# Промышленная безопасность

## Проектная практика при защите АСУ ТП

Хлебников Андрей

Руководитель департамента технологического развития

# Ключевые риски бизнеса

### Технологические нарушения

Нарушение технологических процессов, повреждение оборудования и систем

### Катастрофический ущерб

Разрушение технологических объектов, катастрофический ущерб

### Угроза жизни и здоровью

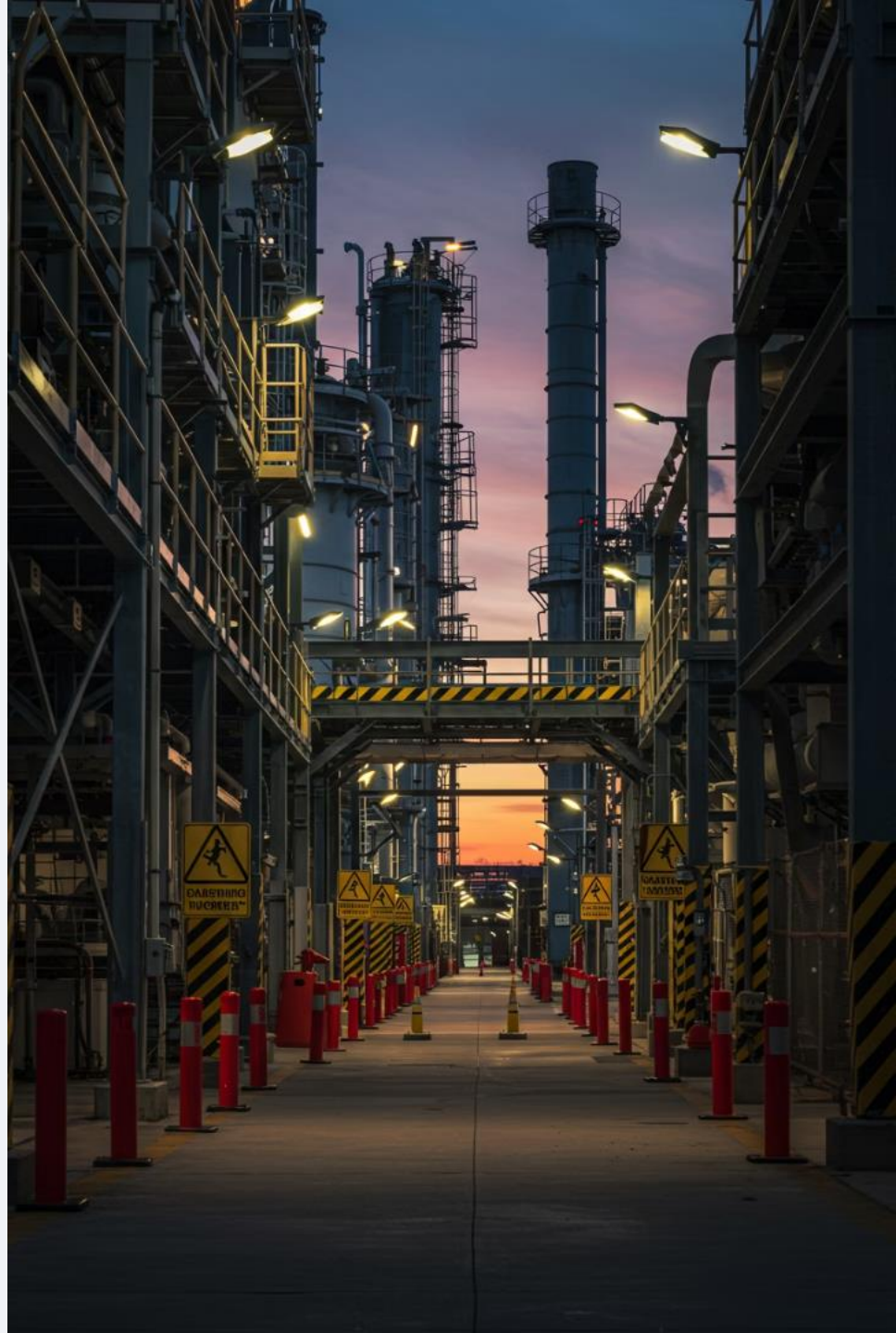
Причинение ущерба здоровью и жизни людей

### Экологический ущерб

Нанесение экологического ущерба территориям

### Производственные простои

Вынужденный простой: сложность перезапуска технологических процессов



# Коммерческие риски бизнеса

- Неисполнение контрактов
- Кража интеллектуальной собственности
- Репутационные риски
- Негативная информация в публичном поле
- Утрата доверия заказчиков и партнеров

# Регуляторные и финансовые риски

### Несоответствие требованиям

Несоответствие стандартам и требованиям законодательства может привести к серьезным последствиям для бизнеса, включая приостановку деятельности

### Внеплановые проверки и предписания

Внеплановые проверки регуляторов могут привести к предписаниям и блокированию производства, что нарушает операционную деятельность

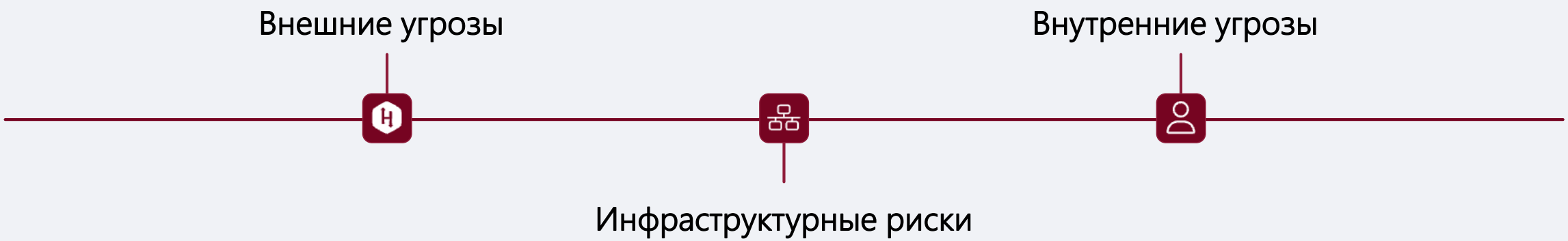
### Финансовые потери

Штрафы, компенсации ущерба, падение стоимости ценных бумаг и судебные издержки представляют значительные финансовые риски для компании

**Комплексный подход к управлению рисками требует постоянного мониторинга и своевременного реагирования на возникающие угрозы**

# Мы оцениваем риски ИБ. Но причем здесь бизнес?

# Ключевые проблемы и риски ИБ,
## ведущие к рискам бизнеса




- Неадекватный уровень решений по аутентификации и авторизации
- Вредоносное ПО и шифровальщики
- Социальная инженерия и фишинг
- Некорректная сегментация сети

- Устаревшие и не обновляемые системы
- Применение сторонних продуктов
- Уязвимые цепочки поставок
- Внутренние нарушители
- Удаленный доступ

# Основные вызовы на производстве

Устаревшее оборудование и неподдерживаемое ПО

Требования бизнеса к управлению производством

Нестабильное электроснабжение

Логистические вызовы

Требования к непрерывному производству

Высокие требования к отказоустойчивости систем

Текущие строительные работы

Высокие требования к физической безопасности

# Общий подход к планированию ИБ решений

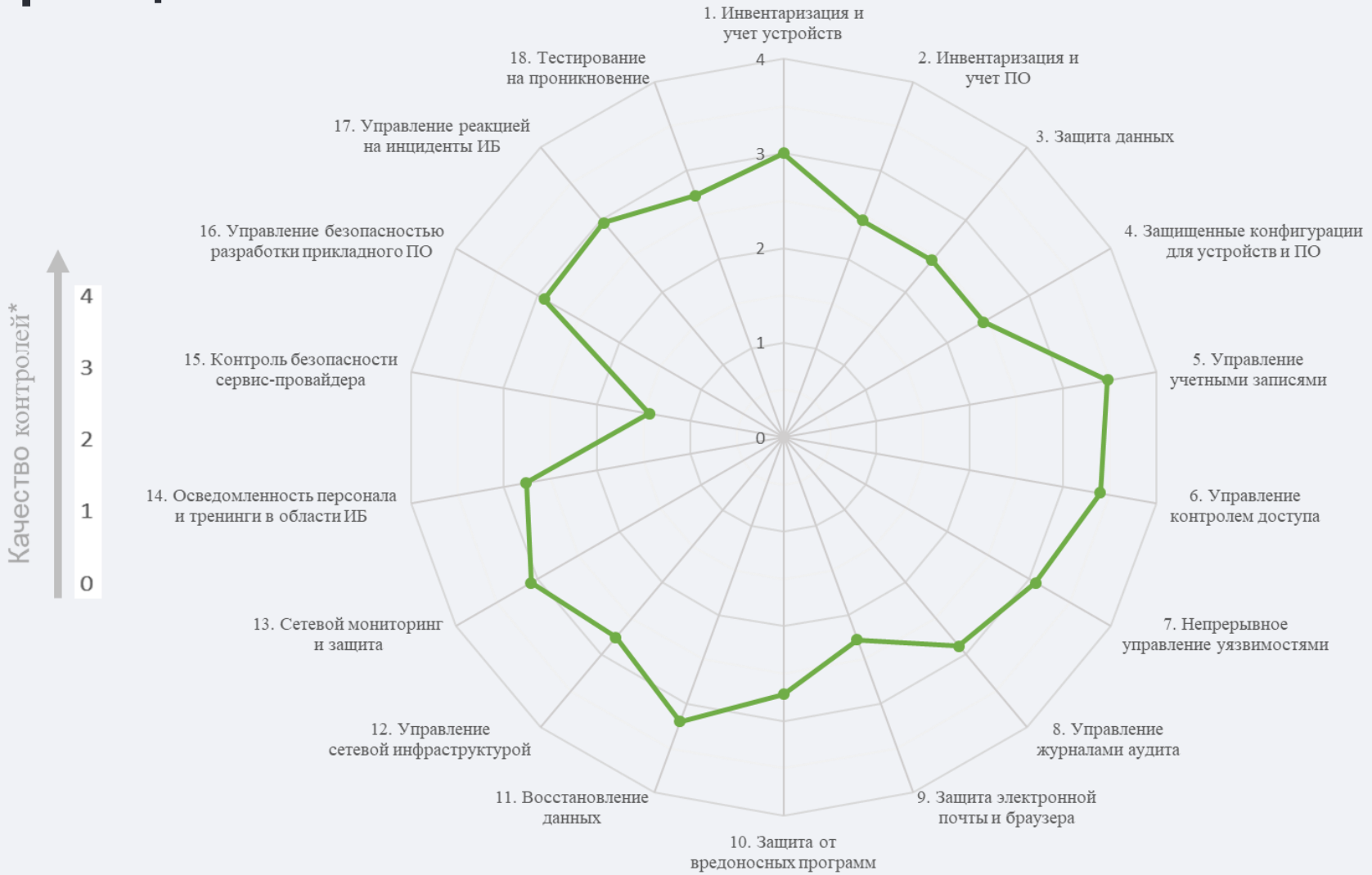

**Фреймворки и стандарты**

- ISO 27xxx
- NIST CSF, CIS
- TOGAF, O-ESA
- FAIR, OCTAVE
- SWOT, RICE
- ISO/IEC 22301, 22317

**Компетенции и сертификации**

- 27001 LA / LI
- CISA, CISM
- CRISC, CISSP
- PMP

# Пример оценки состояния ИБ на основе CIS Controls v8




* качество контролей определяется по 4 критериям: формализация, реализация, автоматизация, отчетность

ИЛЛЮСТРАЦИЯ

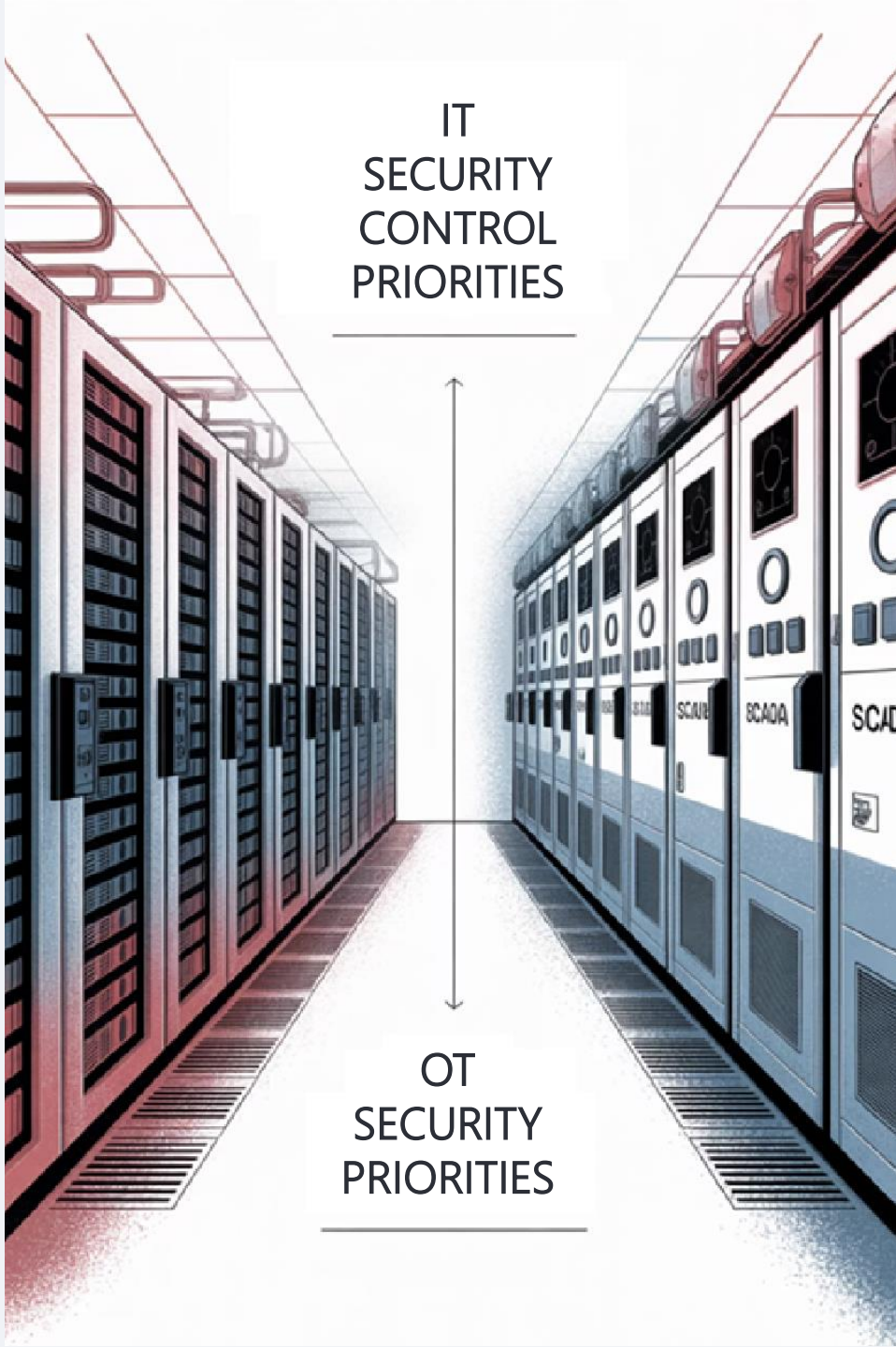
# Разные приоритеты – разный подход

## Безопасность ИТ

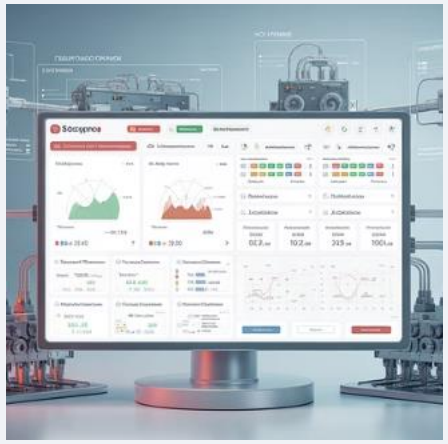
- Приоритет №1 – Конфиденциальность
- Фокус – Не допустить разглашения
- Цель защиты – Сервера, раб. станции
- Условия – кондиционирование

## Безопасность АСУ ТП

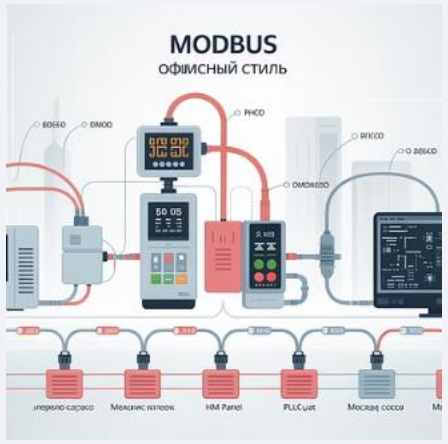
- Приоритет №1 – Доступность и целостность
- Фокус – Не допустить простоев и сбоев
- Цель защиты – Контроллеры, HMI, датчики
- Условия – агрессивная окружающая среда



# Что защищаем?






## Основные вендоры систем АСУ ТП на международных рынках

- Siemens
- Yokogawa
- Emerson
- Honeywell
- Schneider Electric
- HollySys
- ABB
- Rockwell automation

+ работаем с российскими решениями и вендорами


# Стандарты, используемые при реализации проектов

## ИТ-стандарты

- ISO/IEC 27001
- NIST SP 800-53
- Оценка угроз по матрице MITRE ATT&CK

## ОТ-стандарты

- IEC 62443
- NIST SP 800-82

# Комплексный подход к СОИБ АСУ ТП

## Обследование

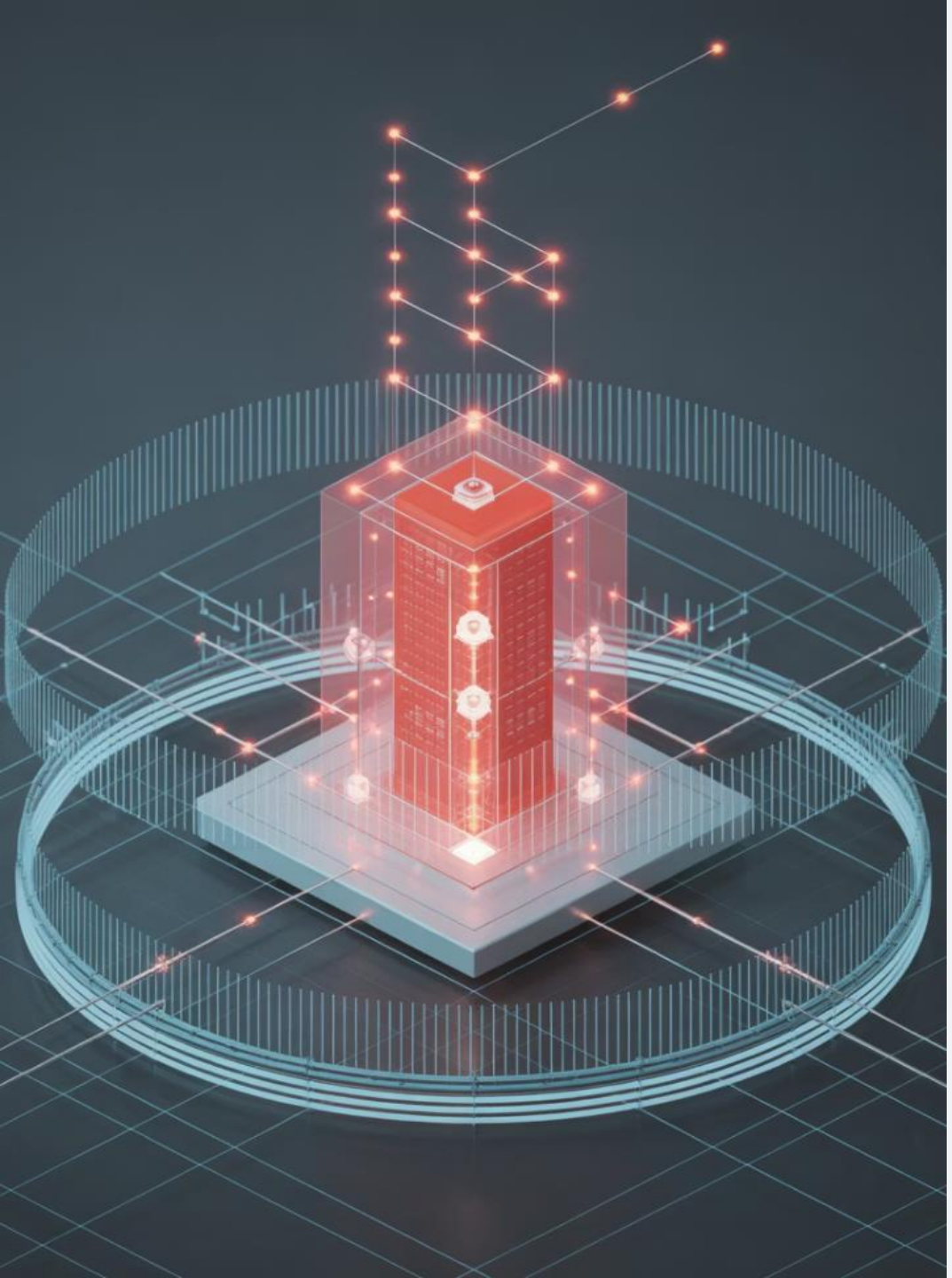
- Инвентаризация, аудит активов в АСУ ТП
- Оценка текущего состояния ИБ
- Определение рисков и угроз ИБ
- Определение требований к системе

## Проектирование СОИБ

- Разработка концепции СОИБ
- Разработка технического проекта
- Оценка нейтрализации актуальных угроз средствами защиты информации
- Разработка РД, ЭД, ПМИ, ОРД

## Внедрение СОИБ

- Настройка встроенных механизмов защиты ОС, АСО, ПЛК, прикладного ПО
- Настройка наложенных средств защиты информации
- Сканирование на уязвимости ОС, АСО, компонентов АСУ ТП и СОИБ, прикладного ПО
- Устранение выявленных уязвимостей или выработка и реализация компенсирующих мер
- Комплексные испытания СОИБ
- Сопровождение и техническая поддержка СОИБ



# Схема развертывания защиты

## Защита на уровне сети

- Обнаружение устройств в ТСПД, учет активов и анализ телеметрии
- Контроль целостности сетевой инфраструктуры
- Мониторинг команд и промышленных протоколов
- Защита сетевого периметра АСУ ТП
- Контроль взаимодействия со смежными системами
- Сегментирование сетей, проектирование и реализация ДМЗ

## Защита конечных устройств

- Антивирусная защита
- Настройка политик безопасности и прав доступа
- Управление подключением устройств
- Аудит действий пользователей и процессов в системе
- Резервное копирование информации

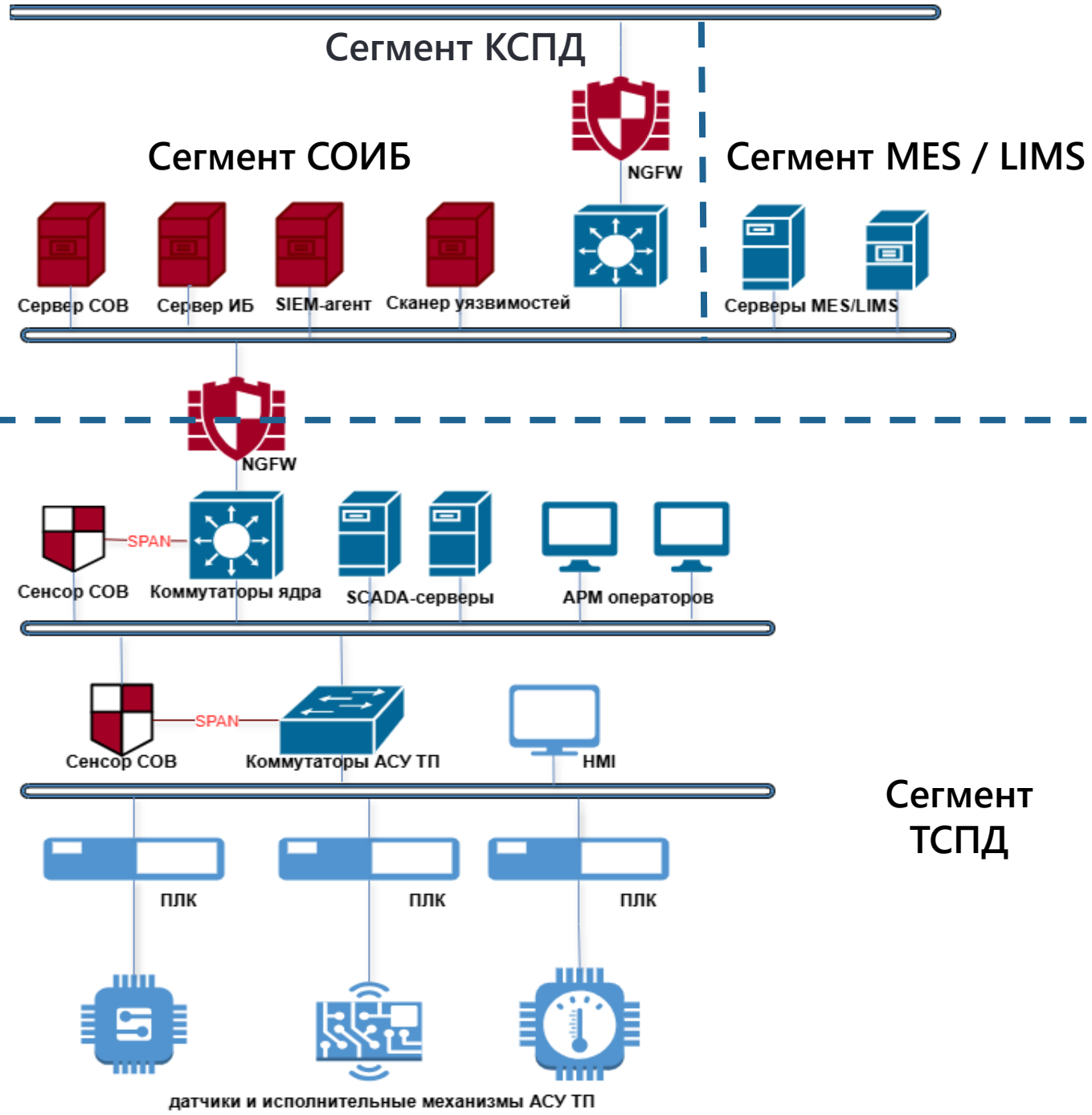
# Типовая архитектура сети
## промышленного предприятия

Демилитаризованная зона

ЛВС верхнего уровня

ЛВС среднего уровня

Сети связи нижнего уровня



# Общий состав СОИБ АСУ ТП

## Технические решения

### Сетевая безопасность

- Сегментирование сети (Routing & Switching)
- Межсетевое экранирование (Firewall, NGFW)
- Криптографическая защита каналов связи (Site-to-site VPN, TLS VPN, Remote Access VPN)

### Защита технологического сегмента

- Решения для обеспечения безопасности на уровне сетевых шлюзов (NTA)
- Решения для расширенного обнаружения и реагирования на угрозы (EDR)
- Резервное копирование

### Анализ вредоносного ПО и файлов

- Защита от известного вредоносного кода (антивирусная защита)
- Анализ неизвестных и целевых угроз (Anti-APT)

### Анализ событий ИБ и реагирование на инциденты

- Система сбора и анализа событий ИБ (SIEM)
- Система обеспечения процессов реагирования на инциденты ИБ (IRP)
- Система автоматизации, обработки и реагирования на инциденты (SOAR)

# Сетевая безопасность в АСУ ТП

## Основные функции

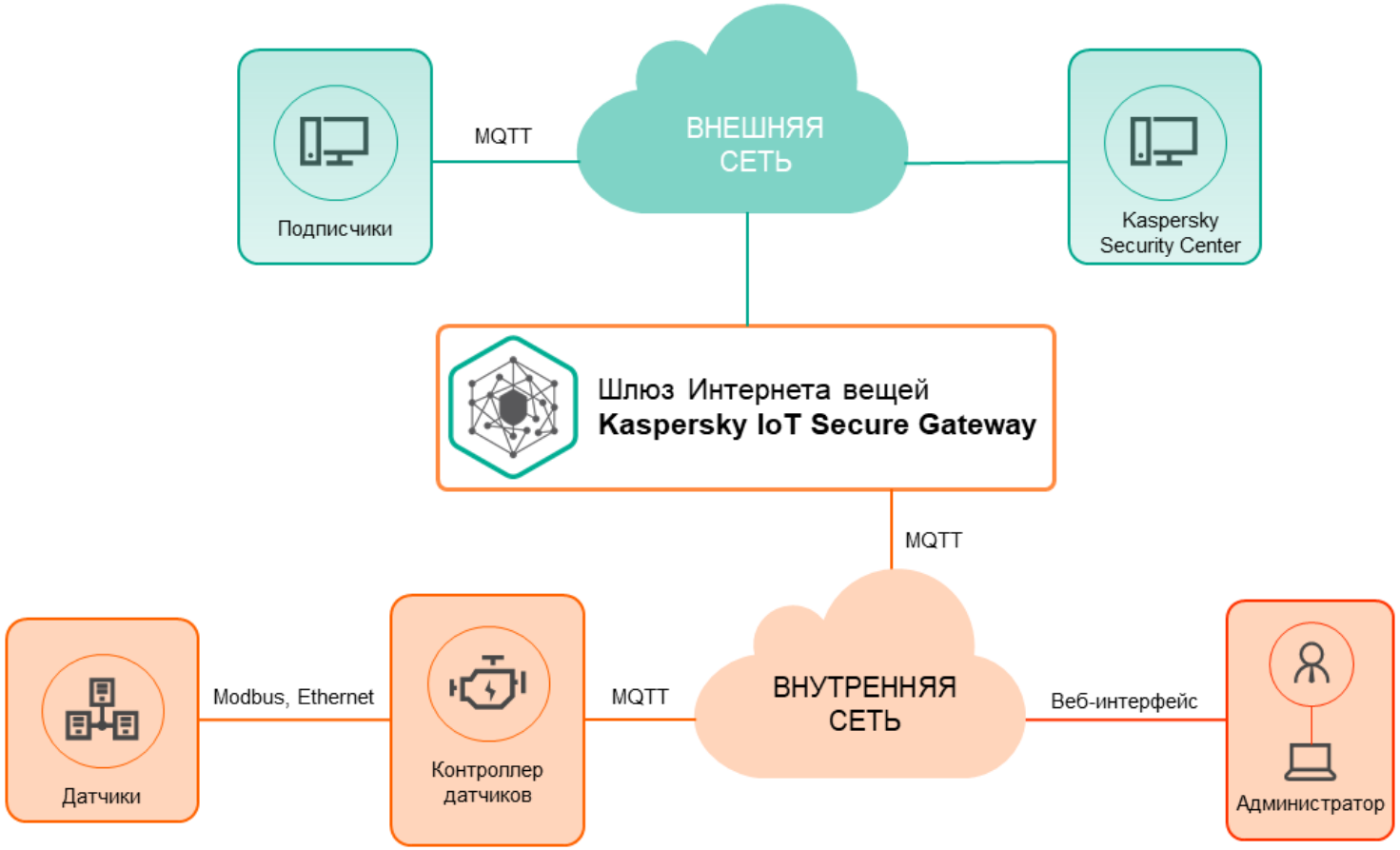
- Шифрование данных VPN с ГОСТ и не-ГОСТ алгоритмами
- Аутентификация и контроль доступа, включая 2FA
- Межсетевое экранирование и контроль сетевых потоков
- Защита от НСД и MITM-атак
- Контроль целостности данных защита от подмены команд и показаний
- Совместимость с промышленными протоколами IEC 60870-5-101/104, Modbus, DNP3, OPC UA и др.

## Применение в SCADA

- Защита каналов связи между RTU и диспетчерскими центрами
- Обеспечение безопасного удаленного доступа для инженеров и администраторов
- Защита от кибератак на критическую инфраструктуру
- Безопасная передача данных с датчиков и концентраторов в центры обработки данных
- Защита от фрода, искажение показаний, перехват данных

# Защита систем сбора телеметрии

## Kaspersky IoT Secure Gateway




### Типовая схема внедрения Kaspersky IoT Secure Gateway

- Датчики передают телеметрические данные (Пр. по протоколу Modbus) на контроллер датчиков
- Контроллер датчиков публикует данные измерений во внутреннюю сеть в виде MQTT-топиков
- Шлюз Интернета вещей получает MQTT-топики и передает их подписчикам (как правило, серверы получения и визуализации данных) во внешней сети

### Функции передачи данных и безопасности KISG

- Диод данных
- Роутер, межсетевой экран, IPS/IDS, DPI, VPN, TLS
- Брокер MQTT
- 3G/LTE

# Защита промышленных систем

## Защита конечных устройств

- Антивирусная защита с минимальным влиянием на работу датчиков, контроллеров и серверов
- Контроль устройств (USB, периферия) – предотвращение заражения через внешние носители
- Защита от эксплойтов (вредоносных скриптов, атак на уязвимости ПО)
- Белые списки приложений – разрешает только доверенное ПО

## Защита ТСПД

- Анализ сетевого трафика (Пр. несанкционированные подключения)
- Обнаружение атак на технологические протоколы (Modbus, DNP3, IEC 60870-5-104)
- Защита от MITM-атак (подмена данных в передаваемых пакетах)

## Применение в АСУ ТП

- Установка на серверы сбора телеметрии и обработки данных
- Защита рабочих станций операторов
- Контроль целостности ПО (если поддерживается ОС)

Решения:
**KES/KEDR/KATA, KICS, Nozomi, McAfee, Symantec**

## Применение в АСУ ТП

- Мониторинг каналов связи (Ethernet, PLC и другие)
- Выявление подозрительных команд (пример: несанкционированное изменение параметров)

Решения:
**KICS, ISIM, Nozomi, Check Point, Fortinet, Cisco**

# Использование решений классов Sandbox и EDR

**Обнаружение сложных атак**

- Применение ML, анализа поведения и сигнатурных методов для выявления APT и целевых атак

- **Минимизация ложных срабатываний**
- Алгоритмы адаптированы для работы в промышленных средах, где критически важна стабильность

- **Защита от zero-day угроз**
- Выявление неизвестных угроз на основе аномального поведения в системе

- **Интеграция с SIEM и SOAR**
- Передача данных для корреляции событий и автоматизации реагирования через API.

# Сценарии использования KATA и EDR Expert для защиты SCADA

## 1

### Блокировка атак

KATA выявляет аномалии, EDR Expert отслеживает путь атаки, вредоносное ПО блокируется, заражённый узел изолируется

## 2

### Защита от подмены

KATA выявляет несанкционированные изменения, EDR Expert определяет источник атаки, изменения автоматически откатываются

## 3

### Реагирование на инсайдеров

KATA фиксирует подозрительные действия, EDR Expert анализирует цепочку событий, сессия блокируется, SOC уведомляется

## 4

### Борьба с шифровальщиками

KATA останавливает атаку на раннем этапе, EDR Expert определяет точку входа, система восстанавливает данные из резервных копий

# Защита рабочих мест операторов и серверов SCADA

## 1

### Защита от вредоносного ПО

Гибкое обнаружение
Минимизация ложных срабатываний

## 2

### Контроль устройств и приложений

Белые списки ПО
Блокировка несанкционированных USB-устройств

## 3

### Защита серверов обработки данных

Защита виртуальных сред (VMware, Hyper-V)
Контроль целостности файлов (конфигураций)

## 4

### Удобное централизованное управление

Единая консоль управления
Поддержка air-gapped сетей

# Сценарии использования АВПО для защиты SCADA

| Сценарий | Угроза | Как предотвращается угроза |
|---|---|---|
| Защита рабочих мест операторов | Атака → заражение ПК оператора → распространение на SCADA | Блокируются вредоносные вложения, предотвращается запуск подозрительных процессов, изолируется зараженный узел |
| Блокировка несанкционированного программного обеспечения | Оператор устанавливает постороннее ПО → потенциальная уязвимость в системе | АВПО разрешает только ПО из белого списка, блокирует запуск посторонних программ |
| Защита виртуальных серверов | Вирус в одной виртуальной машине → заражение всей инфраструктуры | АВПО сканирует виртуальные машины без нагрузки на хост, изолирует зараженные ВМ |

# Мониторинг и реагирование на угрозы ИБ

**Мониторинг сети**

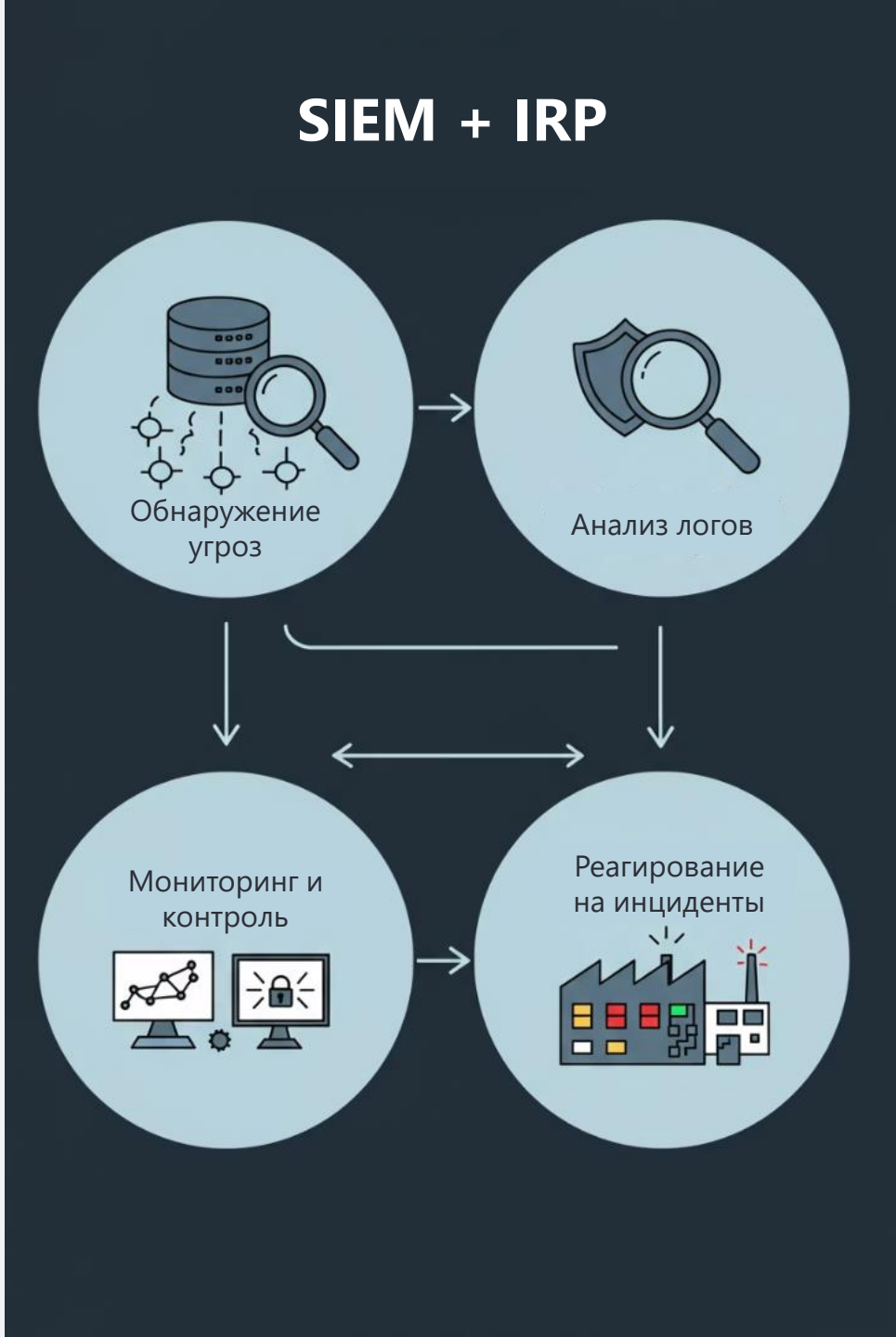
- Анализ трафика между счетчиками и серверами
- Обнаружение атак на протоколы (Modbus/DNP3)

**Базовая функциональность SIEM**

- Сбор и анализ журналов событий с серверов
- корреляция событий
- Возможность детектирования аномалий

**Централизованный контроль и расследование**

- Интеграция с наложенными СЗИ
- Автоматическое выявление и блокирование угроз
- Реагирование на инциденты, расследование инцидентов



# Автоматизация реагирования на инциденты (SOAR)

## Автоматизация реагирования

SOAR автоматизирует рутинные действия, такие как блокировка IP, отключение подозрительных сессий и запуск скриптов, что значительно сокращает время реакции на инциденты.

## Оркестрация процессов безопасности

Интеграция с SIEM позволяет агрегировать данные из различных источников и запускать скоординированные сценарии реагирования на угрозы.

## Ускорение расследования инцидентов

SOAR помогает аналитикам быстрее выявлять угрозы, предоставляя готовые playbook (сценарии реагирования) для типовых ситуаций.

# Сценарии использования SOAR + SIEM для SCADA

1

## Обнаружение и блокировка атак

SIEM обнаруживает подозрительные команды Modbus/DNP3, SOAR автоматически блокирует источник атаки через межсетевой экран или отключает затронутый контроллер, уведомляет администратора и запускает процедуру восстановления.

2

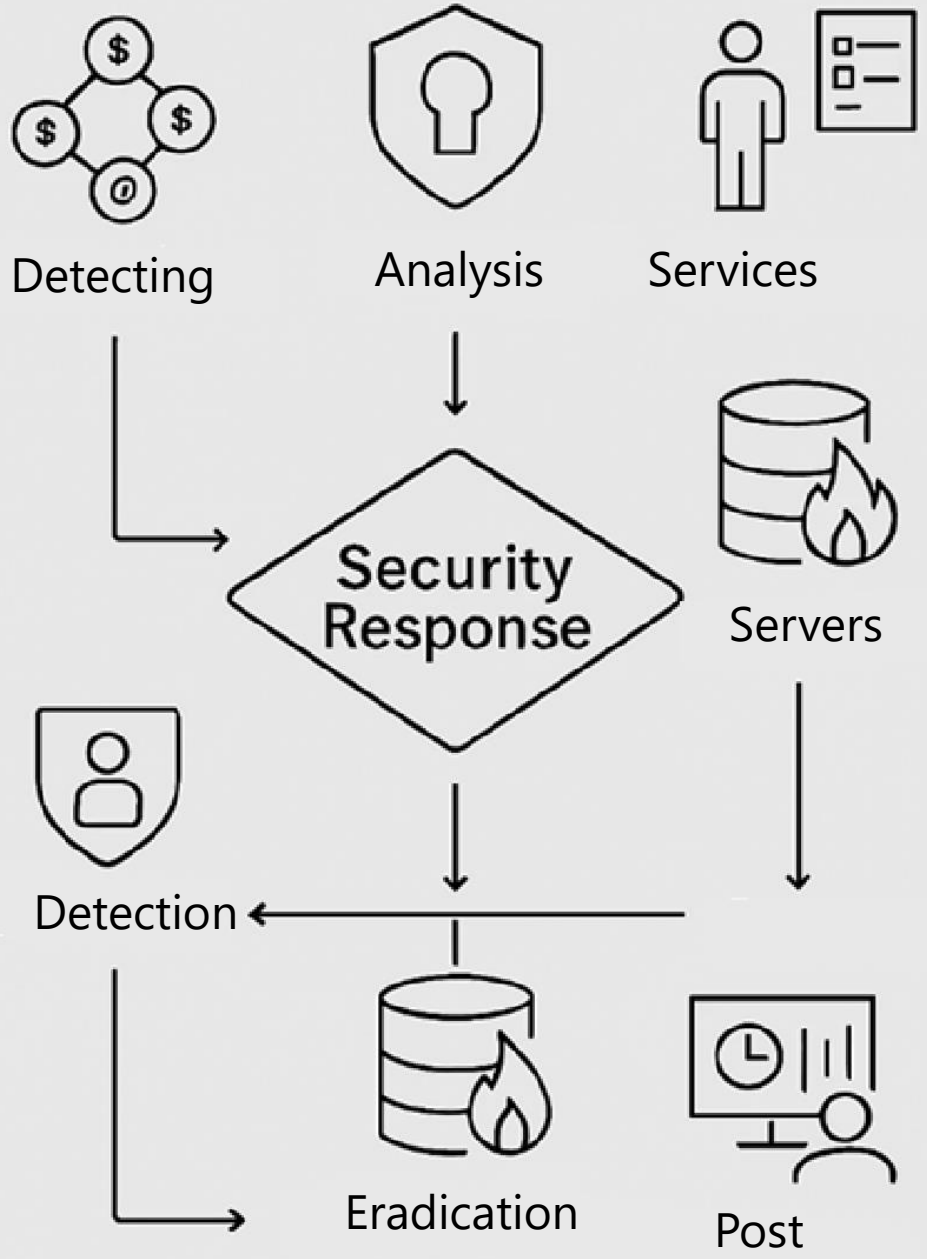
## Защита от манипуляций с данными

SIEM фиксирует аномалии в передаче данных, SOAR проверяет данные с резервных источников и инициирует аварийный режим работы. При подтверждении атаки SOAR блокирует подозрительные соединения и запускает расследование.

3

## Реагирование на инсайдерские угрозы

SIEM обнаруживает подозрительные действия, SOAR приостанавливает сессию, запрашивает подтверждение у вышестоящего сотрудника и фиксирует действия для аудита.



# Возможные результаты

- ✓ Выявление и предотвращение атак на сетевую и серверную инфраструктуру АСУ ТП, влекущих реализацию недопустимых для бизнеса событий
- ✓ Снижение поверхности атаки и вероятности реализации угроз АСУ ТП путем сокрытия топологии сети, межсетевого экранирования, применения средств защиты конечных точек
- ✓ Исключение вмешательства в каналы передачи конфиденциальной информации путем применения СКЗИ для их криптографической защиты
- ✓ Централизованные выявление и контроль угроз на разных уровнях сети
- ✓ Ускорение реагирования на инциденты ИБ путем автоматизации процесса реагирования

# Используемые средства защиты

| Класс решения | Российские | Иностранные |
|---|---|---|
| **Антивирусное ПО** | Kaspersky, Dr. Web | Symantec, McAfee |
| **Резервное копирование** | Кибербэкап, RuBackup | Acronis, Veeam |
| **Промышленные СОВ** | Kaspersky, Positive Technologies | Nozomi networks |
| **Промышленные NGFW** | InfoWatch, UserGate, ИнфоТеКС, и др. | Check Point, Cisco, Fortinet |
| **Сканеры уязвимостей** | Positive Technologies, Алтекс Софт | Tenable, SolarWinds |
| **SIEM-системы** | Kaspersky, Positive Technologies | Hewlett Packard Enterprise, IBM |

# Демонстрационная инфраструктура

## Собственная инфраструктура

Компания располагает комплексной стендовой инфраструктурой для тестирования и демонстрации

## Демонстрация интерфейсов

Возможность ознакомления с пользовательскими интерфейсами всех представленных решений

## Принципы работы

Демонстрация технических принципов функционирования систем защиты в реальном времени

## Представленные решения

KICS for Nodes, KICS for Network, PT ISIM, IW ARMA и другие продукты

# Процесс пилотирования решений

**Формирование требований**

Определение критериев успешности и результатов пилота

**Разработка методики**

Создание ПМИ с учетом специфики предприятия

**Демонстрация возможностей**

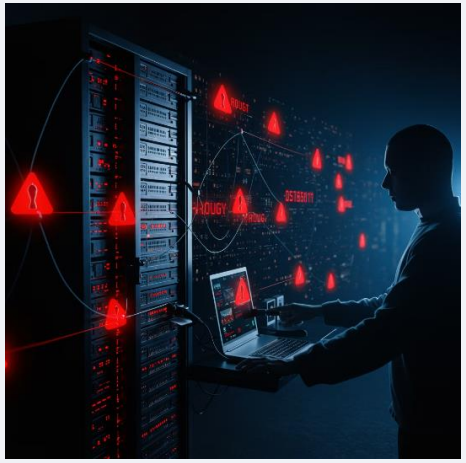
Наглядная демонстрация функций решений в условиях, близких к реальным

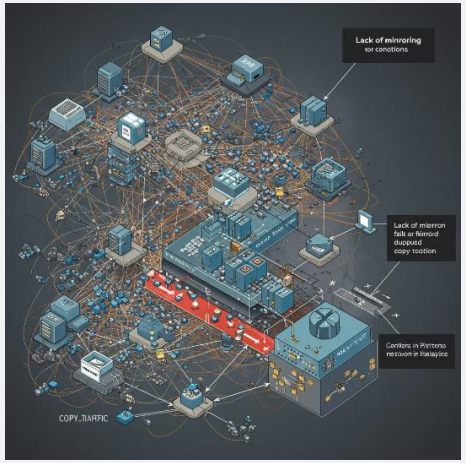
**Формирование отчета**

Подготовка детализированного отчета по результатам

**Внедрение**

Качественный переход от пилота к полномасштабной реализации проекта



# Проектный опыт в различных отраслях промышленности

- Нефтегазовая
- Энергетика
- Химическая
- Атомная энергетика
- Машиностроение
- Металлургия
- Умные города
- Транспорт
- Пищевая

# Газодобывающее предприятие

### Пересмотр проектных решений

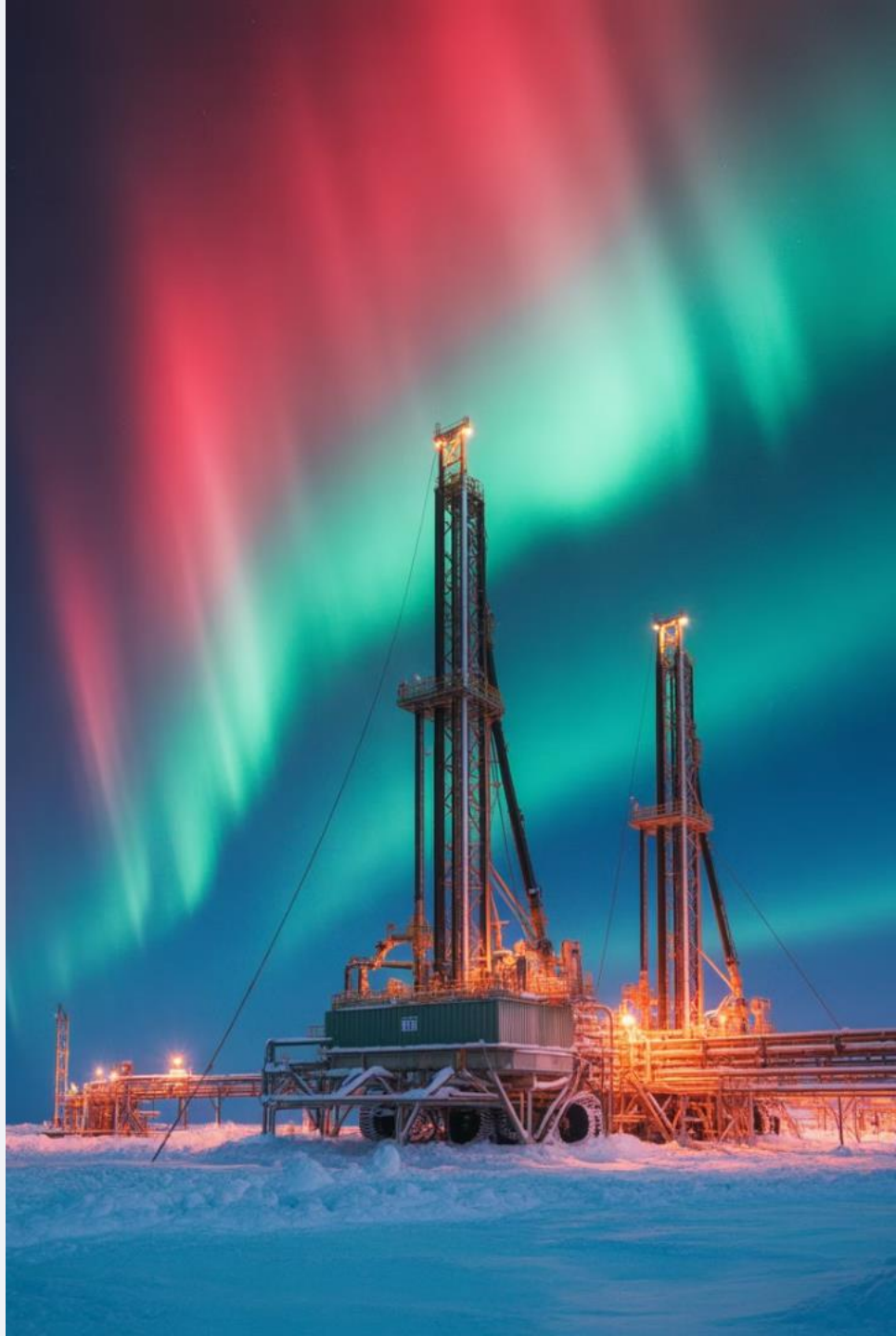
Исправление ошибок сторонних подрядчиков по АСУ, ИТ, ИБ

### Внедрение комплекса СЗИ

Сегментация и организация VPN между удаленными площадками

### ПНР в условиях крайнего севера

Выстраивание сложных логистических цепочек доставки



# Металлургические компании

### Проект 1

Проектирование СОИБ ЗОКИИ, прокладка ВОЛС, внедрение СЗИ АСУТП

Подключение к корпоративному SOC

### Проект 2

Комплексный проект КИИ: пересмотр проектных решений по обеспечению ИБ ОКИИ производства

Включение в корпоративный SOC

### Используемые решения

UserGate NGFW, Astra Linux, Red-Виртуализация, CheckPoint SG, Efros CI, PT MP SIEM

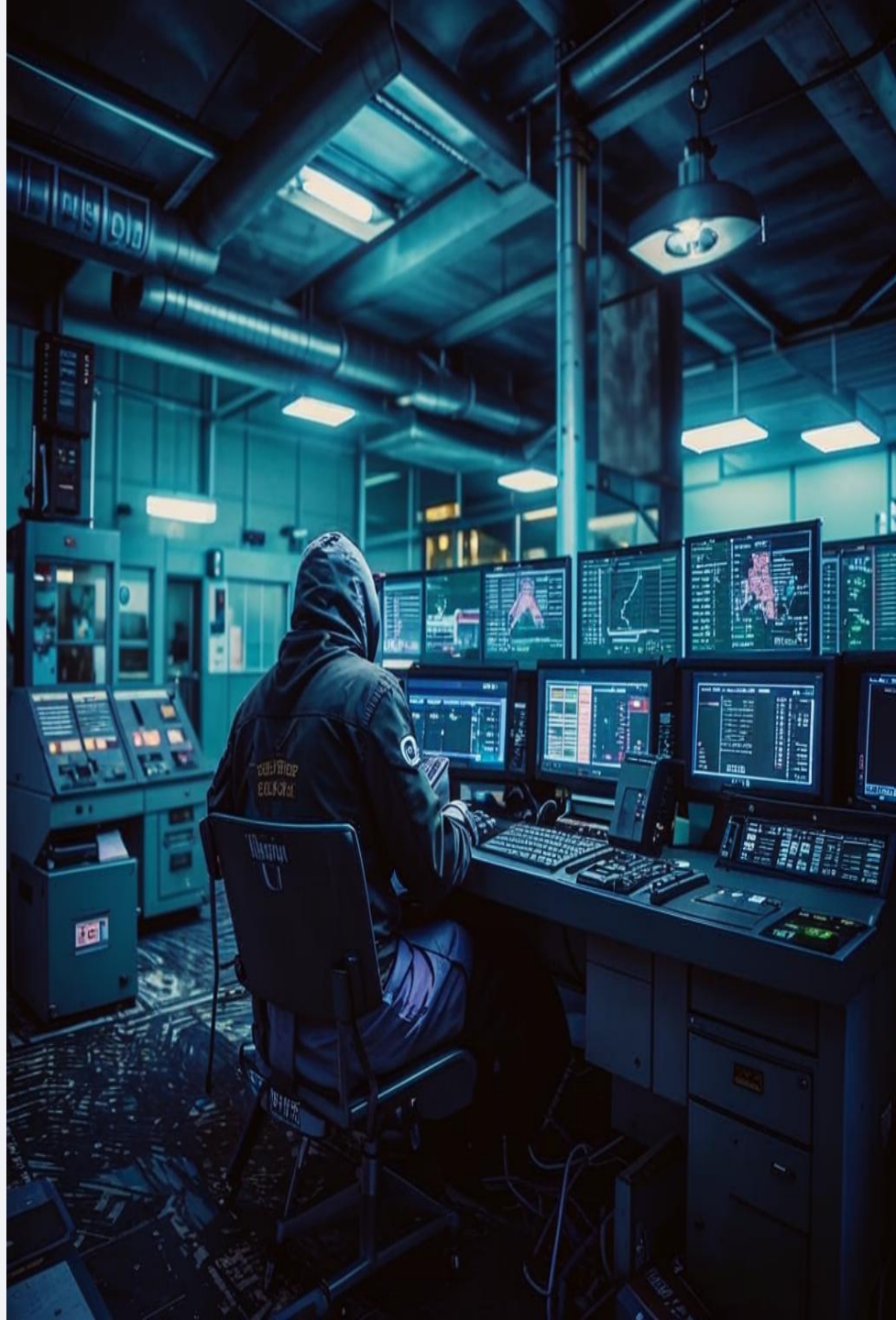
# Минерально-химическая компания

## Реорганизация сети предприятия на 2-х площадках

Разработка проектного решения по безопасному взаимодействию между КСПД и ТСПД

## Внедрение комплекса СЗИ

Сегментация сети АСУ ТП, установка средств защиты на конечных устройствах



# Нефтехимический холдинг

### Проект 1

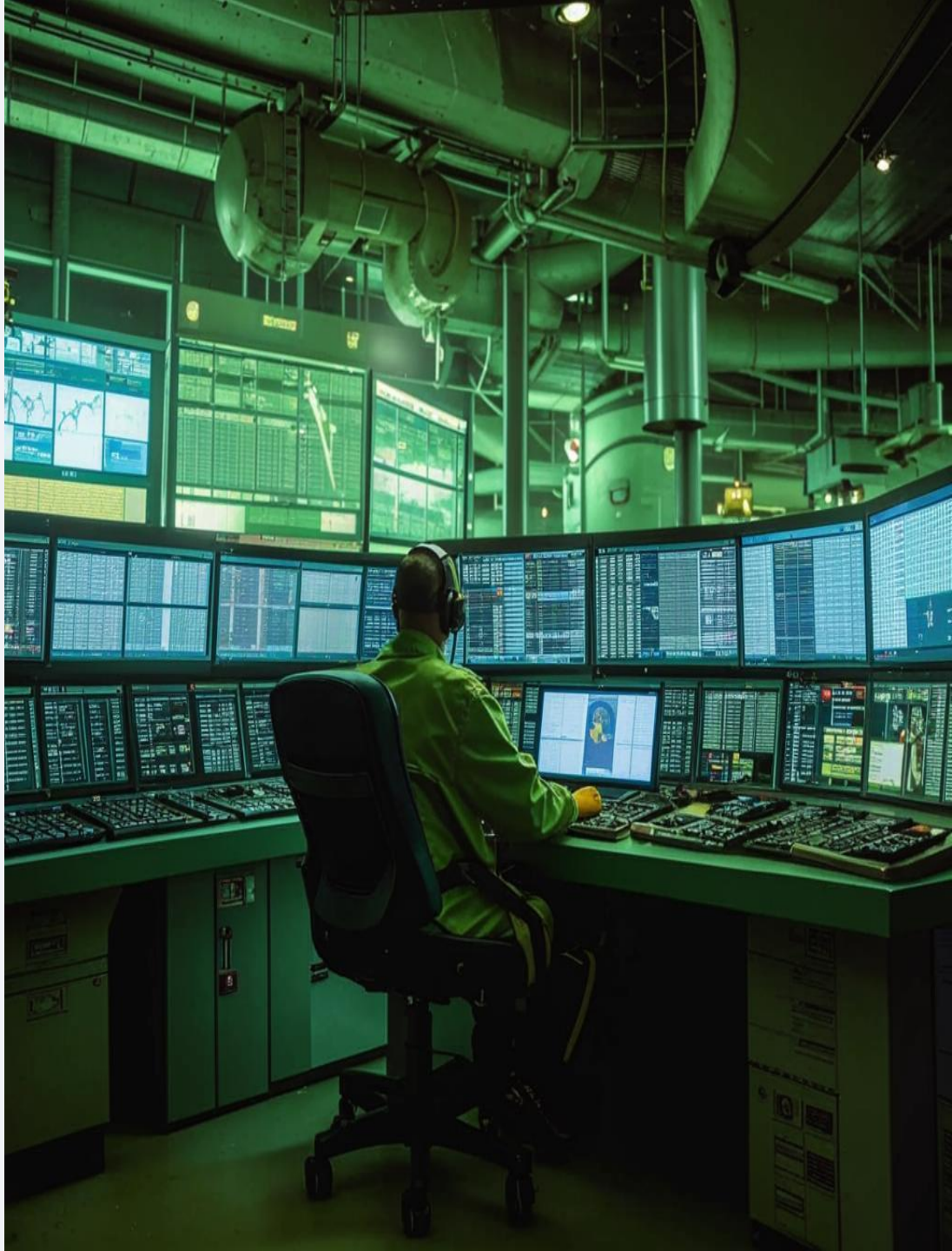
Проектирование централизованной СОИБ ОКИИ, внедрение СЗИ АСУТП

### Проект 2

Проектирование централизованной СОИБ 26-ти АСУ ТП

### Используемые решения

InfoWatch ARMA, С-Терра Шлюз, Astra Linux, Zvirt Макс, Кибер Бэкап, KICS for Nodes, RedCheck, UDV ITM, WNAM



# Химическое предприятие

**Проект 1**

Проектирование комплексной СОИБ ОКИИ предприятия

**Проект 2**

Проектирование DMZ-зоны и системы защиты периметра АСУ ТП

Прокладка ВОЛС, внедрение проектных решений

**Проект 3**

Проектирование и внедрение промышленной системы обнаружения вторжений на верхнем и среднем уровнях АСУ ТП

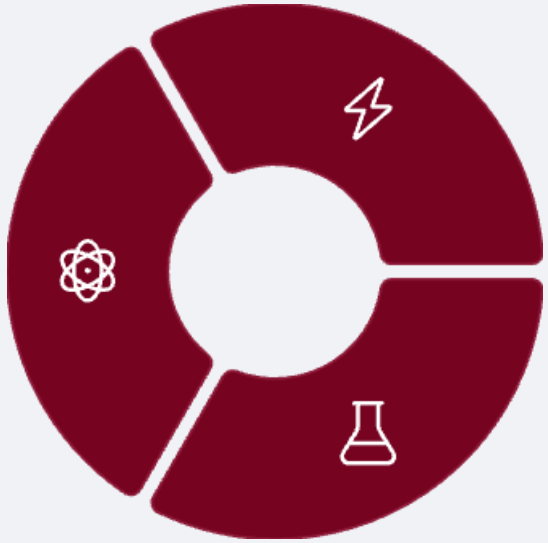
**Используемые решения**

UserGate, MP SIEM, MP VM, KICS for Nodes, KICS for Networks, Кибер Бэкап

# Атомное производство и энергетика

**Атомное производство**

СОИБ АС оперативного диспетчерского управления технологическим процессом переработки ядерного топлива



**Энергосбытовая компания**

Аудит, категорирование ОКИИ на 30 площадках. Внедрение комплекса СЗИ

**Химическая компания**

Категорирование 50+ ОКИИ, проектирование СОИБ ЗОКИИ 1/2/3 категорий


Q&A