

004.65, 004.056.53

## ОБЗОР И АНАЛИЗ МЕХАНИЗМОВ АУТЕНТИФИКАЦИИ В СУБД POSTGRESQL

Морозов С. В. (СПБПУ)

Научный руководитель – к. т. н, доцент Нестеров С. А. (СПБПУ)

**Введение.** СУБД PostgreSQL, которая сейчас в нашей стране все шире используется в информационных системах с разными требованиями к защищенности, предлагает несколько различных методов аутентификации клиентов [2]. Эти методы можно разбить на группы

1. методы аутентификации по паролю, хранящемуся в таблице внутри СУБД;
2. методы аутентификации по паролю, хранимому во внешней службе;
3. методы внешней аутентификации, в подобных случаях аутентификация

происходит вне СУБД.

Ставится задача выбора приоритетного метода аутентификации в зависимости от типа задач выполняемых информационной системой и ограничений на эту систему. В данной работе делается обзор механизмов аутентификации в СУБД PostgreSQL и производится анализ их защищённости.

**Основная часть.** В данной работе выполнен обзор и анализ механизмов аутентификации, использующихся в СУБД PostgreSQL. Рассмотрены такие методы как

1. Методы аутентификации по паролю во внутренней таблице СУБД: password, md5, scram-sha-256;
2. Методы аутентификации по паролю, хранящемуся во внешней службе: LDAP, RADIUS, PAM;
3. Методы внешней аутентификации: peer, cert, gss, sspi [1].

Для проведения эксперимента была развёрнута СУБД PostgreSQL 15 на операционной системе РЕД ОС 7.3.4 и исследованы основные методы аутентификации, доступные в данной СУБД. Выполнялась аутентификация методами внутренней аутентификации по паролю: password, md5, scram-sha-256 и методом внешней аутентификации peer. В первом случае, при использовании методов md5 или scram-sha-256, хеш пароля хранится в системной таблице pg\_authid, во втором случае, при использовании метода peer пароль не запрашивается, так как имя пользователя операционной системы является разрешённым именем пользователя базы данных. Также рассмотрены элементарные методы trust и reject, где trust допускает всех пользователей, а reject не допускает никого. В процессе исследования выявлены ограничения, накладываемые каждым методом, выявлены достоинства и недостатки каждого метода, проведён анализ вышеуказанных методов с определением приоритетности использования того или иного метода.

**Выводы.** Проведён анализ существующих решений, рассмотрены достоинства и недостатки каждого метода. В ближайшей перспективе планируется исследование методов LDAP, PAM и аутентификации через GSSAPI. Результаты работы предполагается использовать в дальнейших разработках, а также при принятии решений по использованию метода аутентификации в зависимости от прикладной задачи.

### Список используемых источников:

1. Документация PostgreSQL и Postgres Pro // PostgresPro URL: <https://postgrespro.ru/docs> (дата обращения: 17.01.2024)
2. Агафонов, А. А. Безопасность систем баз данных: учебное пособие / А.А. Агафонов, А.С. Юмаганов. – Самара: Издательство Самарского университета, 2023. – 272 с

Морозов С. В. (автор)

Нестеров С. А. (научный руководитель)

\_\_\_\_\_

\_\_\_\_\_