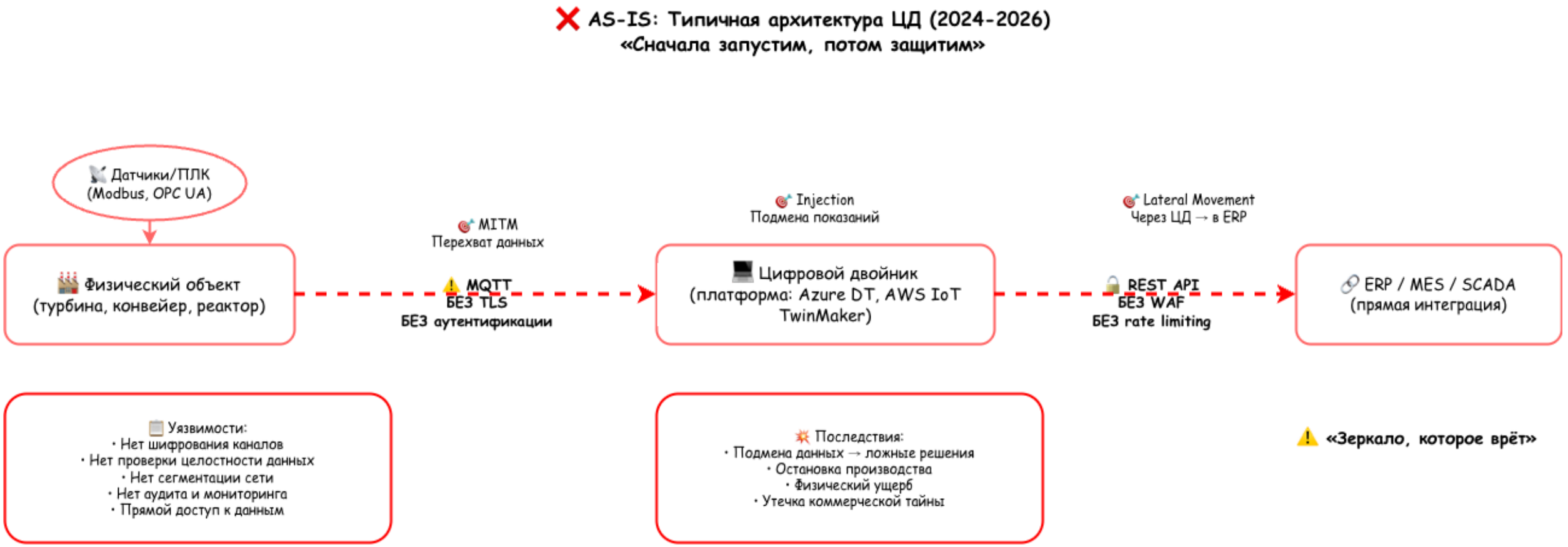
OVODOV

Цифровые двойники: когда «зеркало» начинает врать

Риск-ориентированный подход к ИБ в киберфизических системах

Цифровой двойник — это как зеркало, только дороже, и если его взломать, то разбивается не стекло, а производство



Контекст 2026: что изменилось?

5 лет спустя: новые вызовы для ИБ

- Рост **гетерогенности**: OT + IT + облака + пограничные-узлы = «лоскутное одеяло» уязвимостей.
- ИИ в двойниках: ускорение аналитики, но и новые векторы — adversarial ML, poisoning данных
- Регуляторное давление: требования к целостности данных в критической инфраструктуре (ФЗ-187, ГОСТ Р 57580).

Раньше мы защищали периметр. Теперь периметр — это концепция, как единорог.

Риски ближайших 5-6 лет:

- Компрометация каналов синхронизации физический↔цифровой
- Манипуляция данными для принятия ложных решений (data poisoning).
- Цепочечные атаки через интеграции (MES/ERP/SCADA).
- Недостаточная верификация источников данных (provenance).

Место ИБ в архитектуре цифрового двойника

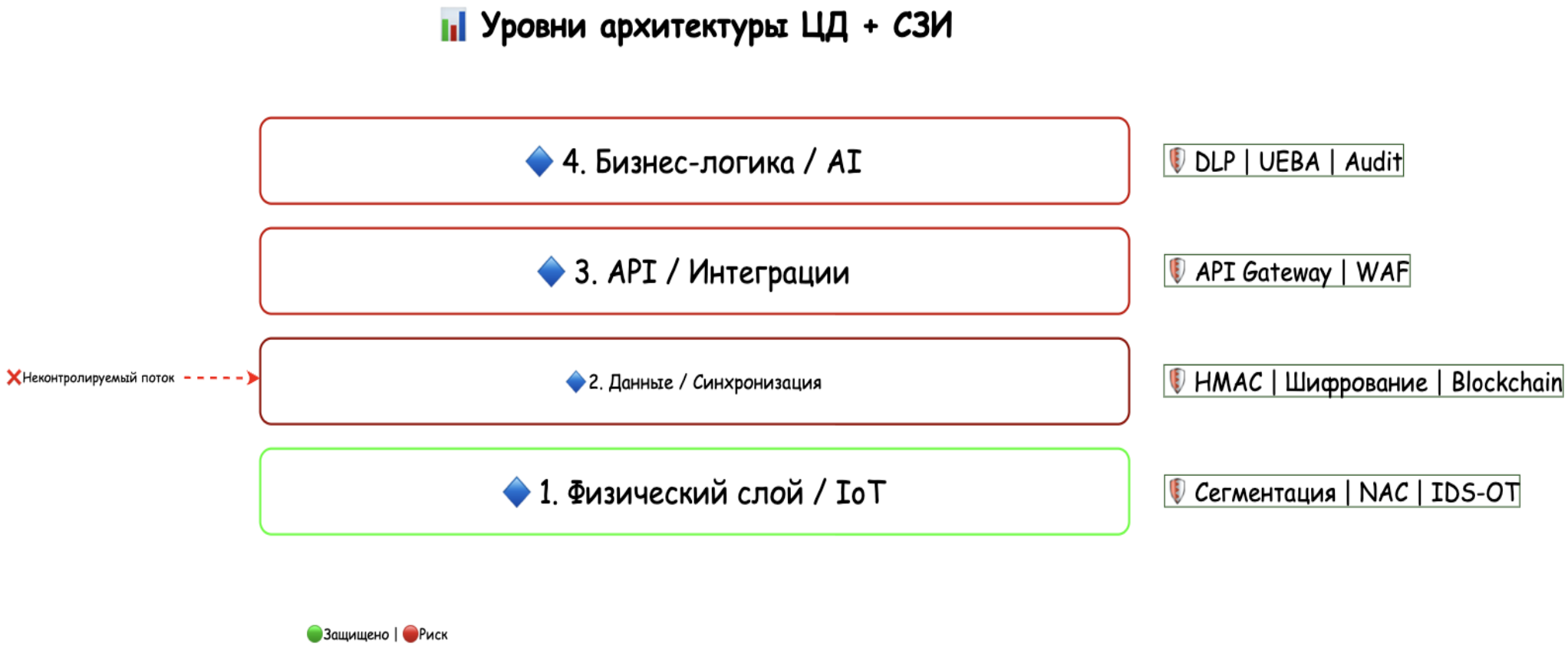
ИБ — не «надстройка», а фундамент (или его часть)

Риск-ориентированный подход: классификация активов двойника по критичности (данные, управление, аналитика).

Связность как угроза: каждый интерфейс — точка входа. Принцип «минимальной связности».

Организационный аспект: ИБ-архитектор участвует в проектировании всех цифровых составных частей с этапа «замысла» - ТЗ, а не «прикручивает» защиту постфактум.

ИБ — не «надстройка», а фундамент (или его часть)



Риск № 1: Компрометация канала синхронизации
Когда «зеркало» показывает не то?

Пример:

Злоумышленник внедряется в канал MQTT между датчиком давления и двойником.
Подменяет показания → система прогнозирования не видит аномалию → авария на физическом объекте.

Исследования показывают, что 68% атак на промышленные двойники начинаются с перехвата данных сенсоров.

Решение:
Обязательное mTLS для всех каналов.

Валидация целостности сообщений (HMAC, цифровые подписи).
Мониторинг аномалий в частоте/объёме данных (SIEM + ML).

Если ваш двойник получает данные без проверки подписи — это не двойник, это фантазёр.

Риск 2: Целостность данных и информация
«Мусор на входе — катастрофа на выходе»

Проблема:
Данные в двойнике должны быть не только конфиденциальны, но и верифицируемы по происхождению (data provenance).
Актуальность: устаревшие данные → ложные решения.
Аналогия с SSDLC (Secure Software Development Lifecycle):

SSDLC для данных двойника:
1. Сбор
2. Валидация источника
3. Шифрование/подпись
4. Хранение с контролем целостности
5. Передача с аудитом
6. Уничтожение по политикам

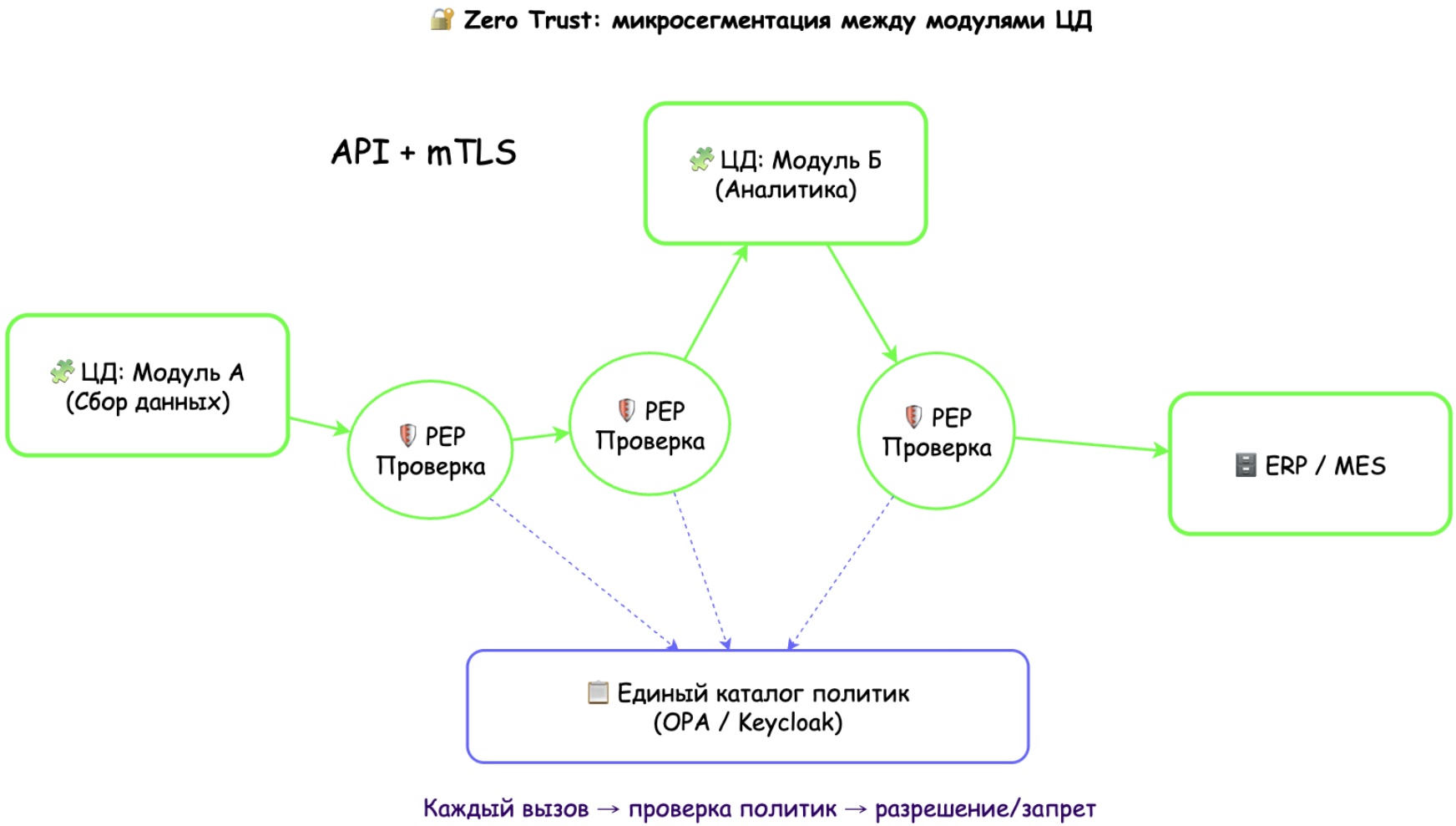
Риск 3: Горизонтальное перемещение через интеграции
«Один взломал — все упали»

Пример:
Двойник интегрирован с системой управления складом.
Злоумышленник через уязвимость в API двойника получает доступ к учетной системе → кража данных о поставках → манипуляции с логистикой.

Источник: В отчёте Digital Twin Consortium подчёркивается, что 43% инцидентов связаны с недостаточной изоляцией компонентов

Решение:
Микросегментация сети (Zero Trust).
Принцип наименьших привилегий для сервисных аккаунтов.
API Gateway с rate-limiting и валидацией схем запросов.

Риск 3: Горизонтальное перемещение через интеграции «Один взломал — все упали»



Обеспечение целостности: технические решения
Как сделать так, чтобы данные «не врали»

Инструменты и подходы:
Криптографическое хеширование цепочек данных: каждый блок данных подписывается, хеш сохраняется в реестре (blockchain или Merkle Tree)

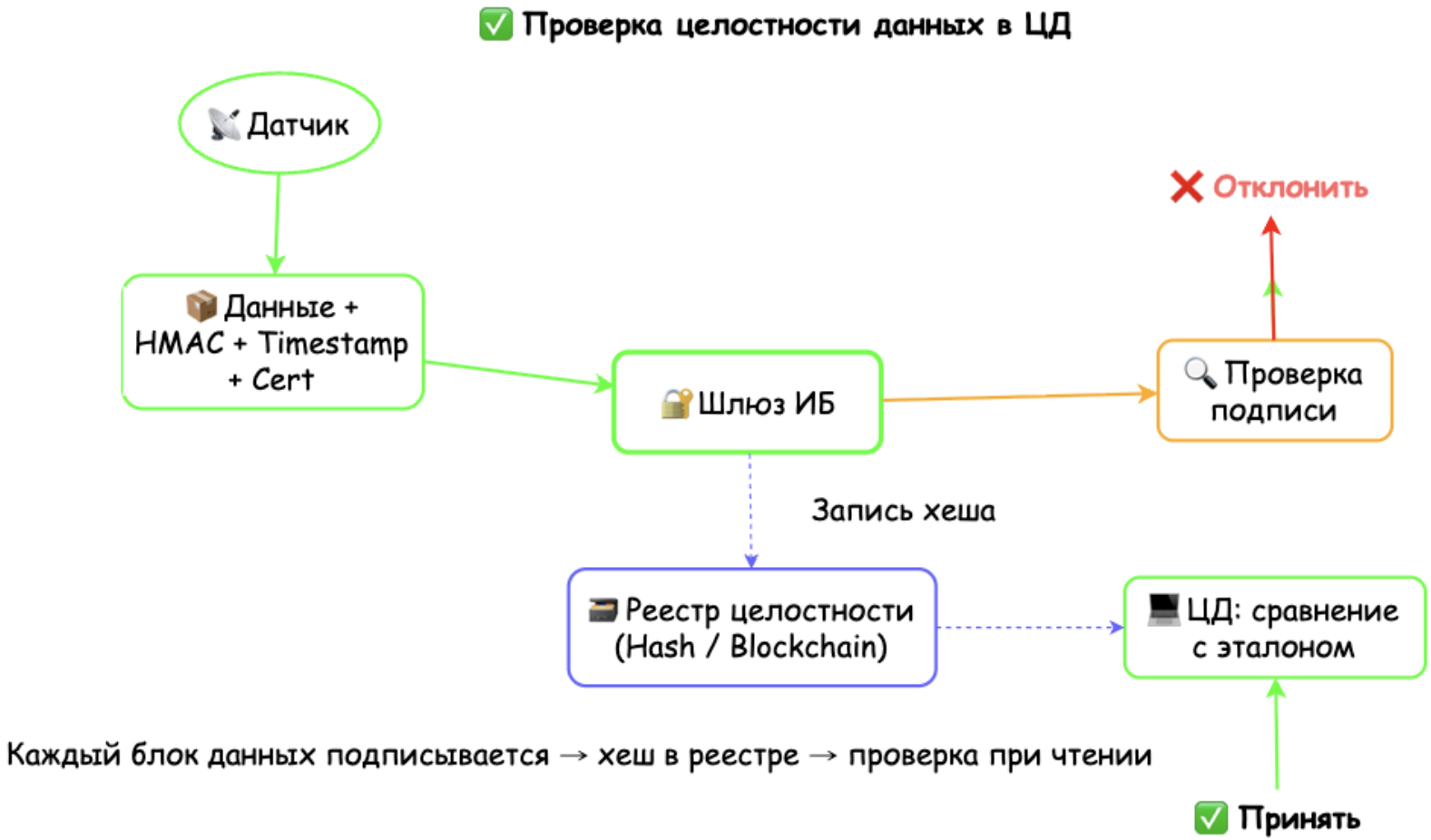
Атрибуция источников: каждый датчик/сервис имеет цифровой сертификат, данные без валидной подписи отклоняются.

Временные метки с доверенным источником времени (NTP+TLS).

Мониторинг аномалий: ML-модели, обученные на «нормальных» паттернах данных, детектируют отклонения.

Хеш данных — как отпечаток пальца. Если не совпадает — это не ваши данные, это подделка.

Обеспечение целостности: технические решения
Как сделать так, чтобы данные «не врали»



Аналогия SSDLC для данных двойника
Безопасность данных — это процесс, а не продукт

Этап жизненного цикла данных	Меры ИБ (аналог SSDLC)
Сбор	Валидация источника, подписи, шифрование на лету
Передача	mTLS, контроль целостности (HMAC), аудит
Хранение	Шифрование at-rest, контроль доступа, версионирование
Обработка	Изоляция сред, контроль целостности вычислений
Уничтожение	Крипто-стирание, аудит удаления

Как в SSDLC: каждый этап имеет чек-лист безопасности, автоматизированный через CI/CD-пайплайны

Zero Trust: базовые принципы для двойников
«Никому не верь, проверяй каждого»

Принципы (NIST SP 800-207):

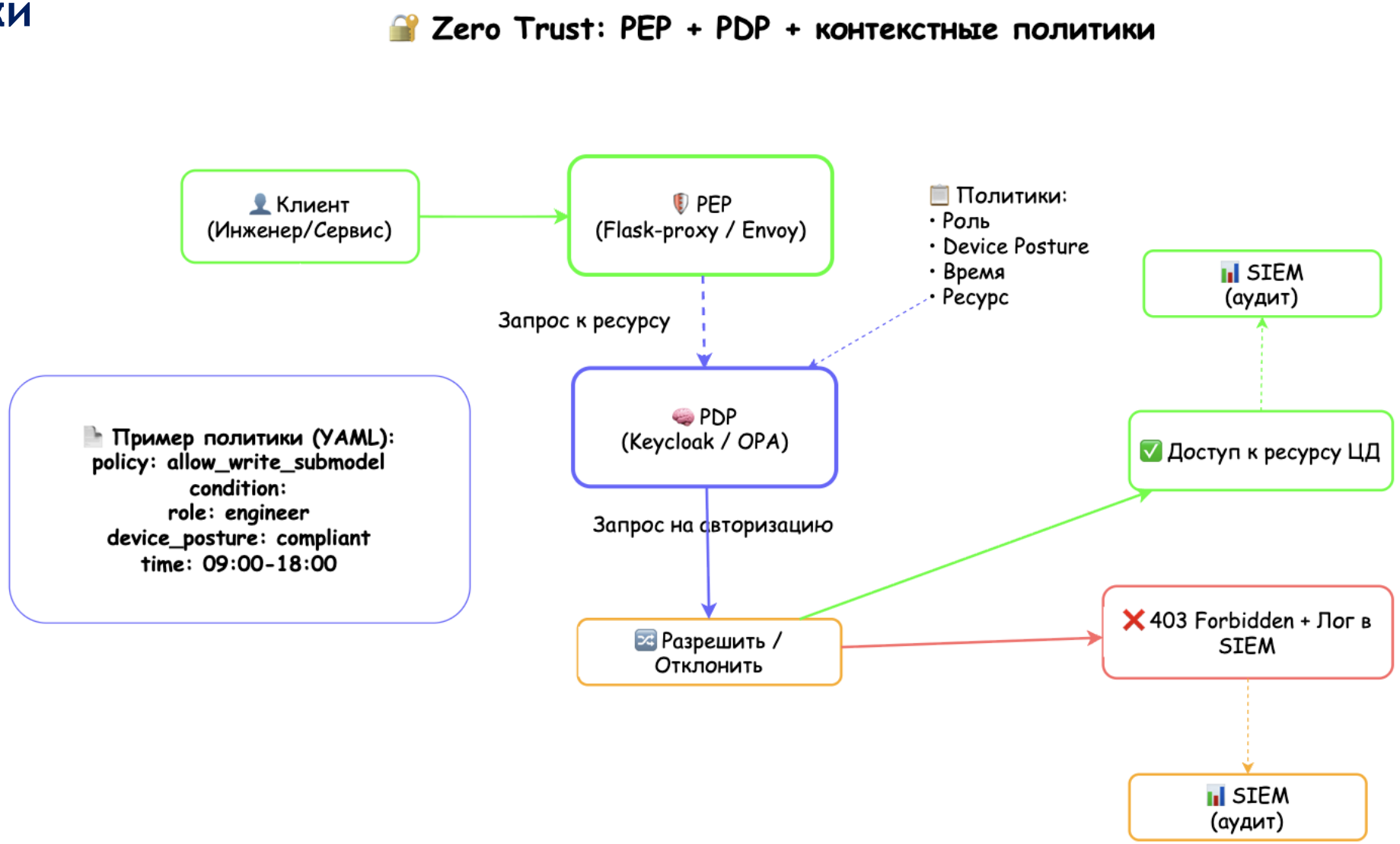
Все запросы аутентифицируются и авторизуются, независимо от источника.
Доступ предоставляется по принципу наименьших привилегий.
Все сессии шифруются, трафик инспектируется.
Политики доступа динамичны и учитывают контекст (устройство, время, поведение).

Пример для двойника:
Инженер подключается к двойнику для настройки. Система проверяет: сертификат устройства, MFA, роль, время суток, геолокацию. Только после этого — доступ к конкретному подмодулю.

Источник: Реализация ZTA на базе Keycloak + PEP-прокси показала снижение поверхности атаки на 73% в тестовых промышленных средах

Раньше мы доверяли внутри периметра. Теперь периметр — это каждый запрос.

Пример реализации Zero Trust для двойника
Архитектура: PEP + PDP + контекстные политики



Интеграция СЗИ/СКЗИ в архитектуру двойника
Где «живут» средства защиты?

! Если СЗИ не на схеме архитектуры — её не существует. Как и вашей безопасности.

Организационные меры: процессы и люди
Технологии — это половина дела

Содержание:
Роль ИБ-архитектора в команде DT: участие в проектировании, ревью кода, тестировании на проникновение.

Процессы:
Регулярный пересмотр политик доступа (quarterly review).
Incident Response-планы для сценариев компрометации двойника.
Обучение команды: «безопасность — ответственность каждого».
Метрики: MTTR для инцидентов с двойниками, % запросов, прошедших проверку политик.

Источник: Эксперты отмечают, что 60% успешных атак на промышленные системы связаны с человеческим фактором и процессными пробелами

Выводы и рекомендации
Итоги: что делать завтра?

ИБ в двойниках — это про целостность и доверие к данным, а не только про конфиденциальность.
Zero Trust — не опция, а необходимость для распределённых киберфизических систем.

Аналогия с SSDLC работает: встраивайте безопасность в каждый этап жизненного цикла данных.
Автоматизация — ваш друг: политики как код, сканирование в CI/CD, мониторинг в реальном времени.

Цифровой двойник без ИБ — это как автомобиль без тормозов: быстро, красиво, и очень страшно.

Наши рекомендации ИБ архитектуру:
1. **Инвентаризация потоков данных и точек интеграции.**
2. **Подготовка и внедрите PEP/PDP для критичных модулей, в последствии для всех систем.**
3. **Автоматизируйте проверку целостности данных.**
4. **Документируйте и тестируйте сценарии компрометации.**

Присоединяйтесь к сообществу, где работают без риска

Объединяем специалистов

800+

Проводим тематических мероприятий в год

50+

Организуем встречи на 300 участников

Контакты и вопросы
Спасибо за внимание!

Контакты:

Юрлов Алексей, Архитектор ИБ решений
url@ovodov.su
ovodov.su

OVODOV
CyberSecurity