Система безопасности MS Access

Microsoft Access обеспечивает два традиционных способа зашиты базы данных: **установка пароля**, требуемого при открытии базы данных, и **защита на уровне пользователей**, которая позволяет ограничить, к какой части базы данных пользователь будет иметь доступ или какую ее часть он сможет изменять. Кроме того, можно предотвратить изменения структуры форм, отчетов и модулей.

Установка пароля

Установка пароля на открытие базы данных достаточно надежна (Microsoft Access шифрует пароль), но после открытия базы данных все объекты становятся доступными для пользователя - изменение структуры и любых данных и т.д. (выход - определить защиту на уровне пользователей).

Порядок действий:

1) Закройте базу данных.

2) Сделайте резервную копию базы данных и сохраните ее в надежном месте.

3) **Файл\Открыть**. Установить флажок "**Монопольный доступ**".

4) **Сервис\Защита\Задать пароль базы данных**.

5) Введите и подтвердите пароль (с учетом регистра).

Пароль проверяется при открытии базы данных и при установлении связи с таблицей из защищенной паролем базы данных.

Пусть на БД1 - установлен пароль, на БД2 - нет. При установлении связи БД2 с БД1 - проверка пароля. При успешном установлении связи, в БД2 будет сохранен пароль из БД1, который будет использоваться в дальнейшем. Если в БД1 пароль поменяется, то необходимо изменить его и в БД1.

Защита на уровне пользователей

Пользователи, группы пользователей и владельцы базы данных

При запуске Access пользователь называет себя и вводит свой пароль. Если данный пользователь есть в списке и пароль введен правильно, то пользователь подключается к Access под своим именем и как член своей группы.

Группы пользователей: "**Admins**" (администраторы), "**Users**" (пользователи) или любые **другие** определяемые вручную группы.

Каждая группа имеет свой определяемый набор прав. Например, члены группы "Users" могут иметь разрешения на просмотр, ввод или изменение данных в таблицы, но им не будет разрешено изменять структуру таблиц. Группа "Users" может быть допущена только к просмотру данных в таблице "Заказы" и не иметь доступа к таблице "Платежная ведомость". Члены группы "Admins" имеют все разрешения на доступ ко всем объектам базы данных. Кроме того, каждый пользователь может иметь свой индивидуальный набор прав. Права пользователя суммируются с правами группы, в которую он входит.

Владелец базы данных - это тот пользователь, который был подключен к Access при создании базы данных. Владелец базы данных всегда может открыть базу данных и получить все разрешения на ее объекты (любые изменения таблиц, форм, отчетов и т.д.).

Создание нового пользователя:

Сервис\Защита\Пользователи и группы. Вкладка "Пользователи" \ кнопка "Создать" - ввести имя нового пользователя и его код (Код - это не пароль. Фактически, к базе данных имеет доступ не имя пользователя, а его уникальный код. Чтобы удаленный по ошибке пользователь заново получил весь свой набор разрешений на доступ к базе данных, необходимо заново создать такого пользователя: не обязательно с тем же именем, но обязательно с тем же кодом).

Используя кнопки "Добавить", "Удалить", переместить в окно "Участие в группе" те группы, в которых будет участвовать пользователь. Участие в группе Admins дает пользователю права администратора. "Users" - только права пользователя. Кнопка "Удалить" – удаление пользователя.

Создание новой группы:

Сервис\Защита\Пользователи и группы. Вкладка "Группы", кнопка "Создать" - ввести название группы и ее уникальный код (смысл кода тот же, что и для пользователя), кнопка "Удалить".

Изменение пароля пользователя:

Сервис\Защита\Пользователи и группы. Вкладка "Изменение пароля" - указать старый пароль, новый пароль и подтверждение пароля. Можно изменить только пароль того пользователя, от имени которого было произведено подключение к Access. Для того чтобы изменить пароль любого пользователя необходимо выйти из Access и снова подключиться к нему от имени этого пользователя. Пользователь, обладающий правами администратора, может отменить пароль любого пользователя, отображаемого на вкладке в окне "Пользователь имя:", нажав кнопку "Снять пароль" на этой вкладке.

Подключение к Access от имени определенного пользователя:

К Access, от имени определенного пользователя, можно подключиться из командной строки (Access.exe /User <имя пользователя> /Pwd <пароль>). Если в командной строке пароль не указан, то Access выведет диалоговое окно, где попросит ввести имя пользователя и пароль. Целесообразно для каждого пользователя создать ярлык Access, где в "Свойствах" ярлыка, на вкладке "Ярлык" в поле "Файл" будет задана командная строка с именем пользователя, но без пароля. Это позволяет легко узнать имена пользователей.

Если пользователей очень много, то создавать большое число ярлыков нерационально. Для избежания этой ситуации можно воспользоваться следующей техникой: Access, по умолчанию (если отсутствует командная строка), пытается подключить всех пользователей как Admin. Таким образом, достаточно установить пароль для пользователя Admin и при стандартном запуске Access всегда будет выводить диалоговое окно с запросом на ввод имени пользователя и его пароля. Чтобы отменить запрос на ввод имени и пароля при запуске Access - надо подключиться с правами администратора и при помощи кнопки "Снять пароль" отменить пароль для пользователя Admin и других пользователей.

Установка зашиты на уровне пользователей:
1) Создать список групп и имен пользователей. 2) Запустить Access без открытия базы данных как пользователь Admin или любой другой с правами администратора. 3) Открыть защищаемую базу данных.

4) Сервис\Разрешения. На вкладке "Разрешения" в поле "Тип объекта" выбрать "База данных", выбрать имя пользователя или название группы, для которой устанавливаются разрешения, флажками отметить, что разрешено данному пользователю или группе (разрешения отдельных пользователей и разрешения групп, в которых они участвую - суммируются).

Например, если не установлен флажок "открытие\запуск" для "базы данных", то этот пользователь не сможет открыть защищаемую базу данных. При этом необходимо учитывать, что, если пользователь принадлежит к группе "Admins" (администраторов), которым разрешено открытие базы данных, то и пользователь получит право открывать базу данных.

5) На вкладке "Разрешения" в поле "Тип объекта" выбрать остальные объекты базы данных: "Таблицы", "Запросы", "Формы", "Отчеты", "Макросы", "Модули" и установить разрешения для них. При этом можно определять набор разрешений, как для каждой из уже существующих "Таблиц" и т.д.. так и для вновь создаваемых "Таблиц" и т.д. - выбор защищаемого объекта в окне "Имя объекта".

Удаление зашиты на уровне пользователей:

1) Подключиться к Access как администратор (Admin). 2) Загрузить защищенную базу данных. 3)Предоставить группе «Users» разрешения на все объекты базы данных. Возвратить права владельца базы данных и ее объектов стандартной учетной записи пользователя «Admin». 4) Выйти из Access и снова подключится к системе под именем «Admin», создать пустую базу данных, а затем импортировать все объекты из защищенной базы данных в новую.

Смена владельца базы данных

1) Запустите Microsoft Access с файлом рабочей группы, в котором есть учетная запись пользователя, которому требуется передать права владельца базы данных. Подключитесь от имени этого пользователя.
2) Создайте новую базу данных. 3) Импортируйте в новую базу данных все объекты из исходной базы данных. Для импорта базы данных пользователь должен иметь разрешение «Открытие/запуск» для базы данных и «Чтение макета» на ее объекты. Для импорта таблиц необходимо кроме этого иметь разрешение «Чтение данных». Если разрешения имеются не на все объекты, Microsoft Access импортирует только те объекты, на которые имеются достаточные разрешения.

Смена владельца отдельных объектов базы данных

Администратор может сменить текущего владельца отдельных объектов базы данных (но не всей базы данных в целом): 1) Откройте базу данных. 2) Сервис\Защита\Пользователи и группы\ вкладка "Смена владельца". 3) Выберите тип объектов в раскрывающемся списке (таблица, запрос, форма, отчет и т.д.). 4) В списке "Объект" выделите один или несколько объектов, для которых требуется произвести смену владельца.

5) В списке "Новый владелец" выберите имя пользователя или группы, которым передаются права владельца объекта, 6) Нажмите кнопку "Сменить владельца".

Слабые места зашиты на уровне пользователей

1) Стандартный пользователь Admin, с правами администратора.

2) Стандартный код группы Admins (группа администраторов), при использовании стандартного файла рабочей группы.

Admin - стандартная учетная запись пользователя, с правами администратора. Данные записи являются одинаковыми для всех экземпляров Microsoft Access и других приложений, использующих ядро базы данных Microsoft Jet, таких как VBA и Excel. По умолчанию (если вы не подключились от имени другого пользователя), Microsoft Access подключает всех пользователей как Admin, и использует Admin как владельца всех создаваемых баз данных и объектов.

Поскольку учетные записи пользователя Admin являются одинаковыми для всех экземпляров Microsoft Access, то первым шагом при организации системы зашиты является создание уникальной учетной записи администратора (не Admin). После этого разработчик базы данных должен удалить пользователя Admin из группы Admins, отобрав таким образом у него права администратора.

Также необходимо отобрать у группы Users, в которой продолжает находиться Admin, все права на доступ к базе данных. Кроме того, если Admin является владельцем базы данных, необходимо передать права владельца новому администратору. До тех пор, пока все это не сделано, любой пользователь Microsoft Access из любой рабочей группы сможет подключиться как Admin и получить все разрешения на доступ к базе данных.

В защите Access есть и еще одно слабое место - это стандартный код стандартной группы Admins. Admins - группа администраторов. Члены группы Admins всегда могут получить все разрешения на базы данных, созданные в рамках одного файла рабочей группы. Код группы Admins определяется кодом файла рабочей группы и фактически, к базе данных имеет доступ не группа Admins, а ее код. По умолчанию Access создает файл рабочей группы со стандартным кодом, который формируется на основании "Имени пользователя" и "Названия организации пользователя", введенных при установке Access.

Поскольку эти данные легко доступны, то любой человек, создавший пустую копию стандартного файла рабочей группы, а затем добавив в группу Admins пользователей без пароля, получит доступ с правами администратора ко всем базам данных, созданных в рамках стандартного файла рабочей группы. Чтобы предотвратить это, необходимо создать файл рабочей группы с уникальным кодом, тогда группа Admins также получит уникальный код.

Все сказанное выше справедливо и для стандартной группы Users, код которой также определяется кодом файла рабочей группы. Таким образом, при создании файла рабочей группы с уникальным кодом, закроется доступ к базе данных членам групп Admins и Users из других файлов рабочих групп, код которых не совпадает с текущим.

Защита базы данных на уровне пользователя с использованием мастера защиты

Мастер защиты автоматически выполняет шаги по защите на уровне пользователя. Используется достаточно просто, но выполнение программы мастера защиты может занимать довольно много времени. При использовании мастера защиты из текущей базы данных будет создана новая, защищенная, а текущая база данных не изменится.

Шифрование и дешифрование базы данных

При шифровании базы данных ее файл сжимается и делается недоступным для чтения с помощью служебных программ или текстовых редакторов. Дешифрование базы данных отменяет результаты операции шифрования.

Порядок шифрования:

1. Запустить Microsoft Access без открытия базы данных (невозможно зашифровать или дешифровать открытую базу данных).
2. Сервис\Защита\Шифровать или дешифровать.
3. Указать имя базы данных, указать имя зашифрованной базы данных (можно указать имя, совпадающее с исходным, тогда исходный файл будет заменен на зашифрованный или дешифрованный базой данных).

Примечание: Если определена защита на уровне пользователей, то для шифрования или дешифрования базы данных необходимо разрешение «Изменение макета» для всех таблиц базы данных.

Сжатие базы данных для дефрагментации файла и освобождения места на диске

После удаления таблиц файл базы данных становится фрагментированным, и место на диске используется нерационально. Сжатие базы данных приводит к созданию ее копии, в которой диск используется более экономно.

Сервис \ Служебные программы \ Сжать базу данных. Допускается сжатие файла базы данных в файл с тем же именем, что и имя файла исходной базы данных (при успешном сжатии исходный файл заменяется на сжатый файл), или создание файла с новым именем.