Технические науки

УДК 681.3

ЗАЩИТНЫЕ МЕХАНИЗМЫ ОХРАНЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА НА ПРИМЕРЕ БАЗ ДАННЫХ [1]

М. А. Родыгин, аспирант МГУ (Россия), ed@lenta.ru

Аннотация. В статье показывается возможность реализации механизмов безопасности базы данных как инструмента общего обеспечения безопасности предприятия и его экономического равновесного состояния. Определяется процедура структурирования процессов защиты и выбор методологического обоснования для ориентации процедур защиты. Выявлены особенности технологического развития средств защиты базы данных.

Ключевые слова: защита, база данных, процедура, безопасность, структура.

Вопросы обеспечения безопасности со стороны пользователей информации затрагивают весьма значительные аспекты для функционирования предприятия:

• если речь идет о коммерческом предприятии, то значение защиты информации может определять возможности развития компании, а также охраны коммерческих секретов. В то же время для коммерческих компаний защита информации в разрезе базы данных состоит не только в сохранении допустим списка полученных патентов, но прежде всего – человеческого потенциала, количества и квалификации работников, их доступности, а также направлений их деятельности;

• для государственных компаний базы данных являются основой деятельности. Для большинства органов власти, а также частных и коммерческих предприятий использование баз данных предполагает работу с личными данными, массивами персонализированных форм. Выявление этих данных и получение к ним несанкционированного доступа может означать не только создание угрозы государственности страны, но также и снижение доверия к государству со стороны граждан. Также не стоит забывать о возможности порчи данных и манипулирования судьбами людей – например по участию их в преступлениях или уничтожения деловой репутации.

Защита же информации наиболее актуальна для предприятий, которые систематизируются в объединения и пользуются распределёнными сетями обмена информации. Здесь появляется необходимость не только формировать принципы защиты внутренних сетей, но также и протоколов, которые обеспечивают транзакцию баз данных по каналам сети Интернет.

В двухзвенной архитектуре «клиент-сервер» прикладная часть выполняется клиентом (на рабочей станции, узле сети и т.п.), а сервер осуществляет доступ к БД. В случае сложности и емкости прикладной обработки в эту архитектуру добавляется сервер приложений, который берет на себя основную логику обработки информации и доступа к

[1] *Рецензент:* М.М. Подколзин, канд. с-х. наук, учредитель ЭНЖ «Наука. Мысль» (Волжский, Россия).

БД. При этом БД может быть централизованной (один сервер) или распределенной (несколько серверов). В распределенной БД основным условием сохранения данных является автономность и отсутствие прямых и транзитивных связей между компонентами БД, расположенных в удаленных разделах БД. Поскольку это условие ограничивает целостность данных, то в состав сервера включаются хранимые процедуры, с помощью которых устанавливаются ссылки на другие разделы БД. Как правило, защиту БД осуществляет специальный сервер. В его функции входит обеспечение парольной защиты, шифрования, установка прав доступа к объектам БД, защита полей и записей таблиц и т.д. Пароли устанавливаются конечными пользователями или администраторами БД, хранятся в защищенном виде в специальных файлах и используются сервером при доступе пользователей к БД. Шифрование осуществляется с помощью ключей фиксированной и нефиксированной длины для засекречивания сохраненной в БД информации или при передаче информации в сети от отправителя к получателю и наоборот. Установка прав доступа к БД заключается в регистрации пользователей для защиты от несанкционированного доступа, а именно: чтение, модификация, добавление, удаление, изменение структур таблиц и т.д. С помощью разрешенных для каждого пользователя прав осуществляется контроль их доступа к объектам БД и принимаются меры для защиты отдельных строк, столбиков, полей или БД в целом. К основным мероприятиям по проведению защиты данных БД относятся:

- режимные, включающие парольную, криптографическую проверки пользователей и т.д.;
- технологические, содержащие резервное копирование данных, правильное их хранение, эксплуатацию и др.;
- системные, с процедурами автоматизированной проверки полномочий и истинности пользователей, которые запрашивают доступ к данным, их привилегий, аудита событий, и т.д.

Режимные и технологические мероприятия поддерживаются методическими материалами и стандартами, регламентирующими действия группы лиц, ответственных за безопасность БД. Системные – образуют сервис безопасности, включающий сервер БД с функциями защиты. Особенностью распределенных БД (РБД) является размещение отдельных разделов данных на разных узлах сети, информация о расположении которых отражается в глобальном словаре данных и используется при доступе к РБД различных пользователей. Для обеспечения безопасности распределенных, многоуровневых и других БД в состав сервера БД включаются хранимые процедуры проверки прав и полномочий пользователей, определенные моделями защиты, средствами контроля доступа, реализованными в сервисе безопасности БД. На рисунке 1 приведен пример архитектуры распределенной системы управления базой данных (СУБД) с защитой информации.

Пользователи 1, 2, ..., N обращаются к данным через сервис безопасности, который контролирует доступ и выполняет только разрешенные операции над БД, в которых содержатся отдельно непубличные данные секретного типа (коммерческая тайна, персональные данные пользователей), секретные и несекретные данные. В запросах на доступ к совершенно секретным, секретным и конфиденциальным данным указываются права и/или полномочия пользователя, проверяются сервисом безопасности по списку

контроля доступа и таблицей полномочий.

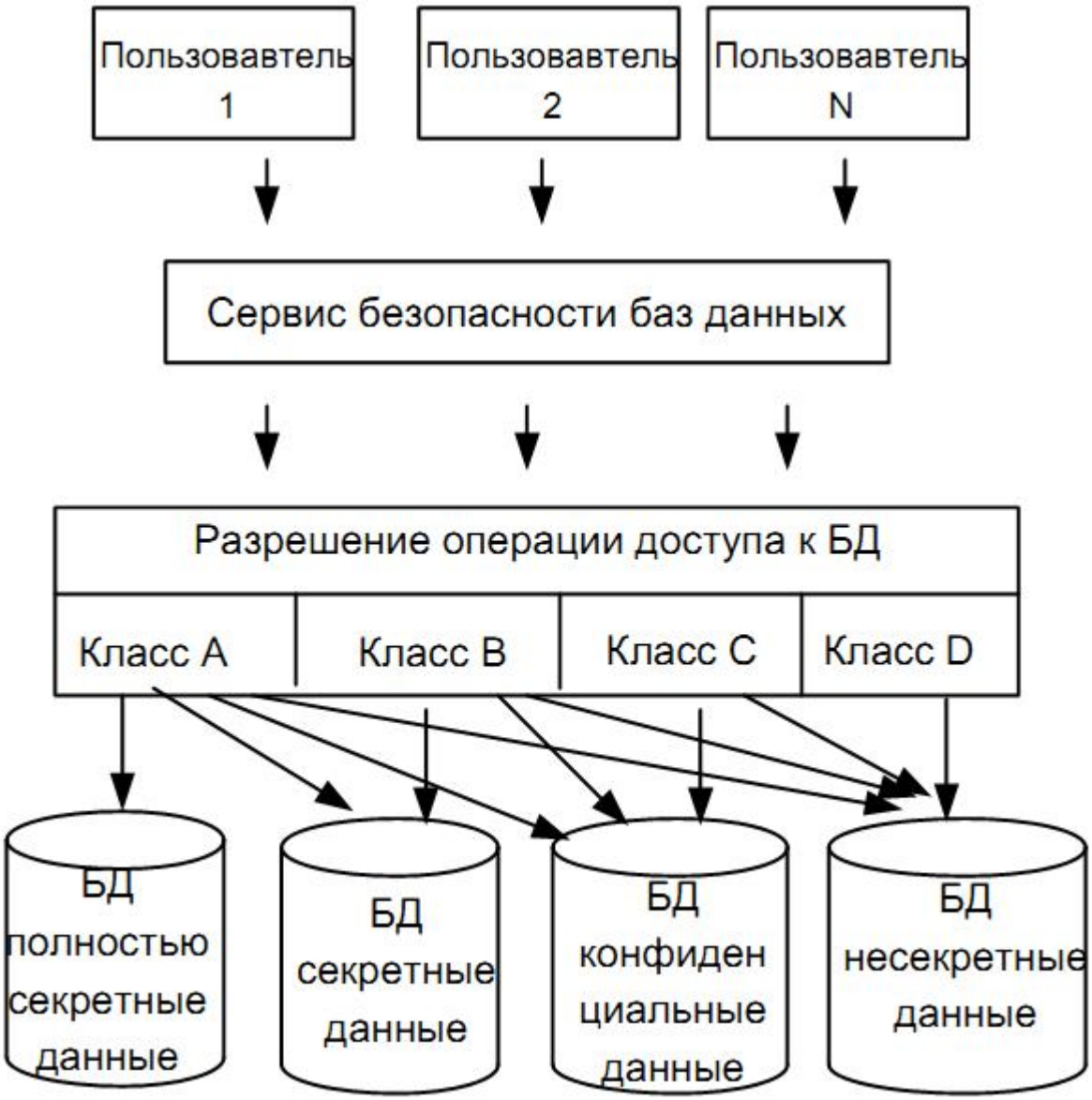

Рисунок 1 – Пример архитектуры распределенной СУБД с защитой информации

Для работы с секретной информацией в БД могут быть приведены многозначные отношения в виде множества последовательных проверок с тем же самым значением первичного ключа. Примером такого отражения могут служить данные о сотрудниках военного заведения, для которых под одинаковой фамилией указаны, наряду с их реальными званиями и видами деятельности, также фальшивые данные для их прикрытия. БД с такими данными требуют многоуровневой защиты, или использование механизмов маскировки данных пустыми значениями. При модификации пустых значений многоуровневая защита СУБД может выдать отказ в доступе, если у пользователя (или процесса) отсутствуют полномочия на проведение модификаций в искомом массиве данных. Модификация обычно проводится с помощью косвенного канала, представляет собой механизм, благодаря которому пользователь, который обладает высоким уровнем полномочий и прав, может предоставить информацию пользователю с меньшими правами

и полномочиями. Многоуровневая защита данных может производиться с помощью мандатного управления доступом, основанная на свойствах модели Bell-LaPool для производных базовых отношений и SQL-представления. Современный язык SQL содержит операторы защиты данных: grant и revoke. Оператор grant дает возможность предоставлять привилегии для доступа и модификации объектов, а также передавать другим пользователям права на привилегии (с помощью конструкции with grant option). Оператор revoke позволяет отбирать права, предоставленные ранее некоторому пользователю. Многие SQL-ориентированные СУБД имеют собственные средства безопасности БД, реализованные на средствах защиты данных на языке SQL.

Для обеспечения безопасности неоднородных систем мультибаз применяются мощные средства многоуровневой защиты данных, защищенные базы данных и информационные менеджеры, которые управляют защитой данных. Пользователь, который имеет определенные полномочия, получает доступ к мультибазе только в том случае, когда в запросе указан соответствующий параметр аутентификации. СУБД с многоуровневой защитой обычно расширяется языковыми средствами DDL (Definition Data Language), которые предназначены для спецификации классов безопасности относительно мультиуровневого языка SQL.

Степень безопасности в объектно-ориентированных БД ниже, чем в развитых реляционных СУБД. Принципы многоуровневой защиты, разработанные для реляционных баз данных, такие, как многозначность и модель Bell-LaPool, получили развитие в объектно-ориентированной системе SODA (Secure Object-oriented Database). В ней модель Bell-LaPool объединена со стратегией присваивания меток безопасности двух видов: объектов и переменных объектов. В первом случае классификация объектов осуществляется путем определения одного общего класса для всего массива или для одного его объекта. Во втором случае каждому переменному объекту присваивается независимая метка, которая соответствует диапазону классификации объектов на уровне элементов массива, при котором каждый параметр имеет собственный допустимый диапазон классификации, а элемент массива – индивидуальную классификацию, независимую от других элементов. С помощью таких меток классифицируются составные или несоставные объекты объектно-ориентированных БД, и создается набор правил для управления уровнями защиты классов объектов и отношений между объектами.

Рассмотренные модели безопасности ориентированы на поддержку нескольких уровней защиты и касаются преимущественно БД с реляционной архитектурой. Эффективность моделей существенно повышается, если дополнительно применяется шифрование информации. Однако каждая из рассмотренных и любая другая известная модель не предоставляют полной защиты информации. В связи с бурным развитием компьютерных сетей, электронной коммерции и электронного бизнеса с использованием Интернет все большую актуальность приобретает проблема обеспечения безопасности РБД и серверов БД. Используя объектно-ориентированный подход любую распределенную БД, которая взаимодействует с пользователями, можно рассматривать как сетевую структуру, для которой применяются разработанные для сетевых сред методы обеспечения безопасности и защиты информации. Совместное рассмотрение моделей, методов и средств взаимодействия и обеспечения безопасности объектов БД с

вышеизложенными моделями защиты информации позволяет по-новому взглянуть на вопросы безопасности информации в среде РБД.

Итогом исследования можно считать те методологические формы и стандарты, которые определяют уровень защиты баз данных от несанкционированного доступа извне. Особое внимание следует уделять таким вопросам, как внутреннее обеспечение безопасности, так как именно на эти риски уходит более 70% случаев регистрации нарушения режима доступа к базам данных. В нашем исследовании мы затрагивали аспект именно технологического противодействия процессам, которые не санкционированы службой безопасности либо иными операторами данных. Также мы считаем, что для предприятий, которые работают с режимной информацией, имеющие элементы "для служебного пользования", "секретно" и "совершенно секретно", недопустимо использование внешних аутсорсинговых моделей размещения баз данных. Если требуется использование данных в распределенной сети, то подобные механизмы должны быть реализованы с привлечением исключительно государственных операторов и аккредитованных для работы с непубличными данными организаций.

Литература:

1. Мирошник М.А. Разработка средств защиты информации в распределенных компьютерных системах и сетях // Системы управления и дистанционного доступа. 2015. № 1 (110). С. 18-25.

2. Насонова В.А., Дрога А.А., Жукова П.Н. О некоторых методиках защиты баз данных от внутренних злоумышленников // В сборнике: Проблемы информационного обеспечения деятельности правоохранительных органов Материалы международной научно-практической конференции. Белгород, 2015. С. 55-62.

3. Пащенко И.Н., Васильев В.И., Гузаиров М.Б. Защита информации в сетях smart grid на основе интеллектуальных технологий: проектирование базы правил // Известия ЮФУ. Технические науки. 2015. № 5 (166). С. 28-37.

4. Утечки конфиденциальной информации. Итоги 2014 года // Защита информации. Инсайд. 2015. № 3 (63). С. 50-55.

References

1. Miroshnik M.A. Razrabotka sredstv zashhity informacii v raspredelennyh komp'juternyh sistemah i setjah // Sistemy upravlenija i distancionnogo dostupa. 2015. № 1 (110). S. 18-25.

2. Nasonova V.A., Droga A.A., Zhukova P.N. O nekotoryh metodikah zashhity baz dannyh ot vnutrennih zloumyshlennikov // V sbornike: Problemy informacionnogo obespechenija dejatel'nosti pravoohranitel'nyh organov Materialy mezhdunarodnoj nauchno-prakticheskoj konferencii. Belgorod, 2015. S. 55-62.

3. Pashhenko I.N., Vasil'ev V.I., Guzairov M.B. Zashhita informacii v setjah smart grid na osnove intellektual'nyh tehnologij: proektirovanie bazy pravil // Izvestija JuFU. Tehnicheskie nauki. 2015. № 5 (166). S. 28-37.

4. Utechki konfidencial'noj informacii. Itogi 2014 goda // Zashhita informacii. Insajd. 2015. № 3 (63). S. 50-55.

Rodygin M. A. Zashhitnye mehanizmy ohrany informacii ot nesankcionirovannogo dostupa na primere baz dannyh / M. A. Rodygin // Nauka. Mysl'. - № 8. – 2015.

– • –

Annotation. The article shows the mechanism for implementing security mechanisms database as a tool for the overall security of the enterprise and its economic equilibrium. The structuring processes of security and the choice of methodological basis for targeting security procedures are determined. The features of the technological development of the database security means are revealed.

Keywords: protection, database, procedure, safety, structure.

– • –

Сведения об авторе:

Михаил Алексеевич **Родыгин**, аспирант МГУ. Россия.

.

– • –

Подписано в печать 22.11.2015.