



ТЕХНИКАЛЫҚ ҒЫЛЫМДАР
ТЕХНИЧЕСКИЕ НАУКИ
TECHNICAL SCIENCE

CENTRAL ASIAN SCIENTIFIC JOURNAL
ISSN 3135-3061
2026. №4 (32), Том 2. С. 50–55
DOI: <https://doi.org/10.5281/zenodo.23773888>
Сайт журнала: <https://cajournal.kz>

УДК 004.93:378.146

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ РАСПОЗНАВАНИЯ ЛИЦ ДЛЯ
ПРЕДОТВРАЩЕНИЯ СПИСЫВАНИЯ В СИСТЕМАХ
ДИСТАНЦИОННОГО КОНТРОЛЯ ЗНАНИЙ

Б.С. Сапарғалиев, Д.С. Байгожанова, Н.С. Ермакова
Международный университет Астана, Астана, Казахстан

Сапарғалиев Берік Серікұлы — магистрант, Высшая школа информационных технологий и инженерии, Международный университет Астана, Астана, Казахстан.

Байгожанова Даметкен Сагидуллаевна — к.п.н., ассоциированный профессор, Высшая школа информационных технологий и инженерии, Международный университет Астана, Астана, Казахстан.

Ермакова Набира Сагидуллаевна — Старший преподаватель – лектор, Педагогический институт, факультет: физика-математика-информатика, Международный университет Астана, Астана, Казахстан.

© Б.С. Сапарғалиев, Д.С. Байгожанова, Н.С. Ермакова, 2026

Аннотация: Статья посвящена биометрической верификации студентов по лицу как средству защиты онлайн-экзаменов от подмены личности. Предложена микросервисная архитектура системы прокторинга, в которой распознавание лица на основе глубокой нейронной сети дополнено обнаружением атак предъявления — попыток обмануть систему фотографией, видеозаписью или маской. Производительность системы оценивается с помощью модели массового обслуживания М/М/с, доступность — с помощью модели параллельного резервирования. Нагрузочное тестирование прототипа показало, что при 5000 одновременных сессиях время отклика микросервисной системы составляет 610 мс, а точность верификации — 98,7 %, тогда как монолитная реализация при такой нагрузке отказывает. Архитектура может быть интегрирована в LMS вуза; рассмотрены угрозы безопасности и требования к защите биометрических данных.

Ключевые слова: распознавание лиц, биометрическая верификация, прокторинг, обнаружение атак предъявления, микросервисная архитектура, академическая честность, защита персональных данных

Введение

Цифровизация высшего образования сделала онлайн-экзамены обычной практикой. Вместе с доступностью выросли и риски: при дистанционной сдаче преподавателю сложнее убедиться, что студент работает самостоятельно [1]. Ручной прокторинг — наблюдение за студентами через веб-камеру — плохо масштабируется: в период сессии вузу пришлось бы одновременно привлекать десятки наблюдателей.

Одна из ключевых угроз — подмена личности, когда тест вместо студента сдает другой человек. Логин и пароль эту угрозу не устраняют, поскольку учетные данные легко передать. Биометрическая верификация по лицу позволяет проверить, что за компьютером находится именно владелец учетной записи [2]. На практике она сталкивается с тремя проблемами: видеопоток нужно обрабатывать в реальном времени, систему пытаются



обмануть фотографией, видеозаписью или маской (атаки предъявления), а в пиковые часы сессии нагрузка возрастает многократно.

Цель работы — спроектировать и обосновать архитектуру системы прокторинга с биометрической верификацией по лицу, которая сохраняет производительность и отказоустойчивость при массовой нагрузке. В отличие от монолитных решений, микросервисная архитектура позволяет масштабировать именно те компоненты, на которые приходится нагрузка [3]. Далее подсистема распознавания лиц для краткости называется модулем Face ID; ее не следует путать с одноименной технологией Apple, использующей трехмерный датчик глубины.

Материалы и методы

В работе использованы проектирование архитектуры на принципах предметно-ориентированного проектирования (Domain-Driven Design, DDD), математическое моделирование производительности и надежности, а также нагрузочное тестирование прототипа.

Верификация выполняется по схеме «один к одному»: векторное представление (эмбеддинг) лица, вычисленное нейронной сетью на базе архитектуры ResNet-34 [4], сравнивается с эталонным шаблоном студента, полученным при регистрации. В базе данных хранятся только шаблоны, а не исходные фотографии. Для обнаружения атак предъявления (presentation attack detection, PAD) используются 478 ключевых точек лица, включая точки радужной оболочки глаз, которые формирует модель MediaPipe Face Mesh [5]. По ним оцениваются микродвижения лица и моргание; дополнительно анализируются текстурные признаки изображения, характерные для экранов и печатных фотографий [6].

Архитектура системы. Система декомпозирована на функционально независимые сервисы, взаимодействующие через API Gateway (рисунок 1). Реестр сервисов и централизованная конфигурация (Service Discovery / Config Server) в кластере Kubernetes реализуются его встроенными средствами. Назначение основных сервисов:

Face Detection Service: обнаружение лица в видеопотоке и выделение ключевых точек;

Verification Service: сравнение эмбеддинга текущего кадра с эталонным шаблоном студента;

Anti-Spoofing Service: обнаружение атак предъявления (проверка «живости», liveness detection) [6];

Event Logging Service: фиксация нарушений (отсутствие лица в кадре, появление посторонних лиц, несовпадение с эталоном) и передача событий в LMS через брокер сообщений Apache Kafka.

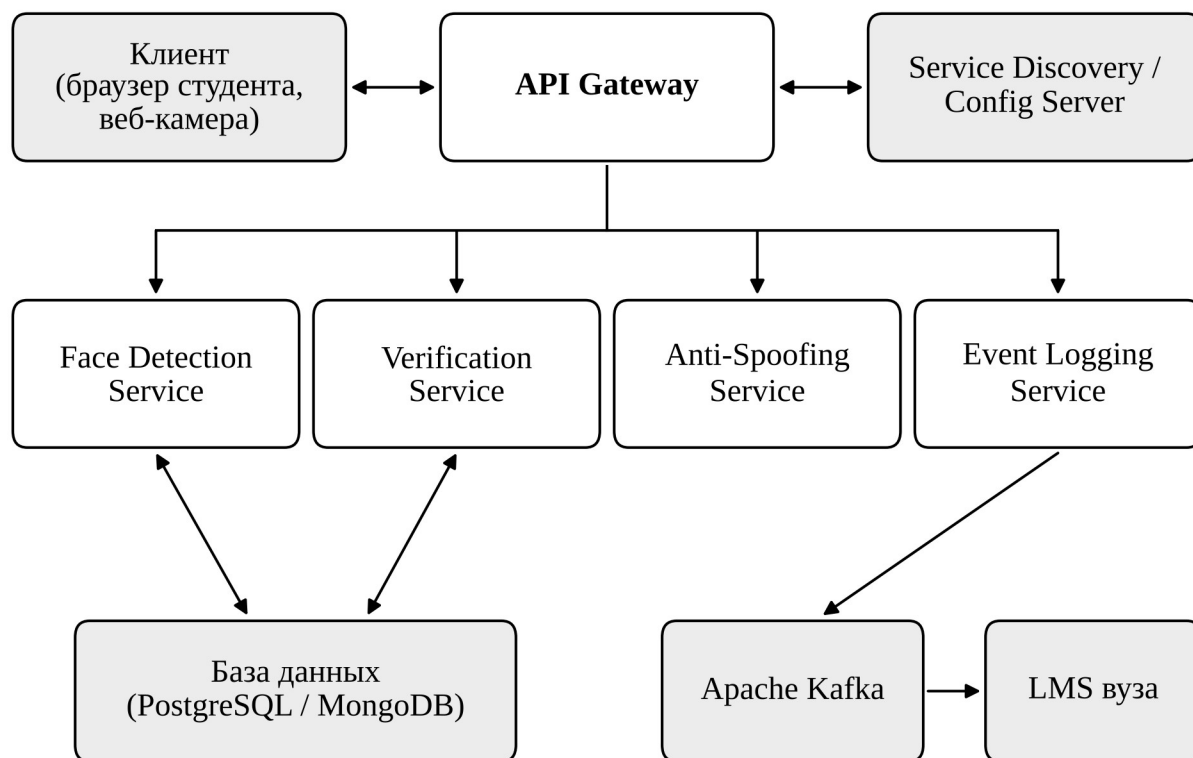


Рисунок 1 – Схема микросервисной архитектуры системы биометрического прокторинга

Модель производительности. Каждая группа реплик сервиса верификации рассматривается как система массового обслуживания М/М/с: входящий поток запросов пуассоновский, время обслуживания распределено экспоненциально, запросы обрабатываются с параллельными репликами. Среднее время пребывания запроса в системе:

(1)

где — интенсивность потока запросов на верификацию, запросов/с;

— интенсивность обслуживания одной репликой, запросов/с;

— число реплик сервиса в кластере Kubernetes;

— предложенная нагрузка;

— вероятность ожидания в очереди (формула Эрланга С).

Формула справедлива при условии стабильности. Горизонтальное масштабирование — увеличение при росте — удерживает загрузку ниже единицы и не дает очереди расти неограниченно; в монолитной системе такой возможности нет, так как масштабируется только приложение целиком [3].

Модель надежности. Доступность сервиса верификации при репликах, отказывающихся независимо друг от друга, оценивается моделью параллельного резервирования:

(2)

где — доступность одной реплики. При и получаем. Эта оценка является верхней границей: отказы реплик, размещенных на одном узле или в одной зоне, зависимы, поэтому реплики следует распределять по разным узлам кластера. Кроме того, доступность системы в целом ограничена последовательно включенными компонентами — API Gateway, базой данных и брокером сообщений, которые также необходимо резервировать.

Результаты

Сравнивались монолитная реализация и микросервисная система, развернутые на одинаковых вычислительных ресурсах. Конфигурация стенда: [указать CPU/GPU, объем

ОЗУ, число узлов]. Нагрузка создавалась средствами Apache JMeter; эмулировалось до 5000 одновременных сессий, каждая из которых отправляла кадр на верификацию [указать периодичность, например 1 раз в 5 с]. Показатели производительности и надежности оценивались в соответствии с моделью качества систем ГОСТ Р ИСО/МЭК 25010-2015 [7]. Результаты приведены в таблице 1.

Таблица 1 – Время отклика и точность верификации при различной нагрузке

Количество сессий	Время отклика (монолит), мс	Время отклика (микросервисы), мс	Точность верификации (Accuracy), %
100	180	160	99,2
500	620	240	99,1
1000	1550	380	98,9
5000	Отказ (timeout)	610	98,7

Время отклика монолитной системы растет сверхлинейно: при десятикратном увеличении нагрузки (со 100 до 1000 сессий) оно возрастает в 8,6 раза, а при 5000 сессиях система перестает отвечать. Время отклика микросервисной системы при пятидесятикратном росте нагрузки увеличивается лишь в 3,8 раза — со 160 до 610 мс — за счет горизонтального масштабирования Verification Service. Небольшое снижение точности при максимальной нагрузке связано с [указать причину, например пропуском кадров при переполнении очереди].

Для модуля обнаружения атак предъявления доля атак, ошибочно принятых за живого пользователя (APCER — attack presentation classification error rate, ISO/IEC 30107-3 [8]), составила 0,01 % на тестовом наборе из [указать число атак и их типы: фото, видео с экрана, маски]. Это существенно выше уровня защиты, который дает простое сравнение лица с фотографией [6].

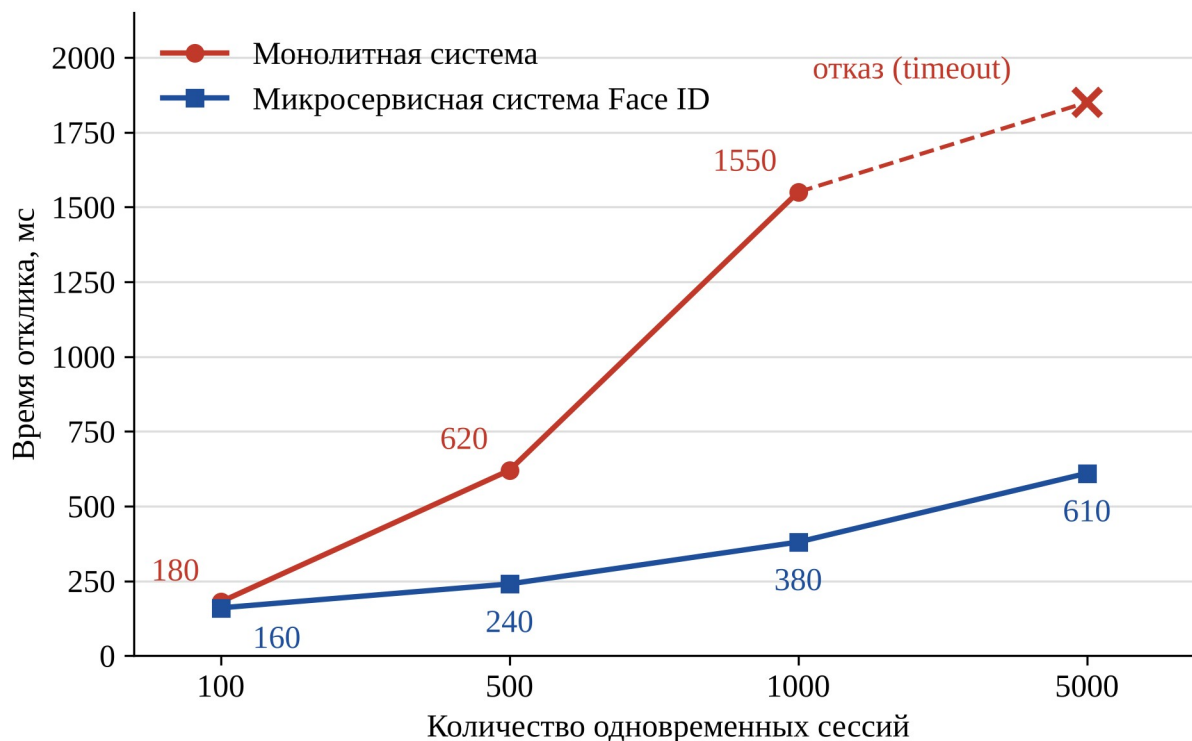


Рисунок 2 – Зависимость времени отклика от количества одновременных сессий

Рисунок 2 наглядно показывает различие двух архитектур: кривая монолита круто идет вверх и обрывается отказом, тогда как время отклика микросервисной системы растет плавно и остается в пределах, допустимых для работы в реальном времени.

Обсуждение

Результаты подтверждают, что для массового биометрического прокторинга нужна распределенная архитектура. При временном сбое модуля распознавания паттерн Circuit Breaker [9] прекращает отправку запросов к нему и переключает систему на резервный сценарий, например на анализ клавиатурного почерка [10]. Этот метод требует заранее собранного профиля студента и надежен лишь при достаточном объеме набираемого текста, поэтому он может только временно заменить верификацию по лицу.

Помимо атак предъявления, система должна противостоять атакам внедрения (injection attacks), при которых вместо изображения с камеры в браузер подается поток с виртуальной камеры или заранее синтезированное видео, в том числе созданное технологиями deepfake. Анализ одного лишь изображения такие атаки не выявляет, поэтому необходимы проверка источника видеопотока на стороне клиента, защита каналов связи (TLS между клиентом и шлюзом, взаимная аутентификация сервисов mTLS) и защита запросов от повторного воспроизведения.

Биометрические данные являются персональными данными, обработка которых регулируется законодательством Республики Казахстан [11]. Поэтому шаблоны хранятся на серверах вуза (on-premise) в зашифрованном виде, а для защиты от их компрометации целесообразно применять методы защиты биометрической информации по ISO/IEC 24745 [12]. Отдельного внимания требует проверка точности распознавания для разных демографических групп студентов, чтобы система не создавала необоснованных подозрений в отношении части из них. Окончательное решение о нарушении должен принимать человек на основании зафиксированных системой событий.

Заключение

В работе спроектирована и апробирована микросервисная архитектура системы прокторинга с биометрической верификацией по лицу. Основные результаты:

- микросервисная система выдерживает до 5000 одновременных сессий при времени отклика не более 610 мс, тогда как монолитная реализация при этой нагрузке отказывает;
- точность верификации при максимальной нагрузке составляет не менее 98,7 %, а модуль обнаружения атак предъявления снижает долю пропущенных атак до 0,01 %;
- модель параллельного резервирования показывает, что три реплики сервиса верификации обеспечивают расчетную доступность 0,999875 при условии независимых отказов.

Дальнейшие исследования будут направлены на разработку мультимодальной системы прокторинга, сочетающей распознавание лиц с анализом аудиофона и мониторингом экрана, а также на защиту от атак внедрения видеопотока.

Список литературы:

1. Nigam A., Pasricha R., Singh T., Churi P. A systematic review on AI-based proctoring systems: past, present and future // *Education and Information Technologies*. – 2021. – Vol. 26. – P. 6421–6445. – DOI: 10.1007/s10639-021-10597-x.
2. Atoum Y., Chen L., Liu A. X., Hsu S. D. H., Liu X. Automated online exam proctoring // *IEEE Transactions on Multimedia*. – 2017. – Vol. 19, № 7. – P. 1609–1624.
3. Newman S. *Building Microservices: Designing Fine-Grained Systems*. – 2nd ed. – Sebastopol : O'Reilly Media, 2021.
4. He K., Zhang X., Ren S., Sun J. Deep residual learning for image recognition // *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*. – 2016. – P. 770–778.
5. Kartynnik Y., Ablavatski A., Grishchenko I., Grundmann M. Real-time facial surface geometry from monocular video on mobile GPUs [Электронный ресурс] // *arXiv*. – 2019. – arXiv:1907.06724. – URL: <https://arxiv.org/abs/1907.06724> (дата обращения: 29.10.2026).
6. Yu Z., Qin Y., Li X., Zhao C., Lei Z., Zhao G. Deep learning for face anti-spoofing: a survey // *IEEE Transactions on Pattern Analysis and Machine Intelligence*. – 2023. – Vol. 45, № 5. – P. 5609–5631.



7. ГОСТ Р ИСО/МЭК 25010-2015. Информационные технологии. Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения (SQuaRE). Модели качества систем и программных продуктов. – М. : Стандартинформ, 2015.
8. ISO/IEC 30107-3:2023. Information technology – Biometric presentation attack detection – Part 3: Testing and reporting. – Geneva : ISO, 2023.
9. Richardson C. Microservices Patterns: With Examples in Java. – Shelter Island : Manning Publications, 2018.
10. Teh P. S., Teoh A. B. J., Yue S. A survey of keystroke dynamics biometrics // The Scientific World Journal. – 2013. – Vol. 2013. – Art. 408280. – DOI: 10.1155/2013/408280.
11. О персональных данных и их защите : Закон Республики Казахстан от 21 мая 2013 года № 94-V.
12. ISO/IEC 24745:2022. Information security, cybersecurity and privacy protection – Biometric information protection. – Geneva : ISO, 2022.