УДК 004.046

Безопасное взаимодействие облачных сервисов по протоколу OAuth 2.0

Березина А.С.

ГБОУ гимназия №446 Колпинского р-на Санкт-Петербурга, 11 класс

Вступление: Интернет Вещей становится все более привычным явлением в нашей жизни, продолжая набирать обороты. Мы видим, что машины становятся способными выполнять все более сложные задачи. Объем обрабатываемой информации неуклонно растет. Все это приближает нас к тому моменту, когда аналитические приложения на основе искусственного интеллекта будут способны делать точные прогнозы в таких сложных областях как, например, медицина. Однако возникает проблема связи аналитических систем и систем сбора информации от разных производителей. Ключевым элементом здесь является безопасный доступ к персональным данным субъекта и возможность субъекта принимать решение о том, кому предоставлять доступ.

Цель работы: Реализация взаимодействия микросервисов, ответственных за сбор информации, и аутентификационного микросервиса в облаке на базе Kubernetes.

Задачи:

1. Реализовать сервер сбора информации – прототип сервера любого приложения.
2. Реализовать сервер для аутентификации пользователей.
3. Создать сервер для хранения пользовательских данных (база данных).
4. Реализовать взаимодействие аутентификационного сервера с пользователем для авторизации.
5. Реализовать получение авторизационного токена сервером сбора информации от сервера аутентификации по протоколу OAuth 2.0.
6. Реализовать вышеуказанные серверы в виде микросервисов в облаке с возможностью масштабирования и обеспечения отказоустойчивости (high availability).

Вывод: Подход на основе протокола OAuth 2.0 идеально решает вышеуказанную проблему и применим в различных сферах деятельности человека: аналитика, умный дом, медицина, банковская деятельность, и т.д.