СЕКЦИЯ 3. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

УПРАВЛЕНИЕ ДОСТУПОМ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БАЗАХ ДАННЫХ

Д.А. БАХАНОВИЧ

Проблема обеспечения защиты информации является одной из важнейших при построении надежной информационной структуры учреждения на базе ЭВМ. В понятие защиты данных включаются вопросы сохранения целостности данных и управления доступа к данным (санкционированность).

Большинство систем БД представляют собой средство единого централизованного хранения данных. Это значительно сокращает избыточность данных, упрощает доступ к данным и позволяет более эффективно защищать данные. Однако, в технологии БД возникает ряд проблем, связанных, например, с тем, что различные пользователи должны иметь доступ к одним данным и не иметь доступа к другим. Поэтому, не используя специальные средства и методы, обеспечить надежное разделение доступа в БД практически невозможно.

Большинство современных СУБД имеют встроенные средства, позволяющие администратору системы определять права пользователей по доступу к различным частям БД, вплоть до конкретного элемента. При этом имеется возможность не только предоставить доступ тому или иному пользователю, но и указать разрешенный тип доступа: что именно может делать конкретный пользователь с конкретными данными (читать, модифицировать, удалять), вплоть до реорганизации всей БД.

В качестве примера, была рассмотрена система отчетности организации, построенная на основе СУБД Microsoft SQL Server 2008R2 и платформы SharePoint 2013. Показана модель безопасности, включающая в себя: архитектуру базы данных, описание операций резервного копирования и моделей восстановления. Были рассмотрены типы подключения к SQL Server, уровни безопасности, регламентация прав пользователей и ролей, таблицы (списки) управления доступом, широко используемые в компьютерных системах, например, в ОС для управления доступом к файлам. Особенность использования этого средства для защиты БД состоит в том, что в качестве объектов защиты выступают не только отдельные файлы (области в сетевых БД, отношения в реляционных БД), но и другие структурные элементы БД: элемент, поле, запись, набор данных. Кроме того, в рамках исследования показан процесс интеграции СУБД Microsoft SQL Server и платформы SharePoint 2013 с использованием встроенных ИТ-инструментов управления, таких как новые модели безопасности SharePoint и Active Directory для отчетов конечных пользователей.

Все перечисленные элементы обеспечивают дополнительную гибкость и повышение удобства использования функций аудита в среде SQL Server, упрощая соблюдение нормативных требований в организациях.

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА БАЗЫ ДАННЫХ «ЭКСПРЕСС-ДИАГНОСТИКА ПСИХОФИЗИЧЕСКИХ ПОКАЗАТЕЛЕЙ»

Н.Л. БОБРОВА

Современные автоматизированные системы обработки данных имеют дело с большими объемами информации. Необходимость быстрой и корректной обработки этой информации обусловливают следующие общие требования к программному обеспечению, в частности, к системам управления базами данных (СУБД):

– многозадачный, многопользовательский режим;
– обеспечение защиты данных;
– достаточная производительность;
– переносимость;
– сетевые функции;
– телекоммуникационные возможности [1].

Комплекс программно-аппаратных средств и организационных (процедурных) решений по защите информации от несанкционированного доступа включает следующие четыре подсистемы:

– управления доступом;
– регистрации и учета;
– криптографическую;
– обеспечения целостности.

Защита базы данных (БД) означает защиту самих данных и их контролируемое использование на ПК сети, а также защиту любой сопутствующей информации, которая может быть извлечена из этих данных или получена путем перекрестных ссылок. Отдельные объекты данных могут быть сами объектами защиты, но могут быть организованы в структуры БД (сегменты, отношения, каталоги и т. д.). Защита таких структур рассматривается в основном при анализе механизмов контроля доступа. Обеспечение защиты данных на ПК может быть описано следующим образом:

1) защита содержания данных (data content protection) объединяет функции, процедуры и средства защиты, которые предупреждают несанкционированное раскрытие конфиденциальных данных и информации в БД.

2) средства контроля доступа (access control security service) разрешают доступ к данным только полномочных объектов в соответствии со строго определенными правилами и условиями.

3) управление потоком защищенных данных (security-consistent flow of data) при передаче из одного сегмента БД в другой обеспечивает перемещение данных вместе с механизмами защиты, присущими исходным данным.

4) предотвращение возможности выявления (prevention of inference) конфиденциальных значений из данных, содержащихся в регулярных или статистических БД, в результате выявления статистически достоверной информации.

5) контроль согласованности (consistency control) при использовании БД предполагает процедуры, которые обеспечивают защиту и целостность отдельных элементов-данных, в частности их значений (зависимость от значений).

6) контекстная защита (content potection) данных, характерная для схем защиты динамических БД, также должна быть включена в состав процедур защиты БД. В этом случае защита отдельного элемента БД в каждый данный момент времени зависит от поведения всей системы защиты, а также предшествующих операций, выполненных над этим элементом (зависимость от предыстории).

7) предотвращение создания несанкционированной информации (presentation of unauthorized information generation) предполагает наличие средств, которые предупреждают, что объект получает (генерирует) информацию, превышающую уровень прав доступа, и осуществляет это, используя логическую связь между данными в БД [2].

Следует отметить, что применение криптографических методов способно существенно повысить стойкость защиты баз данных от несанкционированного доступа. Задача криптографической защиты БД существенно отличается от криптозащиты информации в рамках обычной файловой системы по следующим причинам:

1) возникает задача проектирования защиты информации с учетом СУБД либо путем встраивания защитных механизмов в СУБД, либо в виде внешних защитных оболочек (для систем, работающих без функций защиты).

2) файлы БД — это файлы определенной структуры. Пользователи могут иметь доступ к информации только из определенных частей БД, то есть возникает задача ранжирования прав доступа (избирательной защиты) внутри файла БД.

3) размер шифруемой информации в файле БД в общем случае произволен и ограничен только структурой БД.

Для более полной защиты необходимо ввести следующие уровни:

1) регистрация и аутентификация пользователей, ведение системного журнала. В системном журнале регистрируются любые попытки входа в систему и все действия оператора в системе.

2) определение прав доступа к информации БД для конкретного пользователя (авторизация пользователя) при обращении к СУБД. Все действия пользователя протоколируются в системном журнале. Определение полномочий пользователя при доступе к БД происходит на основе анализа специальной информации — списка пользователей с правами доступа, которая формируется администратором БД, исходя из принципа минимальных полномочий для каждого пользователя.

3) непосредственный доступ к БД. На этом уровне для повышения защищенности системы в целом целесообразно использовать шифрование/расшифрование отдельных объектов БД. Ключи для шифрования можно определять исходя из идентификатора пользователя и его полномочий, то есть «паспорта» пользователя.

В качестве примера можно привести алгоритм, реализованный в программном средстве «Экспресс-диагностика психофизических показателей»

При создании базы данных вводится дополнительное поле, в котором записывается уровень конфиденциальности данной записи. Информация БД шифруется и хранится на диске в зашифрованном виде. В каталоге СУБД создается БД, представляющая из себя регистрационную книгу, где содержится следующая информация: имя или код пользователя, пароль, уровень доступа.

Данный файл и управляющая *.prg-программа также шифруются. Создается и запускается управляющий *.bat-файл. К недостаткам данной реализации относятся:

– возможность удаления и модификации *.bat-файла;

– при некорректном завершении (например, ctrl+a1t+del) на диске может остаться файл базы данных в явном виде.

В заключение следует отметить, что при разработке механизмов защиты БД следует помнить о некоторых их особенностях:

– в БД объекты могут представлять собой сложные логические структуры, определенное множество которых может отображаться на одни и те же физические объекты;

– возможно существование различных требований по защите для разных уровней рассмотрения — внутреннего, концептуального и внешнего для БД; защита БД связана с семантикой данных, а не с их физическими характеристиками.

Литература

1. *Риккарди Г.* Системы баз данных. Теория и практика использования в Internet и среде Java : пер. с англ. М., 2001.

2. *Роб П., Коронел К.* Системы баз данных: проектирование, реализация и управление: пер. с англ. СПб., 2004.

ПРОГРАММНЫЙ МЕТОД ЗАЩИТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ «ЭКСПРЕСС-ДИАГНОСТИКА ПСИХОФИЗИЧЕСКИХ ПОКАЗАТЕЛЕЙ»

Н.Л. БОБРОВА

Защита программного обеспечения на сегодняшний день является одной из актуальных задач. Впервые задача защиты была озвучена в 70-х годах.