10 YEARS JETSECURITY CONFERENCE 2019

Промышленная кибербезопасность в России и мире

Подходы, вызовы, особенности. Кибербезопасность АСУ ТП от Шнейдер Электрик (Сделано в России)

Сухих Ян Андреевич

Руководитель направления ИБ
yan.Sukhikh@se.com

Life Is On Schneider Electric

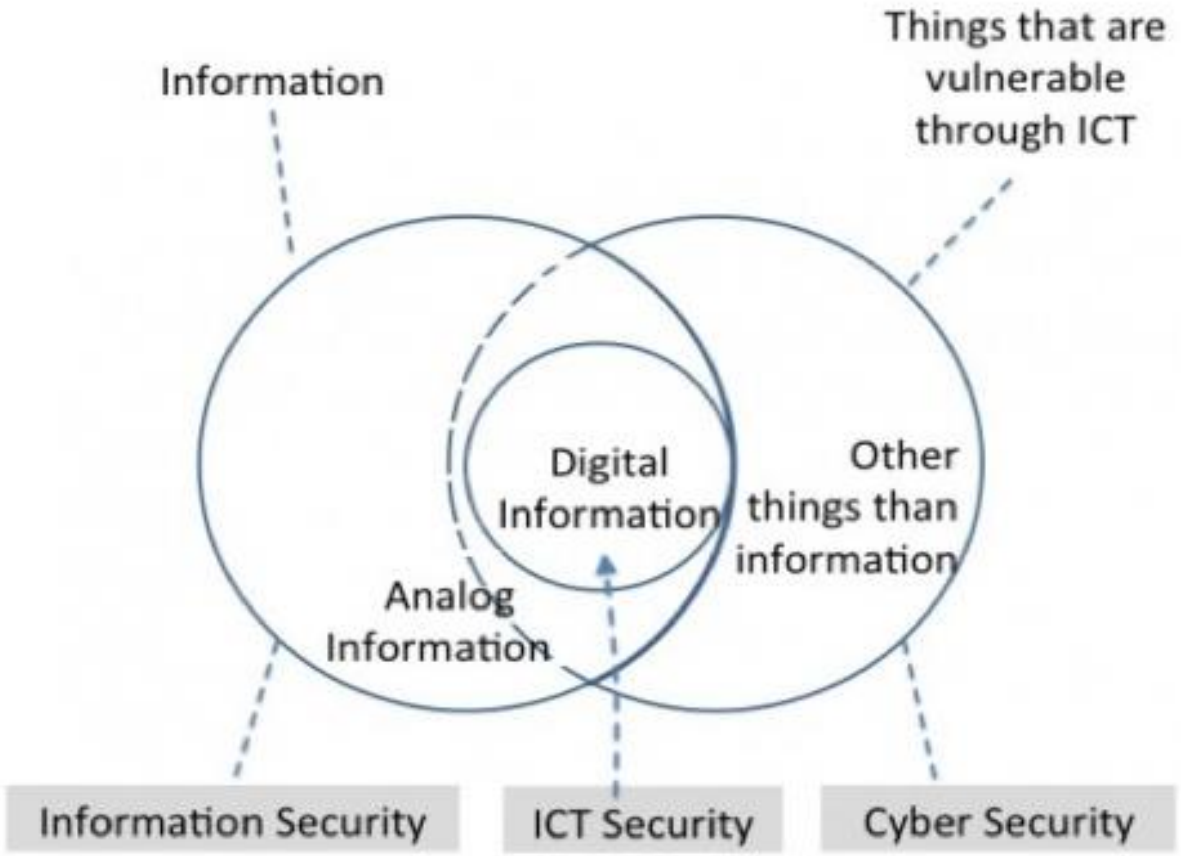
1	Подходы к кибербезопасности
2	Риск-ориентированный подход
3	Типовая защищенная АСУ ТП
4	Вызовы отрасли

10 YEARS JETSECURITY CONFERENCE 2019

Life Is On Schneider Electric

Подходы к кибербезопасности

Терминология



В России термин кибербезопасность не узаконен, поэтому под информационной безопасностью может подразумеваться как Information Security, так и ICT и Cyber Security (Cybersecurity)

ICT - Information and Communication technology (ИКТ)

Подходы к защите КИИ (Россия vs США)

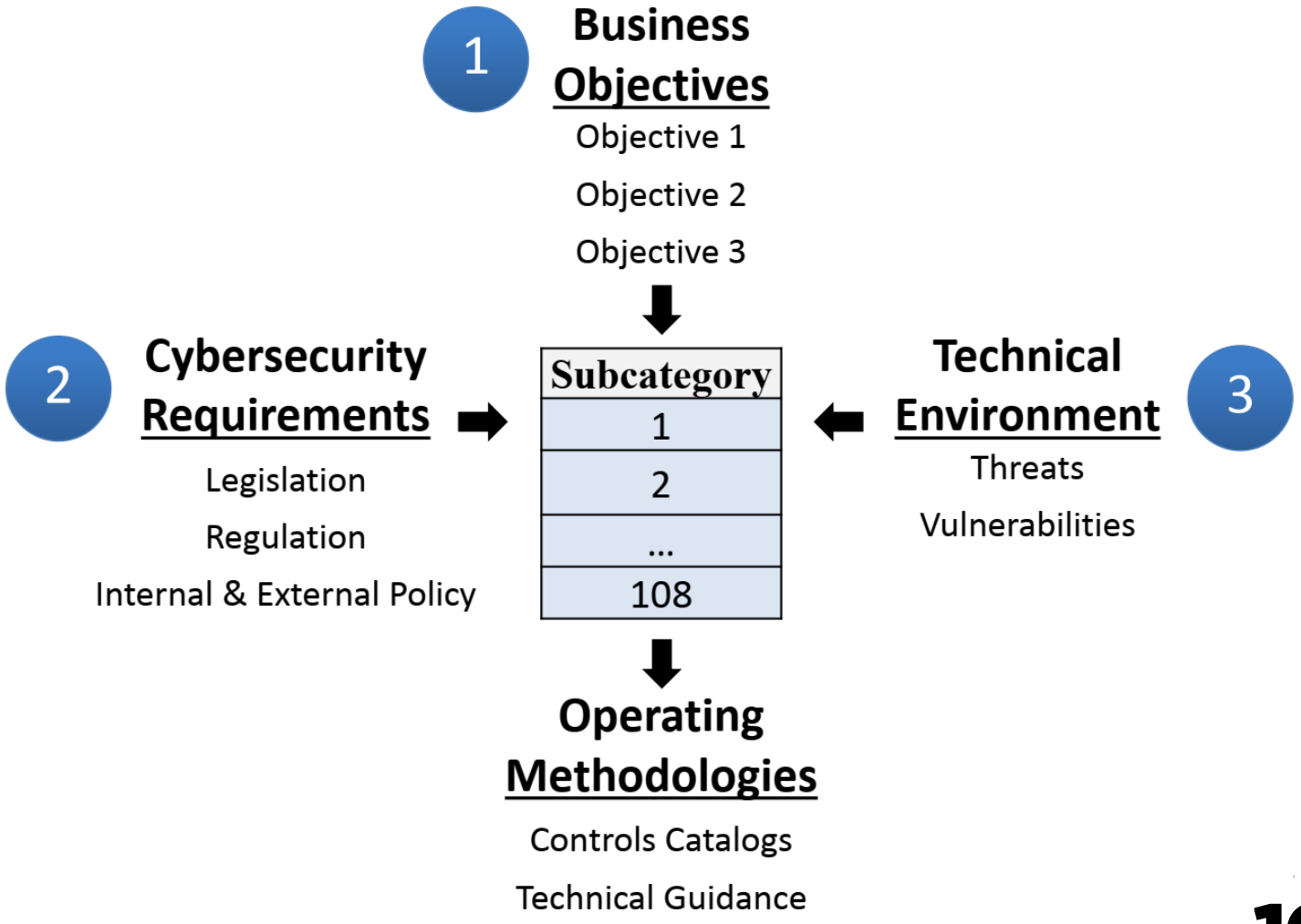
CISA (under DHS)

Cybersecurity and Infrastructure Security Agency (CISA) under Department of Homeland Security (DHS) / ФСТЭК + Правительство РФ

National Cybersecurity and Communications Integration Center (NCCIC)	Critical Infrastructure Cyber Community Voluntary Program (C³VP)	National Infrastructure Coordinating Center
С 2009 года выступает как интеграционный хаб для информации связанной с ИБ, как центр технических компетенций, аналитики и центр по реагированию на инциденты	Добровольная программа/партнерство DHS с собственниками КИ с целью продвижения и популяризации риск-ориентированного подхода, NIST framework for improving critical infrastructure cybersecurity	Координация активностей, обмен информацией между государственными структурами и субъектами КИ при возникновении инцидента с целью минимизации последствий.
Аналог в РФ – НКЦКИ (ГосСОПКА), ФСБ	Аналогов нет/187-ФЗ + УК 274.1	Аналогов нет. МЧС? ФСБ? Ростехнадзор?

Подходы к защите КИИ (Россия vs США)

Подход в США



Подход в России

Методология для построения комплексных систем кибербезопасности. Framework for Improving Critical Infrastructure Cybersecurity, NIST

Структура фреймворка

Функции

- Identify/Идентификация
- Protect/Защита
- Detect/Обнаружение
- Respond/Реагирование
- Recover/Восстановление

- Функции позволяют структурировать активности по основным направления деятельности в области кибербезопасности
- Каждая функция делится на категории и подкатегории, которые детально раскрывают их суть
- Подкатегории ориентированы не на продукты/решения, но на действия/операции, которые должны быть реализованы в организации
- Дополнительно приведены ссылки на стандарты, в которых подробнее описаны возможные варианты реализации

Функция «Защита», категория «Управление идентификаторами, авторизация и контроль доступа»

Защита	**Управление идентификаторами, авторизация и контроль доступа (ЗА.КД):** Доступ к физическим, информационным и смежным ресурсам ограничен и доступен только авторизованным пользователям, процессам и устройствам. Управление доступом осуществляется с учетом выполненного анализа рисков неавторизованного доступа к процессам и транзакциям	ЗА.КД-1: Идентификаторы и учетные данные определены и управляются. Используется практики подтверждения учетной информации, отзыва учетных данных, проводятся аудиты устройств, пользователей, процессов доступ к которым ограничен.	Настройка локальных групповых политик безопасности и/или контроллера домена, установка требований к паролям(сложность, частота смены), уникальность учетных записей, защита передаваемой аутентификационной информации, централизованное управление учетными записями (изменениями, удалением, восстановлением) и т.п.
		ЗА.КД-2: Внедрены практики управления физическим доступом к активам. Свободный доступ ограничен	В зависимости от критичности системы/устройства/процесса, модели угроз и культуры персонала меры по обеспечению физического доступа могут очень сильно разниться
		ЗА.КД-3: Внедрены практики управления удаленным доступом (если используется)	Реализация безопасного удаленного доступа процедура достаточно сложная, но в некоторых случаях необходимая. Реализация зависит от критичности системы/устройства/процесса

Функция ИАФ в приказе ФСТЭК №239

I. Идентификация и аутентификация (ИАФ)	
ИАФ.0	Разработка политики идентификации и аутентификации
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов
ИАФ.2	Идентификация и аутентификация устройств
ИАФ.3	Управление идентификаторами
ИАФ.4	Управление средствами аутентификации
ИАФ.5	Идентификация и аутентификация внешних пользователей
ИАФ.6	Двусторонняя аутентификация
ИАФ.7	Защита аутентификационной информации при передаче

Уровень зрелости организации (C2M2)

Уровень зрелости организации на примере Cybersecurity Capability Maturity Model v1.1

	Управление кибер-рисками	Управленческие практики
MIL0		
MIL1	a. Кибер-риски определены b. Идентифицированные риски управляются	a. Базовые практики применяются, но часто от случая к случаю
MIL2	a. Аудит рисков проводится с целью выявления рисков в соответствии со стратегией по RM b. Риски документируются c. Риски анализируются и расставляются приоритеты в соответствии со стратегией d. Риски постоянно контролируются e. Риски анализируются с учетом архитектур IT/OT сетей	a. Процессы описаны b. Выгодоприобретатели процессов определены и вовлечены в работу c. Адекватные ресурсы выделены (люди, инструменты, финансирование) d. Стандарты и/или руководства используются для управления процессами по внедрении практик

Уровень зрелости организации (C2M2)

Уровень зрелости организации на примере Cybersecurity Capability Maturity Model v1.1

	Управление кибер-рисками	Управленческие практики
MIL3	a. Программа риск менеджмента опирается на политики и процедуры по управлению рисками которые воплощают в жизнь стратегия. b. Актуальная архитектура средств обеспечения кибербезопасности используется при анализе рисков c. Реестр рисков (репозиторий выявленных рисков) используется в процессе управления рисками	a. Активности прописаны в политиках и других руководящих документах, поддерживаются высшим руководством b. Политики включают требования по комплаенсу c. Активности периодически проверяются на соответствие политикам d. Ответственность и полномочия для выполнения необходимых действий назначены конкретным людям e. Персонал имеет адекватные навыки и знания для выполнения задач

Риск ориентированный подход

Безопасность в промышленности

Модель слоев защит / Модель «швейцарского сыра» (Swiss cheese model)

Как происходят аварии и возможная роль кибератак в ней

Пример риск-ориентированного подхода к анализу кибер-рисков

Анализируется рабочая таблица HAZOP + последствия

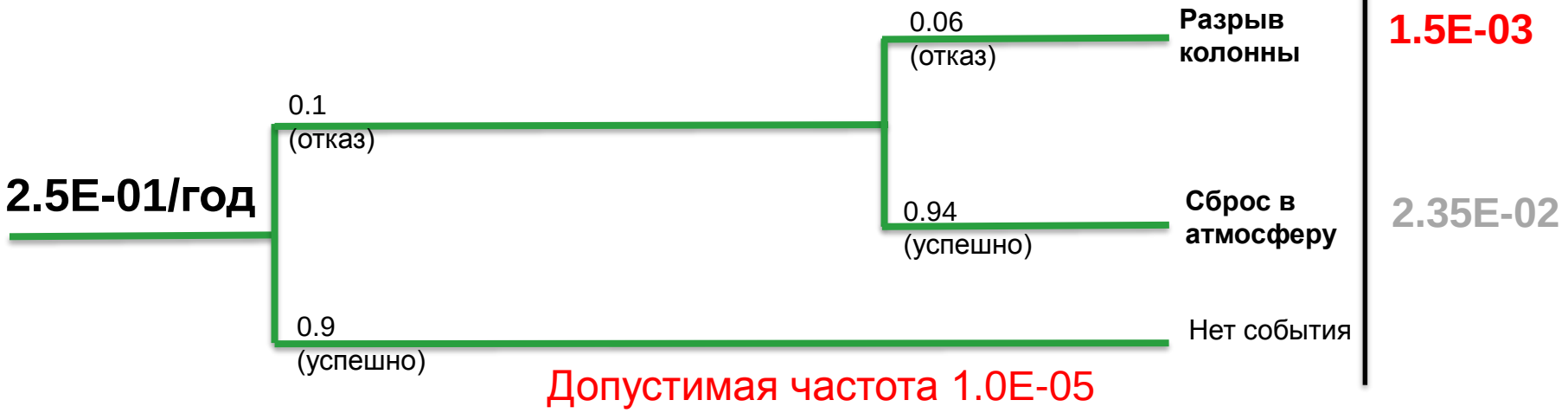
Причина	Последствия	Последствия Категория: человеческие жертвы	Допустимые потери и целевой фактор риска
Слишком высокий расход			
Отказ клапана FV XX (открыт)	Повышение давления в реакторе. Возможен взрыв и выброс материалов	**Смерть одного человека**	Допустимая частота смертельного случая на заводах корпорации «Ч» - 1 чел/год на 100,000 1.0*E-05
Отказ КИП, датчик LT XX (низ шкалы)	Повышение давления в реакторе. Возможен взрыв и выброс материалов	**Смерть одного человека**	

ОТКАЗ КОНТУРА РЕГУЛИРОВАНИЯ – 1 раз в 4 года => 2.5E-01

Пример риск-ориентированного подхода к анализу кибер-рисков

Диаграмма LOPA (дерево отказов)

Событие	СЛОЙ ЗАЩИТЫ №1	СЛОЙ ЗАЩИТЫ №2	Результат	Частота
Отказ контура регулирования давления	Действия оператора на сигнализацию	Предохранительный клапан		

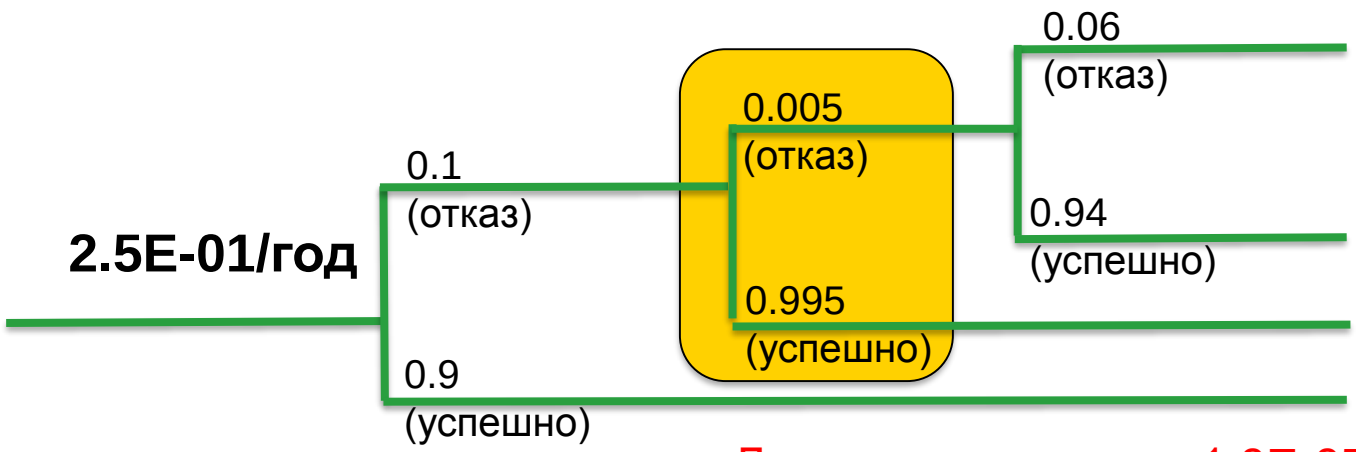


Допустимая частота 1.0E-05

Пример риск-ориентированного подхода к анализу кибер-рисков (продолжение)

Диаграмма LOPA (дерево отказов)

Событие	СЛОЙ ЗАЩИТЫ №1	СЛОЙ ЗАЩИТЫ №2	СЛОЙ ЗАЩИТЫ №3	Результат	Частота
Отказ контура регулирования давления	Действия оператора на сигнализацию	SIL 2 → SIF	Предохранительный клапан		

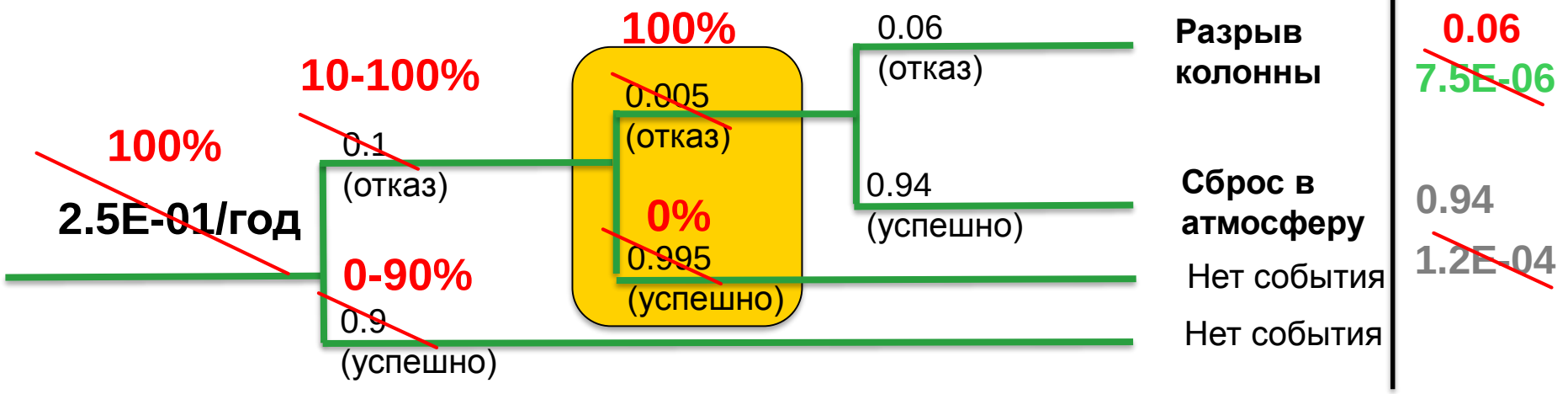


Допустимая частота 1.0E-05

Возможные последствия кибератаки

Диаграмма LOPA (дерево отказов) после успешной кибератаки

Событие	СЛОЙ ЗАЩИТЫ №1	СЛОЙ ЗАЩИТЫ №2	СЛОЙ ЗАЩИТЫ №3	Результат	Частота
Отказ контура регулирования давления	Действия оператора на сигнализацию	SIL 2 → SIF	Предохранительный клапан		



Допустимая частота 1.0E-05

Количественна оценка рисков

Concept	Formula
Exposure factor (EF)	%
Single loss expectancy (SLE)	SLE = AV * EF
Annualized rate of occurrence (ARO)	# / year
Annualized loss expectancy (ALE)	ALE = SLE * ARO or ALE = AV * EF * ARO
Annual cost of the safeguard (ACS)	$ / year
Value or benefit of a safeguard	(ALE1 – ALE2) – ACS

AV – стоимость актива (asset value)
EF – коэффициент воздействия (exposure factor)
SLE – убыток от единичного инцидента (single loss expectancy)
ARO – средняя частота возникновения в год (annualized rate of occurrence)
ALE – ожидаемые ежегодные убытки от воздействия риска (annualized loss expectancy)
ACS – ежегодная стоимость защитных мер (annualized cost of the safeguard)
Эффект от внедрения защитных мер – **(ALE1-ALE2) - ACS**

Какие вызовы стоят перед индустрией?

Мир оказался не готов к безопасной цифровизации

Нехватка кадров

Согласно расчетам мировой дефицит кадров в области кб к 2021 году составит 3,5 млн человек

Низкая защищенность предприятий

Промышленные предприятия не успевают за развитием кибер-угроз + недоверие к серьезности проблемы на уровне высшего руководства

Вызовы

Протекционизм

Огромное количество устаревшего оборудования

Жизненный цикл систем АСУ ТП составляет 15-25 лет

(I)IoT и облачные технологии

Реализация данных технологий многими игроками не учитывает кибер-риски

Выводы и прогнозы

Несмотря на кибер-риски организации продолжат процесс цифровизации производства

- (I)IoT приносит как выгоды, так и большие риски
- Для управления кибер-рисками и для поддержки процессов принятия решений должен применяться риск ориентированный подход
- Зависимость промышленности от цифровых технологий будет расти
- Законодательные требования и ограничения – риск для отрасли в плане цифровизации
- Новые векторы атак и возможные последствия труднопредсказуемы

Недостаток ресурсов в области кибербезопасности заставит компании использовать услуги третьих поставщиков (SOC, облачные технологии и т.п.)

- Развитие полной локальной компетенции в области ИБ выглядит неэффективным

Выводы и прогнозы

Организациям необходимо найти свой баланс между рисками и потенциальной прибылью от внедрения новых технологий

- Панацеи или «универсальной пилюли» не существует
- Необходимо использовать лучшие мировые практики
- Нужно быть более защищенным, чем другие компании отрасли

Сухих Ян Андреевич

Руководитель направления ИБ

АО «Шнейдер Электрик»

M: +7 910 475 1750

D: +7 495 777 999 0 ext. 1268

E: yan.sukhikh@se.com

10 YEARS JETSECURITY CONFERENCE 2019 Life Is On Schneider Electric

10 YEARS JETSECURITY CONFERENCE 2019

СПАСИБО ЗА ВНИМАНИЕ!

Сухих Ян Андреевич

Руководитель направления ИБ
Yan.Sukhikh@se.com

Life Is On Schneider Electric

Типовая защищенная АСУ ТП для распределенных объектов

Распределенные объекты

Состав комплексного решения по кибербезопасности

Доступ

- Авторизация, аутентификация и аккаунтинг
- Многофакторная аутентификация
- Сегментирование сети
- Безопасный удаленный доступ
- Физическая безопасность

Защита

- Защита конечных узлов (Anti Virus, Anti Malware)
- DLP, HIPS, белые списки
- Управление устройствами
- Доверенная загрузка/управление процессами
- Patch Management

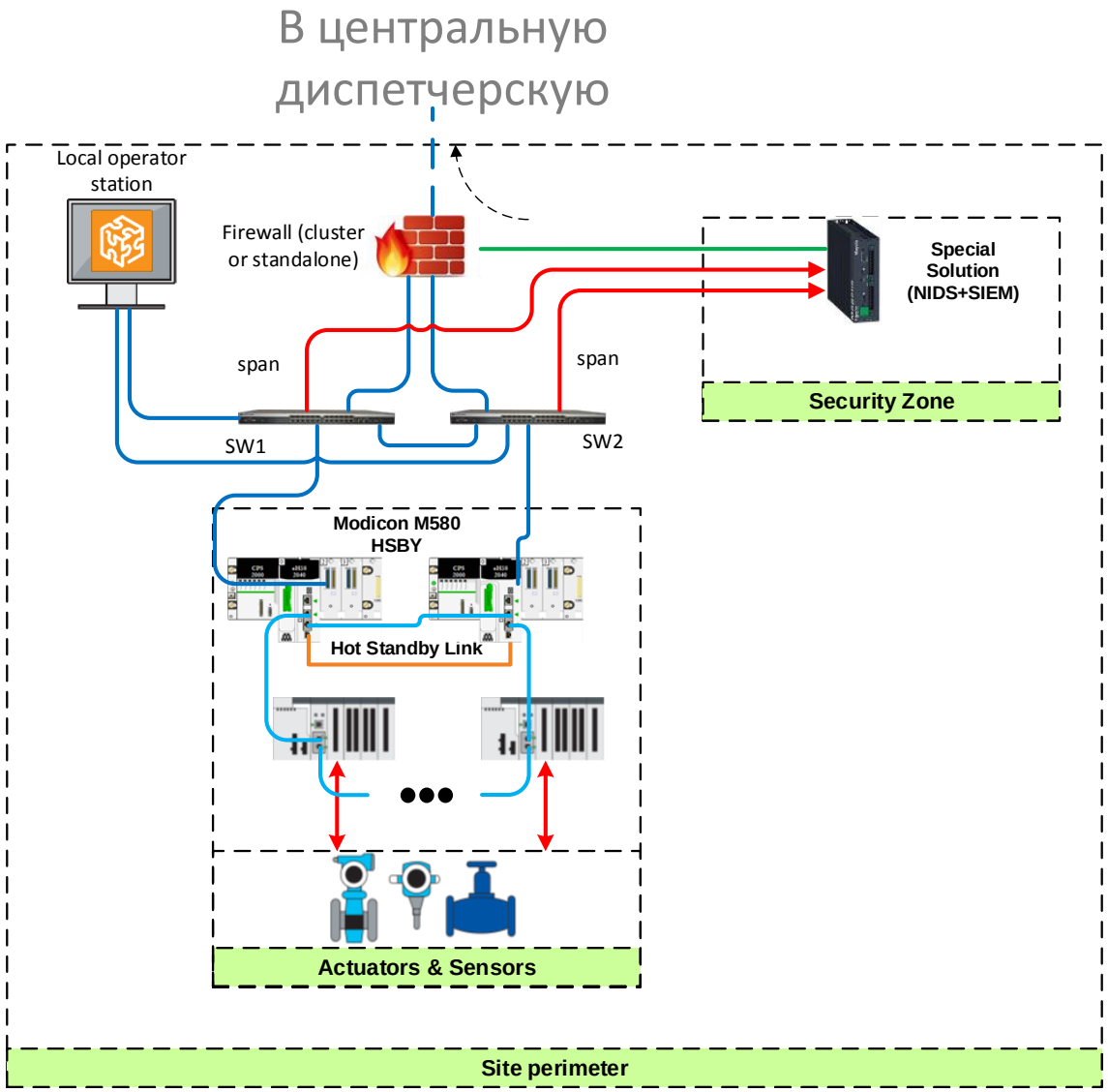
Обнаружение

- Security Information & Event Management (SIEM)
- Системы мониторинга сети
- Обнаружение аномалий
- СОВ/СПВ (NIDS/NIPS)
- SOC (центры управления)

Реагирование

- Резервное копирование и восстановление
- Forensics (расследование киберпреступлений)
- Системы реагирования на инциденты

Защита распределенных объектов



Основные особенности:

- фокус на малые и средние объекты
- Харденинг АРМ
- Антивирусная защита, контроль устройств и запуска приложений
- Харденинг ПЛК (обязательно наличие встроенных функций безопасности)
- Харденинг сетевого оборудования
- МСЭ
- Адаптированное для небольших систем АСУТП решение класса NIDS + SIEM

Защита распределенных объектов

Доступ

- МСЭ
- Встроенный функционал ПЛК, ОС АРМ, сетевого оборудования
- Разделение сетей с выделение зоны безопасности

Защита

- МСЭ
- Встроенный функционал ПЛК, ОС АРМ, сетевого оборудования
- Защита конечных узлов (АВЗ, контроль подключаемых устройств, контроль приложений и тп)

Обнаружение

- Magelis iPC + ISIM
- Службы SOC
- Syslog

Реагирование

- Службы SOC

10 YEARS JETSECURITY CONFERENCE 2019

СПАСИБО ЗА ВНИМАНИЕ!

Сухих Ян Андреевич

Руководитель направления ИБ
Yan.Sukhikh@se.com

Life Is On Schneider Electric