УДК 004.056

ОБЕСПЕЧЕНИЕ ЗАЩИЩЕННОСТИ МИКРОСЕРВИСОВ

А.Н. Крутов
«Самарский национальный исследовательский университет имени академика С.П. Королёва», г. Самара

Ключевые слова: микросервисы, обеспечение защищенности.

При разработке современных информационных систем микросервисная архитектура приложения становится все более востребованной. Она позволяет получить хорошо масштабируемую и легкую в управлении и развертывании архитектуру программного обеспечения, позволяющую быть гибкой и отказоустойчивой.

В монолитной архитектуре приложение выступает как единое целое, состоящее из множества компонентов, главными чертами которых являются тесная связанность и совместная работа [1]. В противовес этому, микросервисная архитектура предоставляет группу сервисов, которые слабо связаны и доступ к которым пользователь получает посредством общего пользовательского интерфейса (рисунок 1).

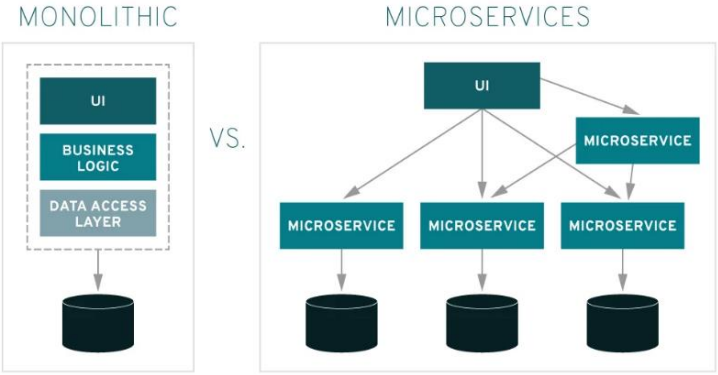

Рисунок 1 – Сравнение микросервисной и монолитной архитектур

При проектировании систем необходимо учитывать механизмы безопасности. Для этого необходимо проанализировать то, в какой защите нуждаются данные при передаче из одной точки в другую и в какой защите они нуждаются в состоянии покоя, также необходимо позаботиться о безопасности базовых операционных систем и сетей.

Аутентификация и авторизация являются основными понятиями, когда речь идет о людях и модулях, которые взаимодействуют с информационной системой. Для монолитных приложений обычно само приложение выполняет проверку подлинности и авторизацию. В случае

микросервисов предполагается, что пользователь не должен входить в систему отдельно для разных систем, используя для каждой свое имя пользователя и пароль. Цель состоит в том, чтобы иметь единую личность, которую можно аутентифицировать один раз.

Единый вход (Single Sign-On, SSO) – это технология, которая позволяет пользователям получать доступ к нескольким приложениям и службам с одним набором учетных данных. Она обычно использует централизованную службу проверки подлинности, такую как поставщик удостоверений или служба маркеров безопасности, которая отвечает за аутентификацию пользователя и выдачу маркеров безопасности, которые можно использовать для доступа к различным службам.

В настройке микросервиса каждый сервис может принять решение об обработке перенаправления и подтверждения связи с поставщиком удостоверений. Очевидно, это может означать много дублированной работы. Чтобы избежать этого, можно использовать шлюз в качестве прокси-сервера, находящегося между службами и «внешним миром» (рисунок 2).

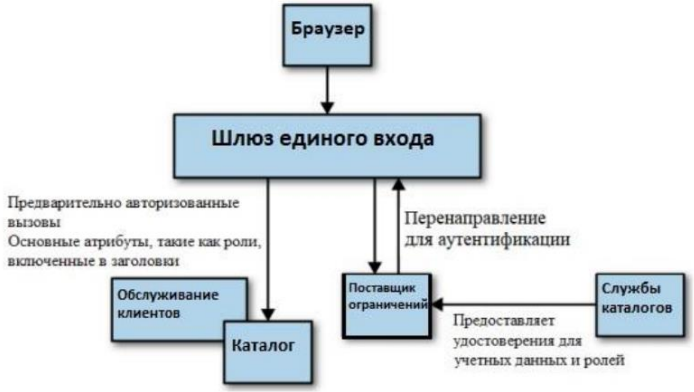

Рисунок 2 – Использование шлюза для обработки единого входа

Базовая проверка подлинности – это простой и широко используемый метод проверки подлинности HTTP(S) в архитектуре микрослужб. Базовая проверка подлинности может использоваться для защиты связи между клиентом и микрослужбами, а также между различными микрослужбами. Он обеспечивает простой и хорошо зарекомендовавший себя способ аутентификации пользователей и обеспечения контроля доступа.

Наиболее предпочтительным в плане обеспечения защищенности, представляется использование глубокоэшелонированной защиты, т.е. подхода к кибербезопасности, в котором используется ряд защитных механизмов для защиты информации. Если один механизм выходит из строя, немедленно включается другой, чтобы предотвратить атаку. Этот

многоуровневый подход с преднамеренной избыточностью повышает безопасность системы в целом и устраняет множество различных векторов атак. Только комплексное использование современных средств по защите информации может поставить надежный заслон на пути потенциального злоумышленника.

Список использованных источников

1. Погодина, Е. К. Цифровая трансформация. Микросервисы против монолитной архитектуры // Использование Big Data в официальной статистике Using Big Data in official statistics : Материалы II Всероссийской научно-исследовательской конференции, Липецк, 29 июня 2022 года. – Липецк: Липецкий государственный технический университет, 2022. – С. 241-245.

Крутов Алексей Николаевич, к.ф-м.н., доцент каф. безопасности информационных систем, krutov.an@ssau.ru

УДК 004.056.5

ОСОБЕННОСТИ ПАРАМЕТРОВ ВХОДНОГО СЛОЯ НЕЙРОННОЙ СЕТИ ПРОГРАММНОГО КОМПЛЕКСА МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ

А.С. Исмагилова, Н.Д. Лушников
Уфимский университет науки и технологий, г. Уфа

Ключевые слова: аутентификация, информационная система, база данных, распознавание личности.

Разработанный программный комплекс многофакторной биометрической аутентификации предназначен для распознавания личности пользователя информационной системы [1]. Для повышения качества и точности обработки данных в рамках разработки программного комплекса были применены нейронные сети.

Целью настоящей работы является повышение уровня защиты информации пользователей информационных систем [1].

Для реализации программного комплекса была составлена архитектура нейронной сети с входными параметрами.

Входными параметрами архитектуры нейронной сети распознавания личности по голосу являются:

1. LPC – коэффициенты линейного предсказания,
2. PLP – перцепционные коэффициенты линейного предсказания,
3. MFCC – мел-кепстральные коэффициенты,
4. CQCC – констант Q-кепстральные коэффициенты,
5. SCF – частоты спектрального центроида,