Содержание:

Защита информации MICROSOFT ACCESS

Защита информации — комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности (целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных.

Защита при помощи пароля

Access предоставляют возможность установить пароль на базу данных, который нужно будет вводить при каждом открытии базы данных. Следует отметить, 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. Поэтому пользоваться паролем нужно предельно осторожно.

Защита на уровне пользователя

Каждая база данных, которая создается или используется в среде MSAccess, содержит информацию обо всех пользователях и их правах доступа к объектам базы. Многие не пользуются защитой, поэтому по умолчанию MSAccess 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. Таким образом, разрешения на доступ к объектам и регистрацию пользователя,

которому выданы соответствующие разрешения, осуществляет только администратор базы или пользователь, обладающий правами администратора.

Пользователи базы данных

Понятие пользователь базы данных относится к базе (или базам) данных, к которым может получить доступ отдельный пользователь. После успешного подключения сервер определяет, имеет ли этот пользователь разрешение на работу с базой данных, к которой обращается.

Единственным исключением из этого правила является пользователь guest (гость). Особое имя пользователя guest разрешает любому подключившемуся к SQL Server пользователю получить доступ к этой базе данных. Пользователю с именем guest назначена роль public.

Права доступа

Для управления правами доступа в SQL Server используются следующие команды:

• GRANT. Позволяет выполнять действия с объектом или, для команды — выполнять ее;

• REVOKE. Аннулирует права доступа для объекта или, для команды — не позволяет выполнить ее;

• DENY. Не разрешает выполнять действия с объектом (в то время, как команда REVOKE просто удаляет эти права доступа).

Объектные права доступа позволяют контролировать доступ к объектам в SQL Server, предоставляя и аннулируя права доступа для таблиц, столбцов, представлений и хранимых процедур. Чтобы выполнить по отношению к некоторому объекту некоторое действие, пользователь должен иметь соответствующее право доступа. Например, если пользователь хочет выполнить оператор SELECT * FROM table, то он должен и меть права выполнения оператора SELECT для таблицы table.

Обеспечение защиты с помощью мастера

Программа-мастер позволяет автоматически установить защиту на уровне пользователя.

Вопросы безопасности доступа

Говоря о преимуществах интеграции с операционной системой, MS SQL Server использует в своей работе сервисы безопасности Windows NT. Напомним, что Windows NT на сегодня сертифицирована по классам безопасности C2/E3. MS SQL Server может быть настроен на работу в одном из трех режимах безопасности. Интегрированный режим предусматривает использование механизмов аутентификации Windows NT для обеспечения безопасности всех пользовательских соединений. В этом случае к серверу разрешаются только трастовые, или аутентифицирующие, соединения (named pipes и multiprotocol). Администратор имеет возможность отобразить группы пользователей Windows NT на соответствующие значения login id MS SQL Server при помощи утилиты SQL Security Manager. В этом случае при входе на MS SQL Server login name и пароль, переданные через DB-Library или ODBC, игнорируются. Стандартный режим безопасности предполагает, что на MS SQL Server будут заводиться самостоятельные login id и соответствующие им пароли. Смешанный режим использует интегрированную модель при установлении соединений по поименованным каналам или мультипротоколу и стандартную модель во всех остальных случаях.
Управление доступом

Система безопасности SQL Server имеет несколько уровней безопасности:

• операционная система;

• SQL Server;

• база данных;

• объект базы данных.

С другой стороны механизм безопасности предполагает существование четырех типов пользователей:

• системный администратор, имеющий неограниченный доступ;

• владелец БД, имеющий полный доступ ко всем объектам БД;

• владелец объектов БД;

• другие пользователи, которые должны получать разрешение на доступ к объектам БД.

Модель безопасности SQL Server включает следующие компоненты:

• тип подключения к SQL Server;

• пользователь базы данных;

• пользователь (guest);

• роли (roles).

Тип подключения к SQL Server

При подключении (и в зависимости от типа подключения) SQL Server поддерживает два режима безопасности:

• режим аутентификации Windows NT;

• смешанный режим аутентификации.

В режиме аутентификации Windows NT используется система безопасности Windows NT и ее механизм учетных записей. Этот режим позволяет SQL Server использовать имя пользователя и пароль, которые определены в Windows, и тем самым обходить процесс подключения к SQL Server. Таким образом, пользователи, имеющие действующую учетную запись Windows, могут подключиться к SQL Server, не сообщая своего имени и пароля. Когда пользователь обращается к СУБД, последняя получает информацию об имени пользователя и пароле из атрибутов системы сетевой безопасности пользователей Windows (которые устанавливаются, когда пользователь подключается к Windows).

В смешанном режиме аутентификации задействованы обе системы аутентификации: Windows и SQL Server. При использовании системы аутентификации SQL Server отдельный пользователь, подключающийся к SQL Server, должен сообщить имя пользователя и пароль, которые будут сравниваться с хранимыми в системной таблице сервера. При использовании системы аутентификации Windows пользователи могут подключиться к SQL Server, не

сообщая имя и пароль.

Список Литературы

- https://studfile.net/preview/2823609/page:6/
- https://poznayka.org/s2707t2.html
- http://5fan.ru/wievjob.php?id=35031
- https://revolution.allbest.ru/programming/00752628_0.html