

# Действительно комплексный подход к кибербезопасности АСУ ТП

Дмитрий Ярушевский | CISA | CISM  
Руководитель отдела Кибербезопасности АСУ ТП  
ЗАО «ДиалогНаука»

**ДиалогНаука**


Тел.: +7 (495) 980 67 76  
<http://www.DialogNauka.ru>  
[Dmitry.Yarushevskiy@DialogNauka.ru](mailto:Dmitry.Yarushevskiy@DialogNauka.ru)

# ЗАО «ДиалогНаука»


Системный интегратор в области информационной безопасности, успешно работающий на рынке более 20 лет.

ЗАО «ДиалогНаука» выполняет проекты по разработке, созданию и внедрению систем обеспечения информационной безопасности в банковской, энергетической, промышленной, оборонной и других отраслях.

# Почему «действительно»?

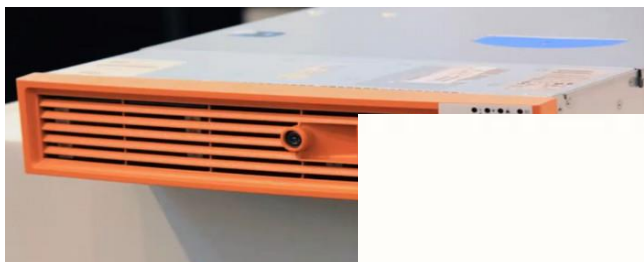


Упускается  
специфика  
АСУ ТП



Упускаются  
процессы  
безопасности

# Почему «комплексный»?



# Что же делает АСУ ТП особенными?



# Ключевые особенности

## Объект защиты

- Объектом защиты является не информация, а технологический процесс

## ЦДК

- Приоритет целостности и доступности над конфиденциальностью

## Режим работы

- Недопустимость сбоев и простоев
- Отсутствие технологических окон и окон «минимальной нагрузки»
- Климатические условия, отсутствие КЗ

## Специфика самой АСУ ТП

- ПО, протоколы передачи данных, оборудование, отсутствие документации
- Отсутствие обновлений
- Отсутствие процессов ИБ

## Последствия

- Возможен ущерб жизни и здоровью людей, окружающей среде и инфраструктуре

## Когда нельзя «внедрить»

Программные или программно-аппаратные СЗИ зачастую вообще невозможно применить, потому что это:



Слишком дорого



Слишком сложно



Технически нереализуемо



Некому управлять



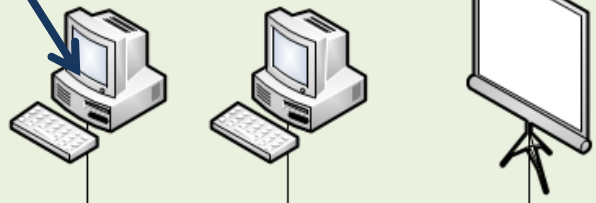
Избыточно



...И более того...

Одна учетная запись, пароль под клавиатурой

Операторы



После наладки не заблокировали учетки разработчиков

SCADA

PLC

Login: admin  
Password: admin

Диагностика

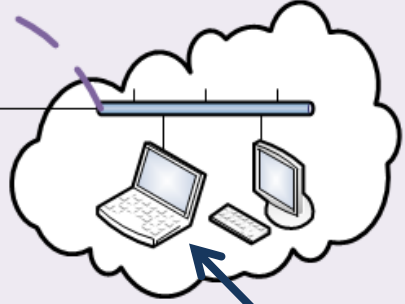
Производственная сеть

20 permit tcp ANY ANY

Офисная сеть

Удаленный доступ

Выделенный сегмент



Дети дома используют для игр и общения

Дорогой и ОЧЕНЬ хороший МЭ



# Как «делать это правильно»?



Изучение объекта  
защиты

Моделирование  
объекта защиты

Идентификация,  
оценка и анализ  
рисков,  
моделирование  
угроз

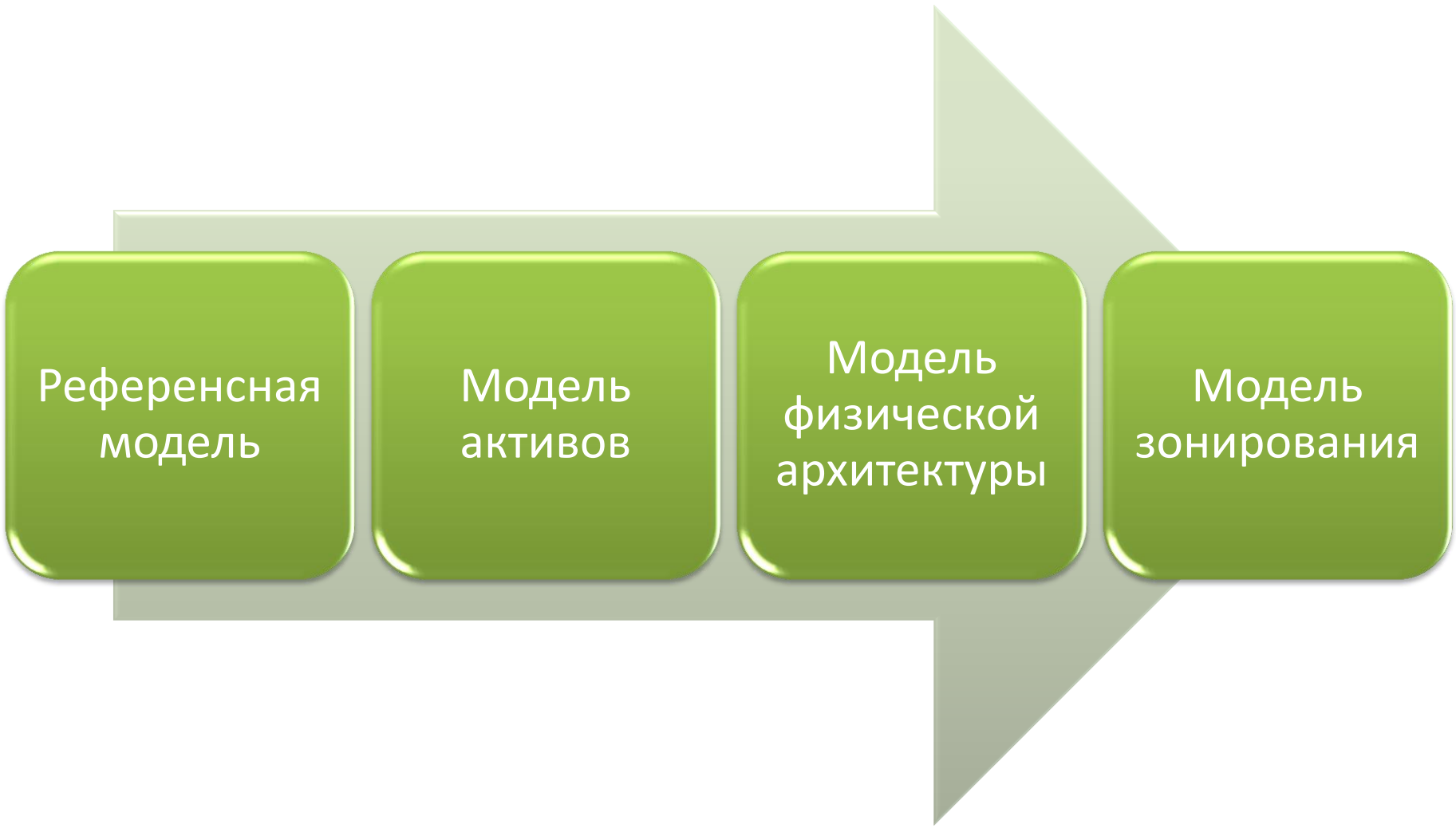
Разработка  
(дополнение) мер  
защиты на основе  
моделирования  
угроз

## Семейство стандартов ISA/IEC 62443

- Методическая основа для исследования крупных распределенных АСУ ТП
- Методология построения систем обеспечения кибербезопасности
- Определение целевого уровня безопасности

## NIST SP-800-82 Guide to ICS security

- Содержит подробные рекомендации по построению защищенных АСУ ТП от сетевой архитектуры до конфигураций АСУ ТП и SCADA-систем
- Методическая основа для организации процессного обеспечения ИБ



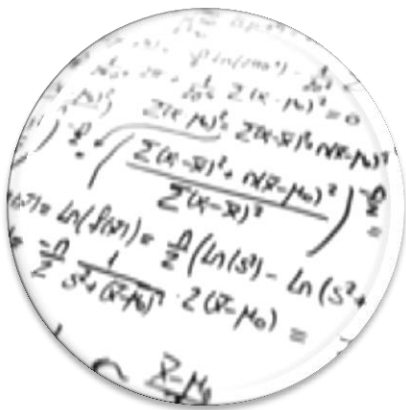
Референсная  
модель

Модель  
активов

Модель  
физической  
архитектуры

Модель  
зонирования





Риск для  
каждой  
угрозы





# Что можно с этим сделать?

- У нас дыра в безопасности.
- Слава богу, хоть что-то у нас в безопасности...

atkritka.com

# Нечто нематериальное, но может помочь

Аудит

Разделение и  
сегментирование  
сетей

Использование  
возможностей  
телекоммуникационно  
го оборудования (ACL,  
port security и т.п.)

Ограничение прав и  
полномочий

Использование  
встроенных  
механизмов  
безопасности

Управление  
конфигурациями

Обучение и  
информирование  
пользователей

Контроль подрядчиков

... и другие  
«традиционные»  
процессы ИБ



снижает риски ИБ без крупных затрат за счет:



Использования имеющегося оборудования



Использования встроенных механизмов защиты



Реализации процессов безопасности



Повышения эффективности организационных и организационно-технических мер

# Как это должно работать?





Хьюстон, у нас проблема

DEMOTIVATORS.RU

# Почему это не работает?

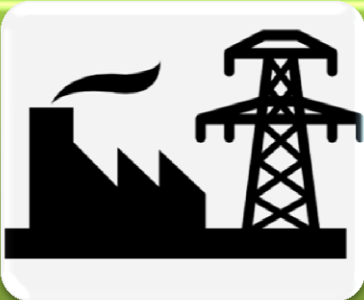




Все равно нужны «красивые блестящие  
штуки»!



# Особенности, влияющие на выбор СЗИ



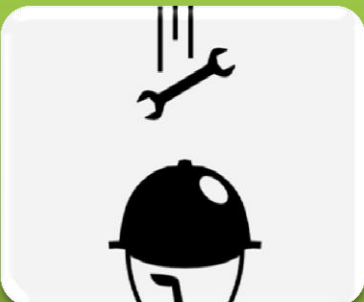
## Отрасль

- Стандарты, нормативы, специфика ТП
- Протоколы передачи данных, ПО, оборудование
- Типичные для отрасли риски



## Специфика рассматриваемой системы

- Уровень документации системы, степень ее актуальности, возможные риски
- Использование проприетарных и слабодокументированных протоколов
- Возможное отсутствие контролируемой зоны
- Климатические условия



## Риски внедрения СЗИ

- Возможное влияние на надежность и доступность АСУ ТП
- Отсутствие или недостаточность технологических окон для полноценной перестройки архитектуры
- Нарушение требований разработчика АСУ ТП
- Сложности с обновлениями
- Отсутствие специалистов

# Особенности, влияющие на эффективность эксплуатации СЗИ

Актуальность и соблюдение требований кибербезопасности

Изменения в объекте защиты, риски и угрозы кибербезопасности

Мониторинг, контроль, анализ и реагирование

Состояние «окружающей среды»: антропогенные и неантропогенные факторы

Развитие технологий, изменения в стандартах, руководящих документах

# Из чего выбирать?





## Palo Alto Next Generation Firewall

- Легкая интеграция сервисов безопасности в существующие сети АСУ ТП за счет подключения в прозрачном режиме или используя сегментацию на L2
- Идентификация и контроль как протоколов общего назначения так и промышленных протоколов, работающих поверх IP (MODBUS, DNP3, IEC-6870-5-104, ICCP,...)
- Возможность создания сигнатур для «самописных» и отечественных протоколов и их отдельных функций
- Применение политик безопасности на уровне приложений и учетных записей операторов, контроль их действий
- Защита от уязвимостей (70+ сигнатур IPS для протоколов Modbus, DNP3, ICCP и SCADA систем)
- Защита от вредоносного ПО (Stuxnet, Duqu,...), в том числе «нулевого дня»

## MaxPatrol

- Обнаружение и анализ уязвимостей, в т.ч. в АСУ ТП
- Инвентаризация и контроль изменений
- Оценка защищенности и контроль соответствия требованиям
- Режимы аудита, инвентаризации и pentest
- Контроль эффективности обеспечения ИБ





## HP ArcSight Security Intelligence



Комплексное решение **HP ArcSight Security Intelligence** обеспечивает централизованный сбор, обработку и хранение событий безопасности от различных источников (решение позволяет осуществить интеграцию практически с любым типом приложения).

**RedSeal** – система визуализации и анализа рисков сетевой безопасности. Позволяет:

- Проводить анализ уязвимостей
- На основе перечня уязвимости и конфигураций сетевых устройств и СЗИ строить карту сетевых угроз, с определением актуальных векторов атаки
- автоматизировать процесс сбора конфигураций сетевых устройств и СЗИ;
- моделировать угрозы и уязвимости ИБ;
- выполнять анализ соответствия требованиям информационной безопасности.



## Промышленный МЭ Tofino Eagle/Xenon



- Разработан в рамках стандарта IEC 62351 (*Security for Industrial Automation and Control Systems*)
- Создание безопасных зон внутри промышленной зоны
- Анализ трафика большинства известных промышленных протоколов с целью инспекции контента (функция DPI)
- Возможность использования L2 VPN
- Поддержка SDK с возможностью разработки собственных модулей (только для Xenon)

## Phoenix Contact mGuard



- Промышленные межсетевые экраны
- Функции Deep Packet Inspection для распространенных промышленных протоколов
- Возможности использования модулей системы обнаружения и предотвращения вторжений и потокового антивируса
- Поддержка IPsec VPN в соответствии с RFC
- Есть версия устройства с GSM/3G модулем и GPS





## Symanitron S200

- Подключение устройств с последовательными и Ethernet портами
- Отказоустойчивое межсетевое соединение через Ethernet либо сотовую сеть
- Поддержка протоколов SCADA систем
- Поддержка протоколов IPSec для распределенных SCADA систем
- Безопасная коммутация с использованием VPN
- Предназначен для использования в тяжёлых промышленных условиях
- Сотовый модем 2G/3G с 2 sim-картами для подключения к двум операторам сотовой связи
- Поддерживается системой сетевого управления Sycon
- Соответствует IEC 61850-3



## АПК «ЩИТ»

АПК «ЩИТ» — многофункциональное устройство для обнаружения и предотвращения несанкционированных вторжений (Intrusion Prevention System — IPS) в информационные инфраструктуры систем автоматического управления различными технологическими процессами

- 83 алгоритма обнаружения атак
- 10 патентов
- 10 промышленных протоколов
- 10 протоколов в разработке





## **Kaspersky Endpoint Security**

- Комплекс антивирусных решений для АСУ ТП
- Мониторинг и контроль запуска программ на основе белых списков
- Контроль устройств
- Мониторинг активности сети
- Персональный МЭ

**Kaspersky Trusted Monitoring System** - комплексное решение для защиты промышленных объектов антивирусных решений для АСУ ТП:

- Контроль целостности сети (инвентаризация IP-устройств)
- Контроль целостности PLC-пакетов (контроль изменений микропрограммы PLC)
- Обнаружение сетевых аномалий и атак (детектирование нетипичных и нелегитимных команд или последовательностей команд)
- Обнаружение управляющих команд, приводящих к нарушению технологического процесса (семантический анализ команд)
- Средства хранения и ретроспективного анализа для расследования инцидентов

Ну и напоследок...



**Даже самые передовые и дорогие СЗИ не будут эффективно работать без выстроенных на объекте организационных мер, процедур и процессов безопасности.**



**Риски в АСУ ТП совсем другие, нежели в корпоративных системах. Другая и цена ошибок.**



Спасибо за внимание!

