“Ярославский государственный университет им. П.Г. Демидова”

Кафедра компьютерной безопасности и математических методов обработки информации

**Реализация RLS (безопасность на уровне строк) в реляционных базах данных**

Направление подготовки: «10.05.01 Компьютерная безопасность»

Выполнил: студент группы KБ-61СО, Попов Сергей Андреевич

Научный руководитель: Старший преподаватель кафедры КБ и ММОИ., Власова О.В.

В последнее время на рынке приложений для коммерческих организаций стало появляться всё больше и больше приложений для которых требуется умное разграничение прав - то есть необходимо иметь возможность создавать политики безопасности, которые бы имели механизм гибкой настройки прав и разрешений для конечных пользователей. Создание гибкой политики безопасности является довольно трудной задачей, так как обычно необходимо учесть очень много факторов. Зачастую это становиться головной болью для разработчиков, так как требования к безопасности растут и механизм должен удовлетворять даже самым замысловатым требованиям.

В последнее время приложения необходимо устанавливать на многие платформы - мобильные устройства, планшеты, часы, настольные компьютеры и web приложения, поэтому возникает проблема выбора языка программирования на котором будет реализована политика безопасности. Сразу написать приложение под все платформы является ещё более трудной задачей на текущий момент из-за несовершенства программ исполняющих код на разных платформах.

Не так давно появился механизм для создания гибких политик безопасности на языке SQL во многих системах управления базами данных. Он позволяет реализовать политику безопасности на уровне сервера базы данных, причём приложение, работающее с данным, поставляемыми сервером БД, не знает ни о какой политике безопасности. Таким способом можно изолировать код приложения от определения и реализации механизма разграничений прав на записи в таблицах.

Объект исследования - гибкие политики безопасности на языке SQL в системах управления базами данных.

Предмет исследования - возможность реализации механизма гибкого разграничения прав на записи базы данных, на основе предикатов.

Цель выпускной квалификационной работы - разработка приложения для просмотра и изменения данных на основе механизма гибкого разграничения прав на записи базы данных, на основе предикатов.

Для достижения цели выпускной квалификационной работы были поставлены следующие задачи:

* Изучить принципы создания политики безопасности в СУБД SQL SERVER 2016
* Изучить способы создания политики безопасности как без использования встроенного механизма RLS, так и с ним
* Спроектировать базу данных, на которую будет накладываться политики безопасности
* Написать приложение для просмотра и изменения данных подготовленной базы данных
* Реализовать механизм гибкого разграничения прав на записи базы данных, на основе предикатов
* Измерить производительность и практичность данного механизма

В данной работе были проведены исследования в создании политик безопасности, как без поддержки встроенных функций и методов сервера базы данных, так и при помощи уже готового фреймворка, предоставляемого СУБД SQL SERVER 2016.

Были исследованы методы создания механизмов для формирования политик безопасности, основанных на предикатах. Также были проведены эксперименты по формированию статических предикатов и динамических, созданных через разбор строки и данных контекста выполнения запросов.

Был реализован гибкий механизм разграничение доступа к данным посредством создания динамически изменяемой системы политик безопасности для созданного в рамках выпускной квалификационной работы приложения управления сущностями базы данных. Была разработана библиотека для анализа и разбора булевого выражения, используемого в качестве функции доступа к конкретной строке.

Можно отметить, что создание политики безопасности с помощью встроенных функций гораздо проще, но не производительнее. Замеры времени запросов к базе данных с включённой политикой безопасности показали, что использование реализованной системы динамических предикатов не является практичной для использовании её в реальном приложении.