ТЕХНИЧЕСКИЕ НАУКИ

МЕТОДЫ ЗАЩИТЫ БАЗ ДАННЫХ

Кучкин В.П.

Кучкин Владислав Павлович – студент,
факультет автоматизированных систем управления,
филиал
Военная академия Ракетных войск стратегического назначения им. Петра Великого,
г. Серпухов, Московская область

Аннотация: *в статье рассмотрены проблемы защиты информации баз данных от различных видов угроз.*

Ключевые слова: *информация, документооборот, атака, вирус, защита.*

Системы управления базами данных СУБД является неотъемлемой частью автоматизированных систем управления (АСУ). При создании инфраструктуры корпоративной АСУ на базе современных компьютерных сетей неизбежно возникает вопрос ее защищенности.

Целью исследования являлся вопрос повышение уровня защиты баз данных.

Задачами исследования являлись: анализ существующих моделей баз данных, исследование методов защиты баз данных, анализ эффективности методов защиты баз данных.

Актуальность данной работы заключается в распространенности применения баз данных во всех сферах жизни общества, и в связи с этим решение проблемы защищенности информации, хранящейся в базах данных.

Существуют многочисленные аспекты проблемы защиты данных: правовые, физические, организационные, аппаратные средства защиты, возможности ОС, аспекты, имеющие отношение непосредственно к самим СУБД.

В современных СУБД обычно поддерживается один из двух широко распространенных методов организации защиты данных - избирательный или мандатный.

В случае избирательного контроля каждому пользователю обычно предоставляются различные права доступа. Обычно разные пользователи обладают различными правами доступа к одному и тому же объекту.

В случае мандатного контроля, наоборот, каждому объекту данных назначается некий классификационный уровень, а каждому пользователю присваивается некоторый уровень допуска. Непреодолимых систем защиты не бывает, настойчивый нарушитель может преодолеть системы контроля, поэтому при работе с важными данными возникает необходимость организации контрольного журнала, в который вносится информация обо всех событиях, происходящих в системе. Любая противоречивость результатов, может свидетельствовать о злонамеренном искажении информации. В этом случае для прояснения ситуации могут использоваться записи контрольного журнала. Журнал представляет собой файл или базу данных, в которую автоматически помещаются сведения обо всех операциях, выполненных пользователями при работе с основной базой данных.

Если пользователь пытается проникнуть в БД не с помощью средств системы, а минуя систему, т.е. перемещая внешние носители информации или подключаясь к линии связи, в таком случае наиболее эффективным методом борьбы является шифрование данных. В базах данных могут использоваться различные алгоритмы, например, AES или RSA.

Отсюда следует, что данные, хранящиеся в БД, должны быть защищены от несанкционированного доступа (НСД), для этого необходимо обеспечить следующие мероприятия:

1. Защита с помощью пароля - позволяет устанавливать права доступа авторизованным пользователям;
2. Ограничение прав доступа к объектам БД;
3. Введение контрольные журналов - предоставляются СУБД для контроля нарушений прав доступа;
4. Шифрование данных - нужно для того, чтобы неавторизованные пользователи, возможно, преодолевшие некоторые уровни защиты БД, не могли использовать данные напрямую.

Данные методы защиты можно считать основными. Они в той или иной форме присутствуют во всех рассматриваемых СУБД.

Для анализа эффективности методов защиты БД были выбраны наиболее распространенные СУБД.

Согласно исследованию ресурса, DB-Engines (датировано апрелем 2015 г.), таковыми являются Oracle Database, MySQL и Microsoft SQL Server. В рейтинге распространенности они расположены на первых трех позициях с большим отрывом от конкурентов.

Основными методами защиты баз данных используемыми в Oracle Database являются:

1. Ограничение доступа легальных пользователей (аутентификация);
2. Управление доступом к данным (авторизация);
3. Обеспечение подотчетности пользователей (аудит);
4. Защита основных данных в базе данных (шифрование).

Аутентификация БД в Oracle Database - это стандартная проверка полномочий доступа пользователя за счет применения паролей БД.

MySQL - система, по умолчанию настроенная на максимально быструю работу, поэтому в ней не предусмотрен встроенный механизм шифрования таблиц БД. Но при этом MySQL поддерживает шифрованные SSL-соединения. Это необходимо для того, чтобы передать данные между клиентом и сервером, без риска ознакомления с этими данными нарушителя. В протоколе SSL используются различные алгоритмы шифрования, обеспечивающие безопасность для данных, передаваемых через общедоступные сети. Этот протокол содержит средства, позволяющие обнаруживать любые изменения, потери и повторы данных.

Для того чтобы идентифицироваться в MySQL необходимо использовать логин и пароль, положительной стороной является то, что пароль хранится в зашифрованном виде, причем без возможности дешифрования и даже если злоумышленник получит доступ к паролю в зашифрованном виде, использовать он его не сможет. Недостатком является отсутствие навязываемой политики паролей, то есть пользователь сам определяет, какой сложности пароль у него будет, очевидно, что использование пароля типа «1111» недопустимо.

Авторизация пользователя представлена системой привилегий, для того чтобы выполнить определенное действие у пользователя должна быть привилегия на данное действие. Достоинством является разделение привилегий на уровни. Недостатком можно указать то, что данная система упрощена по сравнению с другими системами безопасности для СУБД.

Система аудита представлена в MySQL журналами учета, которые опять же реализованы в довольно упрощенном виде.

В MySQL отсутствует встроенная система шифрования таблиц БД, или БД целиком. Но присутствует поддержка защищенной передачи данных между клиентом и сервером с помощью зашифрованных SSL-соединений.

Таким образом, можно сделать вывод, что в MySQL реализованы все основные методы защиты БД, но реализованы в упрощенном виде.

В MS SQL Server представлены все основные методы защиты баз данных.

При создании пользователя БД можно настроить проверку подлинности личности на различных уровнях, как БД, так и ОС. Для реализации авторизации в MS SQL Server присутствуют механизмы разрешений и ролей. Для проверки действий пользователей в MS SQL Server реализована система автоматизированного аудита. В MS SQL Server также имеются системы шифрования данных на различных уровнях, включая как шифрование файлов, так и шифрование столбцов, данных и ключей.

Все сущности, которые могут запрашивать ресурсы SQL Sever - называются участниками. Участники имеют разные области влияния, которые выстраиваются в определенном иерархическом порядке:

1. Участник уровня Windows;
2. Участник уровня SQL Server, по умолчанию имя для входа администратора - “sa”;
3. Участник уровня БД - пользователь БД.

Каждый участник имеет определённое имя входа, которое является идентификатором пользователя или процесса, соединяющегося с SQL Server. Во время процесса установки MS SQL Server необходимо выбрать режим проверки подлинности и настроить его.

При смешанном режиме проверке подлинности, который включает в себя проверку подлинности как Windows, так и SQL Server, учетной записи “sa” необходимо задать и подтвердить надежный пароль.

Проверку подлинности Windows проверяет имя и пароль с помощью токена участника Windows, обеспечивает высокий более высокий уровень безопасности, чем проверка подлинности SQL Server, и имеет возможность реализовать политику паролей ОС, в отношении проверки сложности надежных паролей.

При использовании проверки подлинности SQL Server, в SQL Server создаются имена входа, которые не основаны на учетных записях пользователей Windows. Имя пользователя и пароль хранятся в SQL Server.

Данная проверка позволяет использовать политику паролей, которую можно включить, выполнив инструкцию “ALTER LOGIN”.

Из выше сказанного можно сделать следующие выводы:

1. Согласно исследованию ресурса, DB-Engines самыми распространёнными СУБД в мире являются Oracle Database, MySQL и Microsoft SQL Server, им уделяется основное внимание в работе;
2. Среди методов защиты БД, выделены четыре фундаментальных метода защиты баз данных: аутентификация, авторизация, аудит баз данных, шифрование;
3. Проанализированы основные достоинства и недостатки методов защиты СУБД, что позволит предложить рекомендации по устранению недостатков у имеющихся методов защиты, и повысить уровень защиты данных в БД.

Список литературы

1. *Дейт К. Дж.* Введение в системы баз данных, 8-е издание. М.: Издательский дом «Вильямс», 2005. 1328 с.
2. *Алапати Сэм Р.* Oracle Database 11g: руководство администратора баз данных. М.: Издательский дом «Вильямс», 2005. 1440 с.
3. *Кириллов В.В.* Введение в реляционные базы данных. СПб.: БХВ-Петербург, 2009. 464 с.

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Лузгарев В.Ю.

Лузгарев Валерий Юрьевич – студент,
факультет автоматизированных систем управления,
Военная академия Ракетных войск стратегического назначения им. Петра Великого,
г. Серпухов, Московская область

Аннотация: *в данной статье рассмотрены средства защиты информации в системах электронного документооборота.*

Ключевые слова: *безопасность, аутентификация, защита, информация, документооборот, средства.*

Проблема безопасной и гарантированной доставки электронных документов в настоящее время актуальна. Повсеместная компьютеризация производства привела к тому, что документы в электронном виде циркулируют в информационных системах, начиная и заканчивая свой жизненный цикл, зачастую не будучи ни разу распечатанными. Это большой плюс - экономия времени, бумаги, возможность моментально получить необходимый документ. Однако, такое ведение документооборота требует постоянного внимания службы информационной безопасности компании: лёгкость обращения документов в информационной системе может сослужить плохую службу, если защите информации в ней не уделено должного внимания.

В большинстве организаций циркулирует очень важная информация электронного документооборота. Поэтому при доступе к этой информации обычно используют такой подход, как аутентификация сотрудников.

Аутентификация сотрудников возможна по следующим направлениям:

1) парольная аутентификация (личный номер, криптографический ключ, сетевой адрес компьютера в сети);

2) аутентификация на основе информации хранящейся в электронном виде (смарт-карта, электронный ключ);

3) биометрическая аутентификация (внешность, голос, рисунок радужной оболочки глаз, отпечатки пальцев и другие биометрические характеристики).

В качестве достоинств аутентификации на основе использования паролей, можно выделить следующие:

1) надежность;