УДК 004.9
doi: 10.21685/2587-7704-2024-9-2-1

Open Access RESEARCH ARTICLE

Сравнительный анализ способов защиты информации в автоматизированных системах с использованием системы управления базами данных PostgreSQL

Андрей Александрович Шлыков
Пензенский государственный университет, Россия, г. Пенза, ул. Красная, 40
69shlykov_andrew96@mail.ru

Александр Сергеевич Антипкин
Пензенский государственный университет, Россия, г. Пенза, ул. Красная, 40
antipkin.a@bk.ru

Аннотация. Данное исследование посвящено анализу существующих методов защиты информации для систем, использующих систему управления базами данных PostgreSQL. Целью работы является определить преимущества и недостатки некоторых из существующих методов защиты информации пользователей, использующих автоматизированные системы. Проведенный анализ позволит оптимизировать выбор того или иного метода защиты при создании будущих автоматизированных систем, что ускорит разработку. Результаты также могут использоваться при сравнении с другими методами защиты информации.

Ключевые слова: защита информации, аутентификация, PostgreSQL, хранение данных

Для цитирования: Шлыков А. А., Антипкин А. С. Сравнительный анализ способов защиты информации в автоматизированных системах с использованием системы управления базами данных PostgreSQL // Инжиниринг и технологии. 2024. Т. 9 (2). С. 1–3. doi: 10.21685/2587-7704-2024-9-2-1

Comparative analysis of information security methods in automated systems using database management system PostgreSQL

Andrey A. Shlykov
Penza State University, 40 Krasnaya Street, Penza, Russia
69shlykov_andrew96@mail.ru

Aleksandr S. Antipkin
Penza State University, 40 Krasnaya Street, Penza, Russia
antipkin.a@bk.ru

Abstract. This study is devoted to the analysis of existing information security methods for systems using PostgreSQL database management system. The purpose of the work is to identify the advantages and disadvantages of some of the existing methods of protecting the information of users using automated systems. The analysis will optimize the choice of a particular protection method when creating future automated systems, which will speed up development. The results can also be used in comparison with other information security methods.

Keywords: information security, authentication, PostgreSQL, data storage

For citation: Shlykov A.A., Antipkin A.S. Comparative analysis of information security methods in automated systems using database management system PostgreSQL. *Inzhiniring i tekhnologii = Engineering and Technology*. 2024;9(2):1–3. (In Russ.). doi: 10.21685/2587-7704-2024-9-2-1

Введение

Базы данных – неотъемлемая часть множества автоматизированных систем. Они позволяют структурировать массивы данных, собирать важные сведения и свободно находить уже имеющуюся информацию, что делает их весьма популярным средством хранения данных в настоящее время.

Система управления базами данных (СУБД) PostgreSQL – одна из множества систем, позволяющих создать базу данных и интегрировать ее в систему [1]. Главными ее достоинствами являются: свободное распространение, совместимость со всеми популярными языками программирования и высокая оптимизация.

Однако наряду с преимуществами существуют и некоторые недостатки. Одним из них является возможная утечка данных, содержащих конфиденциальную информацию, что влечет за собой множество проблем. Потому крайне важно позаботиться о способах защиты системы для недопущения кражи данных.

Исходя из этого, были поставлены две задачи.

1. Провести анализ средств защиты непосредственно силами самой СУБД PostgreSQL.

2. Провести анализ типовых решений при реализации защиты на уровне клиентского приложения.

Система управления базами данных PostgreSQL предоставляет возможность настройки прав пользователей в виде «ролей». В качестве роли может быть как отдельный пользователь, так и группа, куда эти пользователи включены. Тогда все настройки прав доступа для одной роли будут передаваться для ролей, включенных в первую.

Как и большинство СУБД, PostgreSQL предлагает назначить привилегию SELECT. То есть для роли можно ограничить столбцы, которые могут вывестись для пользователя при обращении к таблице. PostgreSQL также позволяет назначать привилегии INSERT, UPDATE, DELETE и TRUNCATE, которые ограничивают пользователя в добавлении, изменении и удалении данных из таблицы.

Помимо этого, СУБД позволяет назначить права для подключения к определенным базам данных, создания новых таблиц или столбцов в таблицах, выполнения хранимой функции для данного пользователя и т.д. Однако одной из наиболее продвинутых функций системы привилегий PostgreSQL является безопасность на уровне строк. С помощью специальных «политик» можно организовать проверку, где будет описано условие, при котором будут сравниваться определенные параметры для вывода или обновления каждой отдельной строки таблицы.

Данные возможности СУБД PostgreSQL позволяют реализовать разграничение прав доступа даже в самых сложных предметных областях, но при всем этом нет возможности организовать безопасность на уровне одной ячейки. Данная возможность актуальна в тех системах, где данные в определенном столбце таблицы должны быть доступны пользователю не полностью [2].

Для организации такого уровня защиты необходимо прибегать к решениям на уровне клиентского приложения. В таком случае роли в СУБД не создаются и каждый клиент подключается под основной ролью СУБД PostgreSQL «postgres», которой доступны все возможности как по выборке и изменению данных таблиц, так и по изменению структуры базы данных в целом.

При использовании данного метода должна создаваться таблица, в которой будут перечислены логины пользователей, их пароли, какие-либо бизнес-данные, а также уровень доступа пользователя к данным. При входе в приложение клиента пользователь вводит свои аутентификационные данные, а программа должна реализовывать фильтрацию тех данных, к которым данный пользователь имеет доступ, при этом из самой базы приходят абсолютно все данные из таблицы, к примеру при вызове запроса SELECT. Данный вид защиты крайне сложен в реализации, поскольку для его осуществления необходимо написать огромное множество проверок вручную, но при этом нет никаких ограничений в возможностях фильтрации данных.

Исходя из этого можно перечислить плюсы и минусы каждого из способов реализации прав доступа, а также предположить условия использования данных методов.

Плюсы реализации защиты на уровне СУБД PostgreSQL:

1) простота и удобство настройки прав доступа;

2) облегчение нагрузки на клиентское приложение, которому нет необходимости фильтровать данные, поскольку данные уже пришли в том виде, к которому пользователь имеет доступ.

Минусы реализации защиты на уровне СУБД PostgreSQL:

1) ограниченность в настройке прав доступа;

2) невозможность реализовать защиту на уровне ячейки.

Сфера применения: клиент-серверные приложения, в которых нет необходимости сложной настройки защиты информации.

Плюсы реализации защиты на уровне клиента:

1) высокая надежность данного метода при правильном подходе и соблюдении всех правил;

2) возможность реализации защиты на уровне ячейки.

Минусы реализации защиты на уровне СУБД PostgreSQL:

1) сложность реализации такого вида защиты;

2) повышенная нагрузка на приложение клиента;

3) данный вид защиты имеет место быть лишь при комплексном подходе к защите информации, т.е. не только на программном, но и на сетевом и физическом уровнях.

Сфера применения: автоматизированные системы с повышенными требованиями к защите информации. К таким системам могут относиться, например, системы, хранящие данные мониторинга биомедицинских показателей человека [3], системы для обучения в области медицины [4], где хранятся индивидуальные профили пользователей и результаты выполнения учебных заданий [5].

В результате исследования были поставлены основные задачи, помогающие проанализировать методы защиты информации в автоматизированных системах с использованием СУБД PostgreSQL.

Развитие данной работы заключается в использовании приведенных методов защиты в автоматизированных системах на базе СУБД PostgreSQL.

Список литературы

1. PostgreSQL: The world’s most advanced open source database // Официальный сайт СУБД PostgreSQL. URL: https://www.postgresql.org/ (дата обращения: 08.03.2024).
2. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. М. : Радио и связь, 1999.
3. Сафронов М. И., Кузьмин А. В., Бодин О. Н. [и др.]. Способ и аппаратно-программные средства анализа биоимпеданса для систем мобильного мониторинга ЭКГ // Модели, системы, сети в экономике, технике, природе и обществе. 2020. № 3 (35). С. 118–128. doi: 10.21685/2227-8486-2020-3-10
4. Денисов О. Е., Левашов И. А., Кузьмин А. В. Информационная система для изучения анатомии человека // Модели, системы, сети в экономике, технике, природе и обществе. 2014. № 2 (10). С. 153–157.
5. Колсанов А. В., Назарян А. К., Иващенко А. В., Кузьмин А. В. Сетевой компонент информационного пространства современного хирургического тренажера // Программные системы и вычислительные методы. 2015. № 1. С. 11–20. doi: 10.7256/2305-6061.2015.1.13990

References

1. PostgreSQL: The world’s most advanced open source database. *Official website SUBD PostgreSQL*. (In Russ.). Available at: https://www.postgresql.org/ (accessed 08.03.2024).
2. Romanec Ju.V., Timofeev P.A., Shan'gin V.F. *Zashhita informacii v komp'juternyh sistemah i setja = Information protection in computer systems and networks*. Moscow: Radio i svjaz', 1999. (In Russ.)
3. Safronov MI., Kuz'min A.V., Bodin O.N. et al. Method and hardware and software for bioimpedance analysis for mobile ECG monitoring systems. *Modeli, sistemy, seti v jekonomike, tehnike, prirode i obshhestve = Models, systems, networks in economics, technology, nature and society*. 2020;(3):118–128. (In Russ.). doi: 10.21685/2227-8486-2020-3-10
4. Denisov O.E., Levashov I.A., Kuz'min A.V. Information system for the study of human anatomy. *Modeli, sistemy, seti v jekonomike, tehnike, prirode i obshhestve = Models, systems, networks in economics, technology, nature and society*. 2014;(2):153–157. (In Russ.)
5. Kolsanov A.V., Nazarjan A.K., Ivashhenko A.V., Kuz'min A.V. A network component of the information space of a modern surgical simulator. *Programmnye sistemy i vychislitel'nye metody = Software systems and computational methods*. 2015;(1):11–20. (In Russ.). doi: 10.7256/2305-6061.2015.1.13990

Поступила в редакцию / Received 21.02.2024

Принята к публикации / Accepted 21.03.2024