УДК 004.056 Вестник УрФО № 3(61) / 2026, с. 64–77
DOI: 10.14529/secur260305

Южаков Н.А., Южаков А.А.

АРХИТЕКТУРА БИОМЕТРИЧЕСКОЙ АВТОРИЗАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Yuzhakov N.A., Yuzhakov A.A.

ARCHITECTURE OF BIOMETRIC AUTHORIZATION IN INFORMATION SYSTEMS

Обеспечение надёжного контроля доступа остаётся фундаментальной задачей информационной безопасности. Эволюция архитектуры программного обеспечения в сторону микросервисов увеличивает поверхность атаки и требует внедрения новых архитектурных паттернов разграничения доступа. В то же время классическая парольная аутентификация демонстрирует недостаточную устойчивость к современным угрозам, уступая место биометрическим технологиям.

В работе проведён систематический анализ недостатков существующих архитектурных паттернов авторизации (децентрализованный, централизованный с удалённым PDP, централизованный со встроенным PDP) применительно к интеграции биометрических методов. Выявлены конкретные разрывы: отсутствие метрик обновления биометрических политик, незащищённость от replay-атак в веб-среде, неадаптированность обманных сценариев к микросервисной архитектуре. Для каждого недостатка предложен способ устранения: метрика Policy Update Cost (PUC), протокол привязки биометрического семпла к TLS-сессии, распределённый honeypattern-механизм. Сформулированы практические рекомендации для архитекторов ИБ, позволяющие реализовать принцип defense in depth

Ключевые слова: микросервисная архитектура, аутентификация, авторизация, биометрия, политики доступа, Policy Decision Point (PDP), нейронные сети, распознавание лиц, WebRTC.

Ensuring reliable access control remains a fundamental task in information security. The evolution of software architecture towards microservices increases the attack surface and requires the implementation of new architectural patterns for

access control. At the same time, classic password-based authentication demonstrates insufficient resilience against modern threats, giving way to biometric technologies.

The paper provides a systematic analysis of the shortcomings of existing architectural authorization patterns (decentralized, centralized with a remote PDP, centralized with an embedded PDP) in relation to the integration of biometric methods. Specific gaps have been identified: the lack of metrics for updating biometric policies, vulnerability to replay attacks in the web environment, and the unadaptability of deceptive scenarios to microservice architecture. For each shortcoming, a solution has been proposed: the Policy Update Cost (PUC) metric, a protocol for binding a biometric sample to a TLS session, and a distributed honeypattern mechanism. Practical recommendations have been formulated for information security architects to implement the defense in depth principle.

Keywords: microservice architecture, authentication, authorization, biometrics, access policies, Policy Decision Point (PDP), neural networks, facial recognition, WebRTC.

Введение

Современный ландшафт информационных систем характеризуется двумя противоположными трендами: усложнением архитектуры и стремлением к упрощению пользовательского опыта. Переход к микросервисной архитектуре, продиктованный необходимостью масштабирования и гибкости разработки, существенно расширяет поверхность атаки, делая каждый микросервис потенциальной точкой входа для злоумышленника [1, 2]. При этом классические монолитные системы авторизации становятся неприменимыми, что требует пересмотра архитектурных решений. С другой стороны, пользователь остаётся самым слабым звеном: использование простых и повторяющихся паролей, а также фишинговые атаки делают традиционную парольную аутентификацию малоэффективной. Ответом на этот вызов стало широкое внедрение биометрических технологий, позволяющих идентифицировать личность по уникальным характеристикам – статическим (рис. радужной сетчатки, папиллярные узоры) и динамическим (клавиатурный почерк) [3, 4].

Цель данной работы провести анализ существующих архитектурных патернов, биометрических методов и выявить конкретные недостатки их совместного применения. Задачи исследования:

- провести анализ архитектурных паттернов авторизации в микросервисных системах;
- выявить ключевые разрывы между этими паттернами и требованиями биометрической аутентификации;
- предложить для каждого разрыва формальное решение (метрику, протокол, архитектурный механизм);
- сформулировать проверяемые рекомендации по выбору архитектуры.

Проблема в целом заключается в отсутствии единого, системного подхода к совместному проектированию архитектуры авторизации в микросервисных системах и встраиванию в неё биометрических механизмов аутентификации [11]. На практике это приводит к одному из двух нежелательных сценариев:

Биометрия добавляется «над» устаревшей архитектурой (чаще всего монолитной или с централизованным API-шлюзом), что не устраняет внутренних проблем распределённого контроля доступа (единая точка отказа, сложность обновления политик, высокие задержки при масштабировании).

Внедряется гибкая архитектура авторизации (например, Remote PDP), но без учёта специфики биометрических данных: высокая вычислительная сложность верификации, необходимость защищать биометрические шаблоны, проблема ложных отказов/допусков, отсутствие механизмов «обманных сценариев» на уровне микросервисов.

На основе проведенного анализа выявлены следующие конкретные недостатки (табл. 1).

Таблица 1

Анализ недостатков существующих решений в области безопасности ПО и архитектуры

№	Недостаток	Где проявляется	Почему это критично
D1	Отсутствие формального сравнения паттернов авторизации по критерию «возможность динамической смены биометрических эталонов»	Во всех известных решениях сравниваются только задержки и масштабируемость	При использовании децентрализованного паттерна обновление эталонов (например, при изменении внешности) требует переразвёртыва-

			ния каждого микросервиса – биометрия становится негибкой
D2	Нет методики интеграции биометрических «обманных» сценариев (honeypot) в микросервисную архитектуру	Представлен только алгоритм для монолитного приложения	Невозможно обеспечить согласованное переключение всех микросервисов на фиктивные данные при обнаружении атаки
D3	Биометрическая верификация рассматривается как «чёрный ящик» без учёта её вычислитель-ной сложности при выборе паттерна	Реализованы методы распознавания, но без анализа влияния на задержку авторизации	Архитектор не может выбрать между Remote PDP и Embedded PDP, не зная времени проверки лица/голоса
D4	Отсутствует защита от атак повторного воспроизведения (replay) биометрических данных в веб-среде	Используется способ WebRTC, но не предлагается механизм привязки семпла к сессии	Злоумышленник может перехватить и повторно отправить ранее записанное изображение лица (видео-атака)

Архитектурные паттерны авторизации и их анализ

В терминологии NIST выделяют три основных паттерна реализации авторизации на уровне сервисов, различающихся по месту хранения и вычисления политик доступа (PDP – Policy Decision Point, PEP – Policy Enforcement Point). [6,7,8]

Децентрализованный паттерн. Логика авторизации (PDP и PEP) встроена в код каждого микросервиса.

Достоинства: минимальная задержка, отсутствие сетевых вызовов.

Недостатки: любое изменение политики требует изменения кода и переразвёртывания [5].

Централизованный с удалённым PDP (Remote PDP). Политики хранятся и вычисляются в центральном сервисе; микросервисы обращаются к нему по сети.

Достоинства: обновление политик без перезапуска, централизованное управление.

Недостатки: высокая задержка, зависимость от доступности PDP.

Централизованный со встроенным PDP (Embedded PDP). Политики централизованно хранятся, но доставляются до каждого микросервиса и кэшируются локально; PDP реализован как библиотека.

Достоинства: низкая задержка, централизованное управление.

Недостатки: требуется синхронизация политик, проблема консистентности.

Для оценки пригодности каждого паттерна к работе с биометрическими данными вводится метрика PUC (Policy Update Cost) – стоимость обновления биометрических эталонов (например, шаблона лица). PUC определяется как время (или число операций), необходимое для распространения нового эталона на все сервисы, принимающие решения. Для децентрализованного паттерна стоимость PUC высокая (требуется CI/CD и требуется перезапуск), для централизованных паттернов с удалённым или встроенным PDP – стоимость низкая (достаточно обновить центральное хранилище или канал синхронизации). В табл. 2 показано сравнение паттернов.

Таблица 2

Сравнение паттернов авторизации с учётом биометрических требований

Паттерн	Масштабируемость	Задержка (p95, мс)	Изменение политик "на лету"	Стоимость PUC (биометрические эталоны)	Рекомендуемый сценарий
Децентрализованный	Низкая	< 5	Нет	Высокая	Только статические, редко меняющиеся эталоны (отпечатки пальцев)

Централизованная (Удалённый PDP)	Высокая	50–200	Да	Низкая	Динамическая биометрия (лицо, голос) при терпимости к задержке
Централизованный (Встроенный PDP)	Высокая	5–15	Да (с оговорками)	Низкая	Динамическая биометрия + требование low latency

Биометрические методы и их влияние на архитектурный выбор

Современные системы идентификации используют различные математические модели: свёрточные нейронные сети, скрытые марковские модели, графовые представления [3, 4]. Комплексное применение нескольких методов позволяет достичь приемлемых показателей ошибок: FAR $\leq 10^{-5}$–10^{-6} при FRR $\leq 0{,}01$ [9].

Время верификации

Tver=Tcapture+Tnet+Tmatch+Tlivedet, где Tcapture – захват образца, Tnet – передача на сервер, Tmatch –сравнение с данными. Экспериментальные данные показывают, что для свёрточных сетей Tmatch составляет 300–500 мс на GPU и 50–100 мс на CPU [10], Tlivedet – проверка живости. Это различие критически влияет на выбор паттерна, особенно при жёстких ограничениях по задержке.

Однако помимо времени важны и другие свойства биометрических данных:

Динамичность эталонов – лицо и голос меняются со временем (возраст, болезни, тембр), тогда как отпечатки пальцев и рисунок радужки практически стабильны. Следовательно, частота обновления эталонов определяет стоимость PUC и склоняет выбор в сторону централизованных паттернов для динамической биометрии.

Необходимость обнаружения живости (liveness detection) – распознавание лица уязвимо к атакам по фотографии или видео. Проверка живости тре-

бует отдельного вычислительного слоя (анализ микродвижений, бликов, термограммы) и может добавлять 100–200 мс к Tver. Этот фактор должен учитываться на архитектурном уровне как самостоятельный сервис.

Мультимодальность – комбинирование нескольких биометрических модальностей повышает точность, но кратно увеличивает Tmatch и объём передаваемых данных, что может сделать Remote PDP неприемлемым при ограниченной пропускной способности.

Критерии архитектурного выбора

На основе анализа работ [11, 12, 13] выделяем три группы критериев, которые необходимо оценить до принятия решения.

Бизнес-критерии

Автономность – возможность работы без устойчивого сетевого соединения. Для удалённых объектов (промышленные контроллеры, мобильные устройства) предпочтительна децентрализованная обработка на устройстве.

Допустимый компромисс FAR/FRR – в системах физической безопасности ложный допуск (FAR) может быть катастрофическим, поэтому пороги сдвигают в сторону снижения FAR, что увеличивает Tmatch (более строгие модели) и может потребовать более мощного железа.

Технические критерии

Вычислительные ресурсы – доступность GPU на серверной стороне или на устройстве. Если на устройстве ограниченные ресурсы, то Tmatch на CPU может превысить допустимую задержку, и тогда необходимо выносить сравнение в централизованный PDP.

Пропускная способность сети – большие биометрические семплы могут сделать Remote PDP неэффективным из-за времени передачи Tnet.

Необходимость аудита – централизованные паттерны упрощают сбор журналов всех сравнений, что важно для соответствия регуляторам (GDPR, 152-ФЗ).

Критерии безопасности и приватности

Защита биометрических шаблонов – при централизованном хранении все эталоны находятся в одном месте, что повышает риск компрометации. Децентрализованное хранение (на устройстве) снижает этот риск, но усложняет синхронизацию.

Защита от атак повторного воспроизведения – требует дополнительного протокола привязки к сессии, что реализуемо как в Remote, так и в Embedded PDP, но не в децентрализованном без централизованного управления.

Стандартизация – использование спецификаций (например, NIST SP 500-288 для биометрических веб-сервисов) облегчает интеграцию, но может накладывать ограничения на выбор паттерна.

Исходя из выше приведенных критериев можно составить алгоритм выбора архитектурного паттерна.

Шаг 1. Определение профиля биометрических данных.

Классифицируем биометрию как статичестую (отпечатки пальцев, радужка) или динамическую (лицо, голос, походка). Для статической и редко обновляемой биометрии рассматриваем децентрализованный паттерн как базовый вариант.

Шаг 2. Оценка временных ограничений.

Зададим максимально допустимую задержку Lmax. Оценим Tver для выбранного метода на целевом оборудовании.

Если Tver>Lmax – необходимо аппаратное ускорение или вынос сравнения на более мощный сервер (Remote PDP).

Если Tver≤Lmax – проверяем возможность локального выполнения.

Шаг 3. Оценка стоимости обновления политик (PUC).

Рассчитываем PUC как время на распространение нового биометрического эталона по всем микросервисам.

Для децентрализованного паттерна PUC высока (требуется CI/CD и перезапуск). Если частота обновления > 1 раза в месяц – децентрализованный паттерн исключается.

Для Remote и Embedded PDP – PUC низкая (достаточно обновить центральное хранилище).

Шаг 4. Учёт дополнительных нефункциональных требований.

Проверим:

Необходимость работы в офлайн-режиме → выбираем Embedded PDP или децентрализованный с локальным кэшем эталонов.

Необходимость централизованного аудита → Remote или Embedded PDP (логирование на уровне PDP).

Требования к приватности (хранение шаблонов только на устройстве) → децентрализованный или гибридный (сравнение на устройстве, но политики централизованы).

Шаг 5. Проверка защищённости от атак повторного воспроизведения.

Если система работает в веб-среде, обязательно внедренит протокола с nonce. Это требование не зависит от паттерна, но при децентрализованном

паттерне синхронизация nonce между сервисами становится нетривиальной – это может склонить выбор в сторону централизованного PDP.

Шаг 6. Итоговое решение.

На основе взвешенных критериев выбирается один из трёх паттернов. В табл. 2 (см. выше) приведены базовые рекомендации. Для сложных систем возможна гибридная архитектура: например, локальное извлечение признаков (уменьшение Tnet) и централизованное сравнение с эталонами.

Архитектурный выбор при интеграции биометрии не является одномерным. Он требует системного учёта временных характеристик (Tver), стоимости обновления политик (PUC), бизнес-требований к автономности, безопасности и приватности. Предложенный пошаговый алгоритм позволяет формализовать этот процесс и избежать типичных ошибок, когда биометрия добавляется «поверх» архитектуры без анализа её специфики [11].

Рекомендации по выбору архитектуры

На основе проведённого анализа и предложенных решений сформулированы следующие рекомендации в табл. 3.

Таблица 3

Предложенные решения

Требование	Рекомендуемый паттерн	Обоснование
Динамическая биометрия (лицо, голос) + частота обновления эталонов > 1 раза в месяц	Remote или Embedded PDP	Низкая стоимость PUC (устранение D1)
Динамическая биометрия + low latency (< 50 мс)	Embedded PDP	T_ver мала + нет сетевых задержек (D3)
Использование веб-интерфейса с биометрией	Добавить протокол с nonce	Устранение D4
Необходимость активной защиты от внутреннего нарушителя	Внедрить распределённый honeypot pattern	Устранение D2
Статическая биометрия (отпечатки пальцев), редкое обновление	Децентрализованный паттерн	Низкая задержка, нет сетевых вызовов

Одной из моделей управления доступом является модель на основе атрибутов (Attribute-Based Access Control, ABAC) [13] представляет собой гибкий и масштабируемый подход к разграничению прав доступа, в котором решения о предоставлении или запрете операций принимаются на основании атрибутов субъекта, объекта, действия и контекста окружающей среды. В отличие от дискреционных (DAC) и мандатных (MAC) моделей, где права доступа жёстко привязаны к субъектам и объектам, ABAC обеспечивает динамическое формирование политик безопасности, что позволяет адаптировать систему к изменяющимся условиям функционирования информационной инфраструктуры.

Архитектура системы ABAC строится на взаимодействии следующих фундаментальных компонентов:

Субъекты – сущности, инициирующие запросы на доступ к ресурсам. К субъектам относятся пользователи, процессы, приложения, сервисы и автоматизированные агенты. Каждый субъект характеризуется набором атрибутов, включающих идентификационные данные, уровень допуска, временные параметры аутентификации и динамические характеристики (например, текущее местоположение или уровень доверия).

Объекты – ресурсы, к которым осуществляется доступ. Объектами могут выступать файлы, базы данных, сетевые сервисы, физические устройства и логические сущности. Атрибуты объектов включают классификационную метку, категорию конфиденциальности, владельца ресурса, временные ограничения доступа и структурные характеристики.

Операции – действия, которые субъект намеревается выполнить над объектом. Типовой набор операций включает чтение, запись, выполнение, удаление, создание и администрирование.

Атрибуты окружающей среды – контекстные параметры, не относящиеся непосредственно к субъекту или объекту, но существенно влияющие на принятие решения о доступе. К ним относятся текущее время и дата, географическое положение запроса, тип используемого устройства, уровень защищённости канала связи, результаты многофакторной аутентификации и показатели аномального поведения.

Политики безопасности – формализованные правила, определяющие условия предоставления доступа. Политики представляют собой логические

выражения, связывающие атрибуты субъекта, объекта, операции и окружающей среды. Совокупность политик формирует политику домена, в рамках которой осуществляется управление авторизацией.

Безопасность функционирования системы управления доступом на основе атрибутов оценивается по совокупности критериев, обеспечивающих защиту информационных ресурсов от несанкционированного доступа и гарантирующих корректность авторизационных решений.

Вывод

В работе выполнен комплексный анализ архитектурных паттернов авторизации и биометрических методов идентификации.

Целью следующих исследований является разработка мультимодальной модели аутентификации привилегированных пользователей на основе биометрических сигналов.

Литература

1. Барабанов, А. Аутентификация и авторизация в микросервисных приложениях: обзор архитектурных подходов / А. Барабанов, Д. Макрушин. // Вопросы кибербезопасности. – 2020. – № 4 (38). – С. 32–43.

2. Lu D., Huang D., Walenstein A., Medhi D. A Secure Microservice Framework for IoT // IEEE Symposium on Service-Oriented System Engineering (SOSE). – 2017. – P. 1–10.

3. Исмагилова А.С., Лушников Н.Д. Комплексная биометрическая аутентификация пользователей информационной системы с применением нейронных сетей // Инженерный вестник Дона. – 2024. – № 1. – URL: http://www.ivdon.ru/ru/magazine/archive/n1y2024/8961

4. Ложников П.С., Сулавко А.Е. Алгоритм биометрической идентификации личности с использованием альтернативных сценариев авторизации // Омский государственный технический университет, ООО НТЦ «КАСИБ». 2013 – С. 79–82.

5. Li X., Chen Y., Lin Z. Towards Automated Inter-Service Authorization for Microservice Applications // ACM SIGCOMM Conference Posters and Demos. – 2019. – P. 3–5.

6. Rose, S. Zero Trust Architecture: NIST Special Publication 800-207 / S. Rose, O. Borchert, S. Mitchell, S. Connelly; National Institute of Standards and Technology. – Gaithersburg: NIST, 2020. – 59 p. – URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf (дата обращения: 07.10.2026). – Режим доступа: свободный. – Текст: электронный

7. Yarygina T., Bagge A.H. Overcoming Security Challenges in Microservice Architectures // IEEE Symposium on SOSE. – 2018. – P. 11–20.

8. Siriwardena P., Dias N. Microservices Security in Action // Manning, 2020. – 528 p

9. Grassi P. A., Garcia M. E., Fenton J. L. Digital Identity Guidelines / National Institute of Standards and Technology. – June 2017 (includes updates as of 03-02-2020). – URL: https://doi.org/10.6028/NIST.SP.800-63-3 – DOI:10.6028/NIST.SP.800-63-3

10. Горбунов В.Л., Йе Вин Зо, Жданова И.В. – Обработка данных видеопотока в системах с контролируемым доступом ограниченного круга лиц // Вестник РГРТУ – 2025 – С. 143 – 155

11. Momin M. A., Hussain M. M. M., Islam M. E. An In-Depth Review of Authentication Mechanisms in Microservice Architectures // Daffodil International University. – 2025. – URL: http://dspace.daffodilvarsity. edu.bd:8080/handle/123456789/15922

12. Poorebrahim Gilkalaye B., Mukherjee S., Derakhshani R. A Secure and Private Ensemble Matcher Using Multi-Vault Obfuscated Templates // arXiv preprint arXiv:2404.05205. – 2024. – URL: https://ar5iv.labs.arxiv. org/html/2404.05205

13. Ковтун Д.П., Лапонина О.Р. Использование управления доступом на основе атрибутов и mTLS в микросервисной архитектуре // International Journal of Open Information Technologies ISSN: 2307-8162 vol. 13, no. 6, 2025 С. 75–85.

References

1. Barabanov, A., & Makrushin, D. (2020). Authentication and authorization in microservice applications: An overview of architectural approaches. Voprosy kiberbezopasnosti [Cybersecurity Issues], (4), 32–43.

2. Lu D., Huang D., Walenstein A., Medhi D. A Secure Microservice Framework for IoT // IEEE Symposium on Service-Oriented System Engineering (SOSE). – 2017. – P. 1–10.

3. Ismagilova A.S., Lushnikov N.D. Comprehensive biometric authentication of users of an information system using neural networks // Engineering Bulletin of the Don. – 2024. – No. 1. – URL: http://www.ivdon.ru/ru/magazine/archive/n1y2024/8961

4. Lozhnikov P.S., Sulavko A.E. Algorithm for Biometric Identity Verification Using Alternative Authorization Scenarios // Omsk State Technical University, LLC STC “KASIB”. 2013 – P. 79–82.

5. Li X., Chen Y., Lin Z. Towards Automated Inter-Service Authorization for Microservice Applications // ACM SIGCOMM Conference Posters and Demos. – 2019. – P. 3–5.

6. Rose, S. Zero Trust Architecture: NIST Special Publication 800-207 / S. Rose, O. Borchert, S. Mitchell, S. Connelly; National Institute of Standards and Technology. – Gaithersburg: NIST, 2020. – 59 p. – URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf (дата обращения: 07.10.2026). – Режим доступа: свободный. – Текст: электронный

7. Yarygina T., Bagge A.H. Overcoming Security Challenges in Microservice Architectures // IEEE Symposium on SOSE. – 2018. – P. 11–20.

8. Siriwardena P., Dias N. Microservices Security in Action // Manning, 2020. – 528 p.

9. Grassi P. A., Garcia M. E., Fenton J. L. Digital Identity Guidelines / National Institute of Standards and Technology. – June 2017 (includes updates as of 03-02-2020). – URL: https://doi.org/10.6028/NIST.SP.800-63-3 – DOI:10.6028/NIST.SP.800-63-3

10. Gorbunov V.L., Ye Winzo, Zhdanova I.V. – Processing video stream data in systems with controlled access of a limited number of persons // Bulletin of the Russian State Technical University – 2025 – P. 143-155

11. Momin M. A., Hussain M. M. M., Islam M. E. An In-Depth Review of Authentication Mechanisms in Microservice Architectures // Daffodil International University. – 2025. – URL: http://dspace.daffodilvarsity. edu.bd:8080/handle/123456789/15922

12. Poorebrahim Gilkalaye B., Mukherjee S., Derakhshani R. A Secure and Private Ensemble Matcher Using Multi-Vault Obfuscated Templates // arXiv preprint arXiv:2404.05205. – 2024. – URL: https://arxiv.labs.arxiv.org/html/2404.05205

13. Kovtun D.P., Laponina O.R. Using attribute-based access control and mTLS in a microservice architecture // International Journal of Open Information Technologies, ISSN: 2307-8162, vol. 13, no. 6, 2025, P. 75–85.

ЮЖАКОВ Никита Александрович, аспирант, Пермский национальный исследовательский политехнический университет. 614990, г. Пермь, Комсомольский проспект, 29. E-mail: yuz.nikita@gmail.com

ЮЖАКОВ Александр Анатольевич, доктор технических наук, профессор, заведующий кафедры «Автоматика и телемеханика». Пермский национальный исследовательский политехнический университет. 614990, г. Пермь, Комсомольский проспект, 29. E-mail: uz@at.pstu.ru

YUZHAKOV Nikita Aleksandrovich, Postgraduate Student, Perm National Research Polytechnic University. 614990, Perm, Komsomolsky Prospekt, 29. E-mail: yuz.nikita@gmail.com

YUZHAKOV Alexander Anatolyevich, Doctor of Technical Sciences, Professor, Head of the Department of Automation and Telemechanics. Perm National Research Polytechnic University. 614990, Perm, Komsomolsky Prospekt, 29. E-mail: uz@at.pstu.ru