КОНФИДЕНТ®
ИНТЕГРАЦИЯ

ПРАКТИКА РЕАЛИЗАЦИИ МЕР ПО ЗАЩИТЕ ОКИИ
Ошибки. Опыт. Решения

Зенков Александр Александрович
Руководитель инженерно-технического департамента
Технический директор

Опыт применения СрЗИ при защите КИИ

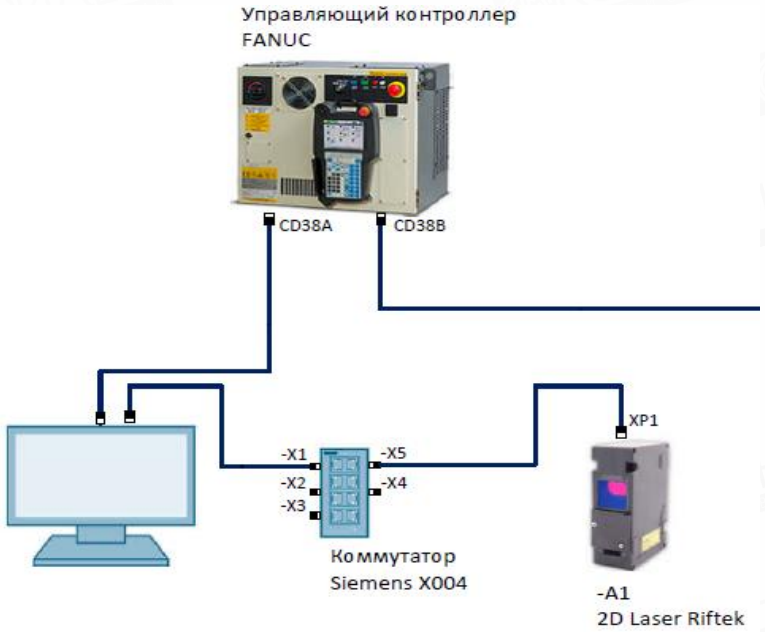
Меры обеспечения безопасности значимого объекта	Продукт
I. Идентификация и аутентификация (ИАФ)	Dallas Lock, SecretNet, KICS For Networks, JMS, встроенные компоненты ОС или SCADA
II. Управление доступом (УПД)	ОРД, Dallas Lock, SecretNet, JMS, Аккорд, Соболь, VPN, встроенные компоненты ОС или SCADA
III. Ограничение программной среды (ОПС)	ОРД, KICS for Nodes, Kaspersky Security Center
IV. Защита машинных носителей информации (ЗНИ)	Dallas Lock, SecretNet, DLP, KICS for Nodes, KSC
V. Аудит безопасности (АУД)	ОРД, KICS for Nodes, KSC, staffcop, Стахановец, TimeInformer, FalconGaze SecureTower, SpectorSoft, RedCheck, MaxPatrol 8, MaxPatrol SIEM, ViPNet IDS, СОА «Континент», АПК «Рубикон», RedCkeck, Сканер-ВС
VI. Антивирусная защита (АВЗ)	ОРД, антивирусы, KICS for Nodes/KICS for Networks
VII. Предотвращение вторжений (компьютерных атак) (СОВ)	ОРД, ViPNet IDS, СОА «Континент», UserGate, KICS for Nodes/KICS for Networks
VIII. Обеспечение целостности (ОЦЛ)	ОРД, KICS for Nodes, KICS for Networks, TimeInformer, FalconGaze SecureTower, SpectorSoft, встроенные компоненты ОС или SCADA
IX. Обеспечение доступности (ОДТ)	ОРД, КиберБекап

Опыт применения СрЗИ при защите КИИ

X. Защита технических средств и систем (ЗТС)	ОРД, СКУД, ИБП
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)	ОРД , СКУД, МЭ, KICS for Nodes / KICS for Networks, KES, TraficInspector, UserGate, Dallas Lock, SecretNet, UserGate, ФПСУ-IP, Континент, Застава, VipNet, VPN Gate, ФПСУ-IP, Дионис, MP ISIM
XII. Реагирование на компьютерные инциденты (ИНЦ)	ViPNet IDS/IPS, СОА «Континент», АПК «Рубикон», АМЭ ALTELL NEO, СОВ Dallas Lock, KSC, MaxPatrol SIEM, R-Vision IRP
XIII. Управление конфигурацией (УКФ)	ОРД, KICS for Nodes / KICS for Networks, KES, KSC
XIV. Управление обновлениями программного обеспечения (ОПО)	ОРД , Dallas Lock, SecretNet, KSC
XV. Планирование мероприятий по обеспечению безопасности (ПЛН)	ОРД
XVI. Обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС)	ОРД, резервное копирование, кластеризация
XVII. Информирование и обучение персонала (ИПО)	ОРД

Виды объектов, которые приходилось защищать

Информационные системы



АСУ ТП

Информационно-телекоммуникационные сети

Информационные системы

1. Программное обеспечение
2. Оконечные АРМ
3. Серверы

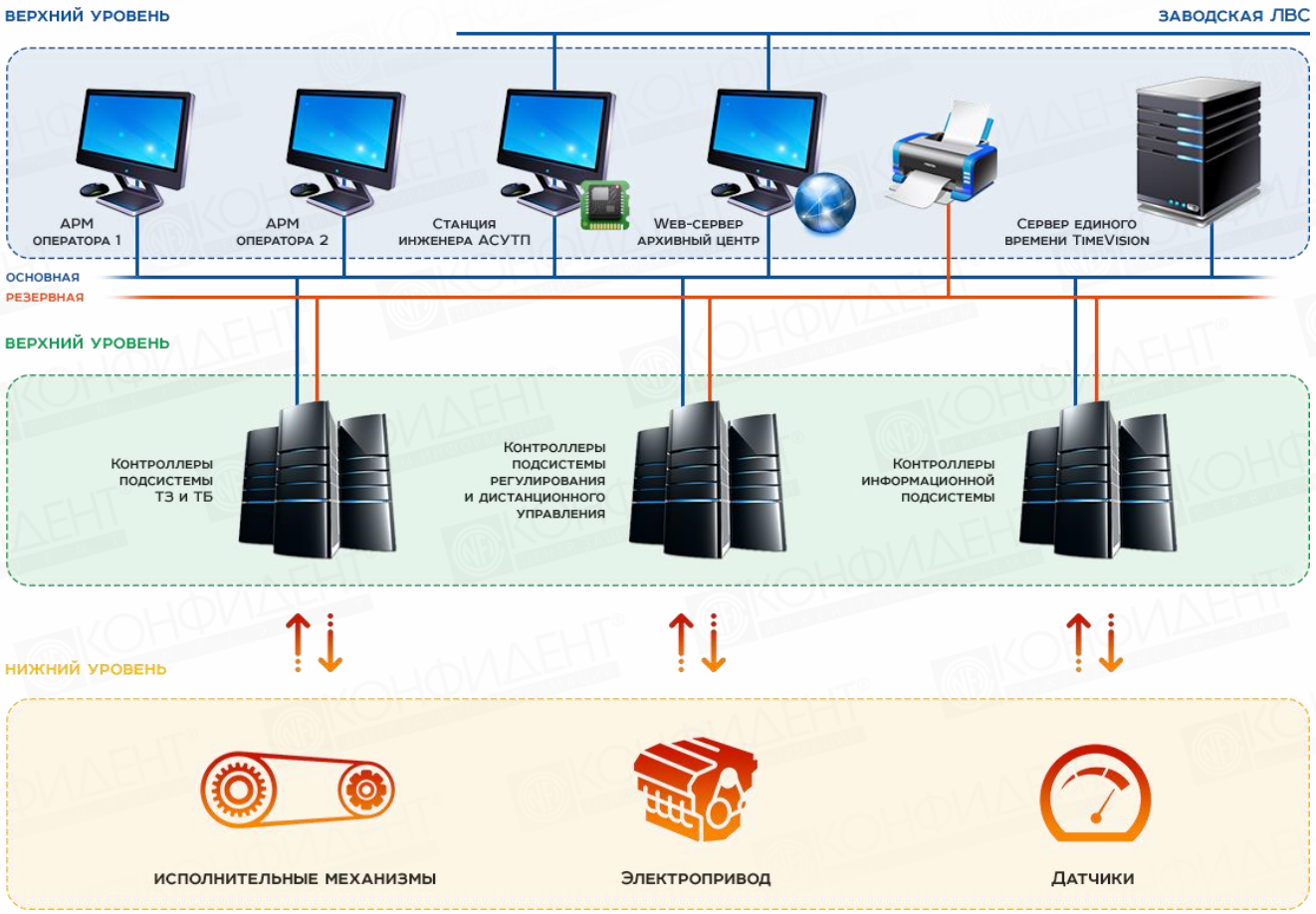
Система анализа защищенности
Система обнаружения вторжений
Система защиты от НСД
Система антивирусной защиты

Информационно-телекоммуникационная сеть

1. Сетевое оборудование
2. Трафик
3. Общая целостность и неизменность компонентов

IDS/IPS
Антивирусная защита
Анализ трафика
МЭ
Сегментирование сети
Обеспечение защиты от НСД

АСУ ТП

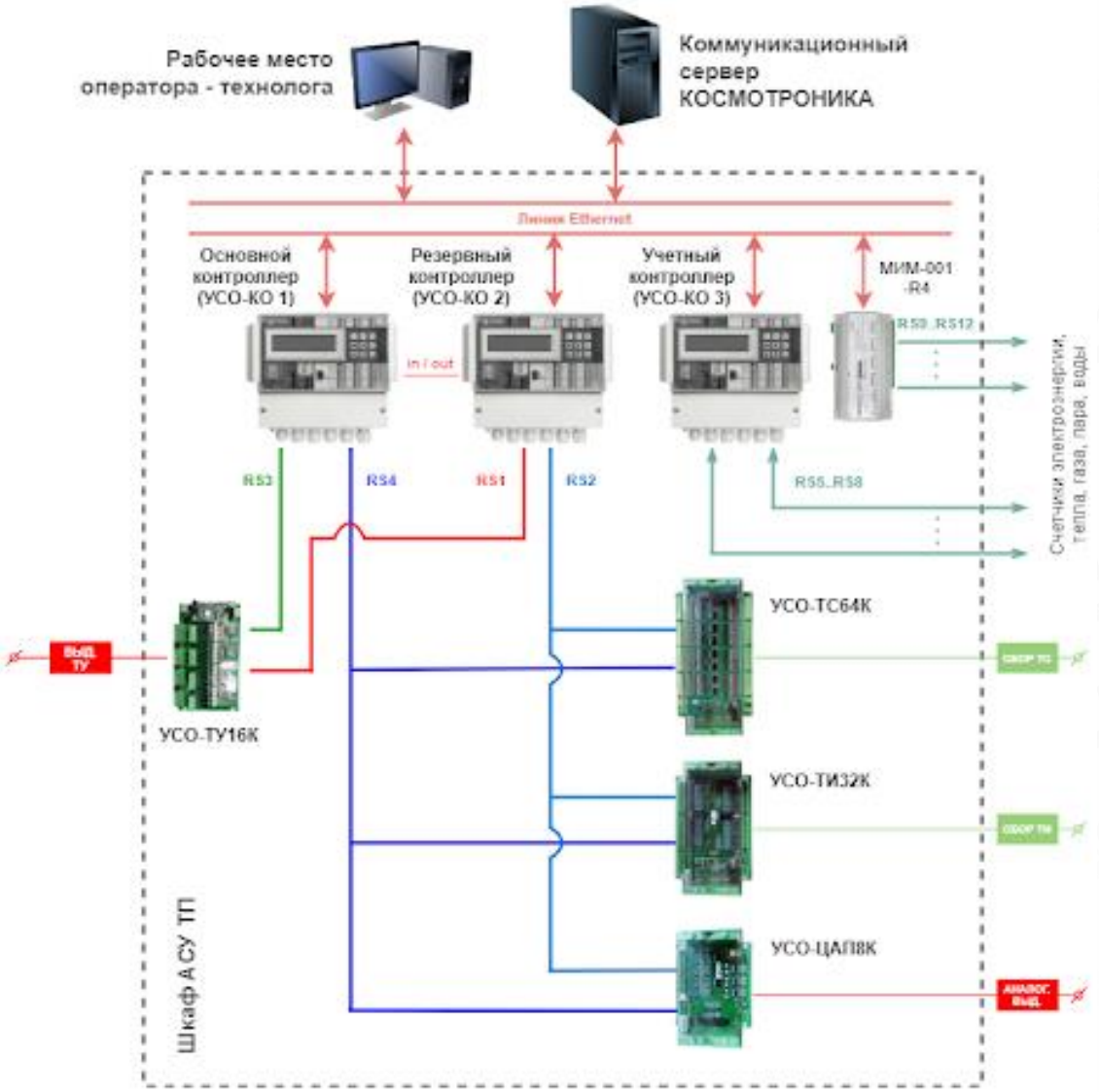


1. Трафик
2. Прошивка ПЛК
3. АРМ инженеров
4. Различное оконечное оборудование
5. Теги, передаваемые с датчиков

Анализ трафика
Антивирусная защита
Сегментирование ТЛВС

Автономные АСУ ТП

Компенсирующие меры



Основные проблемы

1. Неверное определение категории
2. Субъективная трактовка требований законодательства
3. Непонимание выбора средств защиты
4. **Разрозненность подразделений – ИБ, ИТ, АСУ**
5. Устаревшее оборудование
6. Импортозамещение
7. Спустя 6 лет находятся организации, которые еще даже не категорировались

Неверное определение категории

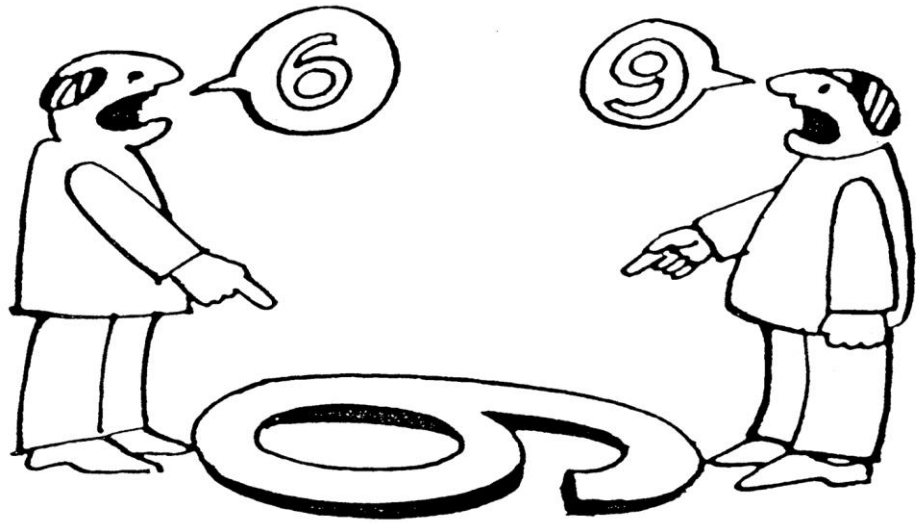
Были выявлены крайности:

1. Нет вообще ЗОКИИ, либо все ЗОКИИ 1 категории
2. Категорировалось абсолютно все, либо явно замалчивали об очевидном объекте

Субъективная трактовка требований

Примеры:

1) Аудит безопасности полностью закрывается SIEM-системой
2) Установка классического АВЗ на технологические ОИ
3) Все требования должны исполняться исключительно СрЗИ



Непонимание выбора средств защиты

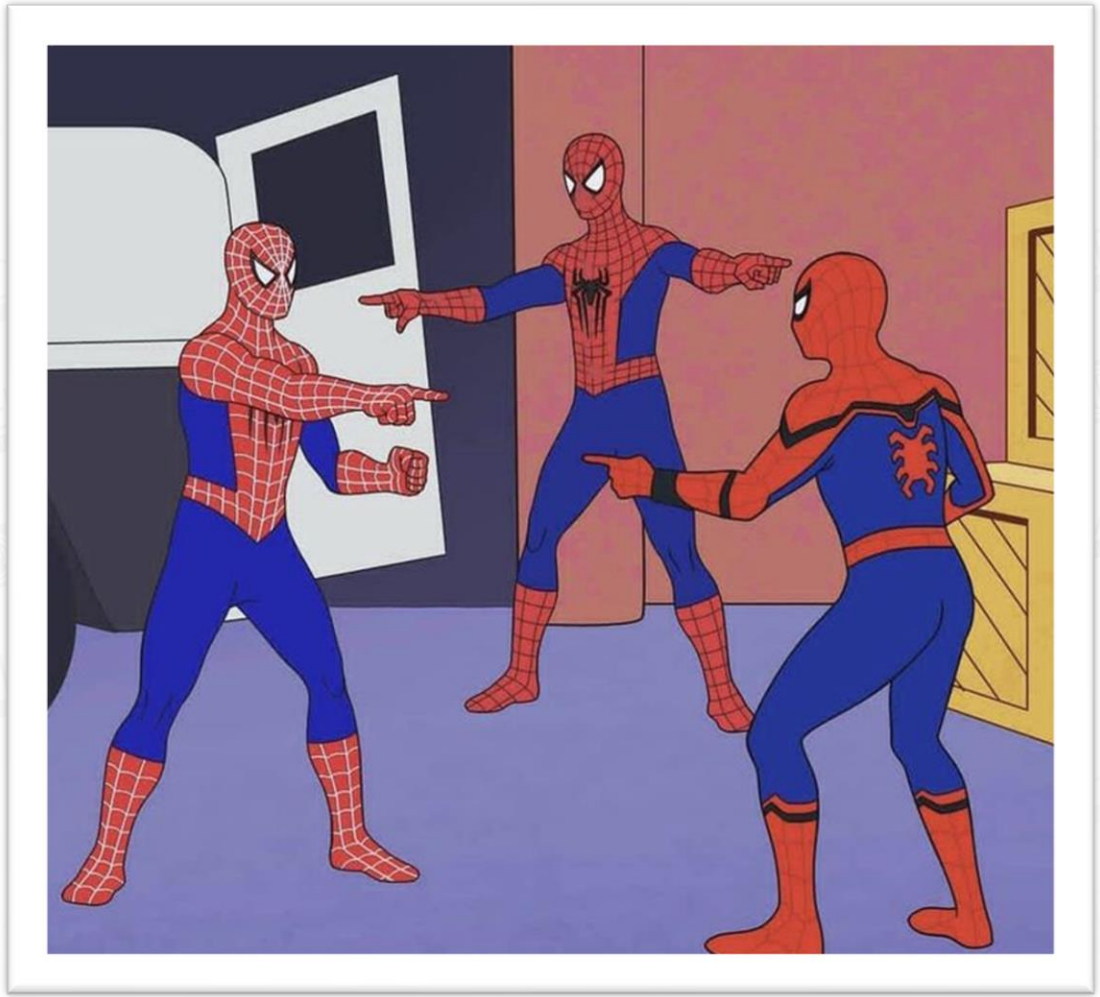
Закон начал действовать в 2018 году.
До этого, в части предприятий, перед ОИБ стояли задачи:

1) По защите ПДн.
2) По организации защиты ГТ.
3) По закупке и обновлению АВЗ.

После начала действия закона ОИБ требовалось очень быстро прокачаться в более сложных или вовсе новых областях по защите ОИ.

Разрозненность подразделений – ИБ, ИТ, АСУ

Классическая проблема при взаимодействии на большом предприятии подразделений ИБ, ИТ, АСУ



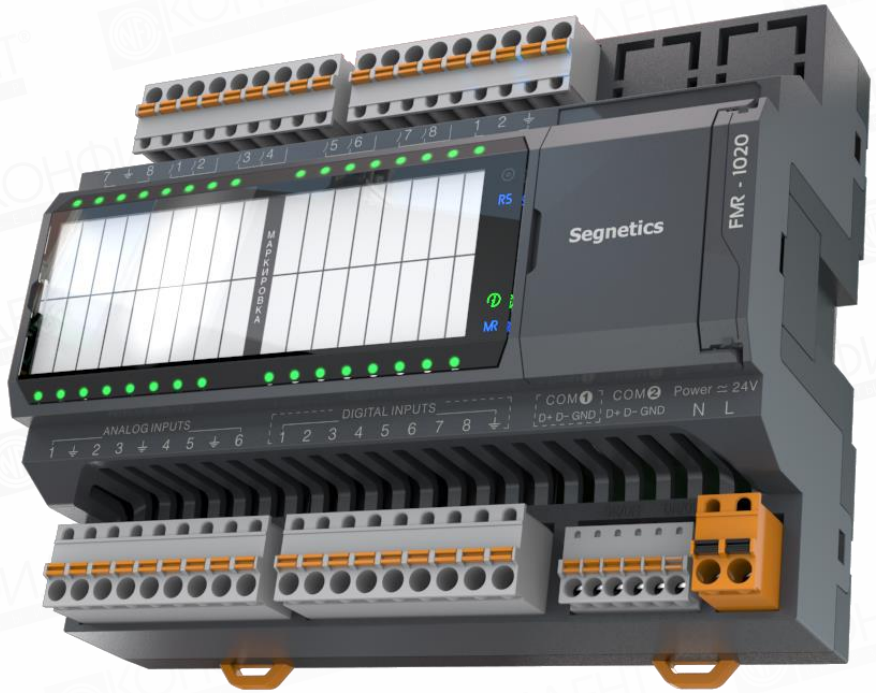
Устаревшее оборудование

Старое технологическое сетевое оборудование не поддерживает Ethernet или SPAN/R-SPAN

Импортозамещение

Большая проблема с переходом с Siemens, Schneider, Emerson, Segnetics и пр. на отечественные решения

<u>Что радует – работа ведется</u>



Бездействие

Закон был анонсирован в 2017 г., издан в 2018 г., выполнить нужно было в 2020 г.

Сейчас 2024 г., и до сих мор много кто еще даже не провел категорирование.

Возможно пропустили

Указ Президента РФ от 08.11.2023 № 846. Новые полномочия ФСТЭК

- Создание ИС для управления ТЗИ и обеспечению безопасности ЗОКИИ.
- Осуществление учета ИС и ОКИИ.
- Осуществление мониторинга текущего состояния ТЗИ и обеспечение безопасности ЗОКИИ.
- Информирование об угрозах ИБ и уязвимостях, а также о мерах защиты от них.
- И пр.

Приказ ФСТЭК России от 20.04.2023 № 69

- Допускается привлечение специалистов со средним профессиональным образованием в области безопасности для обеспечения безопасности ЗОКИИ.

Помощь регуляторов

Выпущены методические рекомендации по категорированию ОКИИ

Здравоохранение

Связь

ТЭК

Выпущены отраслевые перечни типовых ОКИИ (в большинстве отраслей)

Транспорт

Энергетика

ТЭК

Здравоохранение

Химическая, горнодобывающая, металлургическая, оборонная промышленность

Задачи, которые решаем

1. Категорирование
2. Разработка ОРД (стратегическая безопасность)
3. Подбор СЗИ
4. Проектирование
5. Внедрение
6. Эксплуатация

Советуем через 2 года вернуться к 1 пункту

«Конфидент-Интеграция» готова поделиться с Вами своим опытом!

КОНФИДЕНТ®
ИНТЕГРАЦИЯ

Благодарю за внимание!

Зенков Александр
Руководитель инженерно-технического департамента
Технический директор

+7(812) 325-1037, доб. 7985
+7 962-669-50-68
email: zenkov.aleksandr@confident.ru