Иван Мелехин

Заместитель директора по развитию бизнеса в России

Кто отвечает за кибербезопасность АСУ ТП?

POSITIVE TECHNOLOGIES

Пятнадцать лет развития

Проактивный подход

Умная кибербезопасность

2002–2012

- R&D
- Один продукт
- Небольшая команда

2013–2016

- 6 продуктов
- Международная экспансия
- 24x7x365 Поддержка

2018

- >700 человек
- >1,000 заказчиков
- Крупнейший исследовательский центр
- Технологический визионер по версии Gartner

Ключевые факты о компании

POSITIVE TECHNOLOGIES

15 ЛЕТ
НА РЫНКЕ ИБ

Среди клиентов:

Банк России, Сбербанк, Альфа-Банк, Raiffeisen BANK, Ростелеком, РОСБАНК, ЛУКОЙЛ, Связной, МегаФон, Роснефть, Росатом, Газпром, М.видео

КРУПНЕЙШИЙ
В ЕВРОПЕ

исследовательский центр

150 ПАРТНЕРОВ
— ЛИДЕРОВ РЫНКА

Среди технологических партнеров:

Microsoft, Cisco, Check Point SOFTWARE TECHNOLOGIES LTD., Array NETWORKS

МЕЖДУНАРОДНОЕ
ПРИЗНАНИЕ

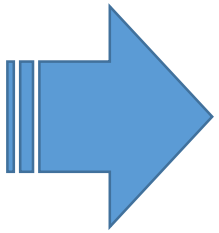
- Члены OWASP, WASC, CIS, CEH, ISACA
- В залах славы Google, Apple, Adobe
- Визионеры магического квадранта Gartner по продуктам класса WAF
- Спикеры международных конференций, включая Defcon, CCC, Black Hat

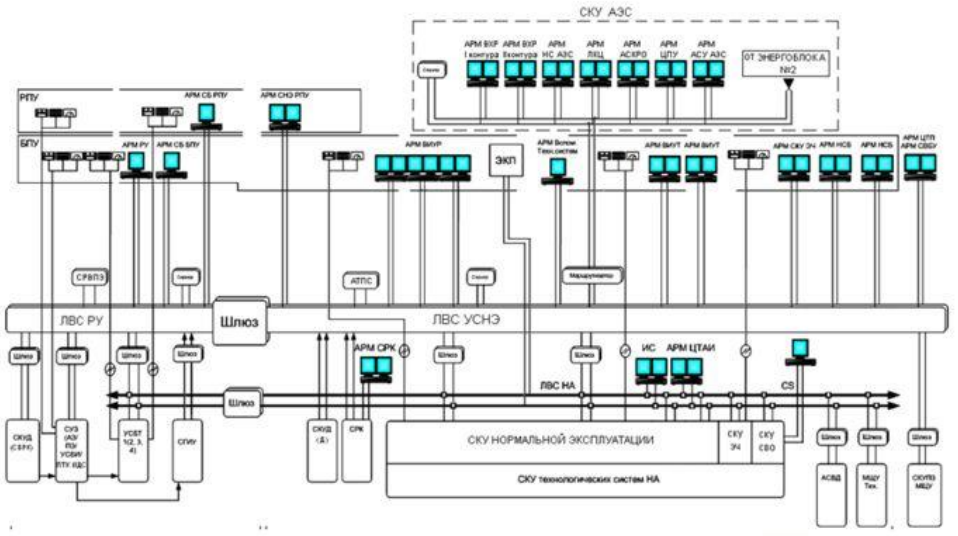
POSITIVE TECHNOLOGIES

Все хорошо, прекрасная маркиза

POSITIVE TECHNOLOGIES

А **что** он сможет, если подключится ?

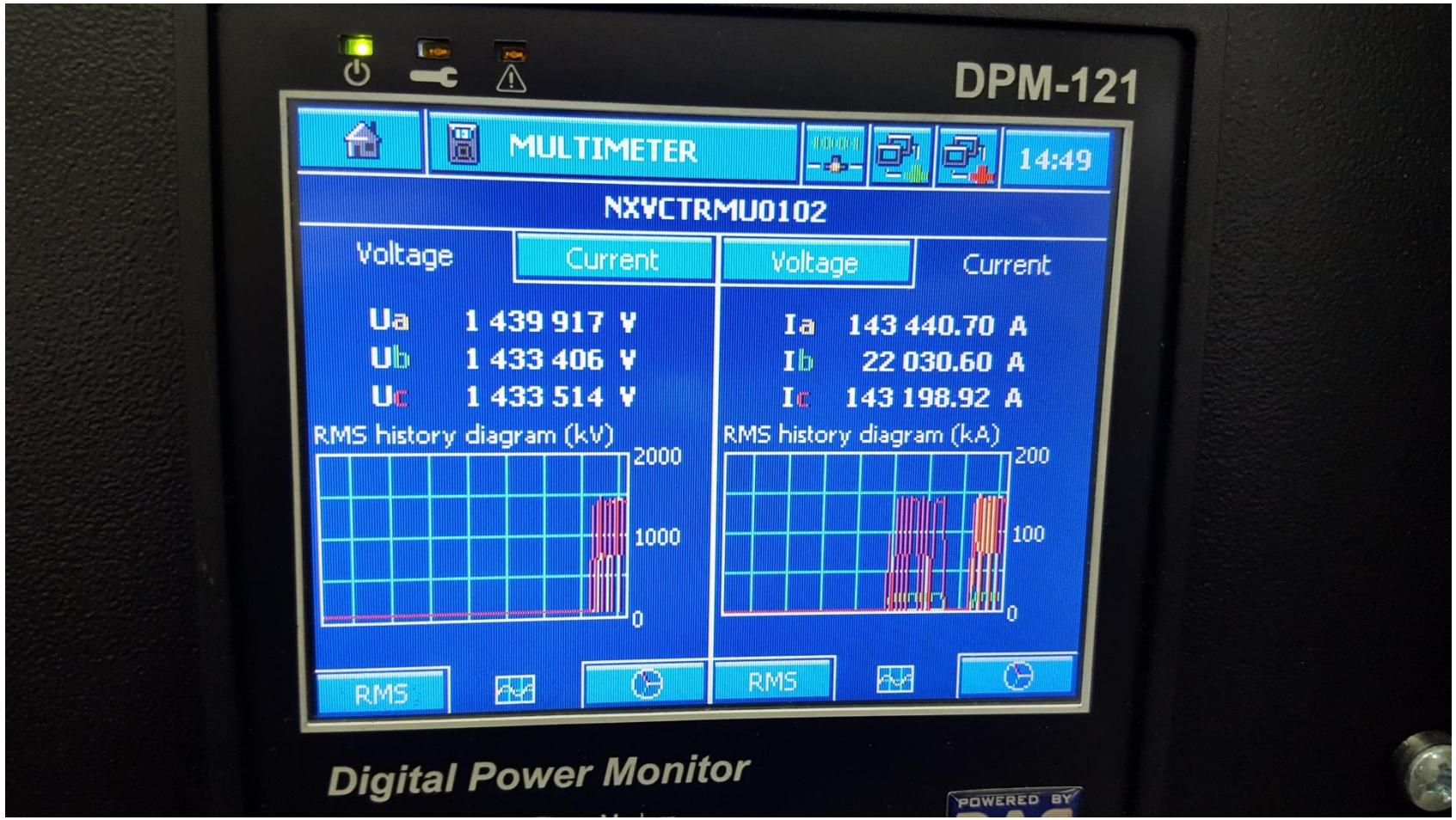




За исключеньем пустяка

POSITIVE TECHNOLOGIES

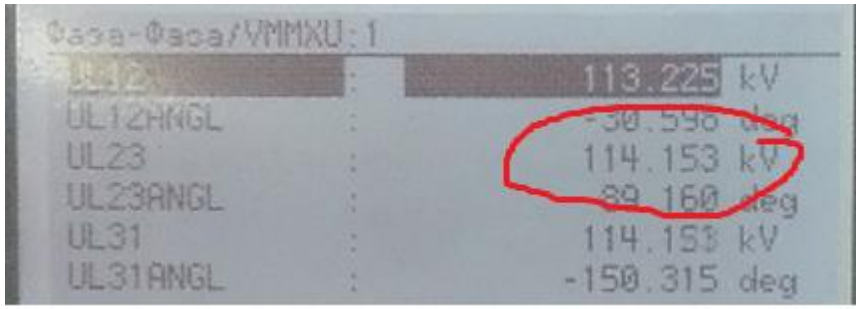
В результате генерирования поддельного SV-потока измерений, в котором были подделаны значения силы тока и напряжения – удалось «обмануть» измерительное устройство:

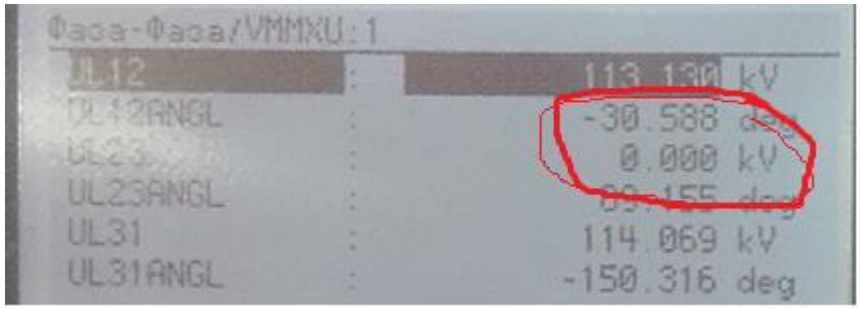


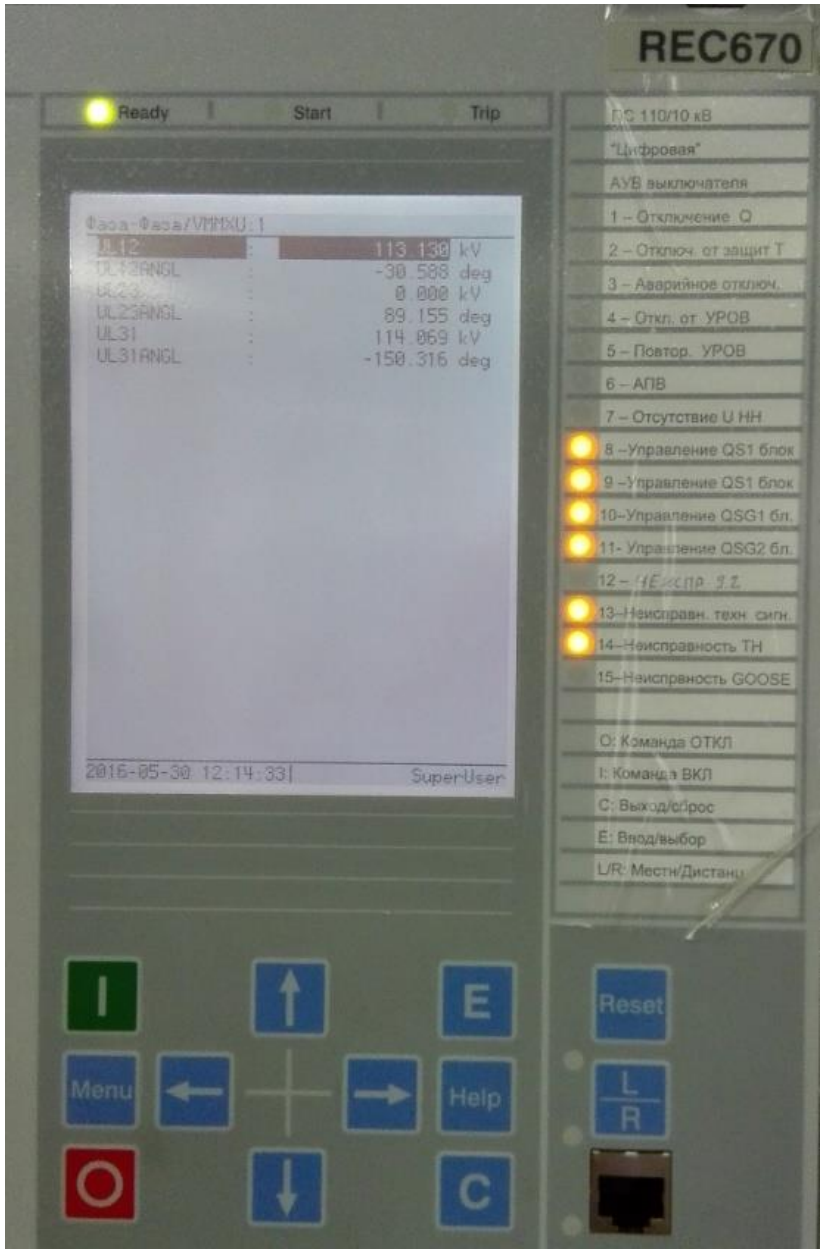
И еще одного

POSITIVE TECHNOLOGIES

Была выполнена отправка команды на замещение значения измерения напряжения на устройстве REC670

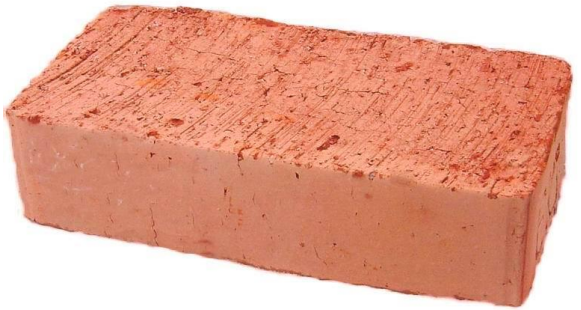






FTP by Schneider Electric PLC

REBOOT
FORMAT
BURNKER



У нас выделенный сегмент!

POSITIVE TECHNOLOGIES

А у нас есть такие приборы….

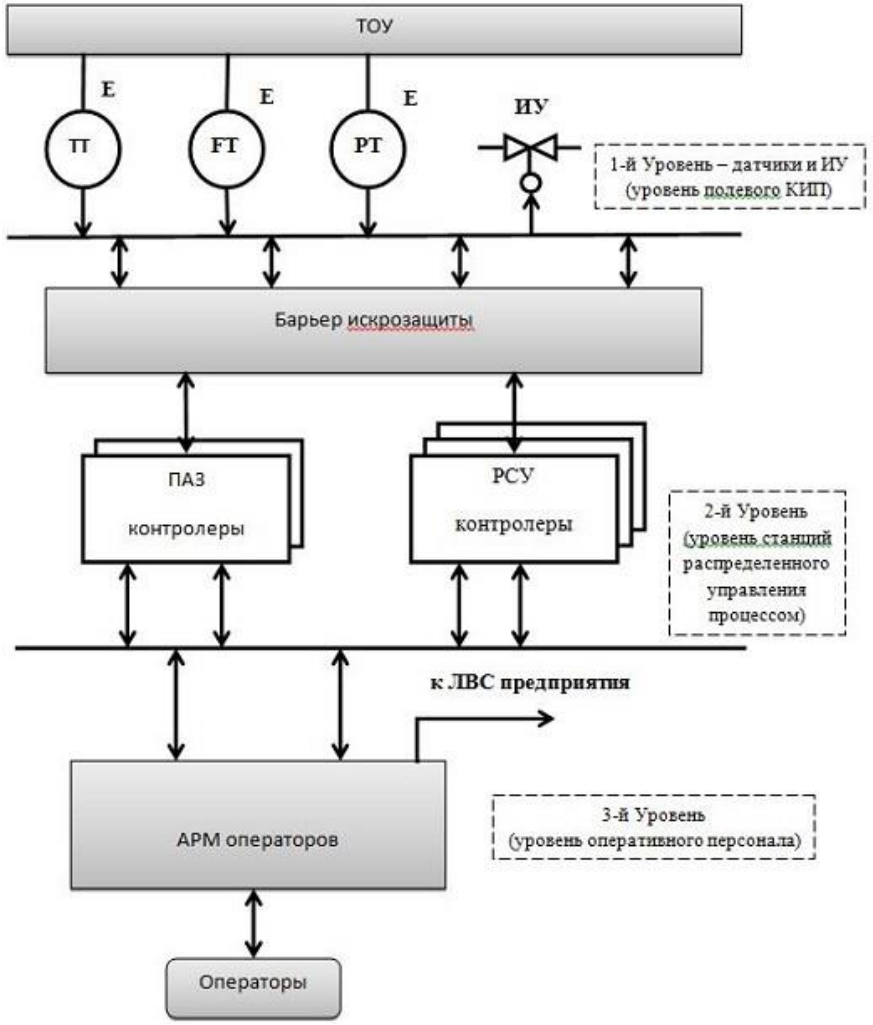
Измененное ПО принтера с реализованными командами:

- **SWITCH OFF** — останов ПЛК
- **SWITCH ON** — запуск ПЛК

Команды активируются через WiFi

ПАЗ! ПАЗ? ПАЗ…..

POSITIVE TECHNOLOGIES



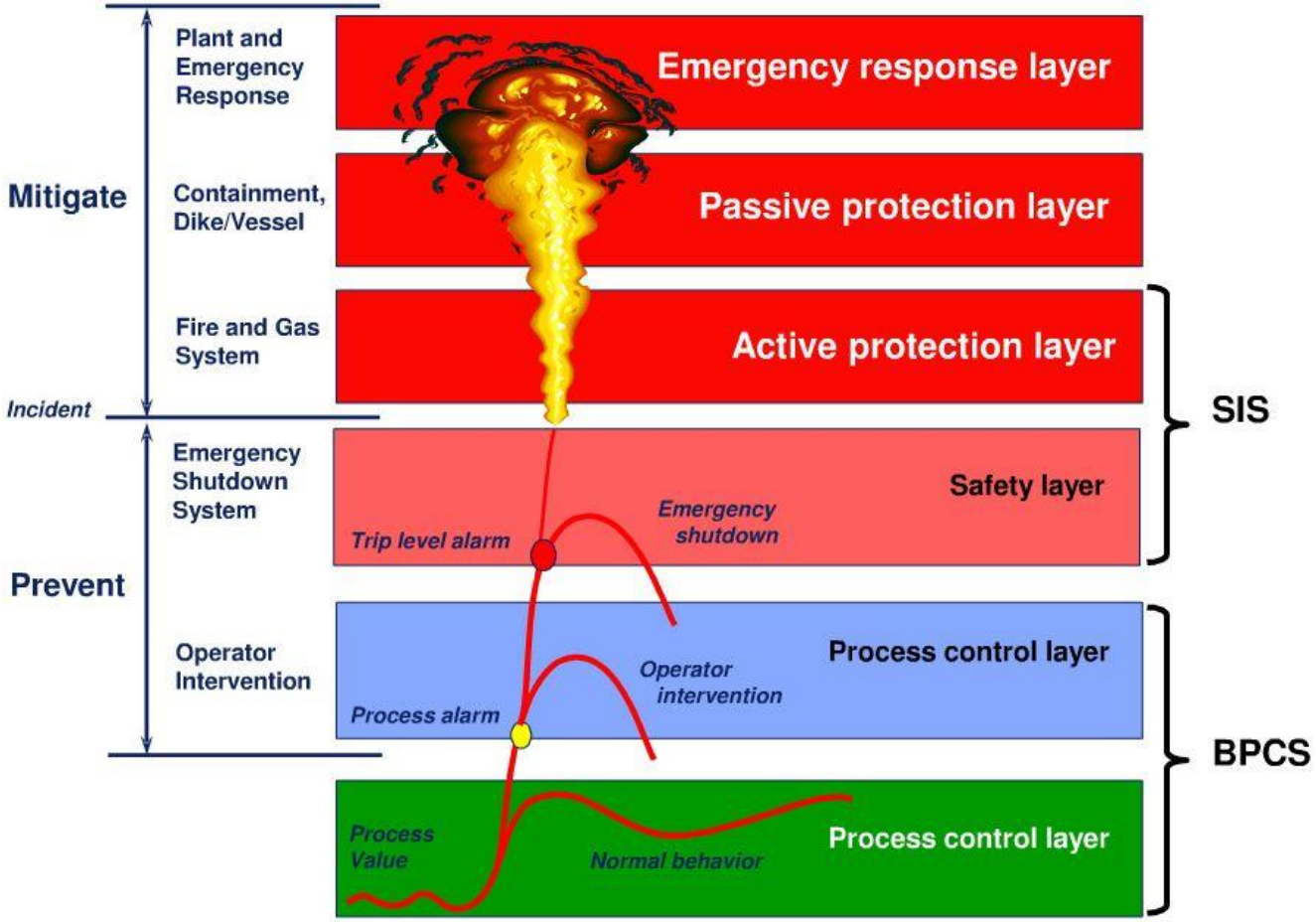
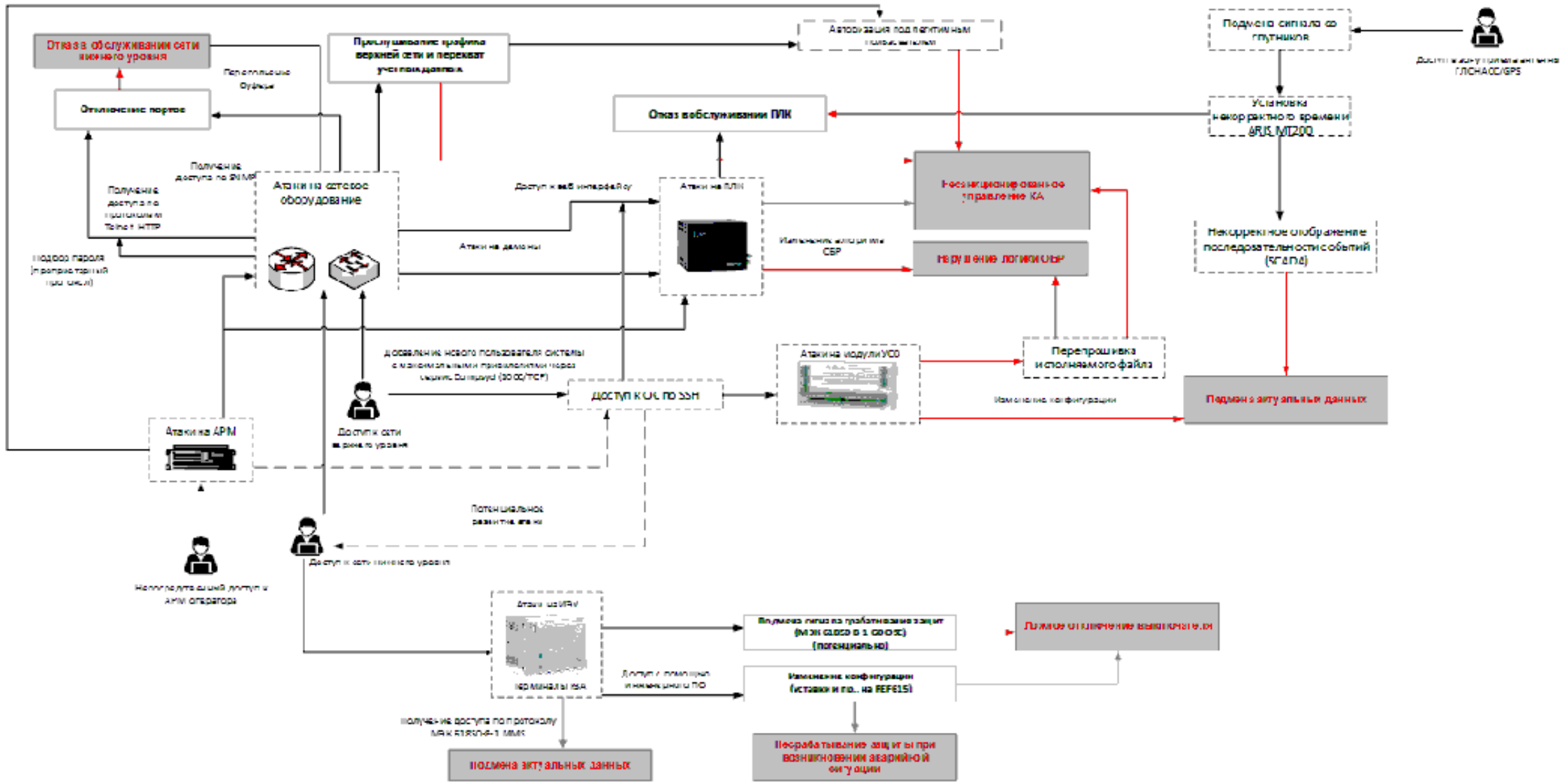


Рис. 3. Архитектура средств АСУТП/РСУ/ПАЗ

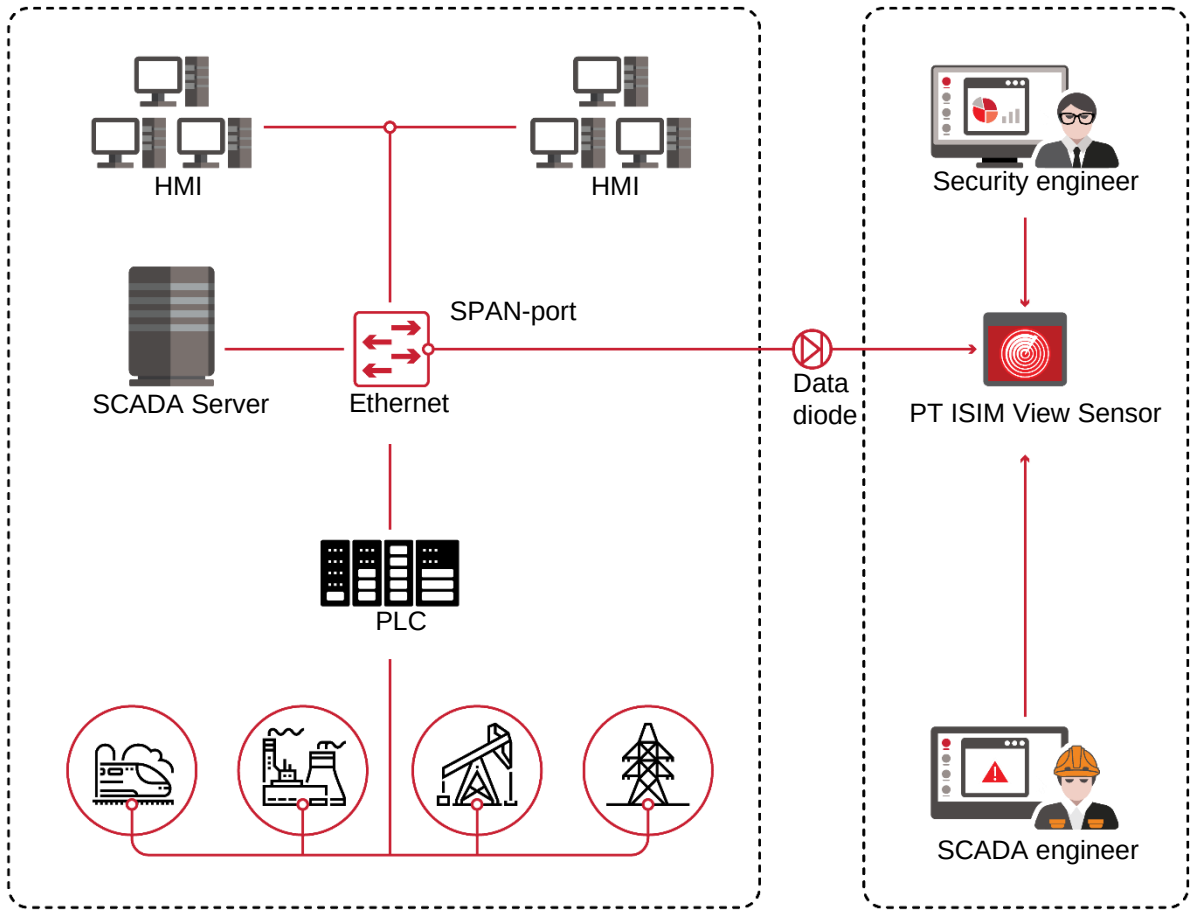
А мы все зашифруем!

POSITIVE TECHNOLOGIES



Ладно, пусть ИБ мониторит

POSITIVE TECHNOLOGIES



Кто виноват?

POSITIVE TECHNOLOGIES

Формально:

В соответствии с решением Коллегии ФСТЭК России от 24.04.2018 № 59 ….

создание (совершенствование созданных) до 1 сентября 2019 г. систем безопасности, включающих в том числе назначение руководящего должностного лица, ответственного за организацию и контроль обеспечения безопасности значимых объектов критической информационной инфраструктуры, создание (назначение) структурного подразделения, ответственного за обеспечение безопасности значимых объектов критической информационной инфраструктуры

Реально:

- операторы
- служба эксплуатации
- ИБ

Итого

POSITIVE TECHNOLOGIES

Угрозы - реальны

Сегментация и ПАЗ – не панацея

На передовой – операторы и службы эксплуатации.

Служба ИБ – второй эшелон.

Киберзащита – неотъемлемая часть АСУ ТП, сильно интегрированная с компонентами системы и технологическим процессом

Что делать?

POSITIVE TECHNOLOGIES

Мы не можем ждать милостей от природы, взять их у нее — наша задача

П(ротиво) А(варийная) К(ибер) З(ащита)

PT ISIM View Sensor

Анализатор трафика промышленной сети

Аудит критически важных технологических систем

Индивидуальная защита от ВСЕХ атак

PT ISIM View Sensors

POSITIVE TECHNOLOGIES

Версия	Ключевые особенности
PT ISIM netView Sensor Идеально подходит для большинства предприятий и для задач пилотного внедрения	▪ Работает «из коробки» — автоматически обучается, не требует настройки и специальных знаний ▪ Производит глубокий анализ трафика и инвентаризацию сети АСУ ТП ▪ Позволяет выявить до 80% актуальных угроз сети АСУ ТП ▪ Является уникальным источником информации для анализа инцидентов ИБ ▪ Удобный web-интерфейс
PT ISIM proView Sensor Идеально подходит для компаний со зрелым походом к ИБ АСУ ТП. Требует анализа защищенности АСУ ТП	В дополнение к возможностям версии netView Sensor: ▪ Позволяет тонко настроить механизмы анализа под модель угроз заказчика ▪ Предлагает уникальные опции и инструменты визуализации инцидентов (отображение затронутых атакой элементов на мнемосхеме технологического процесса, индивидуальный интерфейс для инженера АСУ ТП) ▪ Позволяет выявлять сложные многоступенчатые атаки

PT ISIM View Sensor Editions

POSITIVE TECHNOLOGIES

	PT ISIM netView Sensor	PT ISIM proView Sensor
Внедрение	Не требует сложной настройки, работает «из коробки»	Предоставляет инструменты тонкой настройки под модель угроз предприятия
Поддержка протоколов АСУ ТП	Schneider UMAS, Siemens S7, CIP, PROFINET DCP, OPC DA, Modbus, GOOSE/MMS, IEC104, DIGSI, SPA-Bus, EKRA, YOKOGAWA and more	
Режим автоматического обучения	ДА	ДА
Управление активами	ДА	ДА
Обнаружение атак	Сигнатурное (эксплойты, известные атаки) Поведенческое (на основе результатов авто-обучения)	Сигнатурное (эксплойты, известные атаки) Поведенческое (на основе результатов авто-обучения) Таргетированые атаки (корреляции событий и уникальные детекты)
Контроль целостности сети	Обнаружение неавторизованных подключений и коммуникаций	
Контроль управления элементами сети АСУ ТП	Обнаружение неавторизованного управления ПЛК/RTU: ▪ Команды пуска и остановки ▪ Загрузка и чтение проекта ПЛК ▪ Загрузка прошивок и чтение/запись настроек	
Визуализация сети АСУ ТП	Автоматическая	Автоматическая
Инструменты импорта SCADA-проектов	НЕТ	ДА
Визуализация мнемосхем АСУ ТП	НЕТ	ДА
Визуализация инцидентов на мнемосхеме АСУ ТП	НЕТ	ДА
Интеграция с SIEM	Syslog	Syslog

Спасибо за внимание!

POSITIVE TECHNOLOGIES

ptsecurity.com