ОБ ОРГАНИЗАЦИИ ЗАЩИТЫ КОРПОРАТИВНЫХ ДАННЫХ

М.Г. УСОВА, Д.М. СТЕРИНЗАТ, М.С. ТИВАНОВА

Выбор средств обеспечения безопасности и объем их использования зависит от того, насколько продуманно и эффективно реализованы меры по предоставлению пользователю прав на те или иные корпоративные данные. Авторами предложен следующий подход в решении поставленной задачи.

Пользователей корпоративной информационной системы делят на группы. Это пользователи: а) формирующие данные, входящие в корпоративную информацию, б) выполнение должностных обязанностей которых предполагает использование полной информации о деятельности организации, в) которым предоставляются индивидуальные наборы различных данных. Различия между группами обусловило использование способов защиты информации, как на уровне клиентских приложений системы, так и на уровне базы данных.

Назначение прав на уровне приложения подразумевает наличие в программе участка кода, который определяет имя пользователя и, в зависимости от уровня привилегий, формирует содержание отображаемой страницы. При назначении прав на уровне базы для каждой таблицы перечислен список учетных записей пользователей и привилегии каждого из них на выполнение различного типа запросов. Поэтому при попытке выполнения SQL-запроса, на который данная учетная запись не имеет прав, СУБД реагирует возникновением исключительной ситуации, обрабатывая которую приложение сигнализирует о возникновении аномалии доступа и возвращается к предыдущей странице. Применяя комбинацию приведенных способов, авторы добились упрощения приложения и оптимизации процесса назначения прав. Используя доступ на уровне приложения, мы обеспечиваем выбор из специально созданной таблицы состава

меню для групп, в которые входит одна и та же учетная запись. Далее, исходя из определения прав, в БД путем создания представления пользователя, формируется ограниченный набор данных.