Информационная безопасность технологических систем. Решения компании InfoWatch

INFOWATCH®
МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ

Кибербезопасность АСУ ТП ТЭК

Дмитрий Аносов
Менеджер по развитию направления АСУ ТП

Содержание

- Подход к обеспечению информационной безопасности АСУ ТП
- Комплекс обеспечения информационной безопасности InfoWatch ASAP

Отраслевая специфика:

- Контуры безопасности ТЭК. Возможности атак. Портрет нарушителя
- Частный случай. Сбыт топлива. Система предотвращения хищений

Подход InfoWatch к обеспечению информационной безопасности АСУ ТП

Уровневая модель АСУ ТП

АСУ ТП с точки зрения ИТ

INFOWATCH®

ЗНАКОМО

- Распространенные технологии
- Протоколы стека IP

НЕЗНАКОМО

- Закрытая архитектура
- Проприетарные протоколы и ПО

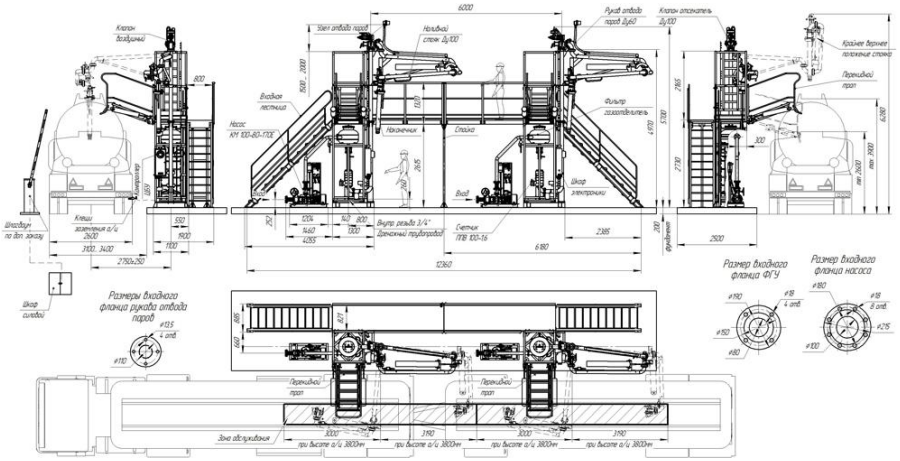
Связность

Приоритеты ИБ в «привычных» сетях:
- Конфиденциальность
- Целостность
- Доступность

Приоритеты ИБ в АСУ ТП:
- Доступность
- Целостность
- Конфиденциальность

От чего и что защищаем?

INFOWATCH®



Объект защиты: технологический процесс

И защищать нужно - от ЛЮБЫХ угроз (информационного характера)

Почему нужна защита?

Кибератаки, направленные на АСУ ТП, могут привести к максимально возможному урону:

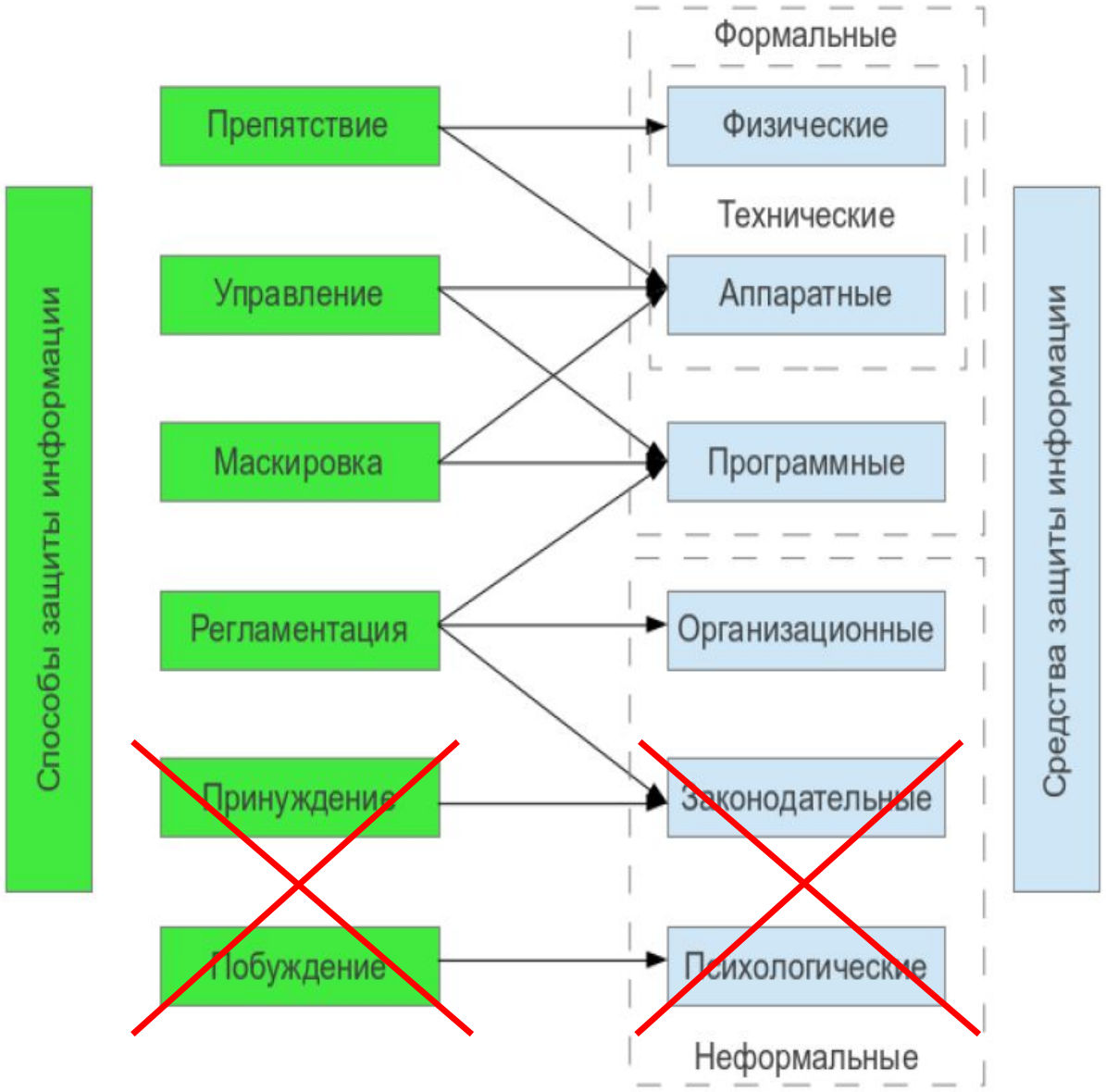
- Человеческие жертвы
- Техногенные катастрофы
- Остановка производства

Только факты:

- Март 2015. Россия. Сбой в работе зарубежных станков на ОПК Урала. Цех остановился.
- Февраль 2015. США. Атака на датчики контроля топлива на АЗС. Работа АЗС парализована.
- 2010 г. Иран. StuxNet атаковал АЭС в Бушере. Более 3 000 центрифуг остановились.
- Список можно продолжать…

Тенденция к удвоению количества инцидентов ИБ

Как защищать?



Комплексный подход

INFOWATCH®

Комплексный подход к обеспечению информационной безопасности системы – это:

Реализация всех уместных способов и связанных с ними средств обеспечения информационной безопасности

Комплексный подход

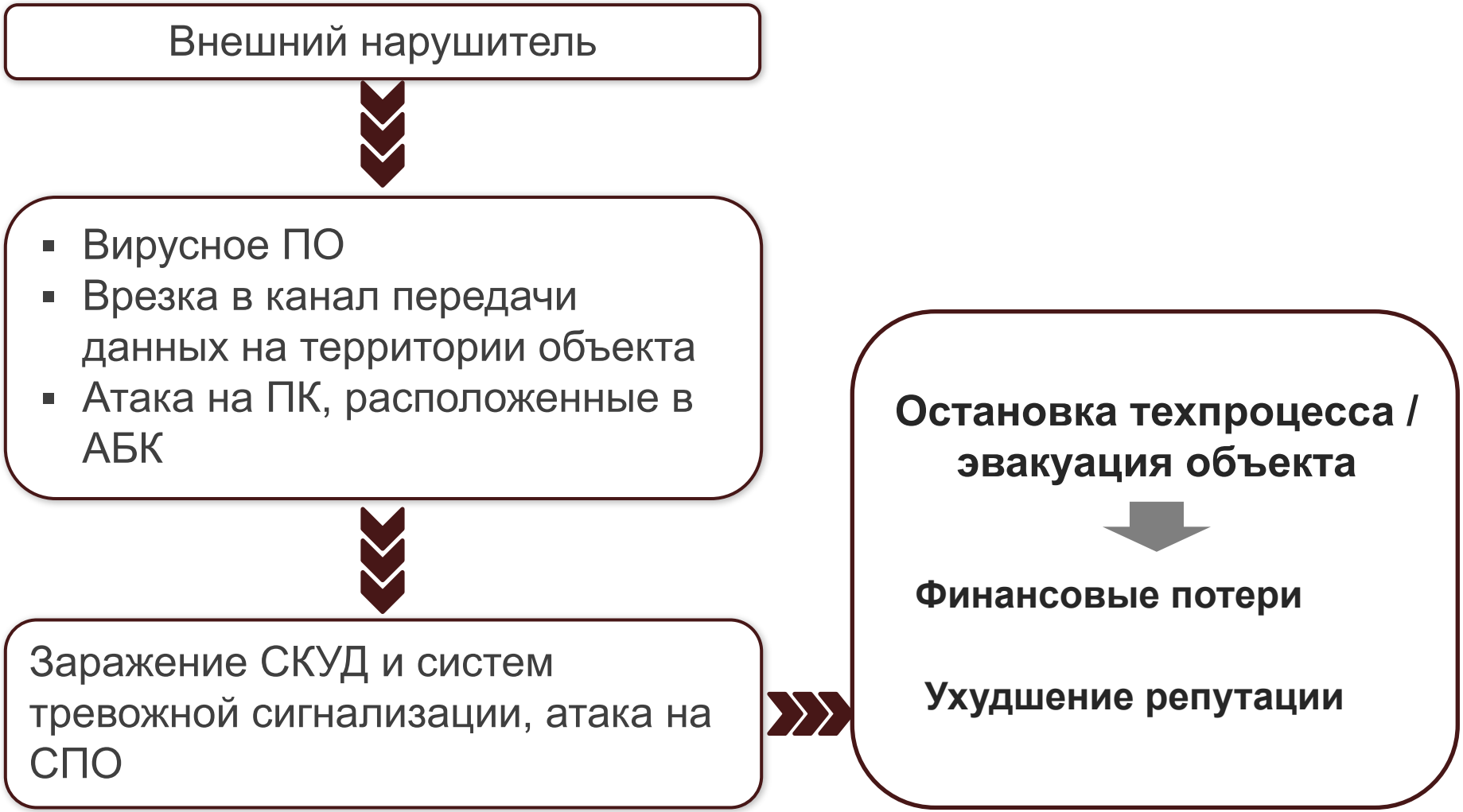
INFOWATCH®

Способ воздействия	Решение InfoWatch
Препятствие	InfoWatch Automation System Advanced Protection (ASAP)
Управление	
Маскировка	
Регламентация	Аудит

Отраслевая специфика предприятий ТЭК

Контуры безопасности ТЭК

Атака на уровень некритичного контура



Атака на уровень подконтрольного контура

Внутренний нарушитель

- Внедрение в канал связи
- Недокументированные возможности оборудования и ПО

Подлог данных, сбой системы автоматизации, контроль техпроцесса

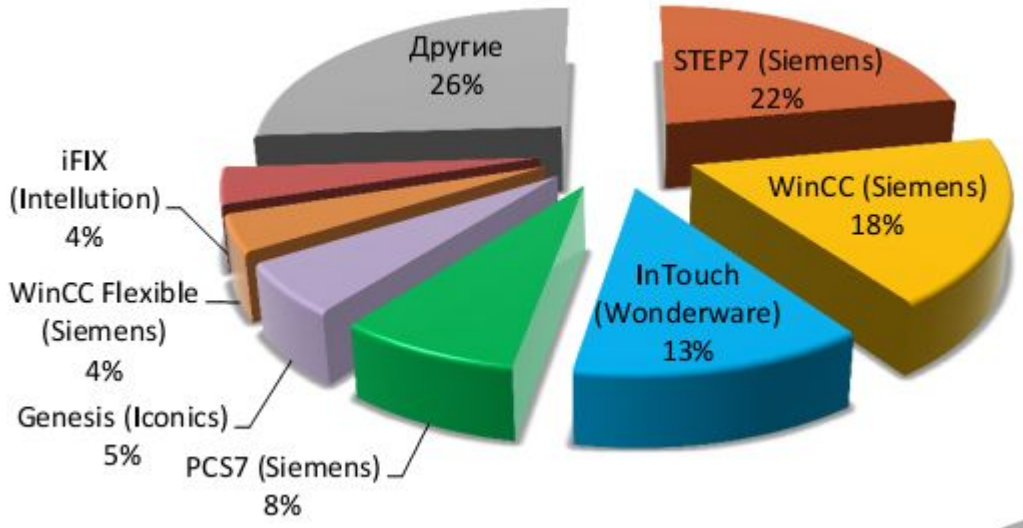
Перехват управления SCADA и вывод АСУ ТП из строя:

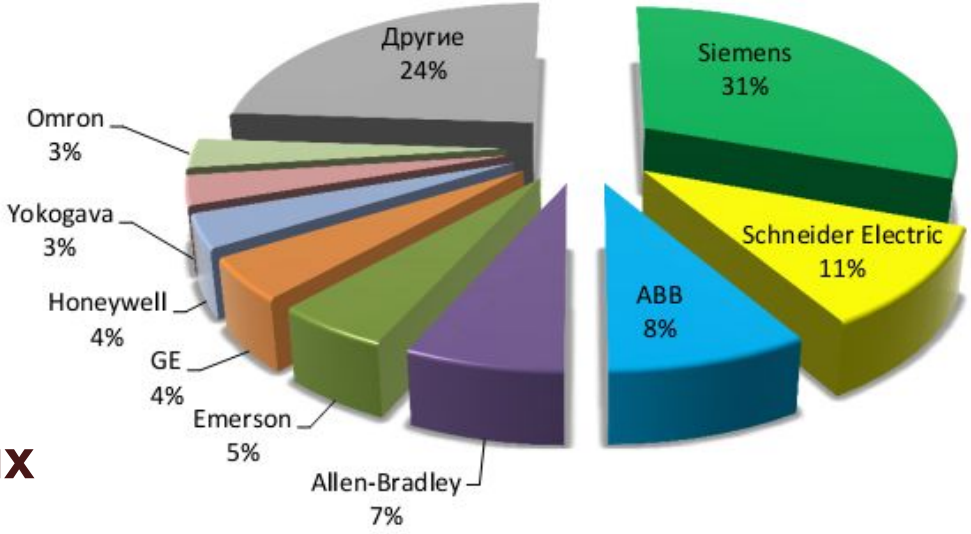
Финансовые потери

Ухудшение репутации

Атака на уровень сверхкритичного контура

Статистика по вендорам





Преобладание иностранных производителей!

По данным компании Positive Technologies

Нормативная документация

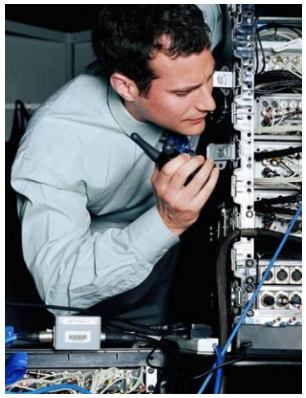
- Приказ №31 ФСТЭК от 14.03.2014
  - Классификация критических объектов
  - Требования к обеспечению информационной безопасности АСУ ТП
- ФЗ № 118 «Обеспечение безопастности объектов ТЭК»
- Проект ФЗ «».....
- Внутрикорпоративные стандарты и нормативные документы

По данным компании Positive Technologies

Портреты нарушителей

INFOWATCH®

Внешние



Злоумышленник

- Технически подкованный специалист способен произвести удаленное вредоносное воздействие

ОПГ

- Группа лиц, имеющих технические средства и знания представляет высокую опасность

Внутренние

Злонамереный инсайдер

- Подкуп сотрудника организации опасен утечкой информации и повышением таргетированности атаки

Неопытный лаборант

- Человеческий фактор ведет к ошибкам и нарушениям технологического процесса

Ключевые возможности

- Интеллектуальная система выявления аномалий
- Контроль правильности выполнения технологического процесса
- Обнаружение скрытых врезок и посторонних устройств на основе анализа электрических параметров сигнала
- Контроль подлинности передаваемых данных
- Инструментарий визуализации полученных данных и выявленных аномалий

Врезка не пройдёт

Архитектура решения

INFOWATCH®

Программный сервер аналитики

Конструктор ПО для АРМ СБ и диспетчера

Внутренние механизмы защиты решения

- Аппаратно-программный модуль доверенной загрузки
- Датчик вскрытия устройств защиты
- Шифрование обмена данными с использованием SSL-сертификатов
- Аппаратный watchdog-таймер
- Реализация механизма bypass в случае установки в разрыв линии

Примеры

Основные производственные этапы ТЭК. Добыча.

- Станция сбора и подготовки нефти к транспортировке
- Головные и промежуточные перекачивающие станции
- Системы обеспечения процесса добычи и транспортировки;

Типовые угрозы:

- Подмена данных об объемах сырья (хищение), датчиков давления (поломка, разрыв)
- Вывод из строя систем обеспечения (например, подача электроэнергии)

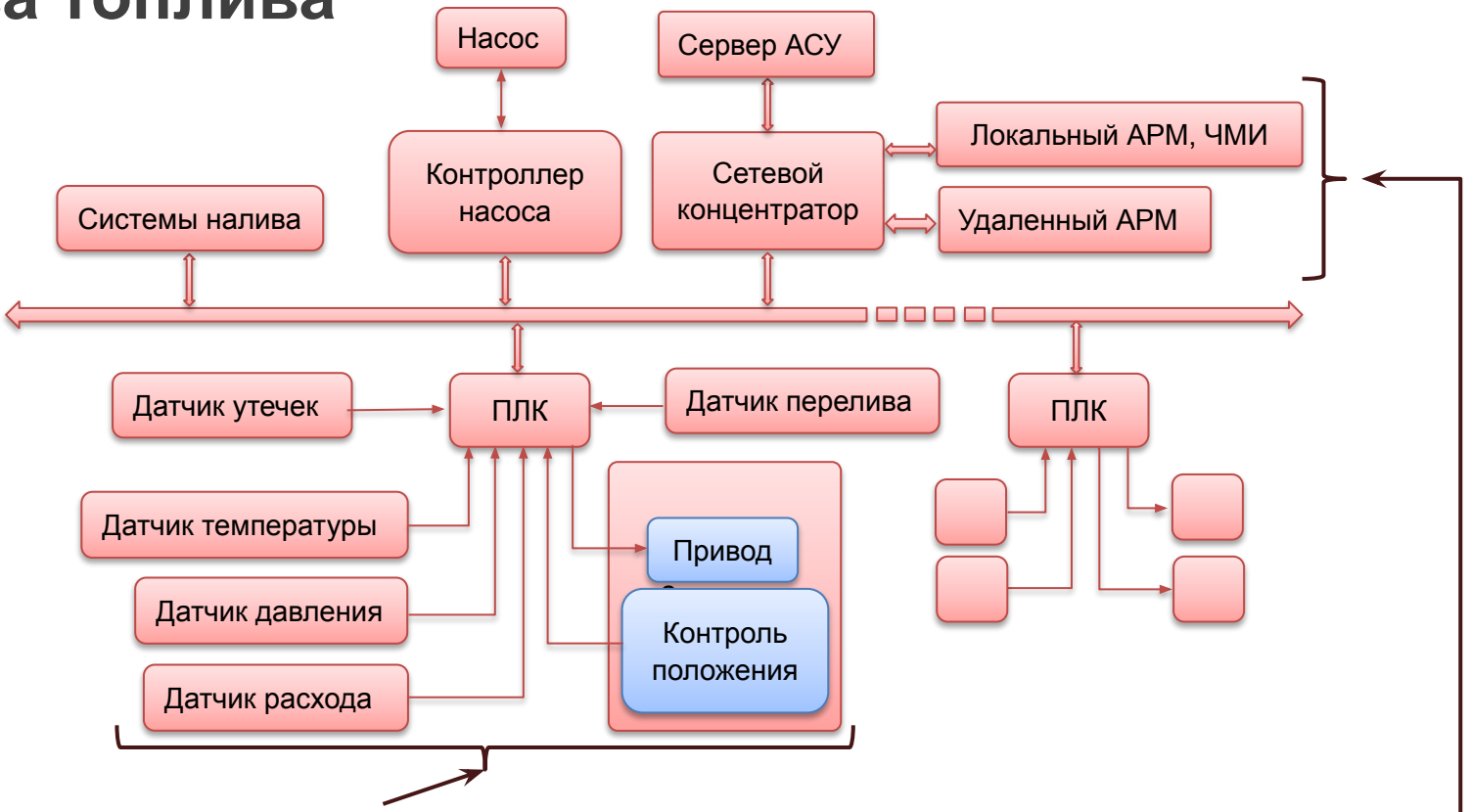
Движение топлива после НПЗ. Опт.

НПЗ

Локальное хранилище

Рассмотрим более подробно

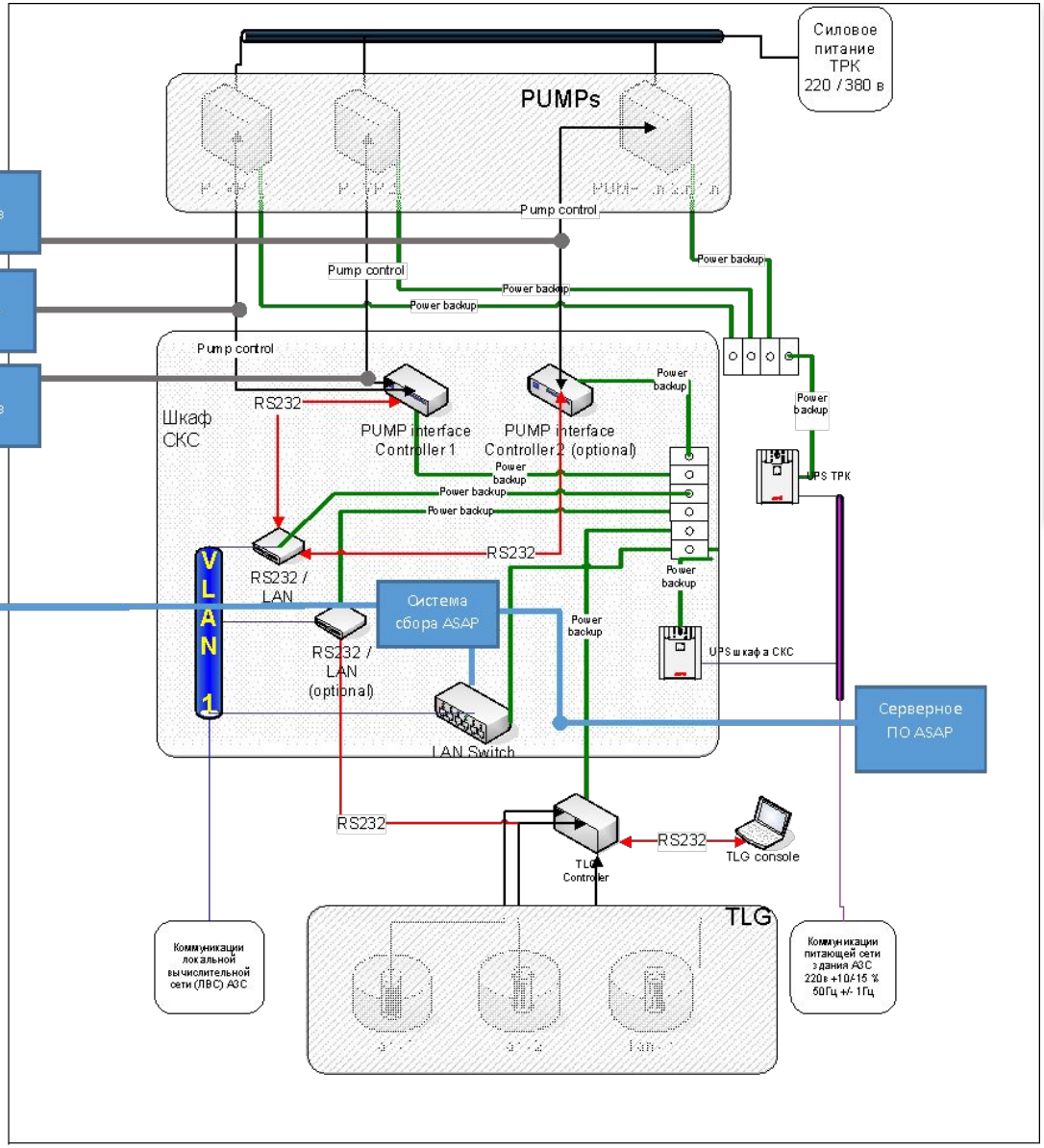
Типовая схема налива топлива



Для сокрытия фактов хищения нужно произвести воздействие на систему обнаружения утечек или систему определения наполнения цистерн. В обоих случаях достаточно будет как изменения уставок (смещение нуля показаний), так и изменения логики технологического процесса.

Организуем удаленный доступ к контроллеру автоматизации. Это возможно при подключении к коммуникационным каналам технологической сети или при получении несанкционированного доступа к АРМ оператора автоматизации.

Розница. АЗК.



Для сокрытия фактов хищения нужно произвести воздействие на систему контроля розлива топлива (смещение нуля показаний), так и изменения логики технологического процесса. Например, путем подмены контролирующей платы на колонке.

Аудит ИБ.
Решения от InfoWatch

Аудит ИБ

INFOWATCH®

Проектирование СЗИ для АСУ ТП начинается с изучения защищаемой системы

- Объекты защиты по своему уникальны
- Каждая АСУ ТП по своему уникальна, у компонентов (ПЛК) также свои особенности. Знать и предугадать заранее нельзя
- Прежде, чем иметь дело с любой уникальной системой, ее необходимо изучить

Аудит ИБ АСУ ТП – максимально эффективный способ исследовать конкретную АСУ ТП с точки зрения информационной безопасности

Проектирование решения

INFOWATCH®

Основные принципы проектирования защиты АСУ ТП:

- Решение должно быть комплексным и максимально стабильным
- Решение от единого вендора – удобно внедрять, удобно поддерживать, удобно управлять. Как следствие – снижение стоимости владения
- Решение должно быть очень гибким, чтобы иметь возможность подстраиваться под любые АСУ ТП и техпроцессы Заказчика, в том числе и те, которые еще не защищены
- **НО ГЛАВНОЕ:**
  - Решение никак не должно влиять на нормальное функционирование АСУ ТП
  - Решение должно полностью обеспечивать защиту Объекта защиты

Процесс внедрения

Направление InfoWatch ASAP

INFOWATCH®

Решения для ИБ АСУ ТП

Услуги

- Аудит (согласно Приказу ФСТЭК 31)
- Комплексный аудит ИБ организации
- Разработка стандартов ИБ и нормативной документации

Продукты

- АПК ASAP

Комплексное решение для обеспечения информационной безопасности АСУ ТП InfoWatch ASAP

Состав системы

INFOWATCH®

Распределенные по объекту ASAP

Аппаратная база определяется исходя из: количества контролируемых интерфейсов связи и их распределенности по объекту, объема обрабатываемой информации, стандартов
и протоколов передачи информации

ПО сервера обработки информации, поступающей с ASAP

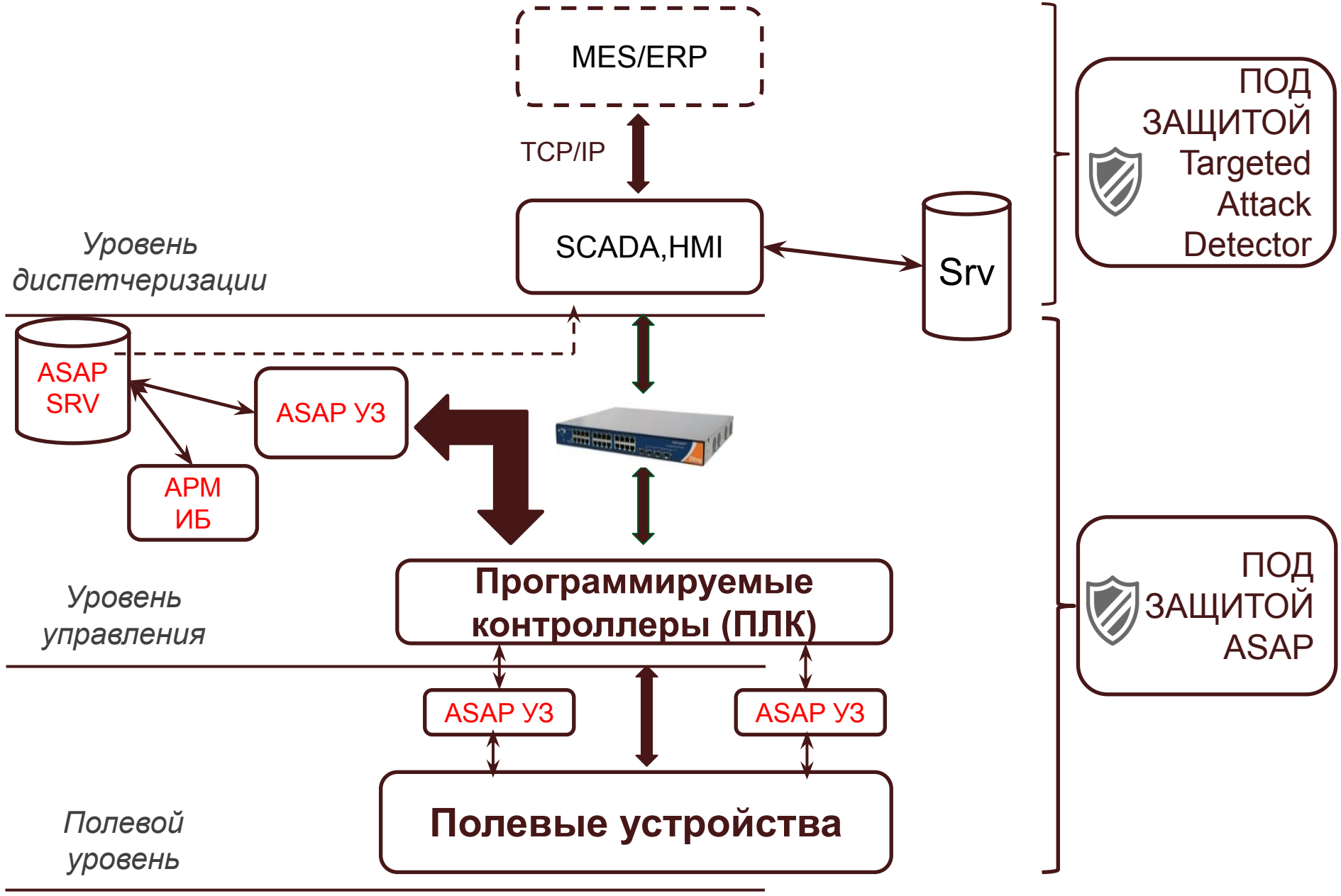
ПО сервера может быть установлено на существующие средства вычислительной техники объекта

ПО для службы безопасности

ПО является тонким клиентом для сервера и может быть установлено на существующие ПК. ПО позволяет формировать аналитические отчеты по заданным параметрам в интересах заказчика. Отчеты могут дополняться графической визуализацией

* ASAP – средства обнаружения аномалий

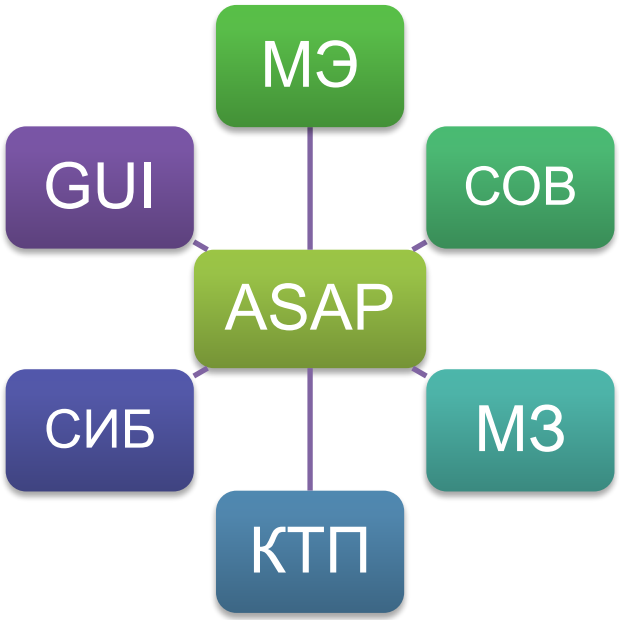
Фокус защиты ASAP



Функциональные блоки защиты

INFOWATCH®

Взаимодействие модулей в рамках единого ядра



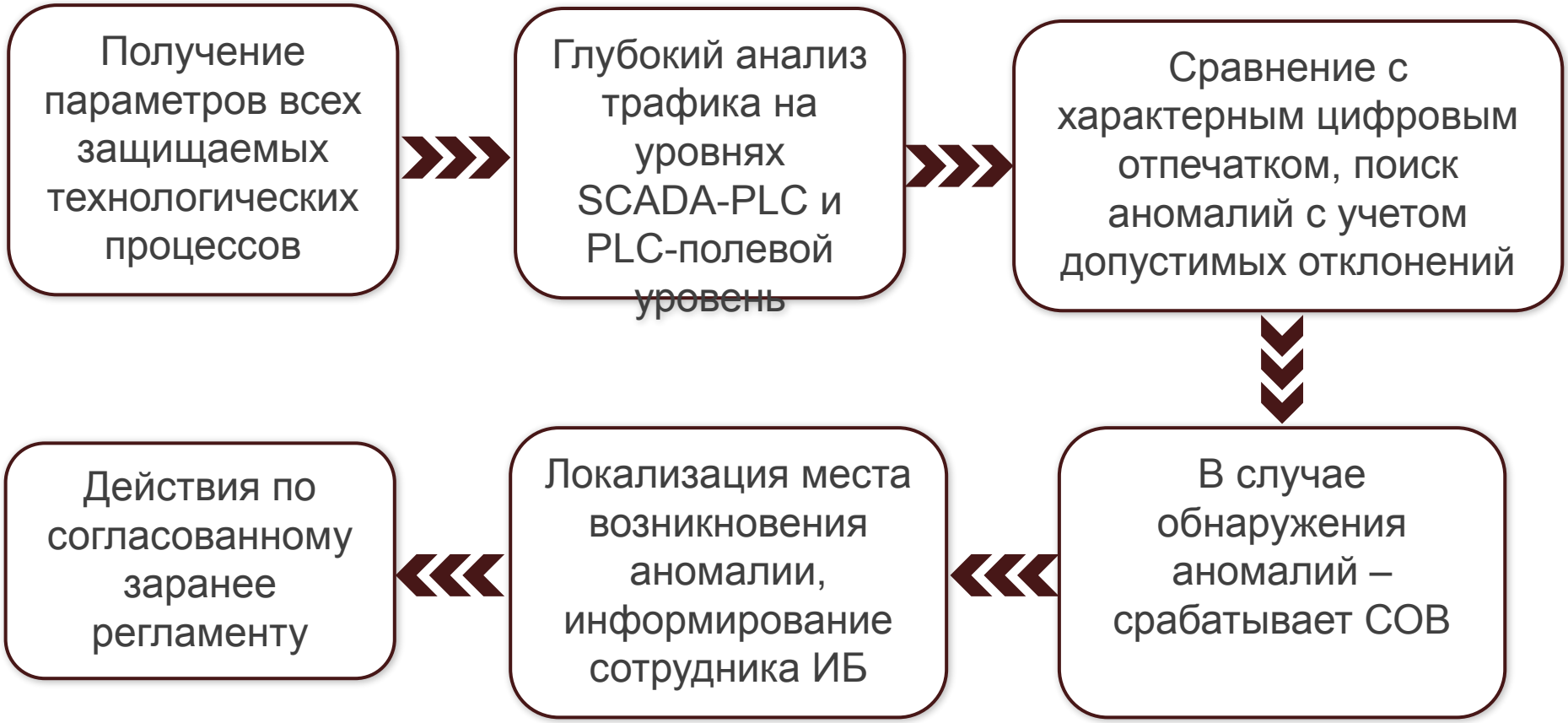
Ядро содержит функционал бизнес-логики и алгоритмов принятия решения

Анализирует поведение системы в целом, используя графы связи и систему анализа изменений совокупности параметров системы – поведенческий анализ

Количество параметров, их взаимосвязи и изменение связей в системе быть изменено в процессе работы системы специалистами

Схема работы решения

INFOWATCH®



InfoWatch ASAP

ASAP

Реализует ВСЕ возможные способы, типы и средства защиты технологических сетей, уместные и применимые на нижних уровнях АСУ ТП

Ключевые возможности:

- Не только мониторинг, но и возможность контроля трафика, в т.ч. нижних уровней АСУ ТП
- Методы поведенческого анализа позволяют эффективно защищать систему вне зависимости от сложности моделей работы и их количества
- Возможность работы непосредственно с протоколами уровня датчиков и исполнительных механизмов
- Возможность работы в качестве маршрутизатора

Функциональные возможности

INFOWATCH®

ASAP обеспечивает:

Автоматизацию деятельности по обеспечению информационной безопасности АСУ ТП

Непрерывный мониторинг событий ИБ, уменьшение времени реакции на инциденты, облегчение информационного взаимодействия, автоматизация рутинных задач

Обнаружение угроз ИБ:

- В корпоративных сетях
- В технологических сетях (АСУ ТП)
- В сетях связи
- В системах автоматического управления (инженерных системах)
- В технических средствах охраны

Обнаружение и предотвращение угроз ИБ, характерных для уровня контроллеров и исполнительных устройств АСУ ТП

ASAP обеспечивает защиту АСУ ТП от ЛЮБЫХ атак, направленных на уровни контроллеров и исполнительных устройств

Приказ №31 ФСТЭК России

InfoWatch ASAP соответствует:

- Руководящему Документу ФСТЭК России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (РД по СВТ) – класс 5
- Руководящему Документу ФСТЭК России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (РД по МЭ) – класс 3
- Методическому Документу ФСТЭК России «Профиль защиты систем обнаружения вторжений уровня сети пятого класса защиты ИТ.СОВ.С5. ПЗ» (РД по СОВ) – класс 5
- Руководящему Документу ФСТЭК России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» - (РД по НДВ) – класс 3

INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Спасибо за внимание!

InfoWatch

www.infowatch.ru
+7 495 22 900 22

Дмитрий Аносов
Dmitry.Anosov@infowatch.com