Вопросы защиты информации АСУ ТП объектов КИИ

Владимир Карантаев

к.т.н. эксперт IEC, IEEE, CIGRE

Автор блога: https://smartgridib.blogspot.com/

Т. +79152211596

МОСКВА 01 Ноября , 2018

Не о чем поспорить? А термины? ОТ или АСУ?

Gartner defines operational technology (OT) as: "hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in asset-centric enterprises, particularly in production and operations."

Автоматизированная система управления (АСУ) - комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами;

В зависимости от вида деятельности выделяют.... следующие виды АС: автоматизированные системы управления (АСУ)...

В зависимости от вида управляемого объекта (процесса) АСУ делят, например на АСУ технологическими процессами (АСУТП), АСУ предприятиями (АСУП) и т.д.

34.003-90

Предыстория в цифрах

5

Специально разработаны для атак на АСУ ТП

- Stuxnet
- Havex
- Blackenergy
- Industroyer
- TRITON

1

Специально разработаны для атак на ПАЗ

- TRITON

3

Специально разработаны для нарушения технологического процесса

- Stuxnet
- Industroyer
- TRITON

Предыстория в развитии методологии

IT KILL CHAIN

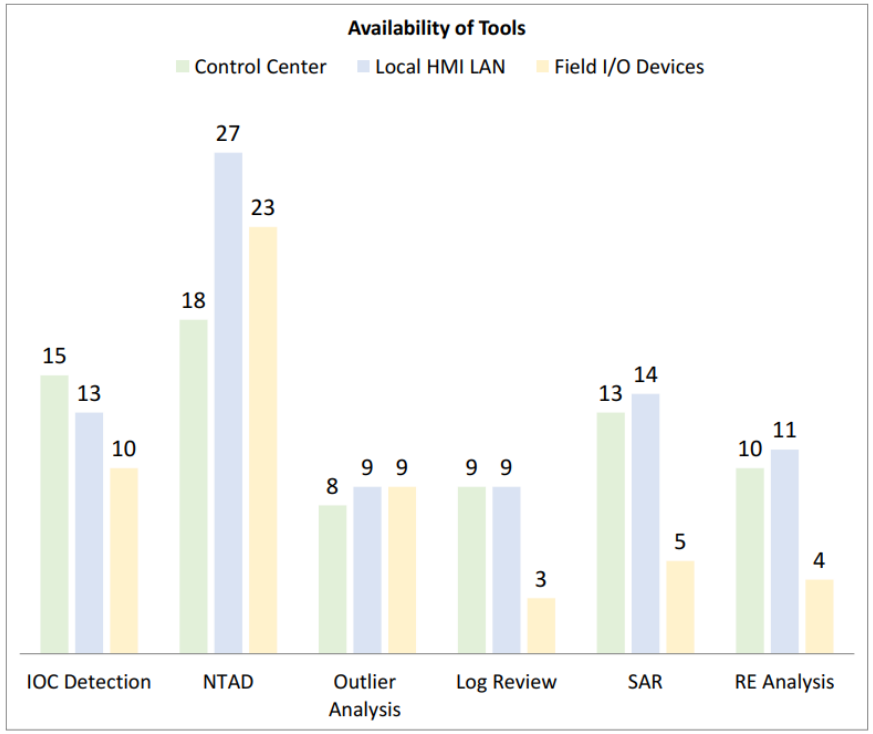
- **Разведка.** Исследование, идентификация и выбор целевой системы для взлома.
- **Вооружение.** Оснащение тулзами и malware для совершения нападения
- **Доставка.** Донесение вредоносного контента до целевой системы
- **Заражение.** Запуск вредоносного кода или эксплуатация уязвимости системы
- **Инсталляция.** Открытие удаленного доступа и другие действия с зараженной системой
- **Получение управления.** Управление зараженной системой.
- **Выполнение действий.** Сбор, кража, отправка данных, шифрование файлов, подмена и удаление данных

OT KILL CHAIN

- **Разработка.** Определение типа целевой системы АСУ. Разработка зловреда.
- **Тестирование.** Тестирование зловреда в инфраструктуре атакущего.
- **Доставка.** Передача зловреда в атакуемую инфраструктуру, с модулями реализующими логику атаки на АСУ
- **Установка/Модифицирование.** Установка и маскирование под легитимное ПО АСУ, изменение логики работы АСУ.
- **Проведение атаки.**

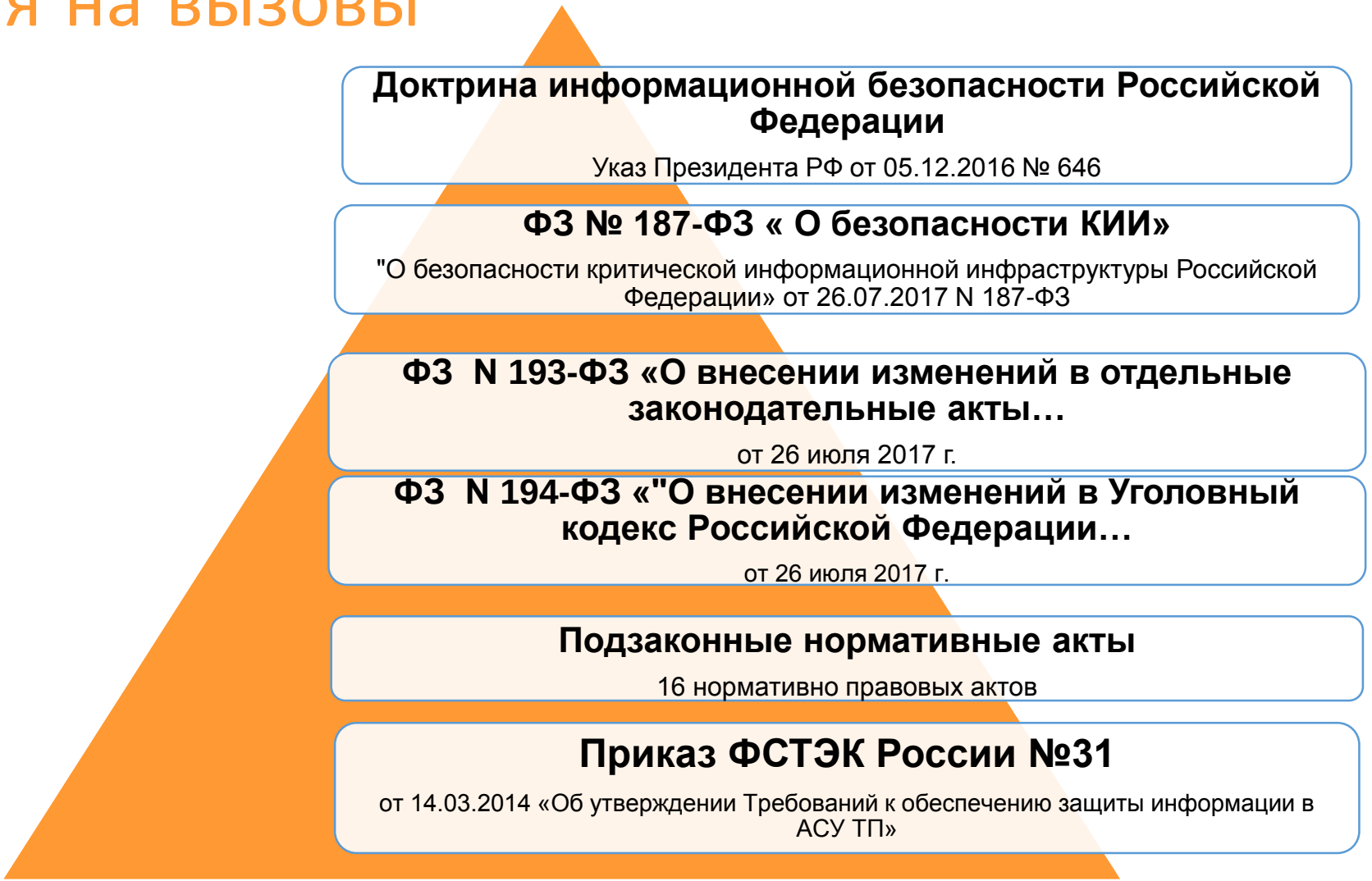
Предыстория в развитии технологий

1. Multi-Purpose Tools
2. IOC Detection Tools
3. Network Traffic Anomaly Detection Tools
4. Outlier Analysis Tools
5. Log Review Tools
6. System Artifact Review Tools
7. Reverse Engineering Analysis Tools



A Survey of Security Tools for the Industrial Control System Environment
The Idaho National Laboratory (INL) USA, 2017

Реакция на вызовы



Доктрина ИБ РФ

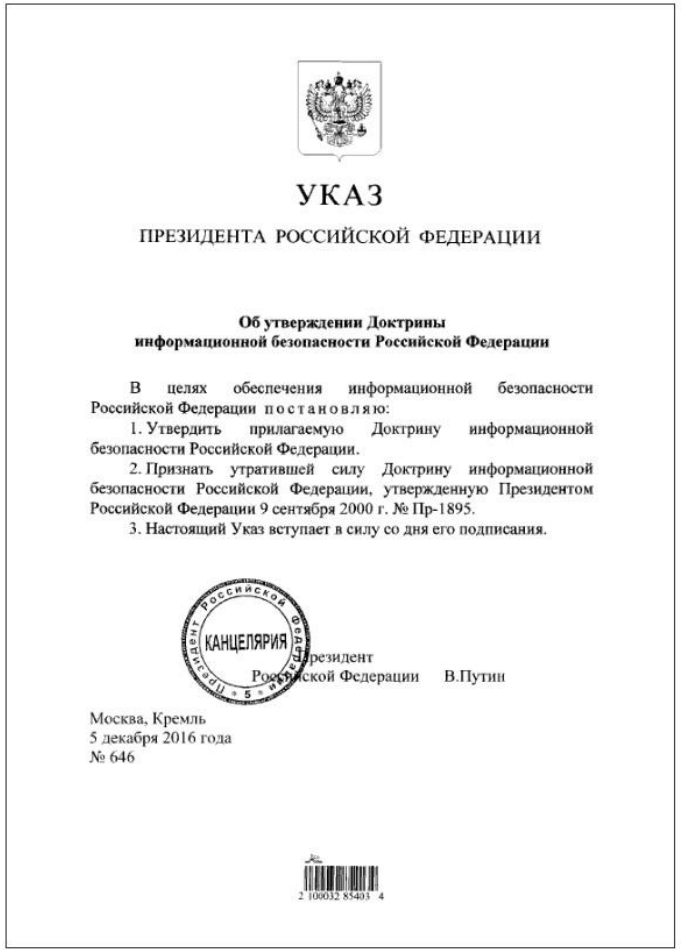
- **Национальные интересы в информационной сфере:**

Обеспечение устойчивого и бесперебойного функционирования ..... критической информационной инфраструктуры Российской Федерации.

- **Основные информационные угрозы и состояние информационной безопасности:**

.... практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз.

.... в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры.



УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

Об утверждении Доктрины информационной безопасности Российской Федерации

В целях обеспечения информационной безопасности Российской Федерации п о с т а н о в л я ю:

1. Утвердить прилагаемую Доктрину информационной безопасности Российской Федерации.

2. Признать утратившей силу Доктрину информационной безопасности Российской Федерации, утвержденную Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.

3. Настоящий Указ вступает в силу со дня его подписания.

КАНЦЕЛЯРИЯ

Президент Российской Федерации В.Путин

Москва, Кремль
5 декабря 2016 года
№ 646

Доктрина ИБ РФ

- **Стратегические цели и основные направления обеспечения информационной безопасности:**

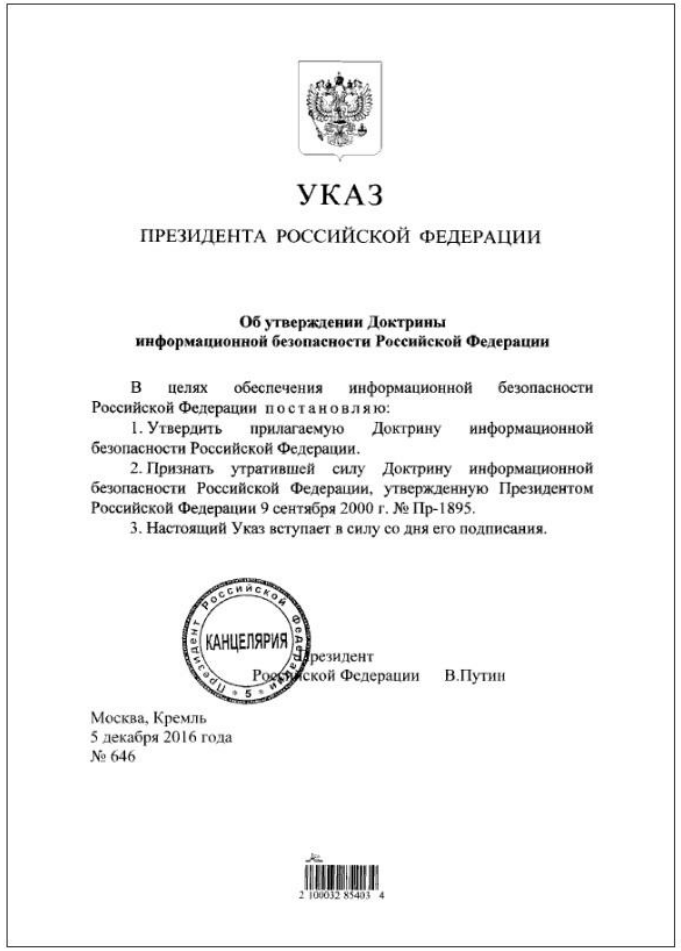
...защита критической информационной инфраструктуры.

Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:

повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры;

создание и внедрение информационных технологий, изначально устойчивых к различным видам воздействия;

Участниками системы обеспечения информационной безопасности являются: собственники объектов критической информационной инфраструктуры



УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

Об утверждении Доктрины информационной безопасности Российской Федерации

В целях обеспечения информационной безопасности Российской Федерации п о с т а н о в л я ю:

1. Утвердить прилагаемую Доктрину информационной безопасности Российской Федерации.

2. Признать утратившей силу Доктрину информационной безопасности Российской Федерации, утвержденную Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.

3. Настоящий Указ вступает в силу со дня его подписания.

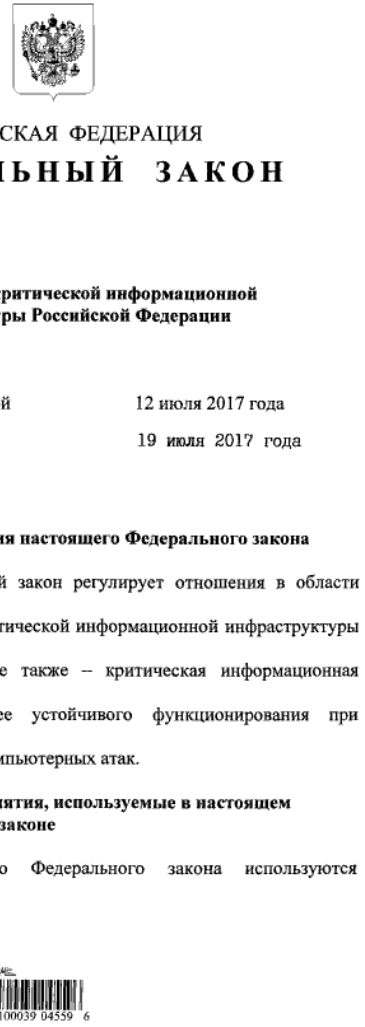
КАНЦЕЛЯРИЯ

Президент Российской Федерации В.Путин

Москва, Кремль
5 декабря 2016 года
№ 646

№ 187-ФЗ О Безопасности КИИ

- Провести категорирование объекта КИИ
- Обеспечить безопасность объекта КИИ
- Обеспечить взаимодействие объекта КИИ с ГосСОПКА



РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О безопасности критической информационной инфраструктуры Российской Федерации

Принят Государственной Думой 12 июля 2017 года

Одобрен Советом Федерации 19 июля 2017 года

Статья 1. **Сфера действия настоящего Федерального закона**

Настоящий Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также – критическая информационная инфраструктура) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Статья 2. **Основные понятия, используемые в настоящем Федеральном законе**

Для целей настоящего Федерального закона используются следующие основные понятия:

Самоидентификация:

ФЗ-187 «О Безопасности КИИ РФ»

Статья 2. Основные понятия…

Субъекты критической информационной инфраструктуры - это

- ✓ **…..** российские юридические лица …, которым на праве собственности, аренды или на ином законном основании принадлежат:
- ✓ информационные системы,
- ✓ информационно-телекоммуникационные сети,
- ✓ автоматизированные системы управления,
- ✓ функционирующие в сфере …. Энергетики…

Остались сомнения? Изучаем:

- ✓Устав организации.
- ✓Лицензии и иные разрешительные документы на различные виды деятельности.
- ✓Общероссийский классификатор видов экономической деятельности (ОКВЭД).

Основные этапы:

1. Обследование (аудит) бизнес-процессов инфраструктуры.
2. Подключение всех объектов КИИ к ГосСОПКА.
3. Категорирование объектов критической информационной инфраструктуры.
4. Создание системы безопасности значимых объектов КИИ.

   Оценка соответствия (аттестация в случае необходимости) значимых объектов КИИ.

Обследование (аудит) бизнес-процессов и инфраструктуры

Работы:

На подготовительном этапе проводится комплексный аудит инфраструктуры, обеспечивающий дальнейшую возможность проведения дальнейших этапов.

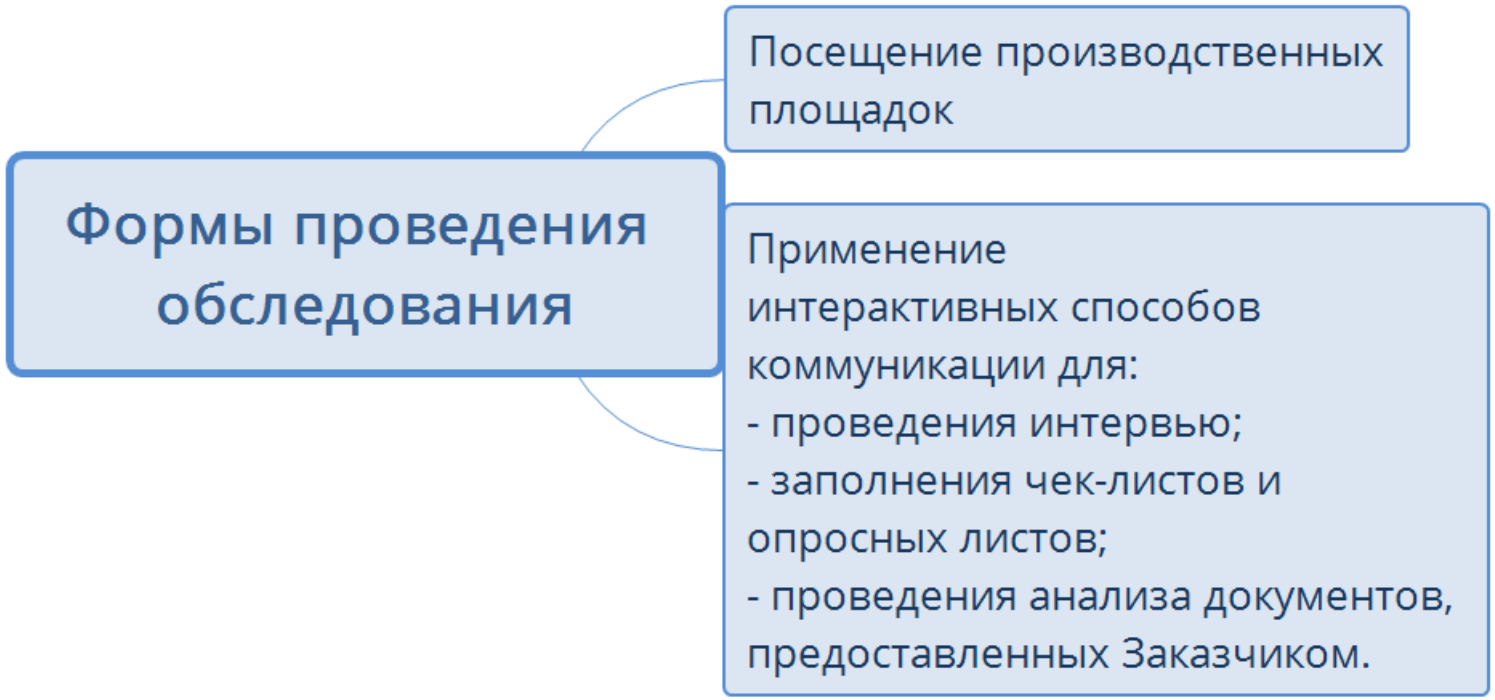
Работы включают в себя:

1. Внешний аудит в виде очного и заочного обследования объектов.
2. Оценку защищённости инфраструктуры заказчика.
3. Проверку корректности собранных заказчиком исходных данных.

Результат:

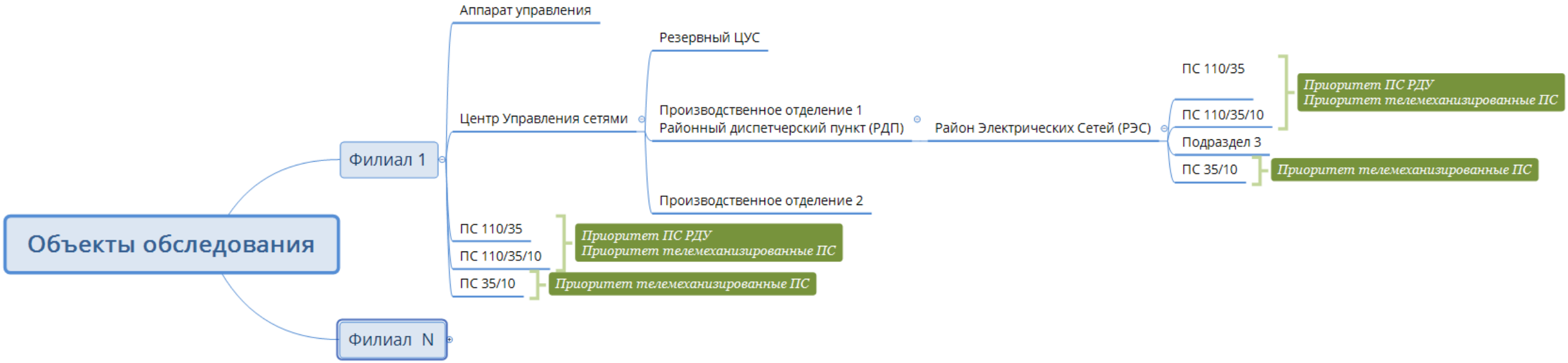
- ✓ Подготовлен «Отчет об обследовании».
- ✓ Подготовлен проект Приказа о создании комиссии по категорированию.
- ✓ Сформирован и согласован перечень объектов КИИ участвующих в них.

Проведение обследования:



Методика проведения базируется на следующих публикациях:
— серия стандартов **ISO/IEC 27000** по вопросам менеджмента информационной безопасности;
— стандарт **ISO 19011:2012**, содержащий руководство по аудиту систем менеджмента;

Объекты обследования:



Пример опросного листа:

№	Вопрос	Примечание
		Заполняются Опросные формы (протоколы интервьюирования) для каждого процесса
1.3.	Укажите вид процесса	
	Процесс может быть управленческим, технологическим, производственным, финансов	
1.4.	Укажите тип процесса	
	Тип процесса может быть основной (глобальный, верхнеуровневый) и вспомогательны	
1.5.	Кто отвечает за процесс?	
	ФИО, должность (как верхнеуровневый ответственный, так и на месте). Сверить с в до "Проект перечня критических процессов"	
2		
2.1.	Нарушение или прекращение процесса может привести к негативным социальным, пол	
	Указывается, является ли по мнению опрашиваемого процесс критическим	
3		
3.1.	Укажите виды обрабатываемой информации в процессе	
	Обрабатываемая информация может быть: персональными данными, конфиденциально тайной, телеизмерениями, телесигнализацией, телеуправлением и др., а таже ее объем (х связи, предоставляемая одновременно оператору и т.д.)	
3.2.	К какому объекту можно отнести процесс?	
	Процесс может происходить в ЦУС, ПО, РЭС, ПС	
3.3.	Укажите другие процессы, с которыми взаимодействует описываемый процесс	
4	Информационные системы (ИС), инф	
4.1.	Какие ИС, ИТС, АСУ реализуют деятельность процесса	
4.2.	Укажите технические средства для каждой ИС, ИТС, АСУ	
	Техническими средствами ИС, ИТС, АСУ могут быть сервера, АРМ, коммутационное мобильные устройства, терминалы обслуживания, администрирования, устройства пол Наличие возможности подключения дополнительных технических средств, программно (включая вопросы по электропитанию, коммутационным портам, местам в стойках)	
4.3.	Укажите программное обеспечение для каждой ИС, ИТС, АСУ	
	Программное обеспечение может быть общесистемными (ОПО), прикладными (ППО) Программное обеспечение может располагаться на любых технических средствах, а так	

Ростелеком

Опросная форма (протокол интервьюирования)

Опросная форма (индивидуальная для каждого процесса)

Информация об Объекте

Наименование объекта: _____ Класс объекта: _____

Расположение объекта: _____

Верхнеуровневый объект: _____ (для ПС указать РЭС, для РЭС

Дата заполнения опросного листа: «___» _____ 2018г.

Информация о контактном лице

ФИО Интервьюируемого: _____ Должность Интервьюируемог

Информация о процессе

1.1. Наименование процесса: _____

1.2. Цель процесса: _____

1.3. Вид процесса: ☐ Управленческий ☐ Технологический

☐ Финансово-экономический ☐ _____

1.4. ТИП процесса: ☐ Основной ☐ Вспомогательный

1.5. Ответственный: _____

2.1. Критический процесс:

☐ Да

☐ Социальная значимость ☐ Политическая значимость

☐ Экономическая значимость ☐ Экологическая значимость

☐ Обеспечение обороны страны, безопасности государства и правопорядка

1

Ростелеком

Опросная форма (протокол интервьюирования)

3.1. Обрабатываемая информация:

☐ ПДн	☐ ГИС	☐ АСУ ТП
☐ УЗ-1	☐ К1	☐ К1
☐ УЗ-2	☐ К2	☐ К2
☐ УЗ-3	☐ К3	☐ К3
☐ УЗ-4		

☐ Коммерческая тайна ☐ Телеизмерения

☐ ААА ☐ Инф. об аварийных событиях

☐ Конфигур. инф-ция

☐ Исторические события (логирование, журналирование)

_____

_____

_____ *(укажите)*

3.2. Процесс принадлежит: ☐ ЦУС ☐ ПО ☐ РЭС ☐ ПС

☐ _____(укажите) ☐ _____(укажите)

Таблица 1 – Взаимодействие процессов

№	Наименование процесса, с которым происходит взаимодействие	Входящий/Исходящий поток	Состав передаваемой информации

Категорирование объектов Критической Информационной Инфраструктуры

Работы:

1. Анализ угроз безопасности и разработка модели угроз и модели нарушителя.
2. Оценка потенциального ущерба в соответствии с перечнем критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ.
3. Категорирование объектов КИИ.
4. Подготовка результатов к отправке во ФСТЭК России.

Результат:

1. Сформирован перечень объектов критической информационной инфраструктуры, с указанием значимости.
2. Определены и документированы угрозы и нарушители безопасности информации.
3. Подготовлены акты категорирования в соответствии с требованиями ФСТЭК.

Создание системы безопасности значимых объектов КИИ

Работы:

1. Разработка технического задания (частного технического задания) на создание системы безопасности
2. Проектирование системы безопасности
3. Разработка рабочей (эксплуатационной) документации
4. Разработка комплекта организационно – распорядительной документации
5. Поставка средств защиты
6. Внедрение организационных и технических мер по обеспечению безопасности значимого объекта

Результат:

1. Спроектирована и разработана и документирована подсистема безопасности.
2. Система внедрена и функционирует

Оценка соответствия значимых объектов КИИ

Работы:

1. Определение формы оценки соответствия.
2. Проведение испытаний системы безопасности.
3. Оформление результатов испытаний.
4. Оформление заключения по оценке соответствия.
5. Сопровождение аттестованных информационных систем КИИ.

Результат:

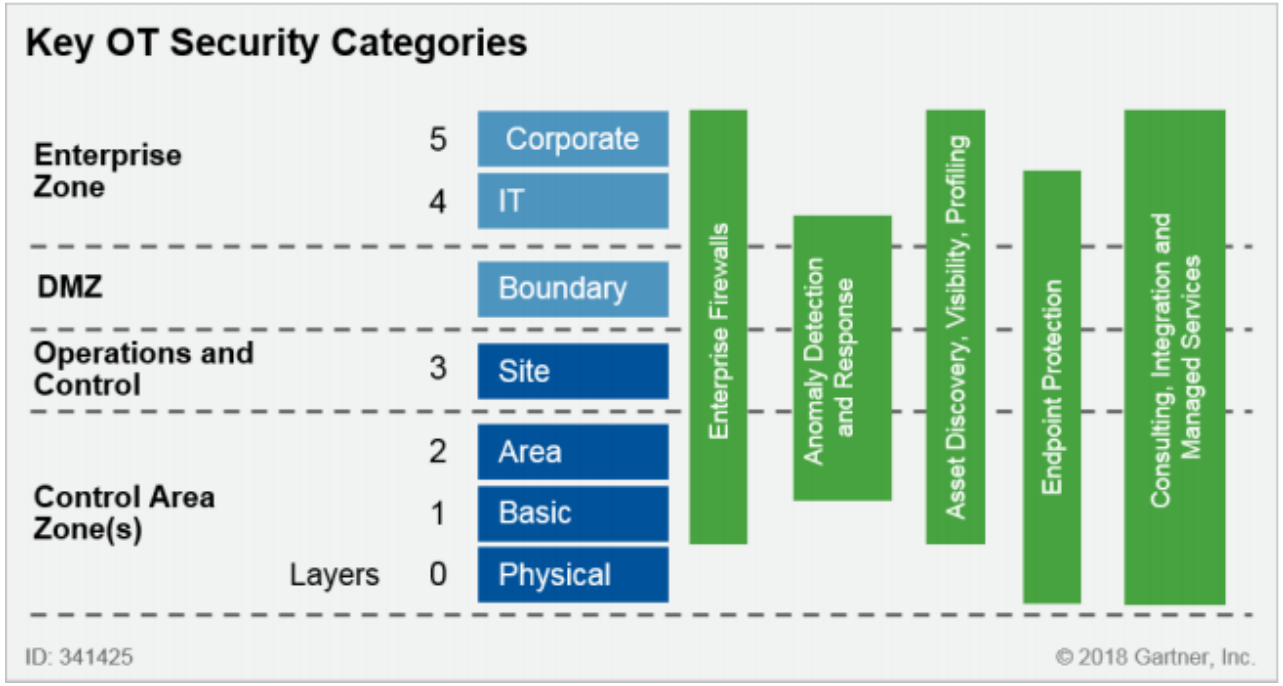
1. Проведены испытания и оценка соответствия.
2. Выданы документы, подтверждающие соответствие объектов КИИ.

Подключение всех объектов КИИ к ГосСОПКА

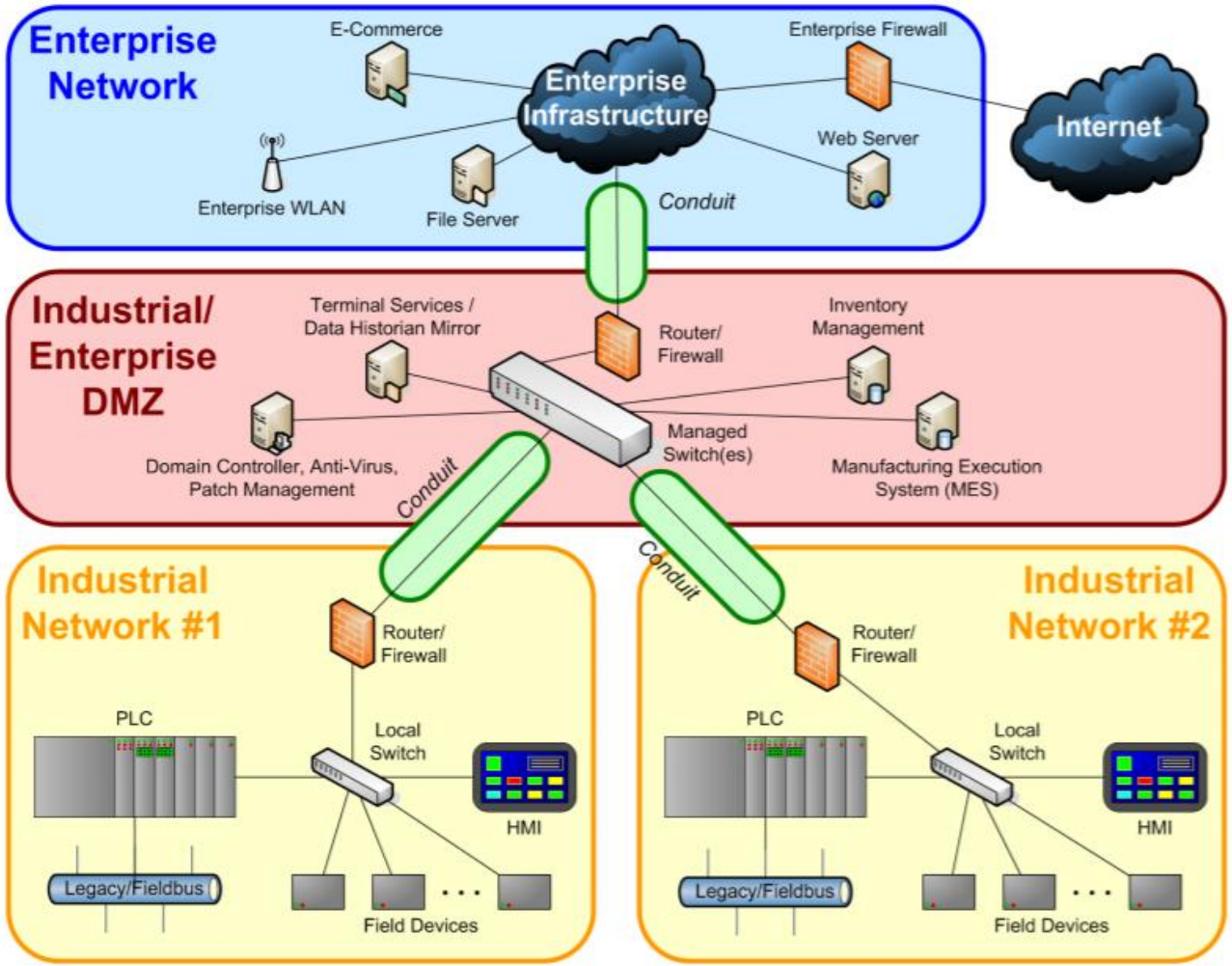
1. В соответствии с федеральным законом от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» все объекты КИИ. Включая незначимые должны быть подключены к ГосСОПКА созданной в рамках указа президента №31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ».

2. Для подключения объектов КИИ к ГосСОПКА должны использоваться ведомственные и/или корпоративные центры, призванные осуществлять мониторинг, анализ и расследование инцидентов, анализ защищённости и целый ряд других функций.

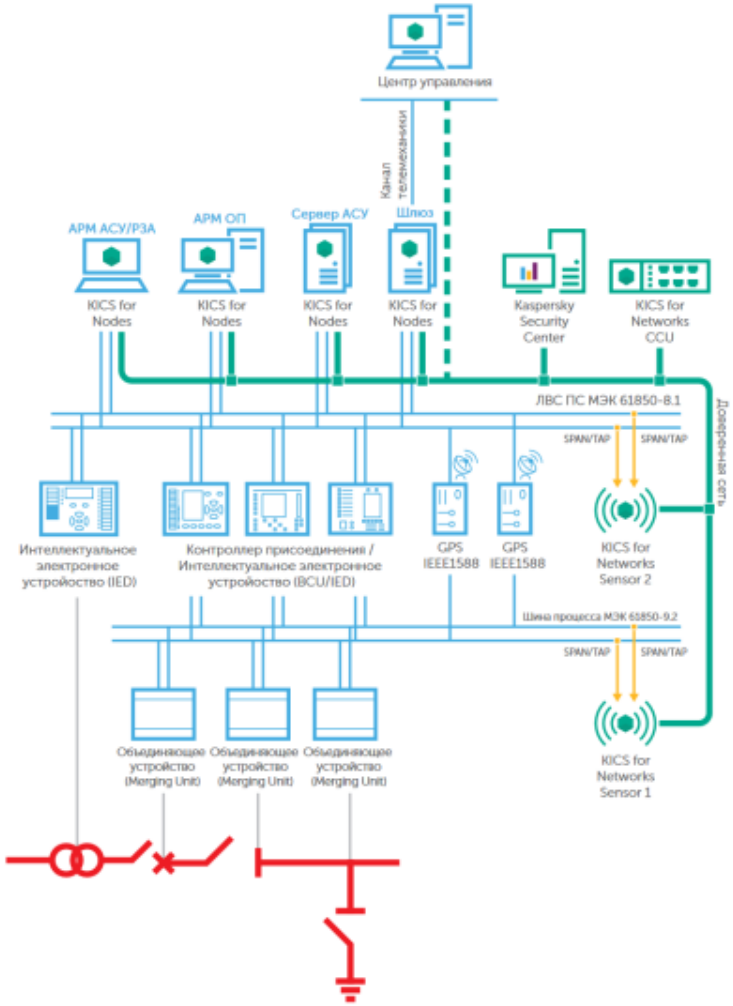
Как защищать АСУ ТП?



Модель зонирования АСУ ТП IEC 62443



СЕГОДНЯ «ЗАКРЫТЬ» ПЕРИМЕТР «ПОВЫСИТЬ НАБЛЮДАЕМОСТЬ»

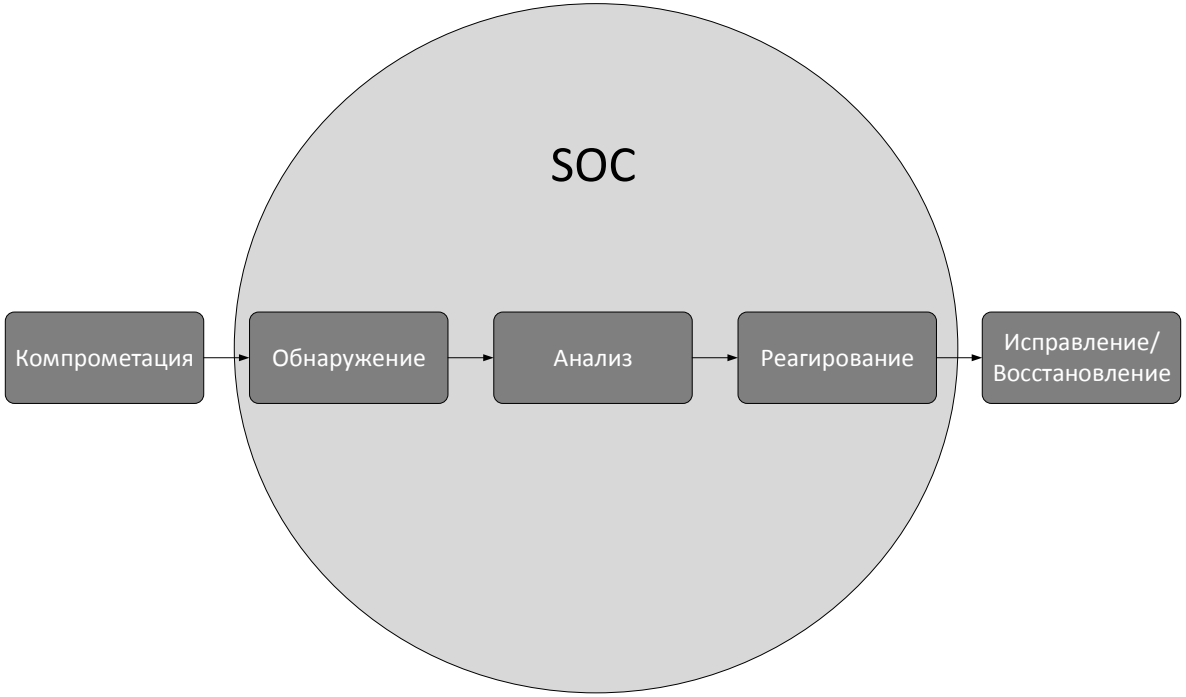


Зрелый SOC для ОТ – это:

- Мониторинг в режиме 24x7x365.
- Высокий уровень экспертизы.
- Выстроенные процессы.
- Выделенный аналитик, контролирующий инфраструктуру.
- Продвинутая аналитика, включающая

Threat Intelligence и Threat Hunting.

- Расследование/изучение каждого события безопасности.
- Индивидуальный план реагирования на инциденты.



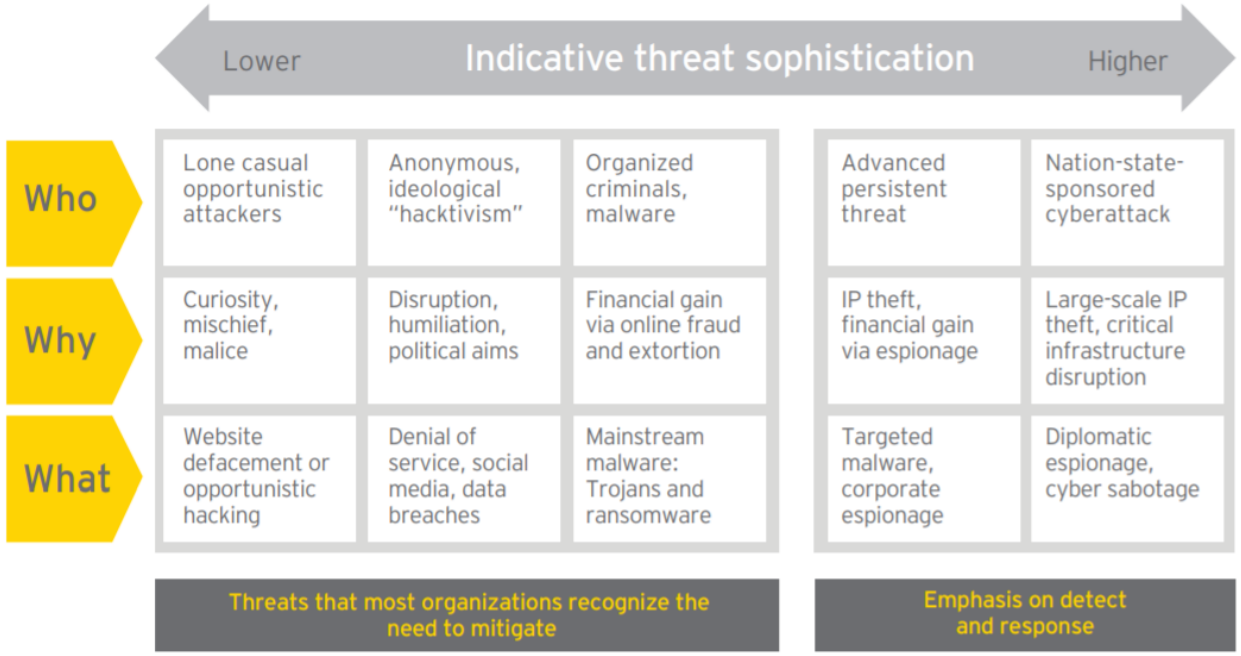
Зачем MDR в АСУ ТП?

Отталкиваемся от уровня предполагаемой угрозы АСУ ТП:

- APT-атаки
- Nation-State sponsored cyberattack

Исходя из этого, акцент должен быть сделан на обнаружении и реагировании.

SOC, построенный как MDR, предназначен для выявления и реагирования на продвинутые угрозы (целевые кибератаки).



EY:https://goo.gl/5qA8rN

Входные условия старта и последующего развития

Этап №1:

- В инфраструктуре объекта защиты отсутствуют средства защиты информации.

Этап №2:

- В инфраструктуре объекта защиты внедрены «базовые» СЗИ:

- Шлюз безопасности на периметре
- Антивирусное ПО

Этап №3:

- На объектовом уровне внедрены специализированные СЗИ для защиты АСУ ТП:

- ICS Threat Detection Systems/ICS Asset Management System/ICS Network Intrusion Detection System (IDS).
- Индустриальные МЭ – Тип «Д» ФСТЭК России.
- EndPoint Protection.

Этап № 4:

- АСУ содержат развитый функционал встроенных СЗИ и СКЗИ.

Выводы/Преимущества:

Внедрение SOC OT позволит:

- Увеличить количество выявляемых инцидентов.
- Обнаруживать аномальное поведение.
- Повысить вероятность выявления APT-атак на более ранней стадии.
- Снизить воздействие подобных инцидентов на технологический процесс.
- Снизить бизнес-риски, угрожающие функционированию предприятия.

Внедрение решений и услуг, **улучшающих ситуационную осведомленность (situational awareness)**, позволит:

- Предлагать обоснованные меры по снижению последствий от компьютерных атак.
- Повысить качество реагирования на инциденты.
- Формулировать выводы на основе количественных данных.
- Выстроить стратегию управления рисками на качественно ином уровне.
- Упрощение соблюдения требований регуляторов и внедрения лучших практик

Вопросы защиты информации АСУ ТП объектов КИИ

Владимир Карантаев

к.т.н. эксперт IEC, IEEE, CIGRE

Автор блога: https://smartgridib.blogspot.com/

Т. +79152211596

МОСКВА 01 ноября, 2018