**Защита каналов (end-to-end):**

* **Что:** сегментация и минимизация открытых путей; TLS/mTLS на API и сервис-к-сервис; VPN/IPsec для внешних связей; WAF/Rate-Limit; контроль протоколов/портов для потоков данных (API, шина сообщений, батч, видео).
* **Как в нашей архитектуре:** единые политики для всех межсистемных каналов (OT↔IT, внешние, DR-репликации, почта/вложения, видео-ингест); сервис-мэш или эквивалент для mTLS и authZ между микросервисами; ACL на шине сообщений.
* **Преимущества:** меньше риск MITM и подмены трафика; сдерживание lateral movement; безопасный обмен с партнёрами; предсказуемость и управляемость сетевых путей.

**Шифрование (in-transit & at-rest):**

* **Что:** TLS 1.2+ для всех транспортов; TDE/шифрование томов/объектов; KMS/Vault/PKI для ключей и ротаций; иммутабельные бэкапы (WORM).
* **Как:** шифрование по умолчанию для Lake/DWH/БД/бэкапов; сквозные сертификаты для API/шины/ETL/DR; короткоживущие токены и ротации.
* **Преимущества:** защита конфиденциальности и целостности данных/моделей; юридическая стойкость доказательств; безопасное восстановление при DR.

**Логирование (сквозная наблюдаемость):**

* **Что:** централизованный сбор структурированных логов и метрик со всех слоёв (приложения, шина, данные, инференс, почта, инфраструктура, доступы), корреляция по trace-ID.
* **Как:** единый лог-пайплайн → SIEM; синхронизация времени; маскирование чувствительных полей; WORM/подписи для критичных журналов.
* **Преимущества:** быстрее MTTD/MTTR; качественная форензика; меньше ложных срабатываний; прозрачность работы моделей и данных.

**Аудит (кто/что/когда/почему):**

* **Что:** аудит доступов (IAM/MFA/PAM), изменений (API-контракты, политика шины, конфиги, инфраструктура как код), и MLOps-артефактов (lineage датасетов/фич, подпись и версии моделей, кто промоутил/откатил).
* **Как:** 4-глазый принцип для критичных изменений; регулярные access-review; неизменяемые реестры изменений.
* **Преимущества:** доказательная база для разборов и проверок; предотвращение несанкционированных изменений; управляемость жизненного цикла моделей и данных.

Соответствие стандартам

**Что делаем:**

* **SoA/каталог контролей:** мэппинг требований на практики защиты каналов, шифрование, логирование/аудит, резервирование/DR.
* **Secure SDLC/Data/ML:** политики для датасетов, артефактов и моделей (подпись, проверка целостности, контроль доступа, дрифт-мониторинг).
* **Операционка:** регулярные тесты DR (RPO/RTO), уязвимости/патчи, обучение персонала.  
  **Преимущества:** сниженные комплаенс-риски и издержки на аудиты; доверие партнёров; ускоренное подключение новых сервисов/поставщиков без просадки по ИБ; воспроизводимость и проверяемость решений на данных и ML.

Предлагаемые KPI (для всех пунктов)

* % зашифрованного трафика и хранилищ; время ротации ключей/сертификатов.
* Покрытие логированием критичных узлов; доля событий с trace-ID; MTTD/MTTR.
* Кол-во несанкционированных изменений, предотвращённых аудитом/SoD.
* Доля реализованных контролей из SoA; закрытые замечания по аудитам; успешные DR-тесты по RPO/RTO.
* **SoA/каталог контролей:** мэппинг требований на практики защиты каналов, шифрование, логирование/аудит, резервирование/DR.
* **Secure SDLC/Data/ML:** политики для датасетов, артефактов и моделей (подпись, проверка целостности, контроль доступа, дрифт-мониторинг).
* **Операционка:** регулярные тесты DR (RPO/RTO), уязвимости/патчи, обучение персонала.  
  **Преимущества:** сниженные комплаенс-риски и издержки на аудиты; доверие партнёров; ускоренное подключение новых сервисов/поставщиков без просадки по ИБ; воспроизводимость и проверяемость решений на данных и ML.

Предлагаемые KPI (для всех пунктов)

* % зашифрованного трафика и хранилищ; время ротации ключей/сертификатов.
* Покрытие логированием критичных узлов; доля событий с trace-ID; MTTD/MTTR.
* Кол-во несанкционированных изменений, предотвращённых аудитом/SoD.
* Доля реализованных контролей из SoA; закрытые замечания по аудитам; успешные DR-тесты по RPO/RTO.

Также требуется учесть обеспечение целостности (силами внутренних возможностей базы данных предусмотреть репликацию и резервное копирование)

Предусмотреть меры по защите персональных данных и коммерческой тайны в случае если кт обрабатывается