Содержание:

Введение

Пожалуй, важнейшей характеристикой качества любой информационной системы является уровень обеспечения ее информационной безопасности.

Есть три способа решить эту проблему и защитить свою базу данных:

- **Конфиденциальности**, т.е. обеспечения пользователям доступа только к данным, для которых пользователь имеет явное или неявное разрешение на доступ;
- **Целостности**, т.е. обеспечения защиты от преднамеренного или непреднамеренного изменения информации или процессов ее обработки;
- **Доступности**, т.е. обеспечения возможности авторизованным в системе пользователям доступа к информации в соответствии с принятой технологией.

Поскольку данные в информационных системах хранится в базах данных, то можно говорить о безопасности баз данных или системы баз данных, имея в виду обеспечение безопасности как при хранении, так и при обработке данных.

Для создания баз данных и управления данными в них используются системы управления базами данных (СУБД). Современные СУБД имеют встроенные средства обеспечения безопасности данных, причем ориентируясь на самые распространённые.

Управляемая система баз данных является распределенной, т.е. физически может быть размещена на нескольких носителях, а иногда, и в нескольких узлах, взаимодействие между которыми осуществляется по протоколам транспортного уровня. Поэтому анализ информационной безопасности СУБД должен быть проведен по двум направлениям:

Безопасность архитектурных решений и их программных реализаций в СУБД, которая включает исследование следующих проблем:

- идентификация и аутентификация субъектов системы;

- технологии реализации дискреционной, мандатной и ролевой модели доступа к данным;
- реализация аудита действий пользователя.

Безопасность взаимодействия с внешними по отношению к СУБД программными и аппаратными компонентами, которая включает исследование следующих проблем:

- сопряжение с элементами операционной системы (анализ информационных потоков вниз), т.е. изучение возможностей пользователей несанкционированно осуществлять чтение и запись в файлы операционной системы, включая возможность модификации записей аудита;
- сопряжение с программным обеспечением промежуточного уровня (анализ управляющих потоков вверх), т.е. выявление портов взаимодействия с внешним программным обеспечением, устойчивость к перегрузкам каналов шумовым трафиком и вставкам ложных пакетов, к перенастройкам параметров протоколов, а также анализ алгоритмов и технологий линейного шифрования трафика межсерверного обмена и взаимодействия клиентского программного обеспечения с серверами баз данных.

В работе в основном ограничимся рассмотрением вопросов, связанных с первым направлением.

Новым направлением для СУБД промышленного уровня является наличие встроенных механизмов шифрования в основном на базе алгоритмов DES и AES.

Средства защиты баз данных MS Access

СУБД MS Access может использоваться как для создания локальных баз данных и пользовательских приложений, так и для создания распределенных баз данных и многопользовательских приложений.

Примечание: Прежде чем устанавливать защиту базы данных при помощи пароля или на уровне пользователя рекомендуется всегда делать резервные копии базы данных и файла рабочей группы (System.mdw) и копировать эти резервные копии в специально отведенное для этого место.

Защита при помощи пароля

Ядро Jet (Join Engine Technology) версии 3.5 и более поздние версии ядра СУБД MS Access предоставляют возможность установить пароль на базу данных, который нужно будет вводить при каждом открытии базы данных. Следует знать, что защита базы данных при помощи пароля и защита на уровне пользователя независимы друг от друга. Это означает, что даже если пользователь знает пароль, ему все равно нужно иметь разрешения на работу с объектами базы. Если пользователь забывает пароль, то не существует способа удалить этот пароль или открыть базу данных. Если пароль не забыт, то его можно удалить. Для этого нужно открыть базу данных в монопольном режиме, имея права администратора или владельца базы.

Защита на уровне пользователя

Каждая база данных, которая создается или используется в среде MS Access, содержит информацию обо всех пользователях и их правах доступа к объектам базы. Многие не пользуются защитой, поэтому по умолчанию MS Access регистрирует вошедшего пользователя под именем администратора (Admin), который имеет полный доступ ко всем объектам базы. Однако мы можем воспользоваться защитой базы данных на уровне пользователя. В этом случае пользователь должен при открытии базы данных ввести имя пользователя и пароль. Только после этого пользователь получит доступ к тем объектам, разрешения на использование которых были выданы ему администратором базы. Вот так, разрешения на доступ к объектам и регистрацию пользователя, которому выданы соответствующие разрешения, осуществляет только администратор базы или пользователь, обладающий правами администратора. Это можно сделать как через интерфейс MS Access, так и программным путем.

Обеспечение защиты через интерфейс Access

В MS Access защита на уровне пользователя задействована всегда. Многие не пользуются защитой, поэтому по умолчанию MS Access регистрирует вошедшего пользователя как пользователя Admin без пароля.

После установки MS Access автоматически создается файл рабочей группы System.mdw. При запуске MS Access информация о пользователях и группах пользователей получается из этого файла. Файл System.mdw - системная база

данных относится к категории скрытых системных файлов. Полное имя этого файла можно узнать, открыв базу данных и выполнив команду *Сервис/Защита/Администратор рабочих групп.*

В файлах рабочих групп можно создавать новые учетные записи отдельных пользователей и групп пользователей. Каждой группе администратор может выдать разрешения на доступ к объектам базы данных. В группу могут входить несколько пользователей, которым предоставляются одинаковые разрешения для работы с объектами базы данных. Такие разрешения называют неявными (все пользователи группы наследуют разрешения, данные группе). Таким образом, использование групп позволяет упростить процедуру предоставления разрешений для пользователей, включенных в группу.

Однако каждому пользователю администратор может выдать дополнительные разрешения (явные разрешения), которые могут отсутствовать у группы, в которую входит пользователь. В этом случае такой пользователь наследует все разрешения своей группы, а также и дополнительные разрешения. Таким образом, но при этом в любом случае будут использоваться разрешения, которые обеспечивают ему максимальный доступ.

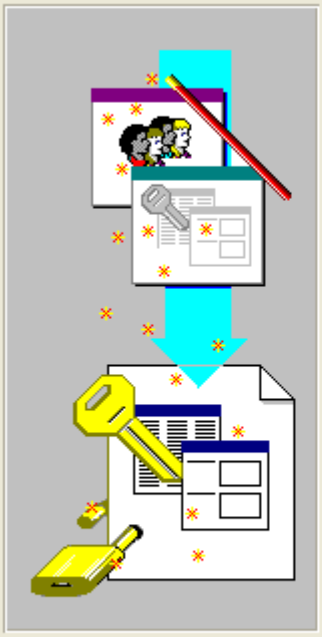
По умолчанию в файле рабочей группы создаются две группы: Admins и Users. Пользователь Admin является членом обеих групп Admins и Users. Пользователь Admin не может быть исключен из группы Admins. Пользователь Admin может добавлять новых пользователей и давать им разрешения. Добавленный пользователь автоматически становится членом группы Users. По умолчанию члены этой группы могут выполнять следующие действия:

- создавать новые базы данных;
- изменять системные установки;
- восстанавливать базы данных;
- сжимать базы данных.

Обеспечение защиты с помощью мастера

Программа-мастер позволяет автоматически установить защиту на уровне пользователя.

Мастер защиты



Мастер защиты создает незащищенную резервную копию текущей базы данных Microsoft Access, а затем выполняет действия по защите базы данных.

Файл сведений рабочей группы содержит имена пользователей и групп, участвующих в разработке приложения или просто работающих с ним. Для изменения текущего файла рабочей группы требуются права администратора. Не используйте файл рабочей группы, устанавливаемый по умолчанию.

Создать файл сведений рабочей группы или изменить текущий файл?

- ○ Создать файл рабочей группы.
- ◉ Изменить текущий файл рабочей группы.

Справка | Отмена | < Назад | Далее > | Готово

Мастер защиты

По умолчанию проверяется защита всех существующих объектов базы данных и всех объектов, создаваемых после выполнения мастера. Чтобы оставить защиту объекта без изменений, отмените его выбор.

Какие объекты базы данных нужно защитить?

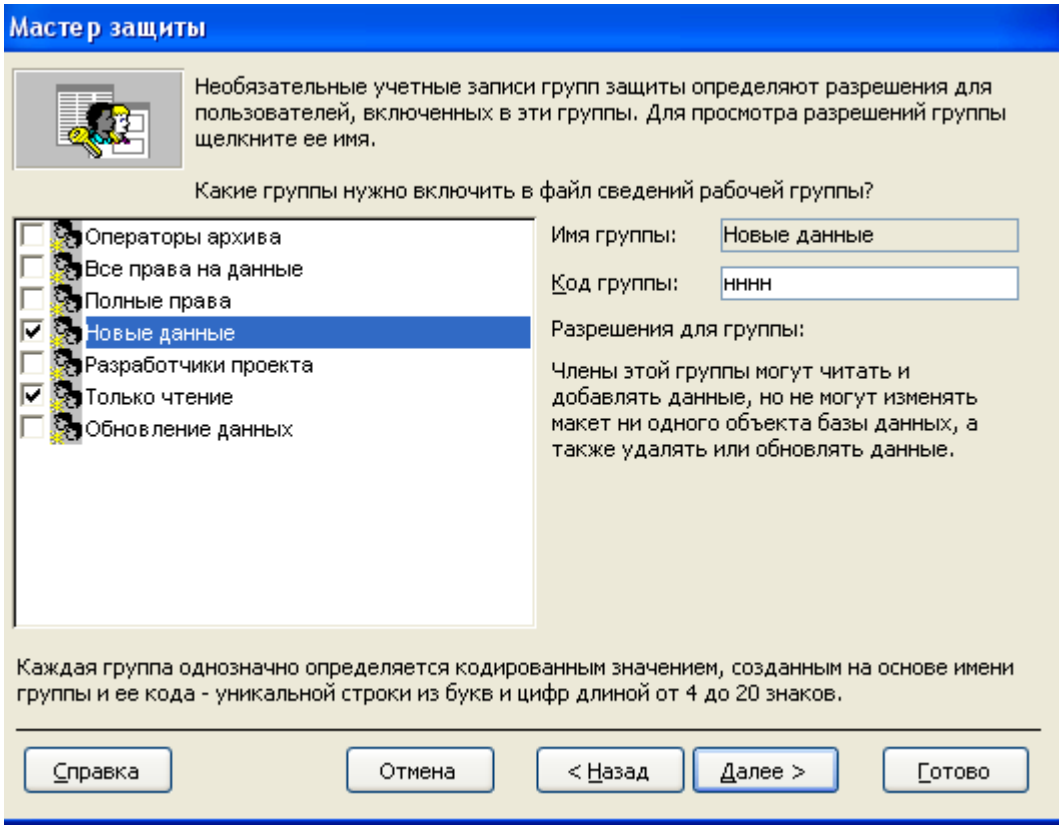
Макросы | Прочее | Все объекты

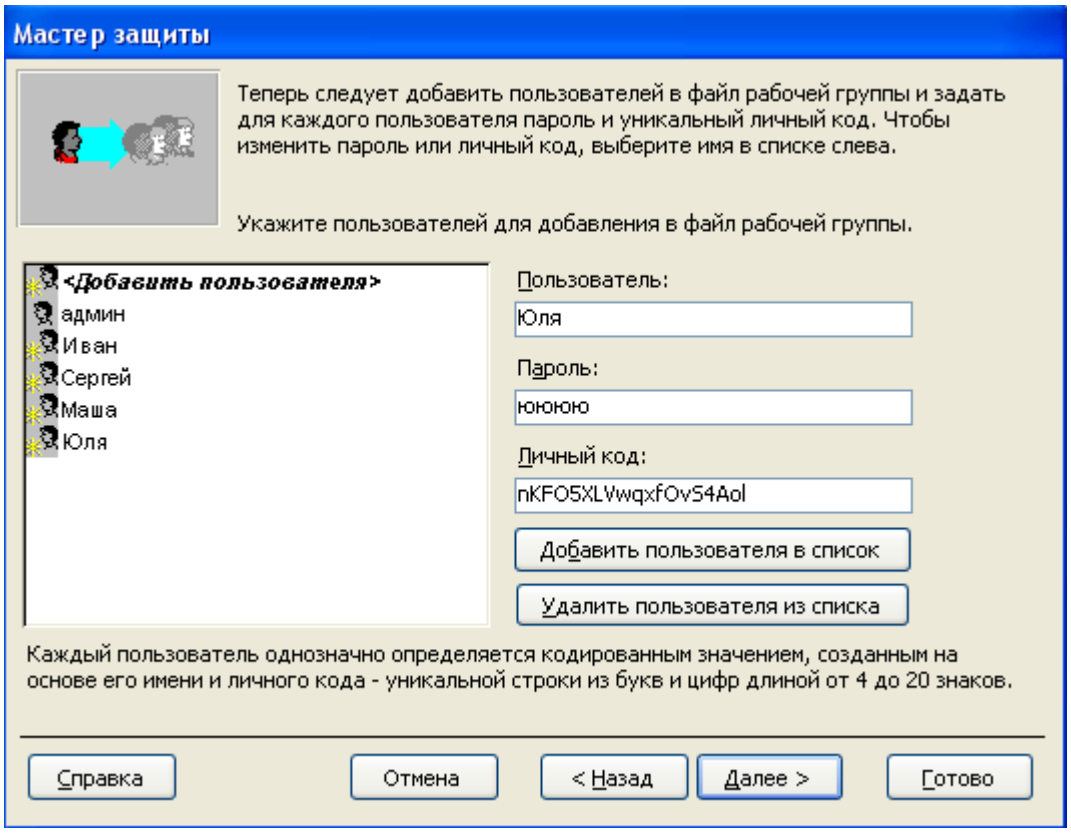
Таблицы | Запросы | Формы | Отчеты

- ☑ детали
- ☑ поставки
- ☑ поставщики

Очистить | Выделить все | Очистить все

Справка | Отмена | < Назад | Далее > | Готово





Тут показана поэтапная работа с мастером. Она облегчает защиту баз данных для менее опытных пользователей, что поможет защитить сами данные куда доступнее.

Выдача разрешений на столбцы таблицы

Выдать разрешения на отдельные столбцы таблицы можно, используя запросы. При этом можно предоставить пользователю возможность добавлять или удалять записи, даже если он не имеет прав на чтение данных из таблицы. Например, возможна ситуация, когда в базе данных сотрудников нужно от пользователей базы скрыть информацию о доходах сотрудников.

Снятие защиты

Иногда бывает необходимо снять защиту базы данных. Если перед установкой защиты была создана резервная копия базы данных, это делается легко. В простейшем случае для снятия защиты нужно выполнить следующую последовательность действий:

- зарегистрируйтесь в системе как член группы Admins;
- дайте пользователю Admin права администратора, включив его обратно в группу Admins;
- выдайте группе Users полные права доступа ко все объектам базы данных;
- сделайте владельцем базы пользователя Admin;
- закройте и заново запустите MS Access;
- зарегистрируйтесь в системе как пользователь Admin;
- задайте пользователю Admin пустой пароль.

Создание MDE-файла

Прежде чем создавать файл с расширением .MDE, рекомендуется создать резервную копию базы данных, поскольку возврат от MDE-файла к MDB-файлу невозможен.

MDE-файл является базой данных, в которой все программы, созданные в MDB-файле, сохранены в скомпилированном виде. Поэтому просмотр и редактирование исходных кодов невозможен. Кроме того, изменение таких объектов базы данных, как формы, отчеты и модули, также невозможен. Режим конструктора для них оказывается недоступным. Можно вносить изменения только в таблицы и запросы.

Если же какие-то недоступные в MDE-файле объекты потребуют доработки или изменения, то следует вернуться к сохраненному MDB-файлу, сделать необходимые изменения, а затем заново создать MDE-файл. Создать базу данных в виде MDE-файла можно, имея права администратора, так:

- открыть исходную базу данных (MDB-файл);
- исполнить команду меню *Сервис/Служебные программы/Создать MDE-файл*, указав местоположение MDE-файла.

Файлы MDE обычно создаются, когда разработчик хочет, чтобы пользователи не имели доступ к исходному коду, а также к объектам интерфейса (формам и отчетам), и вместе с тем разработчик не заинтересован в реализации полной системы обеспечения защиты на уровне пользователя. Хотя, если такая защита реализована в исходном MDB-файле, то она действует и в MDE-файле.

Источники информации

https://studfiles.net/preview/2823609/

https://support.office.com/ru-ru/

https://studopedia.ru/11_126441_zashchita-baz-dannih-MS-Access-.html