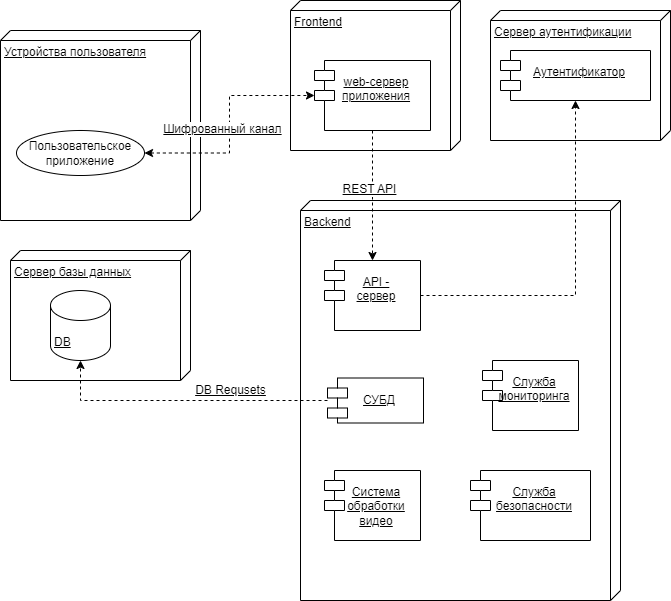
**Тема**: обоснование выбора информационных технологий для реализации программного продукта

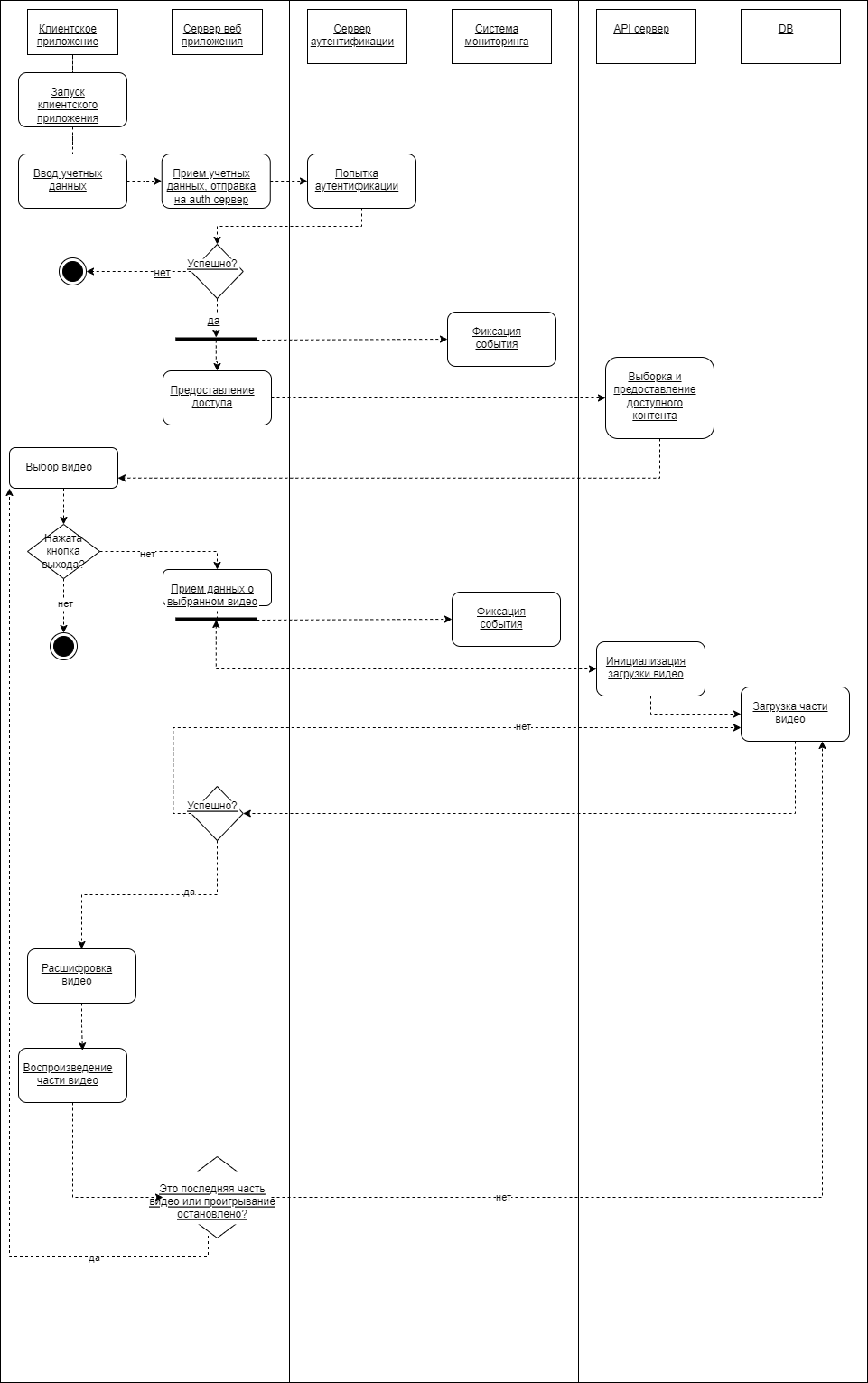
**Цель работы**: На основе анализа требований обосновать и выбрать информационной технологии для реализации.

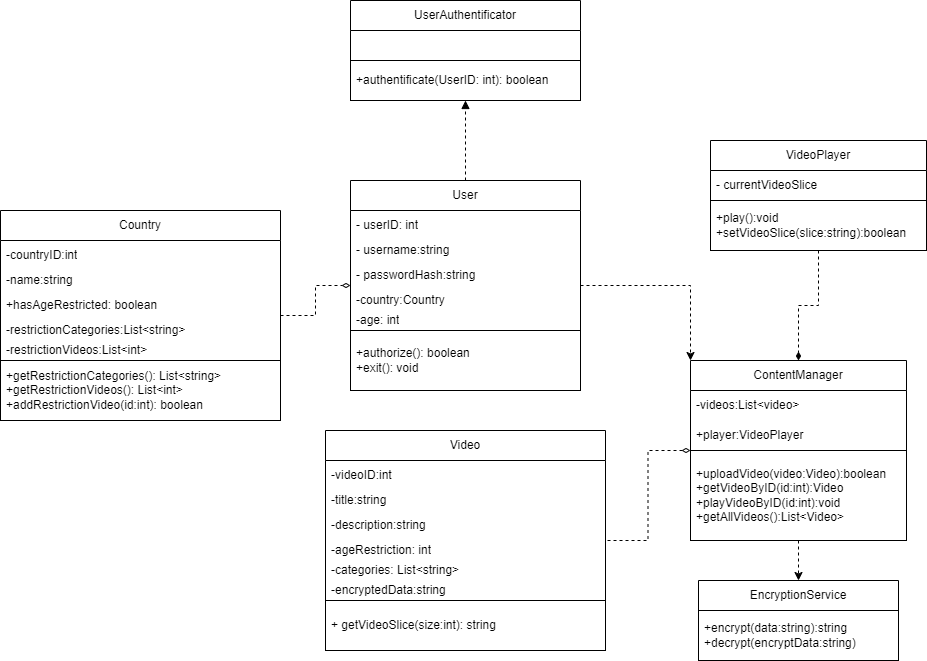
**Ход работы:**



Объяснение узлов

* Пользовательские устройства представляют собой конечные точки, с которых пользователи взаимодействуют с системой через веб-приложение.
* Сервер веб-приложения обрабатывает запросы от пользователей и передает их на API-сервер.
* API-сервер взаимодействует с различными сервисами для выполнения запросов: с сервером аутентификации, хранилищем данных и сервером базы данных.
* Сервер базы данных отвечает за хранение всех данных, связанных с пользователями и видео.
* Система обработки видео обеспечивает нужные функции обработки и конвертации видео.
* Система мониторинга следит за здоровьем и производительностью всей инфраструктуры.





1. Язык программирования и фреймворки

* Backend: Kotlin или Java. Выбор между ними зависит от команды, но Kotlin имеет более лаконичный синтаксис и поддержку корутин, что может упростить работу с асинхронными запросами.
* Client app: С# на платформе .NET для разработки приложения клиента. Эта платформа имеет возможности по созданию удобных и расширяемых приложений.

2. СУБД

* PostgreSQL или MySQL: Обе являются мощными реляционными базами данных, поддерживающими транзакции и масштабируемость. PostgreSQL может предложить дополнительные расширения для обработки сложных запросов и управления данными.

3. Хранение видеофайлов

* Облачные хранилища: Amazon S3 или Google Cloud Storage для хранения видеофайлов. Они предлагают высокую доступность, масштабируемость и встроенные функции безопасности.
* CDN: Использование сети доставки контента, такой как Cloudflare или AWS CloudFront, для снижения задержек и увеличения скорости доступа к видеофайлам.

4. Система безопасности

* Шифрование: Использование протоколов шифрования (например, AES-256) для хранения видеофайлов и других чувствительных данных. Это поможет соблюсти требования безопасности и защиты данных.

5. Аутентификация и авторизация

* JWT (JSON Web Tokens) для безопасного управления сессиями пользователей. Это позволит предоставлять доступ к контенту только авторизованным пользователям.
* Role-based Access Control (RBAC) для управления разрешениями, позволяя ограничивать доступ к контенту в зависимости от страны и других факторов.

6. Логирование и мониторинг

* Использование инструментов, таких как ELK Stack (Elasticsearch, Logstash, Kibana) для логирования и мониторинга системы, что поможет отслеживать потенциальные проблемы и соответствовать требованиям безопасности.

8. Соблюдение юридических требований

* Внедрение механизма для управления возрастными ограничениями в зависимости от региона. Это может быть реализовано через настройки в профиле пользователя и проверки в базе данных.
* Внедрение механизма блокировки контента по определенным тематикам для разных стран.

Обоснование выбора технологий:

* Гибкость: Использование облачных решений позволяет быстро масштабировать и адаптировать систему под изменяющиеся требования.
* Безопасность: Выбор технологий, поддерживающих шифрование и безопасную передачу данных, помогает соответствовать требованиям законодательства, обеспечивая защиту пользовательских данных.
* Совместимость: Выбор языков и фреймворков, которые хорошо работают друг с другом и имеют большое сообщество для получения поддержки.
* Удобство использования: Интуитивно понятные интерфейсы и механизмы аутентификации упрощают взаимодействие пользователей с системой.