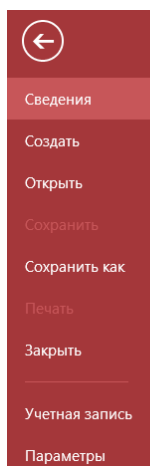
Использование паролей и разрешений для предоставления или ограничения доступа отдельных пользователей или групп пользователей к объектам в базе данных.



### Задать пароль базы данных

Использование пароля для ограничения доступа к базе данных. Файлы в формате Microsoft Access 2007 и более поздних версий будут зашифрованы.

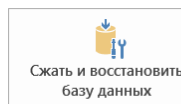
## Формат файла MDB



## Сведения

База данных1

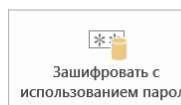
Документы



### Сжать и восстановить

Предотвращение и устранение проблем с файлом базы данных при помощи средства сжатия и восстановления.

[Просмотр и изменение свойств базы данных](#)



### Зашифровать с использованием пароля

Использование пароля для ограничения доступа к базе данных. Файлы в формате Microsoft Access 2007 и более поздних версий будут зашифрованы.

## Формат файла ACCDB

### *Расшифрование и открытие базы данных*

1. Откройте зашифрованную базу данных точно так же, как обычно открываете любую другую.  
Появится диалоговое окно *Необходимо ввести пароль*.
2. Введите пароль в поле *Введите пароль базы данных* и нажмите кнопку *ОК*.

### *Удаление пароля*

1. Откройте базу данных в монопольном режиме (см. *шифрование с использованием пароля базы данных*).
2. Введите пароль в поле *Пароль* и нажмите кнопку *ОК*.
3. На вкладке *Работа с базами данных* в группе *Работа с базами данных* щелкните *Расшифровать базу данных*.  
Откроется диалоговое окно *Удаление пароля базы данных*.
4. Введите пароль в поле *Пароль* и нажмите кнопку *ОК*.

### ***Результаты работы***

Продемонстрировать результаты работы преподавателю и отобразить их в отчете.