КИБЕРЗАЩИТА ЦИФРОВЫХ ПРОИЗВОДСТВ:

Выполнение требований 187-ФЗ «О безопасности КИИ РФ»

Замалиев Руслан Фаридович
Директор по развитию регионального бизнеса

Ростелеком
Солар

Цифровая трансформация

Процесс интеграции цифровых технологий во все аспекты бизнес-деятельности, требующий внесения коренных изменений в технологии, культуру, операции и принципы создания новых продуктов и услуг.

Ростелеком
Солар

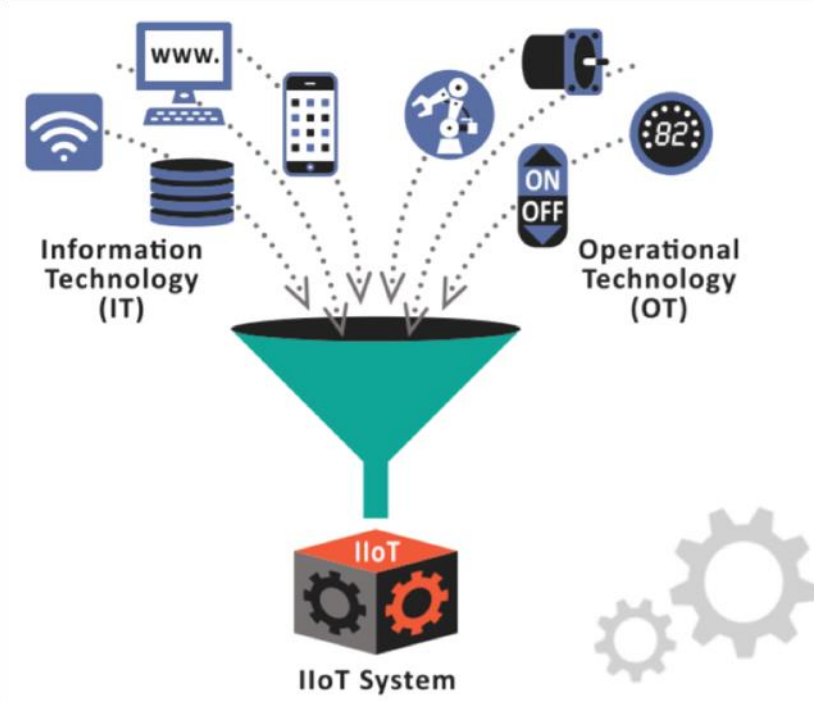
https://www.hpe.com/ru/ru/what-is/digital-transformation.html

Конвергенция IT и OT

Industrial internet of things (IIoT) system - system that connects and integrates industrial control systems with enterprise systems, business processes and analytics.

Industrial internet - internet of things, machines, computers and people, enabling intelligent industrial operations using advanced data analytics for transformational business outcomes.

IT/OT convergence - process of interweaving information technology (IT) and operational technology (OT) in order to create industrial internet of things (IIoT) systems.

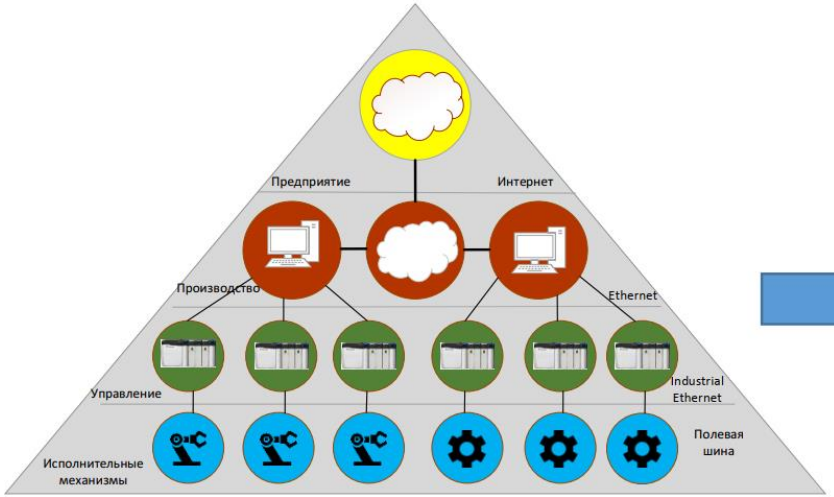


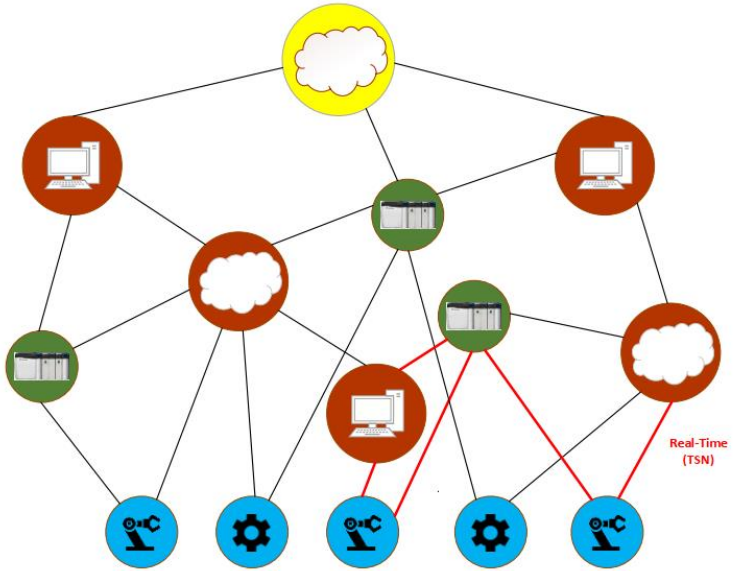
https://goo.gl/uN1UrP

https://goo.gl/YhFF8h

Ростелеком
Солар

Перемены, вызванные INDUSTRY 4.0





От традиционной автоматизации к автоматизации на основе CPS: Cyber Physical Systems

OPC UA
IEEE TSN

Ростелеком
Солар

Источник: https://goo.gl/rtvBrG

Предыстория в цифрах

Ростелеком
Солар

Реакция на вызовы

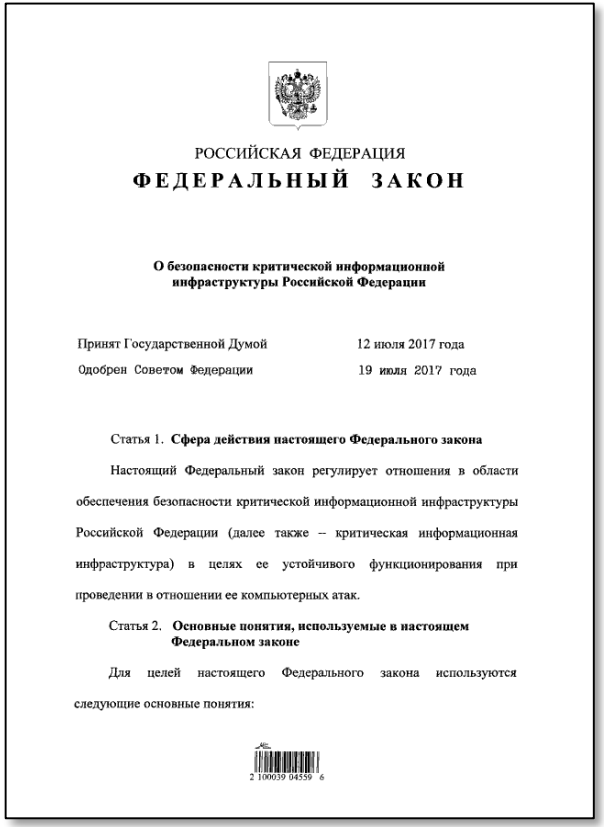
Ростелеком
Солар

Федеральный закон «О безопасности КИИ» N 187-ФЗ

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:

Ростелеком
Солар

Сферы деятельности субъектов КИИ

ЗДРАВООХРАНЕНИЕ

БАНКОВСКАЯ СФЕРА

РАКЕТНО-КОСМИЧЕСКАЯ

НАУКА

ФИНАНСОВЫЙ РЫНОК

ГОРНОДОБЫВАЮЩАЯ

ТРАНСПОРТ

ТЭК

МЕТАЛЛУРГИЧЕСКАЯ

СВЯЗЬ

АТОМНАЯ ЭНЕРГИЯ

ХИМИЧЕСКАЯ

ЭНЕРГЕТИКА

ОБОРОНА

ВЗАИМОДЕЙСТВИЕ СИСТЕМ
из этих сфер

Ростелеком
Солар

Документы, дающие ответы

- Устав организации
- Лицензии и иные разрешительные документы на различные виды деятельности
- Общероссийский классификатор видов экономической деятельности (ОКВЭД)
- Законодательство, дающее определение систем

Подлежащие категорированию объекты

- 187-ФЗ:
  - Объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры

- ПП-127:
  - Категорированию подлежат ОКИИ, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ

Комплекс услуг

- Обследование инфраструктуры (аудит)
- Методологическая экспертная поддержка категорирования объектов КИИ
- Создание системы безопасности значимых объектов КИИ
- Оценка соответствия значимых объектов КИИ и при необходимости аттестация
- Организация взаимодействия объектов КИИ с ГосСОПКА

Ростелеком
Солар

Обследование (аудит) инфраструктуры

Работы

Очное или заочное обследование (аудит)

Оценка защищенности инфраструктуры Заказчика

Проверка корректности собранных Заказчиком исходных данных

Результат

Подготовлен отчет об обследовании

Сформирован перечень объектов КИИ

Ростелеком
Солар

Методологическая поддержка категорирования объектов КИИ

Работы

Анализ угроз безопасности и/или разработка модели угроз и нарушителя

Оценка потенциального ущерба в соответствии с критериями значимости возможных последствий компьютерных инцидентов на объектах КИИ

Присвоение каждому объекту КИИ категории значимости

Подготовка результатов категорирования к отправке во ФСТЭК России

Результат

Определены и задокументированы угрозы и нарушители безопасности информации

Подготовлены внутренние акты по результатам категорирования

Подготовлены формы предоставления во ФСТЭК России сведений о результатах категорирования

Ростелеком
Солар

Создание системы безопасности значимых объектов КИИ*

Работы

Разработка технического задания на создание системы безопасности

Проектирование системы безопасности

Разработка рабочей (эксплуатационной) документации

Разработка комплекта организационно-распорядительной документации

Поставка средств защиты

Внедрение организационных и технических мер

Результат

Система безопасности спроектирована

Разработан комплект организационно-распорядительной документации

Система безопасности введена в эксплуатацию

*Создание и внедрение системы безопасности проводится в том числе с учётом типа значимого объекта КИИ (ГИС, ИСПДн, АСУ ТП и т.д.)

Ростелеком Солар

Оценка соответствия и аттестация значимых объектов КИИ

Работы

Определение формы оценки соответствия

Разработка программы и методики испытаний

Проведение испытаний системы безопасности

Оформление результатов испытаний

Оформление заключения по оценке соответствия

Результат

Разработана программа и методика испытаний

Проведены испытания и оценка соответствия

Выданы документы, подтверждающие соответствие объектов КИИ

Организация взаимодействия объектов КИИ с ГосСОПКА

- Предоставление ресурсов Solar JSOC для автоматизации выявления и предотвращения компьютерных атак
- Построение программно-аппаратной платформы и методической базы для функционирования ведомственного или корпоративного центра ГосСОПКА
- Организация процессов выявления и предотвращения компьютерных атак, включая взаимодействие с головным центром ГосСОПКА, организованным на базе ФСБ России
- Предоставление под ключ услуг по обеспечению защиты объектов КИИ от компьютерных атак и взаимодействию с ФСБ России
- Подключение всех объектов КИИ к ГосСОПКА

Лаборатория Кибербезопасности АСУ ТП

Корпоративный центр компетенций Ростелеком-Solar, предназначенный для сбора, систематизации, распространения, приумножения знаний и лучших практик по обеспечению безопасности систем промышленной автоматизации

Комплексные решения по защите АСУ ТП

на базе инфраструктуры "Лаборатории Кибербезопасности АСУ ТП"

Шоурум

Демонстрационная зона продуктов, решений, сервисов компании по направлению Защита АСУ ТП

Стратегическое сотрудничество

с вендорами АСУ ТП и ИБ

Тестовый полигон для Заказчиков

Работы по поиску и анализу уязвимостей в АСУ ТП

Тестовый полигон для подготовки к пентестам

Ростелеком
Солар

Поиск и анализ уязвимостей

Рейтинг исследователей, предоставивших сведения об уязвимостях программного обеспечения

Благодарим исследователей за предоставленную информацию об уязвимостях программного обеспечения!

Рейтинг исследователя определяется суммированием всех рейтинговых баллов, полученных исследователями за предоставленные сведения об уязвимостях программного обеспечения. Рейтинговые баллы рассчитывается в соответствии с Порядком определения рейтинга, установленным в соответствии с Регламентом включения уязвимостей.

Позиция в рейтинге	Исследователь	Кол-во	Важность	Качество	Критичность	Рейтинг
1.	Ростелеком-Solar	**32**	**10.00**	1.50	8.38	**618.00**
2.	zer0way	31	5.32	**3.00**	6.39	444.00
3.	Владислав Савченко	7	7.14	**3.00**	5.71	104.00
4.	ООО "НеоБИТ"	4	7.00	**3.00**	6.00	60.00
5.	Андрей Ловянников	3	**10.00**	1.00	4.67	44.00
6.	Георгий Кигурадзе	3	5.00	**3.00**	4.00	33.00
7.	Иван Полотнянщиков	2	**10.00**	**3.00**	4.50	30.00
8.	Руслан Черткоев	1	**10.00**	**3.00**	**10.00**	23.00
9.	Виктор Никитин	1	**10.00**	**3.00**	7.00	20.00
10.	ЗАО "Перспективный мониторинг"	1	**10.00**	1.00	7.00	18.00

http://bdu.fstec.ru/site/rating

Ростелеком
Солар

О компании

«Ростелеком-Солар», компания группы ПАО «Ростелеком» – национальный провайдер сервисов и технологий для защиты информационных активов, целевого мониторинга и управления информационной безопасностью

В основе наших технологий лежит понимание, что настоящая информационная безопасность возможна только через непрерывный мониторинг и удобное управление системами ИБ. Этот принцип реализован в продуктах и сервисах «Ростелеком-Солар»

№1
на рынке сервисов кибербезопасности

500+
экспертов кибербезопасности

50+
клиентов из топ-100 российского бизнеса

10 минут
на обнаружение кибератаки

30 минут
на реагирование и защиту

72 млрд
анализируемых событий ИБ в сутки

Ростелеком Солар

Филиалы Solar JSOC и ПАО «Ростелеком»

Ростелеком
Солар

ПАО «Ростелеком»

Филиалы Solar JSOC

Контакты

Центральный офис

125009 г. Москва,
Никитский переулок, 7с1

+7 (499) 755-07-70

info@rt-solar.ru

Ростелеком
Солар