Лабораторная работа № 7
«Особенности защиты информации в базах данных»

Цель работы:

Закрепление теоретического материала по изучению особенностей защиты информации в базах данных.

Изучение способов и систем защиты информации в базах данных.

Приборы и оборудование:

Персональный компьютер
ОС MS Windows 7 (MS Windows 10), MS Office, Браузер Microsoft Internet Explorer (Edge)

Пояснения к работе и задание:

Базы данных рассматриваются как надежное хранилище структурированных данных, снабженное специальным механизмом для их эффективного использования в интересах пользователей (процессов). Таким механизмом является система управления базами данных (СУБД). Под системой управления базой данных понимаются программные или аппаратно-программные средства, реализующие функции управления данными, такие как: просмотр, сортировка, выборка, модификация, выполнение операций определения статистических характеристик и т.п. Базы данных размещаются:

- на компьютерной системе пользователя;
- на специально выделенной ЭВМ(сервере).

Как правило, на компьютерной системе пользователя размещаются личные или персональные базы данных, которые обслуживают процессы одного пользователя.

В вычислительных сетях базы данных размещаются на серверах. В локальных и корпоративных сетях, как правило, используются централизованные базы данных. В таких сетях серверы размещаются на различных объектах сети. В качестве серверов часто используются специализированные ЭВМ, приспособленные к хранению больших объемов данных, обеспечивающие сохранность и доступность информации, а также оперативность обработки поступающих запросов. В централизованных базах данных проще решаются проблемы защиты информации от преднамеренных угроз, поддержания актуальности и непротиворечивости данных. Достоинством распределенных баз данных, при условии дублирования данных, является их высокая защищенность от стихийных бедствий, аварий, сбоев технических средств, а также диверсий.

Защита информации в БД, в отличии от защиты в файлах, имеет и свои особенности:

- необходимость учета функционирования СУБД при выборе механизмов защиты;
- разграничение доступа к информации реализуется не на уровне файлов, а на уровне частей БД.

При создании средств защиты информации в БД необходимо учитывать взаимодействие этих средств не только с ОС, но и с СУБД. При этом возможно встраивание механизмов защиты в СУБД или использование их в виде отдельных компонент. Для большинства СУБД придание им дополнительных функций возможно только на этапе разработки СУБД. В эксплуатируемые СУБД дополнительные компоненты могут быть внесены путем расширения или модификации языка

управления. Таким путем можно осуществлять наращивание возможностей, например, в СУБД CA-Clipper 5.0.

В современных БД довольно успешно решаются задачи разграничения доступа, поддержания физической целостности и логической сохранности данных. Алгоритмы разграничения доступа к записям и даже к полям записей в соответствии с полномочиями пользователя хорошо отработаны, и преодолеть эту защиту злоумышленник может лишь с помощью фальсификации полномочий или внедрения вредительских программ. Разграничение доступа к файлам БД и к частям БД осуществляется СУБД путем установления полномочий пользователей и контроля этих полномочий при допуске к объектам доступа.

Полномочия пользователей устанавливаются администратором СУБД. Обычно стандартным идентификатором пользователя является пароль, передаваемый в зашифрованном виде. В распределенных компьютерных системах процесс подтверждения подлинности пользователя дополняется специальной процедурой взаимной аутентификации удаленных процессов. БД, содержащих конфиденциальную информацию, хранятся на внешних запоминающих устройствах в зашифрованном виде.

Физическая целостность БД достигается путем использования отказоустойчивых устройств, построенных, например, на технологии RAID. Логическая сохранность данных означает невозможность нарушения структуры модели данных. Современные СУБД обеспечивает такую логическую целостность и непротиворечивость на этапе описания модели данных.

В БД, работающих с конфиденциальной информацией, необходимо дополнительно использовать криптографические средства закрытия информации. Для этой цели используется шифрование, как с помощью единого ключа, так и с помощью индивидуальных ключей пользователей. Применение шифрования с индивидуальными ключами повышает надежность механизма разграничения доступа, но существенно усложняет управление.

Возможны два режима с зашифрованными БД. Наиболее простым является такой порядок работы с закрытыми данными, при котором для выполнения запроса необходимый файл или часть файла расшифровывается на внешнем носителе, с открытой информацией производятся необходимые действия, после чего информация на внешнем запоминающем устройстве(ВЗУ) снова зашифровывается. Достоинством такого режима является независимость функционирования средств шифрования и БУБД, которые работают последовательно друг за другом. В то же время сбой или отказ в системе может привести к тому, что на ВЗУ часть БД останется записанной в открытом виде.

Второй режим предполагает возможность выполнения СУБД запросов пользователей без расшифрования информации на ВЗУ. Поиск необходимых файлов, записей, полей, групп полей не требует расшифрования. Расшифрование производится в ОП непосредственно перед выполнением конкретных действий с данными. Такой режим возможен, если процедуры шифрования встроены в СУБД. При этом достигается высокий уровень защиты от несанкционированного доступ, но реализация режима связана с усложнением СУБД. Придание СУБД возможности поддержки такого режима работы осуществляется, как правило, на этапе разработки СУБД.

При построении защиты БД необходимо учитывать ряд специфических угроз безопасности информации, связанных с концентрацией в БД большого количества разнообразной информации, а также с возможностью использования сложных запросов обработки данных. К таким угрозам относятся:

– инференция;

– агрегирование;
– комбинация разрешенных запросов для получения закрытых данных.

Под инференцией понимается получение конфиденциальной информации из сведений с меньшей степенью конфиденциальности путем умозаключений. Если учитывать, что в базах данных хранится информация, полученная из различных источников в разное время, отличающаяся степенью обобщенности, то аналитик может получить конфиденциальные сведения путем сравнения, дополнения и фильтрации данных, к которым он допущен. Кроме того, он обрабатывает информацию, полученную из открытых баз данных, средств массовой информации, а также используются просчеты лиц, определяющих степень важности и конфиденциальности отдельных явлений, процессов, фактов, полученных результатов. Такой способ получения конфиденциальных сведений, например, по материалам средств массовой информации, используется давно, и показал свою эффективность.

Близким к инференции является другой способ добывания конфиденциальных сведений - агрегирование. Под агрегированием понимается способ получения более важных сведений по сравнению с важностью тех отдельно взятых данных, на основе которых и получаются эти сведения. Так, сведения о деятельности одного отделения или филиала корпорации обладают определенным весом. Данные же за всю корпорацию имеют куда большую значимость.

Если инференция и агрегирование являются способами добывания информации, которые применяются не только в отношении баз данных, то способ специального комбинирования запросов используется только при работе с базами данных. Использование сложных, а также последовательности простых логически связанных запросов позволяет получать данные, к которым доступ пользователю закрыт. Такая возможность имеется, прежде всего, в базах данных, позволяющих получать статистические данные. При этом отдельные записи, поля, (индивидуальные данные) являются закрытыми. В результате запроса, в котором могут использоваться логические операции AND, OR, NOT, пользователь может получить такие величины как количество записей, сумма, максимальное или минимальное значение. Используя сложные перекрестные запросы и имеющуюся в его распоряжении дополнительную информацию об особенностях интересующей записи (поля), злоумышленник путем последовательной фильтрации записей может получить доступ к нужной записи (полю).

Противодействие подобным угрозам осуществляется следующими методами:
– блокировка ответа при неправильном числе запросов;
– искажение ответа путем округления и другой преднамеренной коррекции данных;
– разделение баз данных;
– случайный выбор записи для обработки;
– контекстно-ориентированная защита;
– контроль поступающих запросов.

Метод блокировки ответа при неправильном числе запросов предполагает отказ в выполнении запроса, если в нем содержится больше определенного числа совпадающих записей из предыдущих запросов. Таким образом, данный метод обеспечивает выполнение принципа минимальной взаимосвязи вопросов. Этот метод сложен в реализации, так как необходимо запоминать и сравнивать все предыдущие запросы.

Метод коррекции заключается в незначительном изменении точного ответа на запрос пользователя. Для того, чтобы сохранить приемлемую точность статистической информации, при меняется так называемый свопинг данных. Сущность его

заключается во взаимном обмене значений полей записи, в результате чего все статистики i-го порядка, включающие i атрибутов, оказываются защищенными для всех i, меньших или равных некоторому числу. Если злоумышленник сможет выявить некоторые данные, то он не сможет определить, к какой конкретно записи они относятся.

Применяется также метод разделения баз данных на группы. В каждую группу может быть включено не более определенного числа записей. Запросы разрешены к любому множеству групп, но запрещаются к подмножеству записей из одной группы. Применение этого метода ограничивает возможности выделения данных злоумышленником на уровне не ниже группы записей. Метод разделения баз данных не нашел широкого применения из-за сложности получения статистических данных, обновления и реструктуризации данных.

Эффективным методом противодействия исследованию баз данных является метод случайного выбора записей для статистической обработки. Такая организация выбора записей не позволяет злоумышленнику проследить множество запросов.

Сущность контекстно-ориентированной защиты заключается в назначении атрибутов доступа (чтение, вставка, удаление, обновление, управление и т. д.) элементам базы данных (записям, полям, группам полей) в зависимости от предыдущих запросов пользователя. Например, пусть пользователю доступны в отдельных запросах поля: «идентификационные номера» и «фамилии сотрудников», а также «идентификационные номера» и «размер заработной платы». Сопоставив ответы по этим запросам, пользователь может получить закрытую информацию о заработной плате конкретных работников. Для исключения такой возможности пользователю следует запретить доступ к полю «идентификатор сотрудника» во втором запросе, если он уже выполнил первый запрос.

Одним из наиболее эффективных методов защиты информации в базах данных является контроль поступающих запросов на наличие «подозрительных» запросов или комбинации запросов. Анализ подобных попыток позволяет выявить возможные каналы получения несанкционированного доступа к закрытым данным.

Ход выполнения лабораторной работы:

1. Изучить приведенный в методическом описании к лабораторной работе материал.
2. Выполнить практическое ознакомление с разделами с применением возможностей лаборатории.
3. Оформить отчет в установленной форме по разделам.
4. Ответить на контрольные вопросы.
5. Представить результаты работы преподавателю.

Контрольные вопросы:

1. В чем заключается особенность размещения баз данных?
1. В чем заключаются особенности защиты информации в базах данных?
2. Какие задачи решаются в рамках реализации защиты баз данных?
3. Перечислите режимы работы с защищенными базами данных.
4. Перечислите виды угроз информации, размещенной в базах данных.
5. Какие виды противодействия угрозам информации в базах данных Вы знаете?