Определение правил доступа к данным и мер безопасности

Информационная безопасность

Информационная безопасность — практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные. Основная задача информационной безопасности — сбалансированная
защита конфиденциальности, целостности и доступности данных, с учётом целесообразности применения и без какого-либо
ущерба производительности организации.

Информационная безопасность в СУБД

Для СУБД важны три основных аспекта информационной безопасности - конфиденциальность, целостность и доступность.

Политика безопасности определяется администратором данных. Однако решения защиты данных не должны быть ограничены только рамками СУБД. Абсолютная защита данных практически не реализуема, поэтому обычно довольствуются относительной защитой информации - гарантированно защищают ее на тот период времени, пока несанкционированный доступ к ней влечет какие-либо последствия. Разграничение доступа к данным также описывается в базе данных посредством ограничений, и информация об этом хранится в ее системном каталоге.

Идентификация пользователя

В СУБД на этапе подключения к БД производится идентификация и проверка подлинности пользователей. В дальнейшем пользователь или процесс получает доступ к данным согласно его набору полномочий. В случае разрыва соединения пользователя с базой данных текущая транзакция откатывается, и при восстановлении соединения требуется повторная идентификация пользователя и проверка его полномочий.

Дискреционная защита

В современных СУБД достаточно развиты средства дискреционной защиты.

Дискреционное управление доступам — разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту.

Дискреционная защита является многоуровневой логической защитой.

Набор привилегий можно определить для конкретного зарегистрированного пользователя или для группы пользователей.

Привилегии конкретному пользователю могут быть назначены администратором явно и неявно, например через роль.

Мандатная защита

Мандатное управление доступом — это разграничение доступа субъектов к объектам данных, основанное на характеризуемой меткой конфиденциальности информации, которая содержится в объектах, и на официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности.

Использование СУБД с возможностями мандатной защиты позволяет разграничить доступ собственно к данным, хранящимся в информационной системе, от доступа к именованным объектам данных.

Основные категории пользователей

Пользователей СУБД можно разбить на три категории:

- администратор сервера баз данных. Он ведает установкой, конфигурированием сервера, регистрацией пользователей, групп, ролей и т.п. Прямо или косвенно он обладает всеми привилегиями, которые имеют или могут иметь другие пользователи.
- администраторы базы данных. К этой категории относится любой пользователь, создавший базу данных, и, следовательно, являющийся ее владельцем. Он может предоставлять другим пользователям доступ к базе и к содержащимся в ней объектам. Администратор базы отвечает за ее сохранение и восстановление.
- прочие (конечные) пользователи. Они оперируют данными, хранящимися в базах, в рамках выделенных им привилегий.

Виды привилегий

Привилегии в СУБД можно подразделить на две категории: привилегии безопасности и привилегии доступа. Привилегии безопасности позволяют выполнять административные действия. Привилегии доступа, в соответствии с названием, определяют права доступа субъектов к определенным объектам.

- Привилегии безопасности - Привилегии безопасности всегда выделяются конкретному пользователю во время его создания или изменения характеристик.
- Привилегии доступа - Привилегии доступа выделяются пользователям, группам, ролям или всем посредством оператора GRANT и изымаются с помощью оператора REVOKE. Эти привилегии, как правило, присваивает владелец соответствующих объектов или обладатель привилегии security.

Шифрование содержимого баз данных

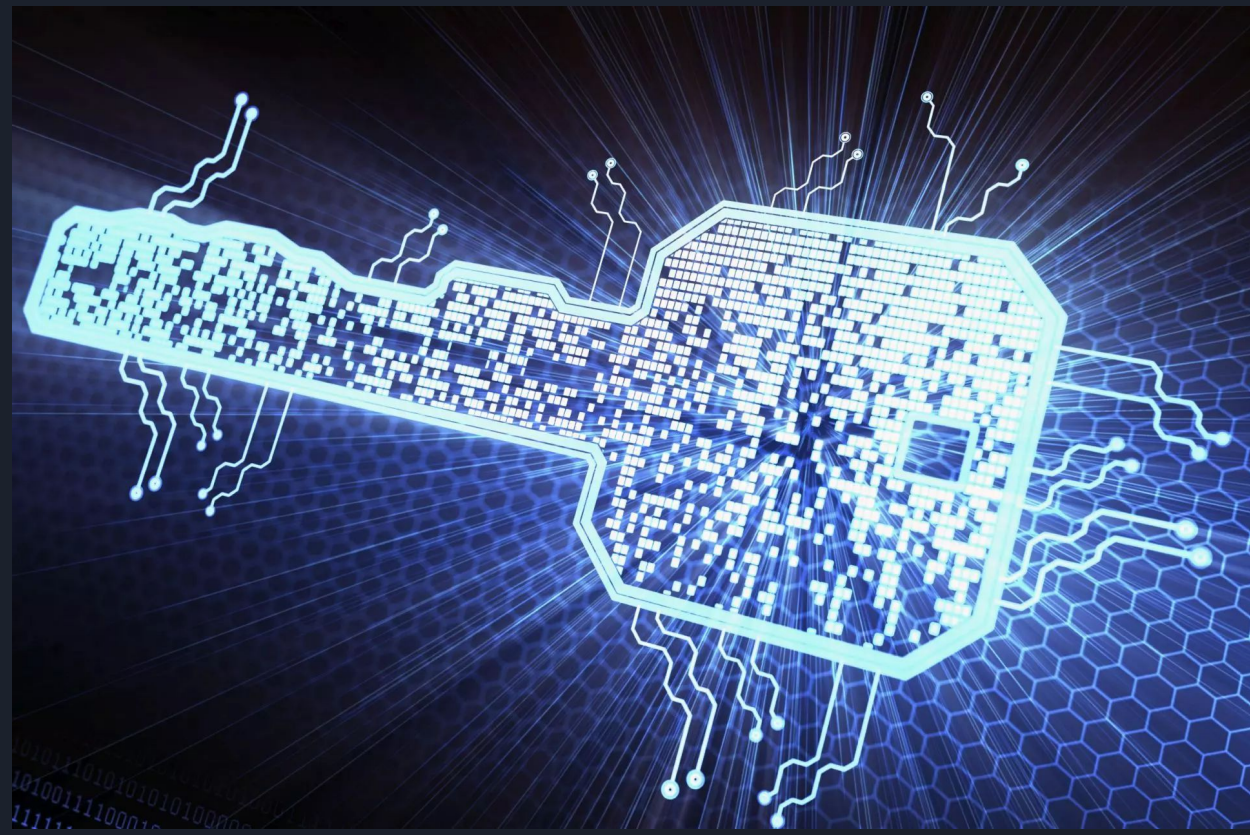
База данных может быть зашифрована и храниться на диске в зашифрованном виде.

Шифрование– это преобразование исходных данных по специальным алгоритмам в новое представление, скрывающее содержание исходной информации.

Дешифрование – это обратный шифрованию процесс. При шифровании базы данных ее файл кодируется и становится недоступным для просмотра информации с помощью служебных программ.

Шифрование содержимого баз данных

Наиболее простым является режим, при котором информация дешифруется на внешнем носителе, с ней производятся необходимые действия, после чего для записи на внешней носитель информация снова зашифровывается. Достоинством такого режима является независимость функционирования средств шифрования и СУБД, которые работают последовательно друг за другом. В то же время сбой или отказ в системе может привести к тому, что на внешнем носителе часть базы данных останется записанной в незашифрованном виде.



Точка Зрения

По моему мнению, актуальность безопасности содержимого баз данных неоспорима, многие СУБД имеют встроенные средства защиты, такие как шифрование и уровень доступа пользователя.

В первую очередь, безопасность данных должен обеспечивать сам администратор СУБД, выдавая права и уровни доступа в иерархии пользователей.

Спасибо за внимание!