

ПРОИЗВОДСТВО НЕЛЬЗЯ ОСТАНОВИТЬ, ЗАЩИТУ НЕЛЬЗЯ ОТЛОЖИТЬ

Как обеспечить видимость и контроль АСУ ТП,
не создавая рисков для технологического процесса



КОНФИГУРАЦИЯ



СЕТЕВЫЕ ВЗАИМОДЕЙСТВИЯ



АКТИВЫ



КОНТРОЛЬ И ВИДИМОСТЬ



ЧАСТИЧНО ИЗВЕСТНО



СОБЫТИЯ

UDV DATAPK **Industrial Kit**

Комплексная киберзащита АСУ ТП
и объектов КИИ

Специфика промышленной инфраструктуры

ЗАЩИТИТЬ НЕЛЬЗЯ ОСТАНОВИТЬ

В корпоративной сети можно остановить работу — изолировать подозрительный хост, установить обновления и так далее. В АСУ ТП такая остановка может стоить дороже, чем последствия инцидента

СРЕДСТВО ЗАЩИТЫ НЕ ДОЛЖНО НАРУШАТЬ ТОТ ПРОЦЕСС, КОТОРЫЙ ОНО ЗАЩИЩАЕТ



УСТАНОВКА АГЕНТА

Не на все оборудование



АКТИВНОЕ СКАНИРОВАНИЕ

Требует оценки допустимости



ОБНОВЛЕНИЕ И ПЕРЕЗАГРУЗКА

Могут требовать технологического окна



ОСТАНОВКА ДЛЯ ПРОВЕРКИ

Допустима не всегда

ОБОРУДОВАНИЕ РАБОТАЕТ ДЕСЯТИЛЕТИЯМИ, ТЕХНОЛОГИЧЕСКИЕ ОГРАНИЧЕНИЯ ОСТАЮТСЯ

01

ОБОРУДОВАНИЕ БЕЗ ПОДДЕРЖКИ АГЕНТОВ

Часть ПЛК и специализированных устройств не позволяет устанавливать дополнительное программное обеспечение

**СЛЕПЫЕ ЗОНЫ
ДЛЯ АГЕНТСКИХ СРЕДСТВ**

02

ПО БОЛЬШЕ НЕ ОБНОВЛЯЕТСЯ

Устаревшие операционные системы, прошивки и прикладное ПО могут содержать известные уязвимости

**РИСК СОХРАНЯЕТСЯ, ДАЖЕ ЕСЛИ
ОБОРУДОВАНИЕ РАБОТАЕТ ШТАТНО**

ШИФРОВАНИЕ — НЕТ

АУТЕНТИФИКАЦИЯ — ОГРАНИЧЕНА

ПОДДЕРЖКА
ЗАВЕРШЕНА

03

ПРОМЫШЛЕННЫЕ ПРОТОКОЛЫ БЕЗ ЗАЩИТЫ

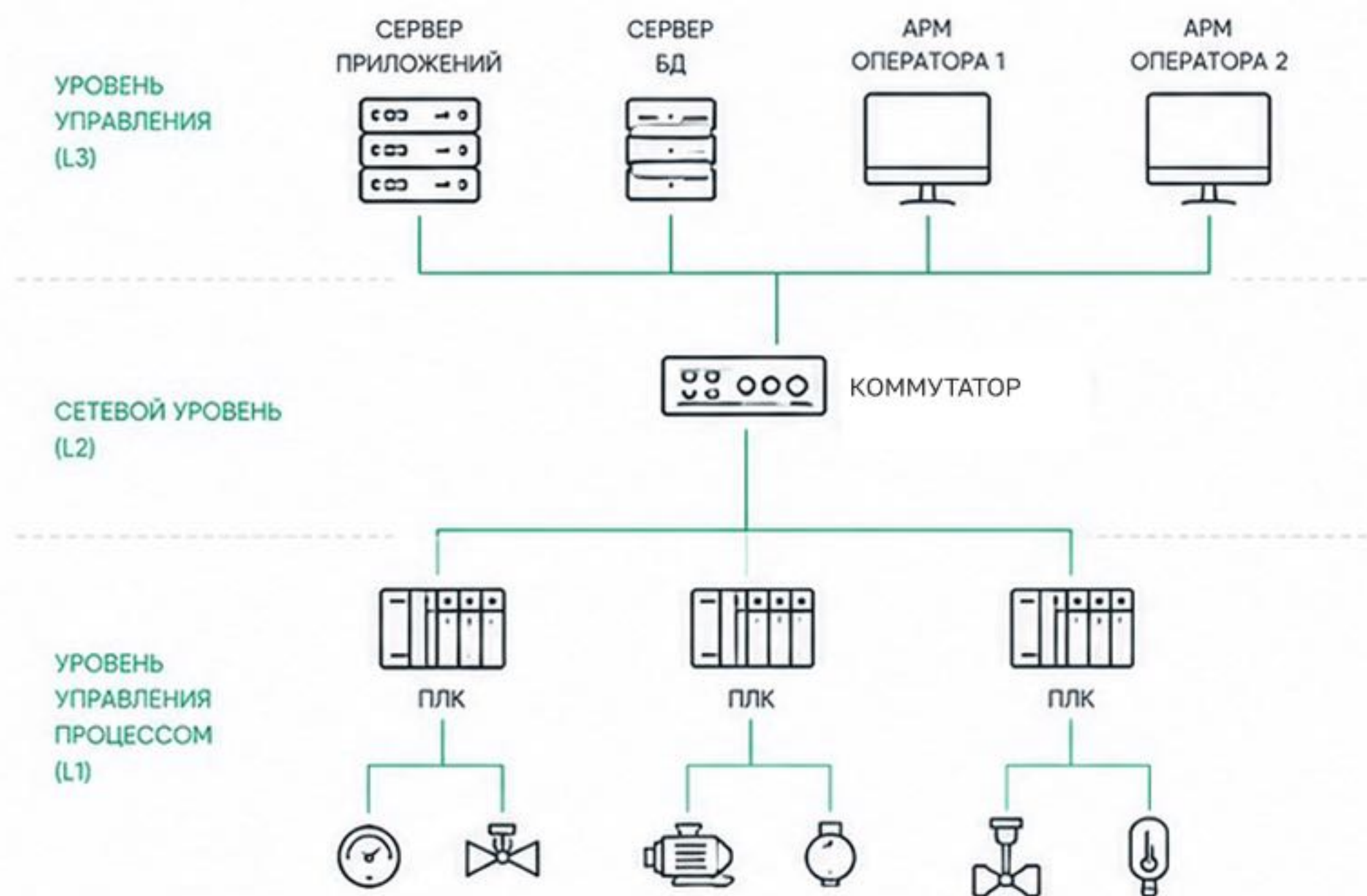
В ряде протоколов отсутствует шифрование или используется слабая аутентификация

**КОМАНДЫ И ДАННЫЕ МОГУТ
ПЕРЕДАВАТЬСЯ БЕЗ ДОСТАТОЧНОЙ
ЗАЩИТЫ**

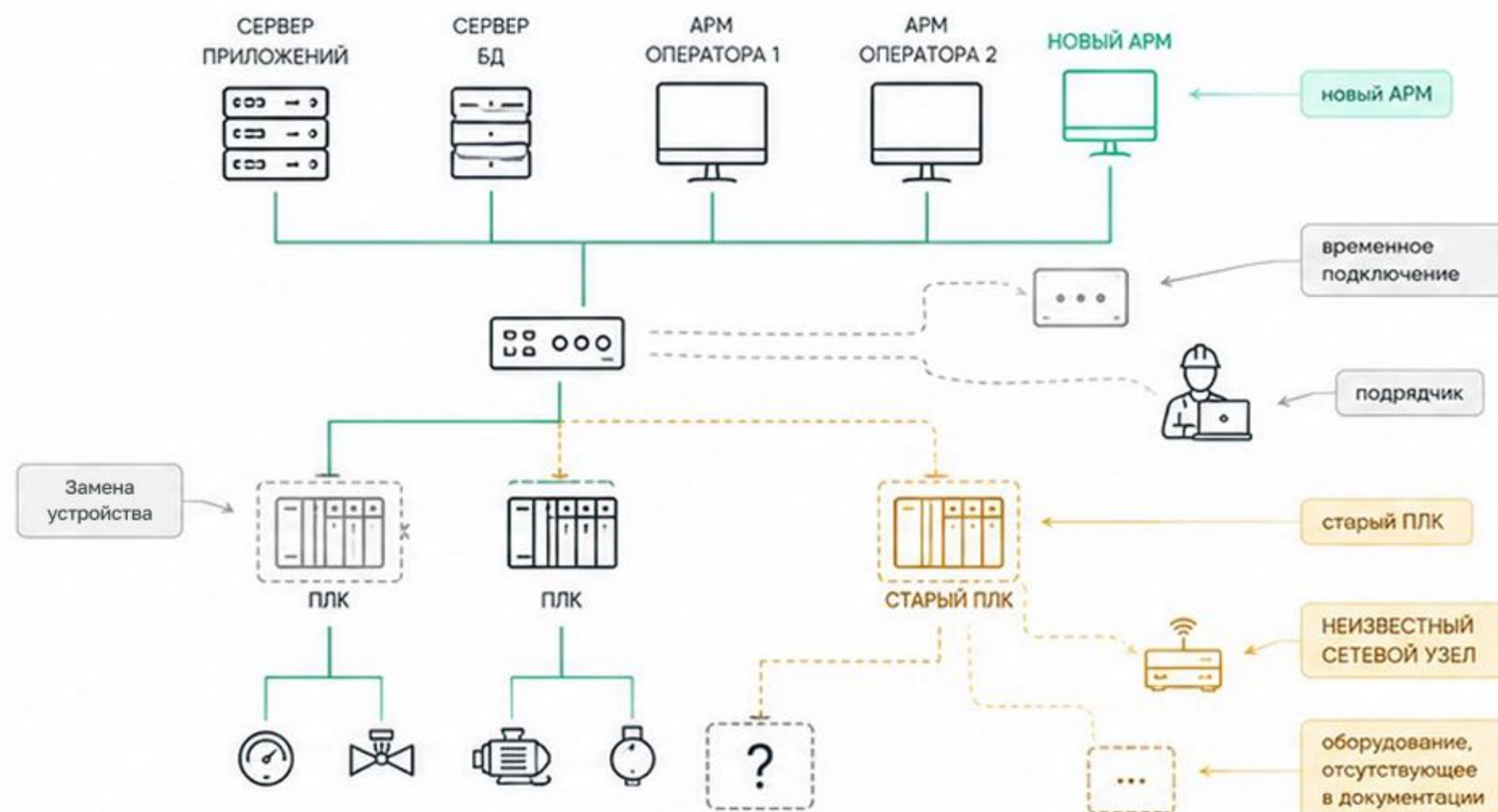
ШТАТНАЯ РАБОТА ОБОРУДОВАНИЯ НЕ ОЗНАЧАЕТ, ЧТО ОНО ЗАЩИЩЕНО

ОБОРУДОВАНИЕ РАБОТАЕТ ГОДАМИ, КАРТА ИНФРАСТРУКТУРЫ **УСТАРЕВАЕТ БЫСТРЕЕ**

ПРОЕКТНАЯ СХЕМА



ФАКТИЧЕСКАЯ ИНФРАСТРУКТУРА



НЕЛЬЗЯ УПРАВЛЯТЬ ЗАЩИТОЙ КОНТУРА, СОСТАВ КОТОРОГО НЕИЗВЕСТЕН

ПРОМЫШЛЕННЫЙ ИНЦИДЕНТ НЕ ВСЕГДА УКЛАДЫВАЕТСЯ В ОДИН КЛАСС СЗИ

1. СЕТЕВОЙ ТРАФИК

10:21:15	192.168.1.25	→	192.168.1.10	Modbus/TCP	
10:21:16	192.168.1.10	→	192.168.1.25	Modbus/TCP	
10:21:17	192.168.1.35	→	192.168.1.10	OPC UA	
10:21:18	192.168.1.10	→	192.168.1.35	OPC UA	
10:21:19	192.168.1.50	→	192.168.1.10	S7comm	
...					

2. КОНФИГУРАЦИИ



IP-адрес	192.168.1.10	
Маска сети	255.255.255.0	
Шлюз	192.168.1.1	
Режим	RUN	
Время цикла	20 ms	
...		

3. УЯЗВИМОСТИ

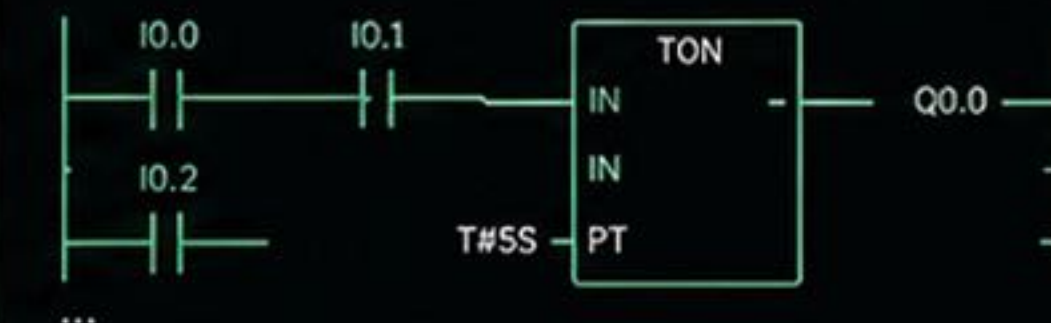


⚠ CVE-2019-12345	Высокая	7.8	
⚠ CVE-2011-42282	Средняя	5.6	
⚠ CVE-2018-100105	Средняя	4.3	
⚠ CVE-2020-1472	Низкая	3.1	
...			

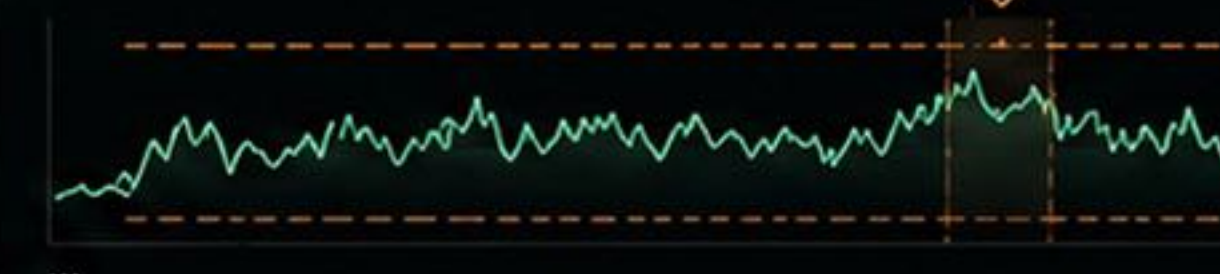
4. ВНЕШНИЕ СОБЫТИЯ

10:18:03	⚠	Отклонение параметра давления
10:17:41	i	Плановое обслуживание
10:16:22	⚠	Повышение вибрации насоса
10:15:07	i	Запуск технологической линии
...		

5. ПРОЕКТЫ ПЛК



6. ПОВЕДЕНИЕ ПЛК



СКОРОСТЬ ЛИНИИ



+4.7% ⚠

ОТКЛОНЕНИЕ
ОТ НОРМЫ

ДАННЫЕ ЕСТЬ, КОНТЕКСТА ИНЦИДЕНТА — НЕТ

НУЖНО НЕ БОЛЬШЕ СРЕДСТВ, НУЖЕН ЕДИНЫЙ КОНТУР ПРОМЫШЛЕННОЙ КИБЕРЗАЩИТЫ

- 👁 Видеть фактическую инфраструктуру
- 🔗 Связывать активы, трафик, конфигурации и события
- 🛡 Своевременно обнаруживать уязвимости

КАК РЕШИТЬ ЭТИ ЗАДАЧИ В РАМКАХ
ОДНОГО ПРЕДПРИЯТИЯ, НЕ ВЛИЯЯ
НА ПРОИЗВОДСТВЕННЫЙ ПРОЦЕСС?



Комплексная защита АСУ ТП

ВИДЕТЬ, КОНТРОЛИРОВАТЬ,
ЗАЩИЩАТЬ, НЕ ВМЕШИВАЯСЬ
В ТЕХНОЛОГИЧЕСКИЙ ПРОЦЕСС

UDV DATAPK Industrial Kit

Модульная платформа для комплексной
киберзащиты АСУ ТП с полной видимостью атак,
угроз и выполнением требований законодательства



ВИДИМОСТЬ



КОНТРОЛЬ



КОНТЕКСТ

ЗНАТЬ, ЧТО ДЕЙСТВИТЕЛЬНО РАБОТАЕТ В АСУ ТП

Анализ копии промышленного сетевого трафика без установки агентов



АКТУАЛЬНАЯ КАРТА АКТИВОВ И ВЗАИМОДЕЙСТВИЙ БЕЗ АКТИВНОГО ВОЗДЕЙСТВИЯ НА ОБОРУДОВАНИЕ

ВИДЕТЬ НЕ ТОЛЬКО СОЕДИНЕНИЕ, ПОНИМАТЬ, ЧТО ПРОИСХОДИТ ВНУТРИ ПРОТОКОЛА



ИНЖЕНЕРНАЯ
СТАНЦИЯ
ENG-01



ПЛК
PLC-07



ТЕХНОЛОГИЧЕСКОЕ
ОБОРУДОВАНИЕ
(НАСОС / БАК)

ГЛУБОКИЙ РАЗБОР ПРОТОКОЛА

1260001 tag_control

Дата создания: 11.05.2026, 18:42:33.789

	Отправитель	Получатель
Актив:	SCADABR	OPENPLC
IP-адрес:	10.51.203.19	10.51.203.9
Порт:	55836	502
MAC-адрес:	00:50:56:B7:2C:3C	00:50:56:B7:2C:3C
Идентификатор:	f37b0f20-c1f5-4401-9240-0cfccd9daa58	2098ebf1-7e32-4d8f-8b0e-3cfc92e9e921
АСУ ТП:	Региональная пультовая	Центральная АСУ ТП

Событие

Важность:	Критическая
Категория события:	Контроль тегов
Протокол:	MODBUS
Сообщение:	Переполнение блока. Значение тега "Уровень воды" = 1960
Действие:	Detected
Обоснование:	Прекратилась работа активов

ПРИМЕРЫ ОБНАРУЖЕНИЙ



НЕСАНКЦИОНИРОВАННОЕ
СОЕДИНЕНИЕ



ОПАСНАЯ
УПРАВЛЯЮЩАЯ
КОМАНДА



НЕТИПИЧНАЯ
ПЕРЕДАЧА ФАЙЛА
ИЛИ ДАННЫХ



ВЛИЯНИЕ НА ПРОЦЕСС:
превышение уровня
воды в баке.
Риск переполнения
и остановки насоса.

ОТ СЕТЕВОГО ПАКЕТА — К ПРОМЫШЛЕННОМУ КОНТЕКСТУ ИНЦИДЕНТА

УСТРОЙСТВО МОЖЕТ РАБОТАТЬ, НО БЫТЬ **НАСТРОЕНО НЕБЕЗОПАСНО**



НЕОБХОДИМОЕ СОСТОЯНИЕ



Разрешённые службы
SSH, RDP, WinCC



Сетевые настройки
IP по регламенту,
только нужные порты



Установленное ПО
ПО из утверждённого
перечня



Критичный параметр
Ограничение на запись
включено



ИНЖЕНЕРНАЯ СТАНЦИЯ



ФАКТИЧЕСКАЯ КОНФИГУРАЦИЯ



**ИЗМЕНЁН
КРИТИЧНЫЙ ПАРАМЕТР**
Ограничение на запись
отключено



**ОТКЛЮЧЕНА
ЗАЩИТНАЯ НАСТРОЙКА**
Брандмауэр для входящих
соединений отключён



**ОБНАРУЖЕНО ПО,
ОТСУТСТВУЮЩЕЕ
В ПЕРЕЧНЕ РАЗРЕШЁННОГО**
Удалённый доступ



ИЗМЕНЕНИЕ ЗАФИКСИРОВАНО
Требует проверки



НЕ ПРОСТО НАЙТИ АКТИВ, А **ПОНЯТЬ, НАСКОЛЬКО БЕЗОПАСНО ОН НАСТРОЕН**



НАЙТИ УЯЗВИМОСТЬ — НЕ СОЗДАВАЯ НОВЫЙ РИСК ДЛЯ ПРОИЗВОДСТВА

01 ДАННЫЕ ОБ АКТИВЕ И УСТАНОВЛЕННОМ ПО



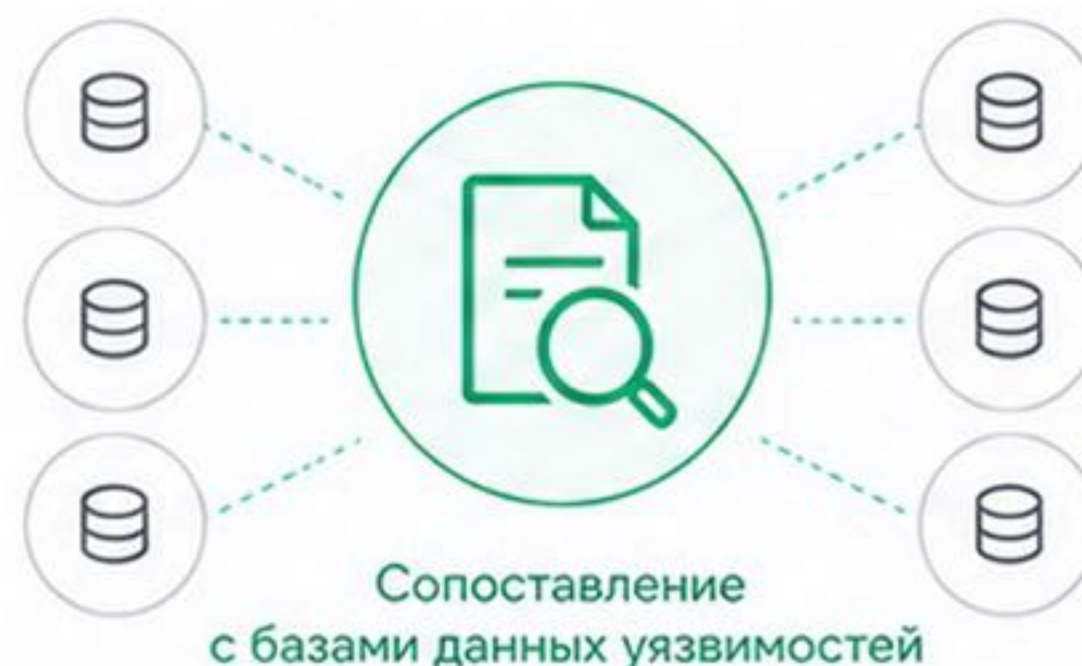
Инженерная станция SCADA-01

	Операционная система	Windows 10 IoT Enterprise 2019 LTSC
	Установленное ПО	AVEVA InTouch 2020 R2
	Доп. компоненты	Microsoft .NET Framework 4.8
	Роль актива	APM оператора



Инвентаризационные данные получены пассивно (без активного сканирования)

02 СОПОСТАВЛЕНИЕ С БАЗАМИ УЯЗВИМОСТЕЙ



Сопоставление с базами данных уязвимостей



Поддержка различных БДУ, включая БДУ ФСТЭК России

03 ПЕРЕЧЕНЬ РИСКОВ, ТРЕБУЮЩИХ ПРОВЕРКИ

Просмотр уязвимостей: WIN2008-SCADA

CVE	Оценка уязвимости	CVSS	БДУ ФСТЭК
CVE-2021-3712	Высокий	7.4	БДУ:2021-04571
CVE-2014-0224	Высокий	7.4	БДУ:2015-00125
CVE-2019-10935	Высокий	7.2	БДУ:2019-04229
CVE-2023-2460	Высокий	7.1	БДУ:2023-02380
CVE-2014-3567	Высокий	7.1	БДУ:2015-00640
CVE-2015-1791	Средний	6.8	БДУ:2015-11038
CVE-2015-0209	Средний	6.8	БДУ:2015-09820
CVE-2014-4686	Средний	6.8	БДУ:2014-00409
CVE-2014-0195	Средний	6.8	БДУ:2015-00144
CVE-2013-0674	Средний	6.8	
CVE-2012-2333	Средний	6.8	БДУ:2015-09677

Уязвимость CVE-2019-10935

Описание Рекомендации

БДУ ФСТЭК России

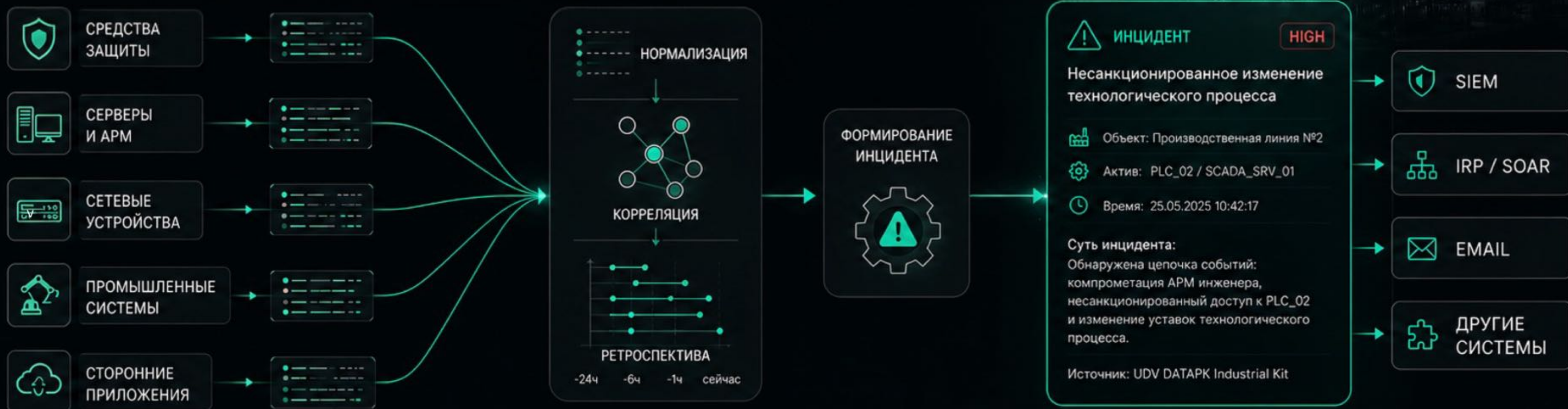
БДУ:2019-04229

Уязвимость веб-приложения SIMATIC WinCC DataMonitor связана с недостаточной проверкой вводимых данных. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, загрузить произвольный ASPX код.

Закрыть

АУДИТ ЗАЩИЩЁННОСТИ БЕЗ АКТИВНОГО СКАНИРОВАНИЯ АСУ ТП

СОБЫТИЯ ИЗ РАЗНЫХ ИСТОЧНИКОВ ДОЛЖНЫ СКЛАДЫВАТЬСЯ В ПОНЯТНЫЙ ИНЦИДЕНТ

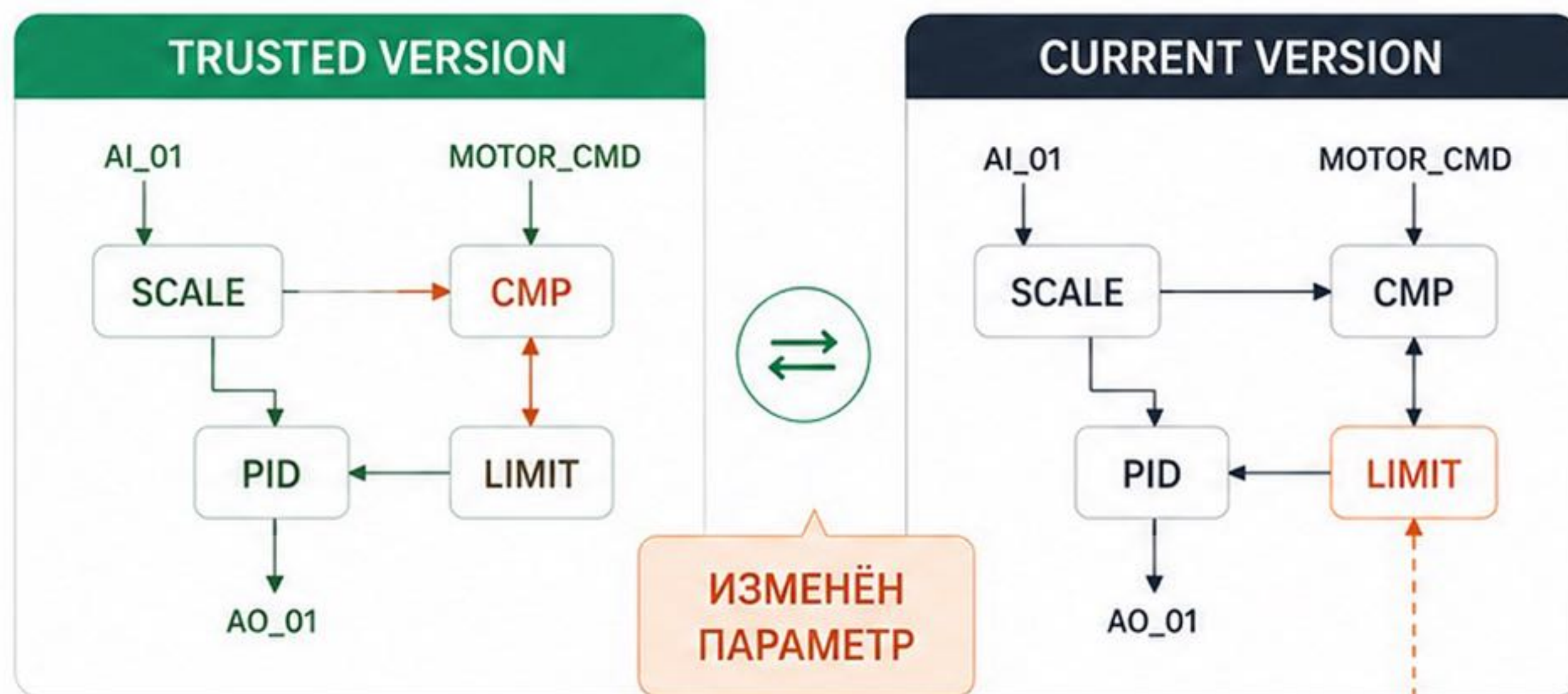


НЕ ЗАМЕНЯТЬ СУЩЕСТВУЮЩИЙ SOC,
ДОБАВЛЯТЬ ЕМУ ПРОМЫШЛЕННЫЙ КОНТЕКСТ

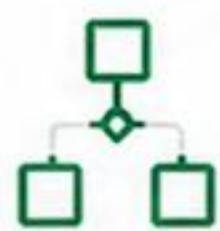


ИЗМЕНЕНИЕ В ПРОЕКТЕ ПЛК МОЖЕТ ИЗМЕНИТЬ ФИЗИЧЕСКИЙ ПРОЦЕСС

ВЕРСИИ ПРОЕКТА ПЛК



ИЗМЕНЕНИЕ
В ПРОЕКТЕ



ИЗМЕНЕНИЕ
УПРАВЛЯЮЩЕЙ ЛОГИКИ



ВОЗМОЖНОЕ ОТКЛОНЕНИЕ
ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА

АКТИВ И КОНФИГУРАЦИЯ



ЦЕНТРАЛИЗОВАННОЕ ХРАНЕНИЕ



СРАВНЕНИЕ ВЕРСИЙ



ИСТОРИЯ ИЗМЕНЕНИЙ



ВОССТАНОВЛЕНИЕ
ДОВЕРЕННОЙ ВЕРСИИ



ЗНАТЬ, ЧТО ИЗМЕНИЛОСЬ. ПОНИМАТЬ, ЧТО ВОССТАНАВЛИВАТЬ

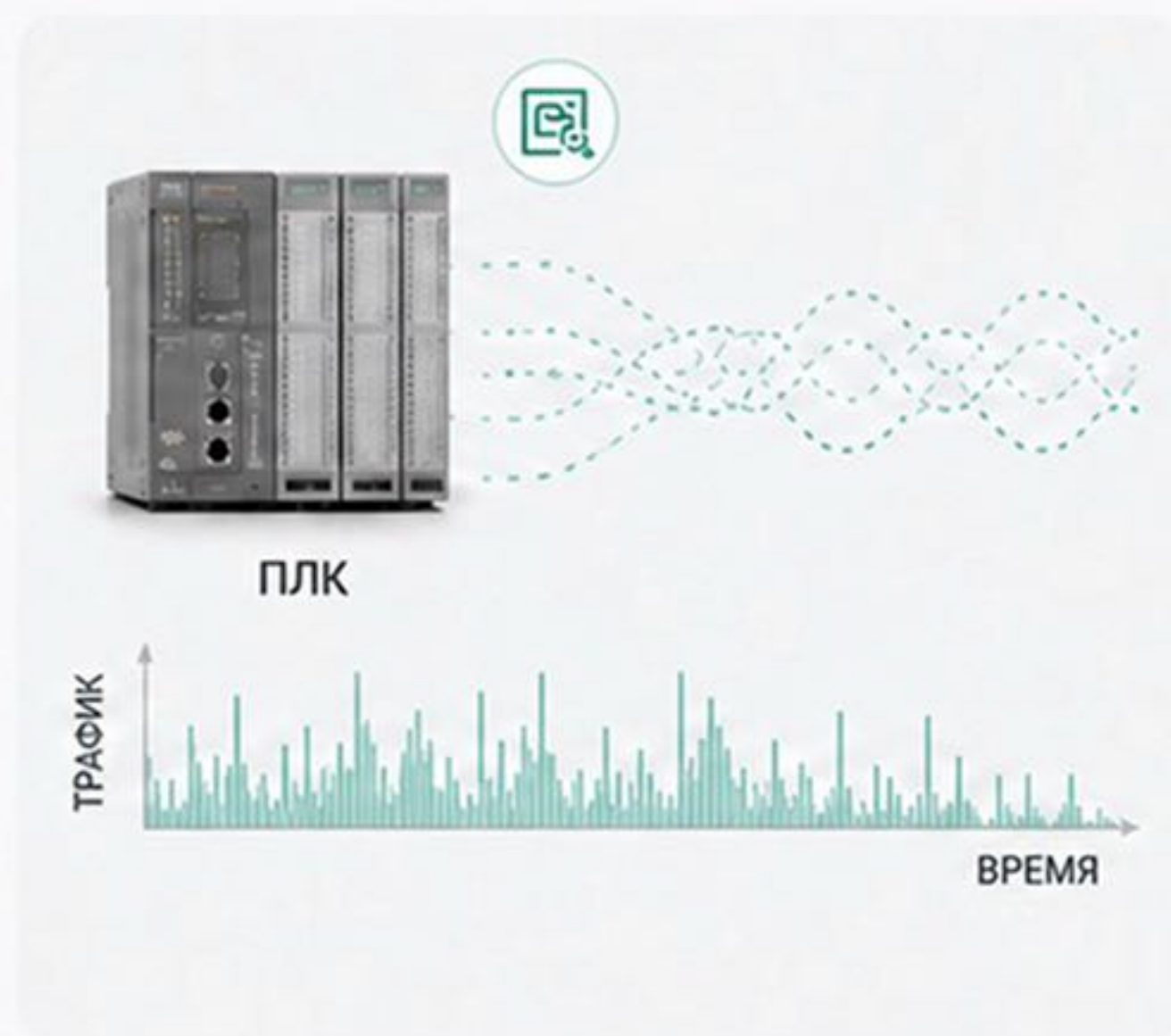


НЕ ВСЁ ОПАСНОЕ НАРУШАЕТ ПРАВИЛО, ИНОГДА ОНО НАРУШАЕТ ПРИВЫЧНОЕ ПОВЕДЕНИЕ

КОПИЯ СЕТЕВОГО ТРАФИКА ПЛК

ЛОКАЛЬНАЯ МОДЕЛЬ НОРМАЛЬНОГО ПОВЕДЕНИЯ

ВЫЯВЛЕННОЕ ОТКЛОНЕНИЕ



БЕЗ АГЕНТОВ



ЛОКАЛЬНОЕ
ОБУЧЕНИЕ



ВОЗМОЖНОСТЬ
ДООБУЧЕНИЯ



ДЕТАЛИЗИРОВАННЫЙ
КОНТЕКСТ АНОМАЛИИ



ВЫЯВЛЕНИЕ АНОМАЛИЙ В ПОВЕДЕНИИ ПЛК, КОТОРЫЕ НЕ МОГУТ БЫТЬ ОПРЕДЕЛЕНЫ КЛАССИЧЕСКИМИ **DPI И SCADA-СИСТЕМАМИ**



ИНЦИДЕНТ СТАНОВИТСЯ ПОНЯТНЕЕ, КОГДА ИЗВЕСТЕН ВСЕ **КОНТЕКСТ**



СЕТЬ И СОБЫТИЯ

Какие взаимодействия и сигналы предшествовали инциденту



АКТИВ И КОНФИГУРАЦИЯ

Что это за устройство и соответствует ли его состояние необходимому



ПО И УЯЗВИМОСТИ

Какие известные риски относятся к активу



ПРОЕКТ ПЛК

Были ли изменения логики или версии



ПОВЕДЕНИЕ

Соответствует ли активность нормальному профилю



ИНЦИДЕНТ



Затронутый актив



Последовательность событий



Критичность



Что требует проверки



ДАННЫЕ



СОПОСТАВЛЕНИЕ



ПРОМЫШЛЕННЫЙ КОНТЕКСТ



РЕШЕНИЕ АНАЛИТИКА



НЕ ОБЯЗАТЕЛЬНО ВНЕДРЯТЬ ВСЁ СРАЗУ

01

НУЖНА ВИДИМОСТЬ СЕТИ

Начать с Industrial NTA



03

02

01



02

ДОБАВЛЯЕМ КОНТРОЛЬ КОНФИГУРАЦИЙ И УЯЗВИМОСТЕЙ

Подключить Configuration Management
и Vulnerability Management



03

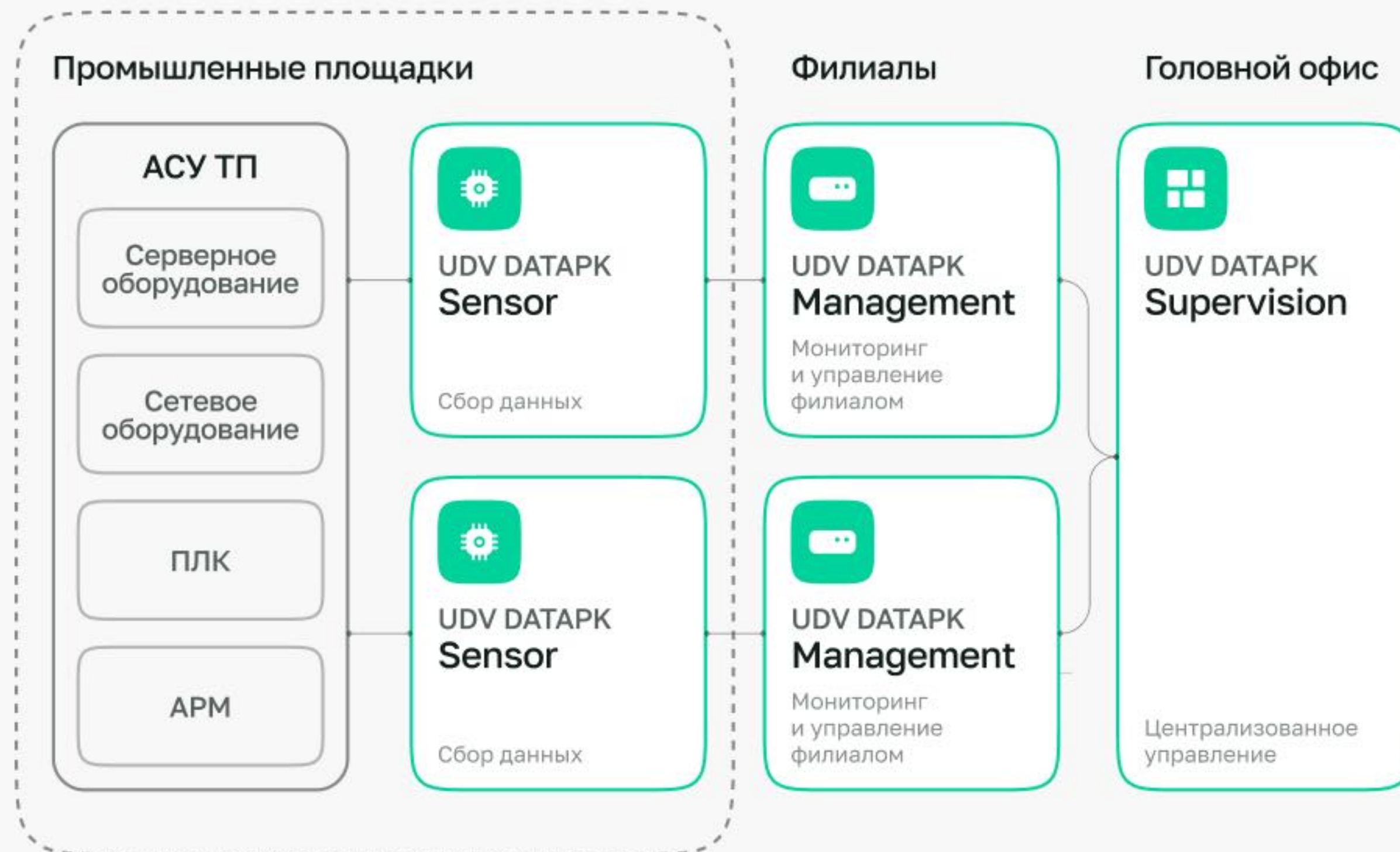
РАСШИРЕННЫЙ КОНТЕКСТ ДЛЯ РАССЛЕДОВАНИЙ

Добавлять External Events
Management, Version Control
и ML for PLC по мере необходимости



НАСТРАИВАЙТЕ ЗАЩИТУ ПОЭТАПНО, **В СООТВЕТСТВИИ С ВАШИМИ ПРИОРИТЕТАМИ**

Компоненты UDV DATAPK Industrial Kit



UDV DATAPK Supervision

- Устанавливается в корпоративном или технологическом сегментах сети
- Получает данные от подключенных Management
- Предоставляет централизованную аналитическую информацию об общем состоянии защищённости АСУ ТП
- Осуществляет централизованное управление УЗ пользователей системы



UDV DATAPK Management

- Устанавливается в технологическом сегменте сети или за его пределами
- Получает данные от подключенных Sensor
- Осуществляет конфигурацию и администрирование связи Management + Sensor
- Осуществляет хранение обработанных данных
- Предоставляет детальные данные пользователю
- Предоставляет базовые панели мониторинга
- REST API для автоматизации
- Передает ключевые данные на Supervision



UDV DATAPK Sensor

- Устанавливается в технологическом сегменте сети
- Получает и хранит копию сетевого трафика
- Получает события ИБ от внешних источников
- Осуществляет сбор данных с активов
- Иницирует подключение к Management
- Передает пред-обработанные данные на Management

Доверенное решение для КИИ

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ РЕГУЛЯТОРОВ

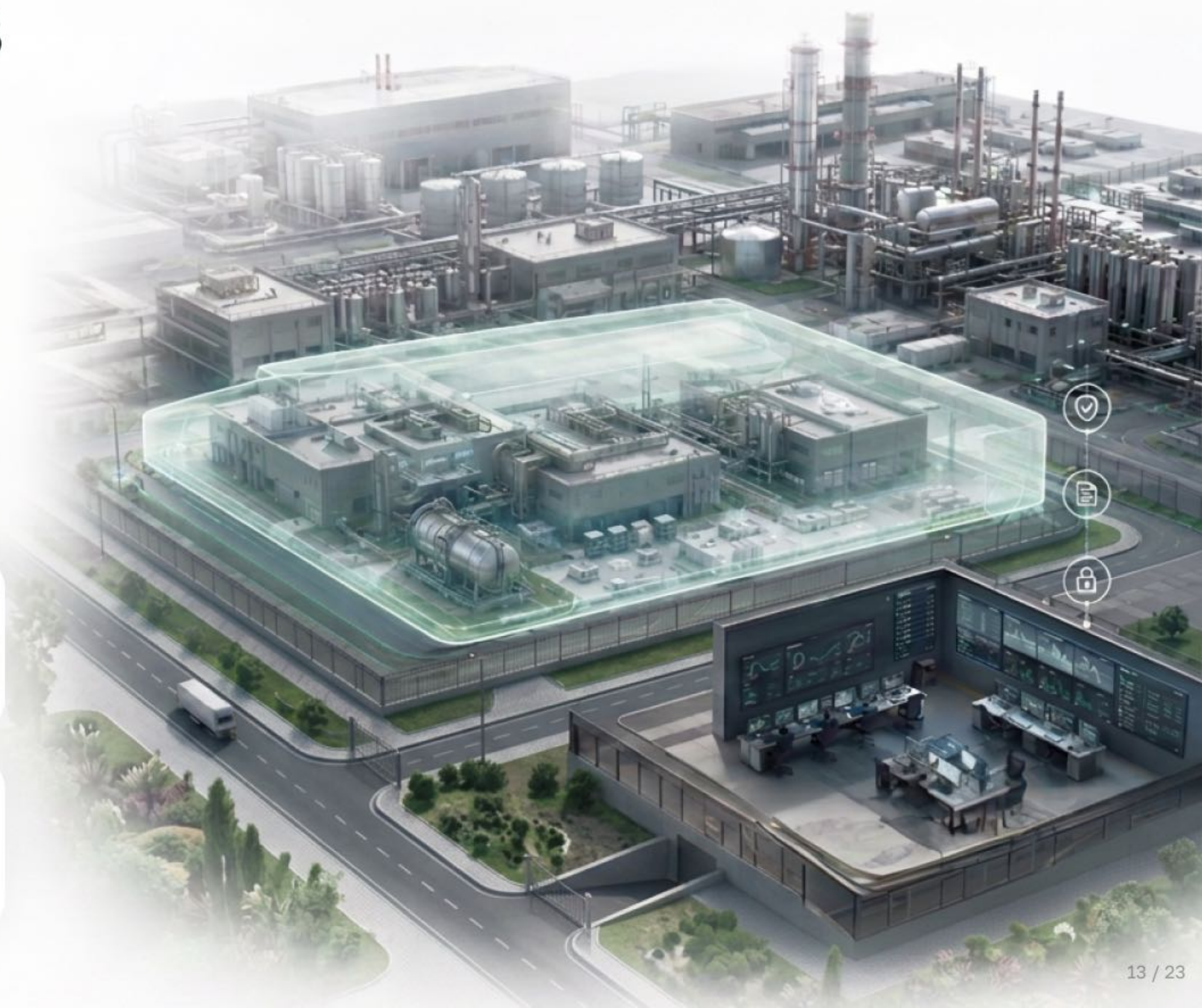
UDV DATAPK Industrial Kit позволяет выполнить требования приказов ФСТЭК России № 239 и № 31 к организационным и техническим мерам проектирования и эксплуатации систем безопасности значимых объектов КИИ и защите АСУ ТП



Сертифицирован ФСТЭК России
по 4 уровню доверия (сертификат № 4719)



Входит в Реестр российского ПО
(запись № 4732)



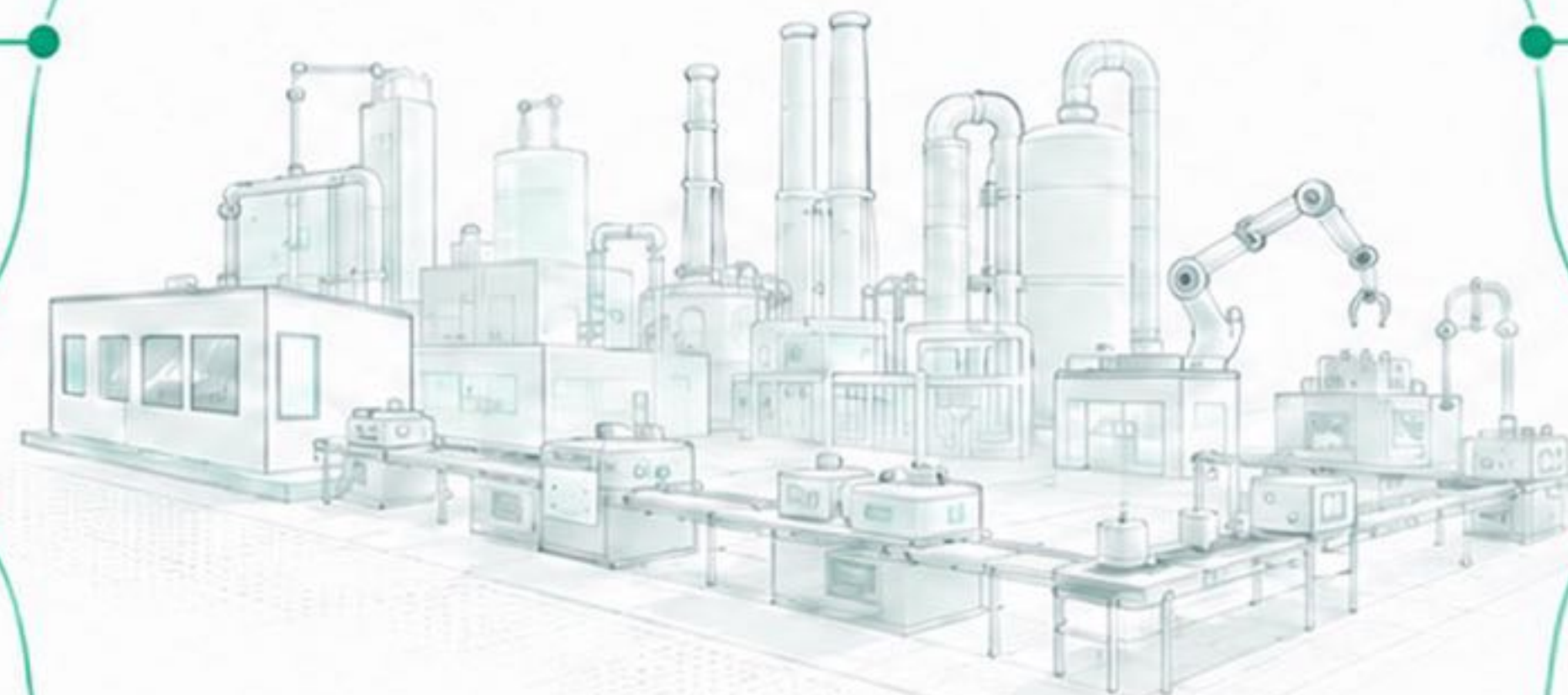


БОЛЬШЕ КОНТРОЛЯ, БЕЗ ВМЕШАТЕЛЬСТВА В ПРОИЗВОДСТВО



АКТУАЛЬНАЯ КАРТИНА АСУ ТП

Активы, связи, конфигурации
и изменения собраны в едином контексте



РАНЬШЕ ВЫЯВЛЯТЬ РИСКИ

Подозрительные действия, уязвимости
и отклонения становятся заметнее



СОКРАЩАТЬ РУЧНУЮ РАБОТУ

Данные для расследований, аудита
и отчётности собираются централизованно



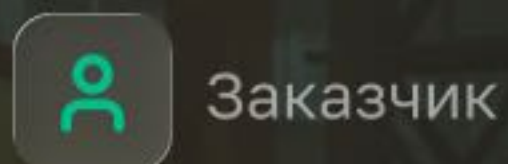
РАСШИРЯТЬ ЗАЩИТУ ПОЭТАПНО

Можно начинать с приоритетной задачи
и подключать новые модули по мере
необходимости

КИБЕРЗАЩИТА СТАНОВИТСЯ ЧАСТЬЮ УПРАВЛЕНИЯ УСТОЙЧИВОСТЬЮ ПРОИЗВОДСТВА

Доказанная эффективность

ЗАЩИТА ПРОМЫШЛЕННЫХ СЕТЕЙ НА ПЕРМСКОМ ЗАВОДЕ «МАШИНОСТРОИТЕЛЬ»



«Машиностроитель»

Отрасль

Машиностроение

Профиль

Производство ракетных двигателей для нужд военно-промышленного комплекса и ракетно-космической отрасли. В гражданском секторе завод серийно производит критически важные компоненты и узлы реверса для российских авиационных двигателей ПС-90А, а также дозировочные системы и нефтехимическое оборудование.

Особенности проекта

Сегменты предприятия являются объектами КИИ. Деятельность Пермского завода «Машиностроитель» критически важна для государства и национальной безопасности, так как он обеспечивает обороноспособность страны.

ЗАДАЧА



Обеспечить глубокий анализ сетевого трафика, своевременное обнаружение вторжений и аномалий и оперативное реагирование на угрозы, а также - выполнить требования законодательства по защите объектов КИИ

РЕЗУЛЬТАТЫ ВНЕДРЕНИЯ



Значительно улучшена видимость промышленной сети. Инженеры АСУ ТП получили четкое представление о том, какие устройства и приложения взаимодействуют друг с другом, и как они используются.



Решение помогло выявить уязвимости в промышленных системах, которые ранее оставались незамеченными



Предотвращен ряд кибератак. Решение помогло выявить и остановить несколько попыток несанкционированного доступа к промышленным системам предприятия



Сокращено время реагирования на инциденты, связанные с безопасностью, за счет оперативного получения необходимой информации

UDV DATAPK Industrial Kit ОСОБЕННО ЭФФЕКТИВЕН, КОГДА:

01

В ИНФРАСТРУКТУРЕ МНОГО LEGACY-ОБОРУДОВАНИЯ

Агенты и активное сканирование
применимы не везде

02

ИСПОЛЬЗУЮТСЯ РАЗНЫЕ СРЕДСТВА ЗАЩИТЫ

Не хватает единого
промышленного контекста

03

НЕТ АКТУАЛЬНОЙ КАРТЫ АСУ ТП

Фактические активы и связи
отличаются от документации

04

ЕСТЬ НЕСКОЛЬКО ПРОИЗВОДСТВЕННЫХ ПЛОЩАДОК

Нужна локальная детализация
и централизованная аналитика

05

ТРЕБУЕТСЯ РЕАЛИЗОВАТЬ МЕРЫ ПРИКАЗОВ №239 И №31

Необходимы технические механизмы
и доказательная база



UDV Group — группа компаний российских разработчиков высокотехнологичных решений для обеспечения киберустойчивости промышленных, коммерческих и государственных предприятий.

Мы помогаем компаниям эффективно управлять состоянием их цифровой инфраструктуры, обеспечивая полную видимость технологического и ИТ — контура, контролировать состояние сети и устройств, своевременно нейтрализовать угрозы — до того, как они повлияют на бизнес.

- ✓ **Защита АСУ ТП и объектов КИИ**
- ✓ **Мониторинг инфраструктуры**
- ✓ **Реагирование на инциденты ИБ**
- ✓ **Предиктивная аналитика киберугроз**
- ✓ **ИБ консалтинг и техническая поддержка**
- ✓ **Выполнение требований регуляторов**

12+ лет

на рынке
информационной
безопасности

Подтвержденный опыт
интеграции в нефтегазовой
отрасли, энергетике,
металлургии

1000+

инсталляций

Проекты по защите АСУ ТП
и корпоративных сетей



Глубокая экспертиза в АСУ ТП
и кибербезопасности
в промышленности



Наличие сертификатов ФСТЭК
по 4 уровню доверия



Сильная инженерная база,
продукты высокого уровня
зрелости



Гибкий подход, возможность
кастомизации решений
под запрос

ВЫ ВИДИТЕ, ЧТО ПРОИСХОДИТ В КАЖДОМ СЕГМЕНТЕ ВАШЕЙ АСУ ТП?

UDV DATAPK Industrial Kit

Покажем, как выстроить комплексную киберзащиту технологической инфраструктуры без вмешательства в производственный процесс

НАЧНИТЕ С ОДНОЙ ПЛОЩАДКИ И ОДНОЙ ПРИОРИТЕТНОЙ ЗАДАЧИ

- какие активы и взаимодействия остаются вне контроля;
- какой модуль нужен для первой задачи;
- как встроить решение в существующую архитектуру;
- как расширить контур на другие площадки.

8-800-511-65-51

Телефон для связи

zapro@udv.group

Электронная почта

udv.group

Сайт

@udv_group

Телеграм

