Технология мониторинга безопасности АСУ ТП: настоящее и будущее

Алексей Шанин
Директор лаборатории DATAPK

УЦСБ ИНТЕГРАТОР СИЛЬНЫХ РЕШЕНИЙ

Мониторинг безопасности – что это?

Мониторинг – процесс сбора информации с целью наблюдений, оценки и прогноза изменений состояния объекта

Безопасность – состояние защищенности …

Мониторинг безопасности – что это?

Мониторинг – процесс сбора информации с целью наблюдений, оценки и прогноза изменений состояния объекта

Безопасность – состояние защищенности …

Мониторинг безопасности – что это?

Мониторинг – процесс сбора информации с целью наблюдений, оценки и прогноза изменений состояния объекта

Безопасность – состояние защищенности …

как мерить?

чем мерить?

что делать с результатом?

Мониторинг безопасности - стратегия защиты АСУ ТП в оперативном режиме

АСУ ТП в оперативном режиме:

- Функционирование АСУ ТП в полном объеме с выполнением всех доступных функций
- Не вносятся никакие изменения в оборудование и ПО (за исключением текущего ремонта)
- Взаимодействие с пользователем (оператором) в режиме «киоска»
- Крайне критична корректность и время выполнения функций АСУ ТП
- Нарушение работы АСУ ТП напрямую влияет на технологический процесс

- Формирование *изолированной программной среды*
- Исключение автоматического вмешательства системы защиты в работу АСУ ТП

АСУ ТП в режиме ТО/инженерного сопровождения

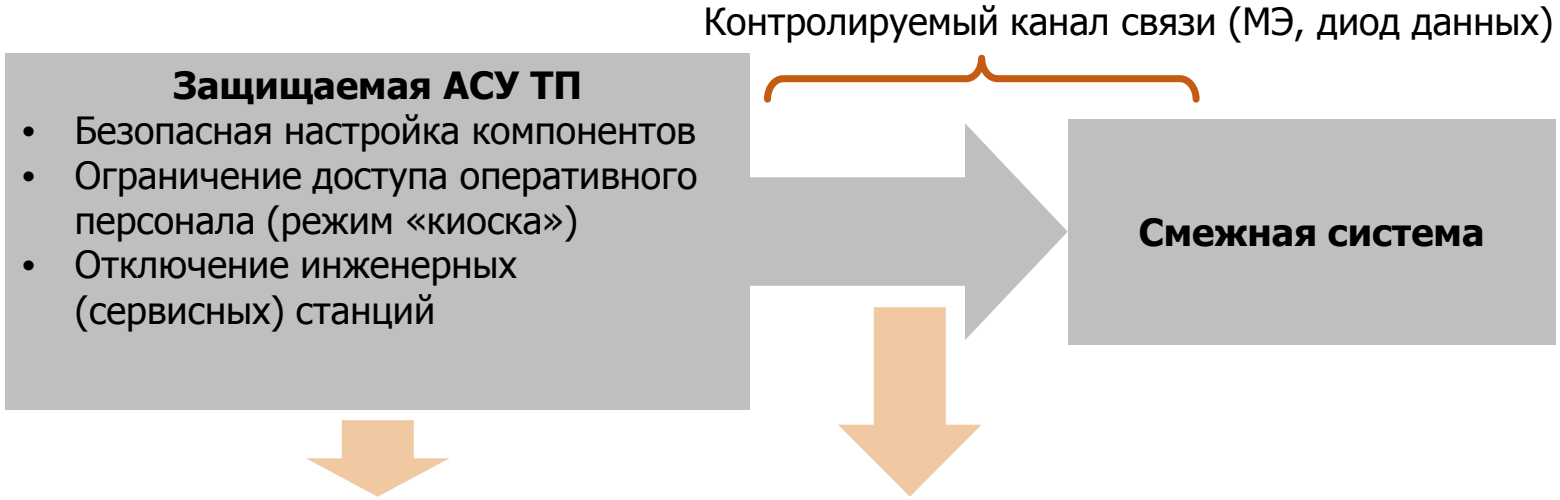
- Основные функции АСУ ТП не реализуются
- Проводятся работы с отдельными компонентами АСУ ТП: СВТ, АСО, ПЛК и пр.
- Активно вносятся изменения
- Подключаются дополнительные устройства (сервисные компьютеры, съемные носители и пр.)

- Реализация полного спектра традиционных механизмов ИБ
- *Управление конфигурацией*

Модель изолированной программной среды

Аксиомы ИПС	Реализация ИПС в АСУ ТП
1 Субъекты ИПС не могут изменять друг друга	В составе АСУ ТП не должно быть средств разработки/изменения конфигурации (либо доступ к ним должен блокироваться)
2 В ИПС контролируется целостность субъектов	Должен осуществляться мониторинг целостности субъекта на уровне: • Исполняемых файлов • Файлов конфигураций • Состава информационных потоков
3 В ИПС допускается создание субъектов только из фиксированного «белого» списка	Должен вестись «белый» список • Аппаратных компонентов АСУ ТП • ПО АСУ ТП • Конфигураций ПО и аппаратных компонентов АСУ ТП

Модель мониторинга безопасности АСУ ТП



Непрерывный мониторинг отклонений от эталонной модели:

- Состав компонентов АСУ ТП
- Конфигурации ПО и оборудования
- Схема информационных потоков
- Анализ событий ИБ
- Анализ конфигураций на соответствие требованиям/наличие известных уязвимостей

Модель мониторинга безопасности АСУ ТП

Контролируемый канал связи (МЭ, диод данных)

Защищаемая АСУ ТП

- Безопасная настройка компонентов
- Ограничение доступа оперативного персонала (режим «киоска»)
- Отключение инженерных (сервисных) станций

Смежная система

Непрерывный мониторинг отклонений от эталонной модели:

- Состав компонентов АСУ ТП
- Конфигурации ПО и оборудования
- Схема информационных потоков
- Анализ событий ИБ
- [illegible] конфигураций на соответствие требованиям/наличие известных уязвимостей

Модель – это упрощение действительности. Поэтому, кроме перечисленного, необходимо осуществлять сбор и анализ событий безопасности со всех компонентов системы

Мониторинг безопасности в лучших практиках по обеспечению ИБ АСУ ТП

Приказ ФСТЭК России №239 «Об утверждении требований по обеспечению безопасности значимых объектов КИИ РФ»:

- Группа мер управление конфигурацией (УКФ)
- Меры: АУД.1 – инвентаризация информационных ресурсов, АУД.4 – регистрация событий безопасности, АУД.5 – контроль и анализ сетевого трафика, АУД.7 – мониторинг безопасности, ОЦЛ.1 – контроль целостности ПО, ОЦЛ.2 – контроль целостности информации,

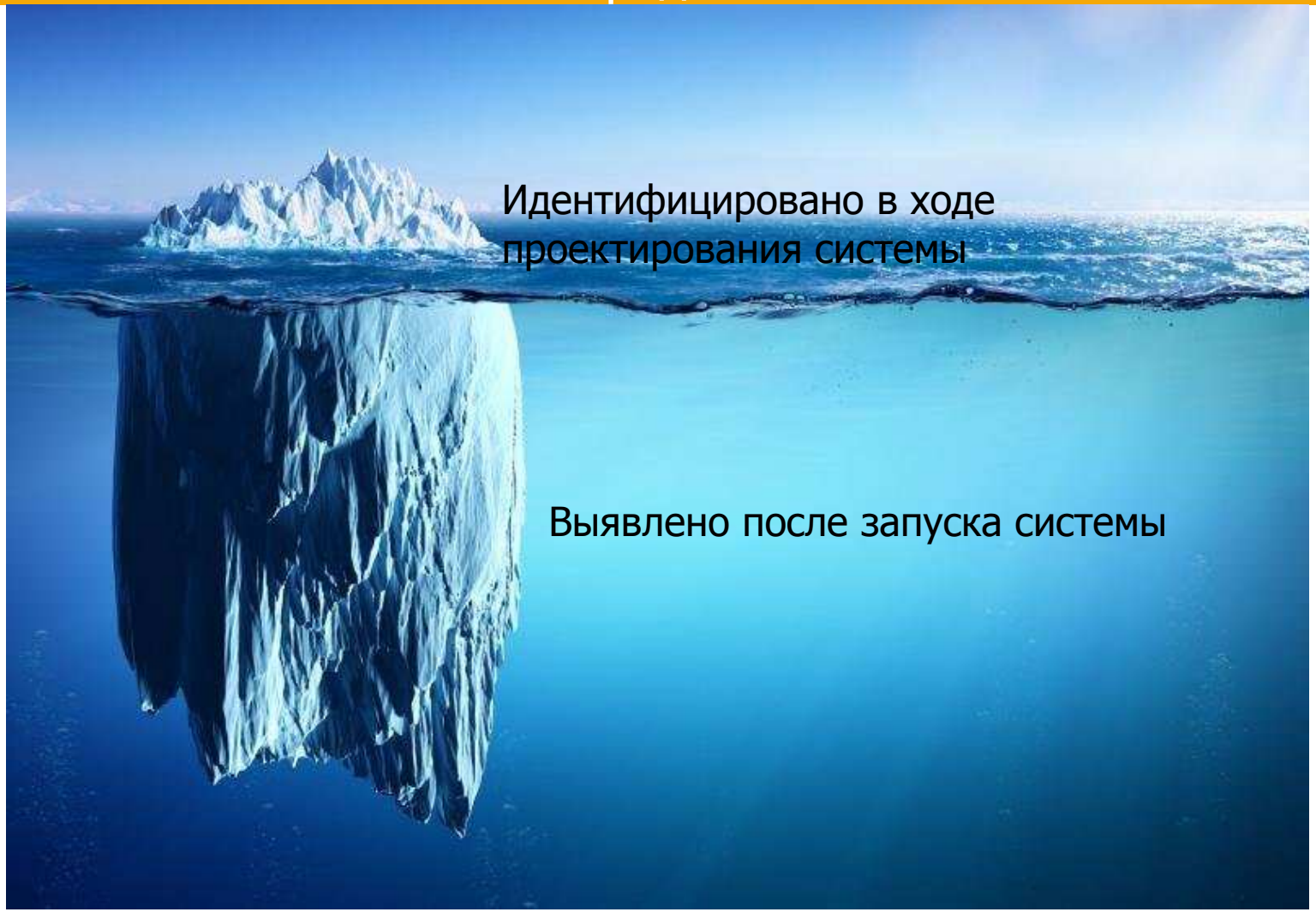
SP 800-137 «Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations»:

- Домены автоматизации безопасности: управление уязвимостями, управление событиями, управление инцидентами, управление активами, управление конфигурацией, управление сетью
- Трёхуровневая референсная модель непрерывной системы мониторинга ИБ

RIPE Framework:

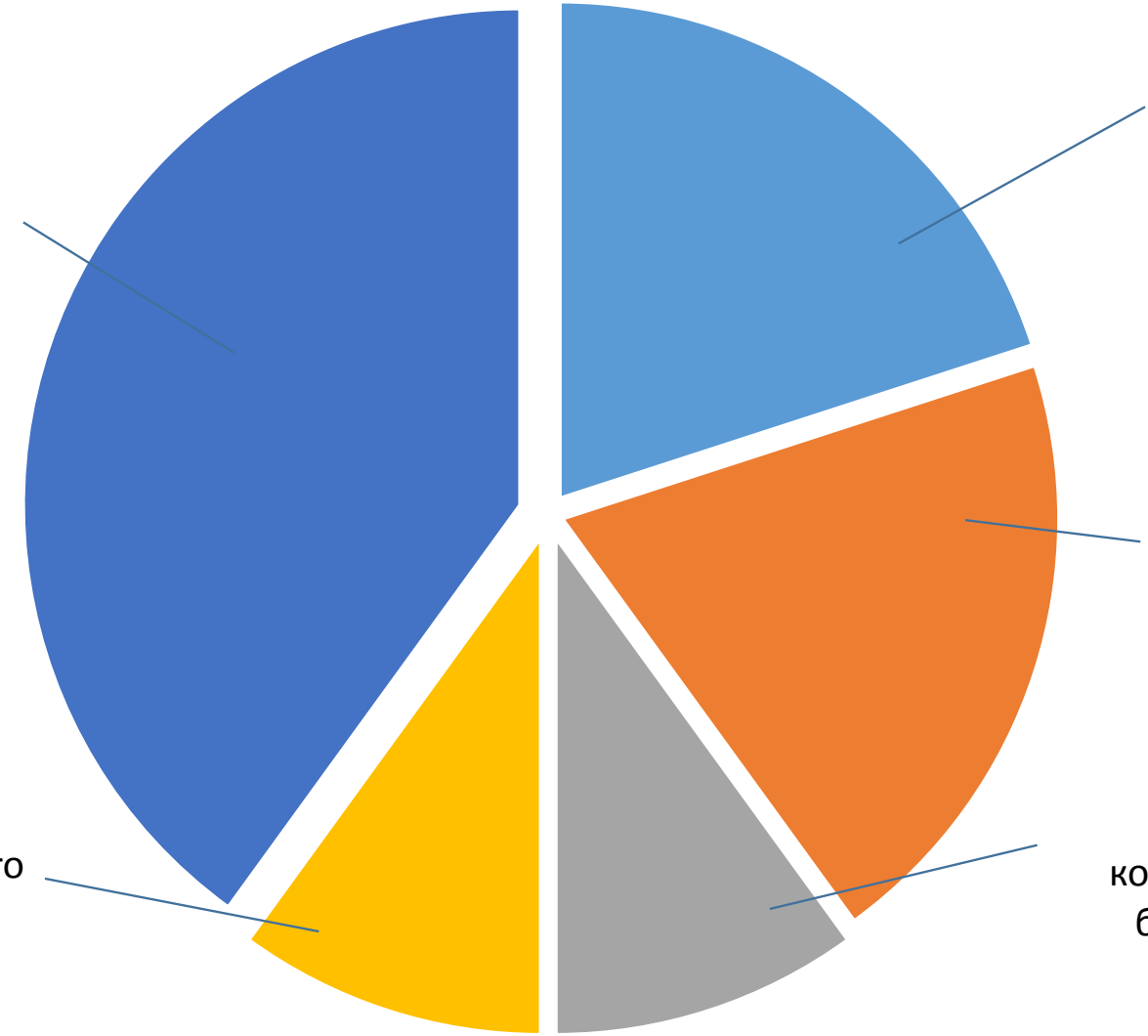
- System population characteristics – инвентаризационная информация об АСУ ТП
- Network Architecture – схема сети
- Component Interaction – информация о сетевом взаимодействии компонентов АСУ ТП

Практический опыт создания системы мониторинга безопасности АСУ ТП. Определение состава компонентов



- Нет информации о расположении неизвестных объектов
- Нет реквизитов доступа к объектам
- Нет ответственного (не знали, что объект управляемое сетевое устройство)
- Гораздо выше трудозатраты на настройку ОЗ для сбора данных

Практический опыт создания системы мониторинга безопасности АСУ ТП. Схема информационных потоков



~ 40% неизвестный трафик специального ПО АСУ ТП

~ 20% трафик известный службе автоматизации

~ 20% стандартный служебный трафик сети

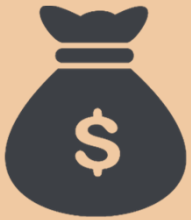
~ 10% известный служебный трафик, легитимность которого должна быть уточнена

~ 10% трафик, которого не должно быть (нарушения политики)

Практический опыт создания системы мониторинга безопасности АСУ ТП. Сбор и обработка событий ИБ

Приоритезация:

- Действующие политики сбора событий: либо все – либо ничего
- Переполнение баз долговременного хранения событий (десятки Гб с одной АСУ ТП в день)



Обогащение:

- Для определения контекста события нужна информация из смежных систем (CMDB, MES и пр.)
- Множество уникальных источников – необходимо разрабатывать большое количество правил нормализации

Развитие системы мониторинга безопасности АСУ ТП

USSC

Мониторинг безопасности сегодня

- Сложное описание и настройка ОЗ
- Трудозатратная аналитика информационных потоков
- Трудозатратное описание правил нормализации событий ИБ
- Полностью «ручной» режим реагирования

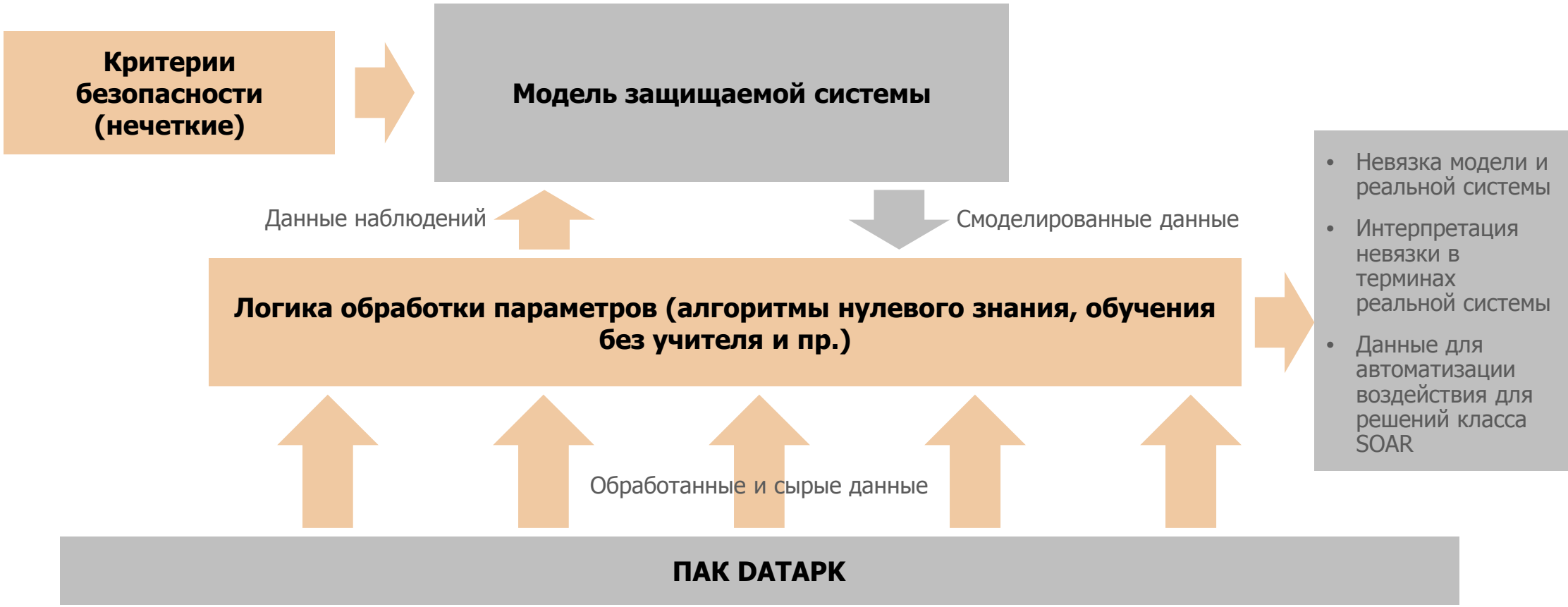
Мониторинг безопасности завтра

- Автоматическое определение сетевой топологии АСУ ТП
- Анализ трафика при помощи алгоритмов с нулевым знанием
- Построение модели защищаемой системы и анализ отклонений
- Интеграция с решениями класса SOAR

The obstacle is complexity. Dealing with it is the single most important challenge facing the I/T industry.

It is our next Grand Challenge.

Концепция автономных вычислений в системе мониторинга безопасности - «DATAPK 2.0»



USSC

СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

Алексей Шанин

Директор лаборатории DATAPK

ООО «УЦСБ»

ashanin@ussc.ru

+7 (343) 379-98-34

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ | USSC.RU