Вопросы реализации киберзащищенной цифровой подстанции на основе российских технологий

Владимир Карантаев

Руководитель направления
«Кибербезопасность АСУ ТП»

E-mail: v.karantaev@rt-solar.ru

Ростелеком
Солар

План доклада

«Лаборатория кибербезопасности АСУ ТП». Центр компетенции

Актуальные угрозы. Результаты инициативного НИР

Актуальные тренды кибербезопасности АСУ ТП

Проблемы остались. Основные выводы отчета Лаборатории

Что делать: сегодня, завтра

Лаборатория Кибербезопасности АСУ ТП

Корпоративный центр компетенций «Ростелеком-Солар» для сбора, систематизации, распространения и приумножения знаний и лучших практик по обеспечению кибербезопасности систем промышленной автоматизации

Комплексные решения по защите АСУ ТП на базе инфраструктуры «Лаборатории Кибербезопасности АСУ ТП»

Шоурум - демонстрационная зона продуктов, решений и сервисов направления Защита АСУ ТП для внешних контрагентов и ЗЛ ПАО «Ростелеком»

Стратегическое сотрудничество с зарубежными вендорами АСУ ТП

Тестовый полигон для заказчиков

Работы по поиску и анализу уязвимостей в АСУ ТП

Тестовый полигон для подготовки к пентестам

Ростелеком
Солар

Реальность vs теория

Вам приходилось слышать?

- У нас есть периметр безопасности в АСУ ТП
- Проблемы внутреннего нарушителя - нет. У нас контролируемая зона
- **Одиозное:** наша (наши) АСУ ТП - это закрытая система. Это в век IIoT и SmartGrid!

А мы помним о?

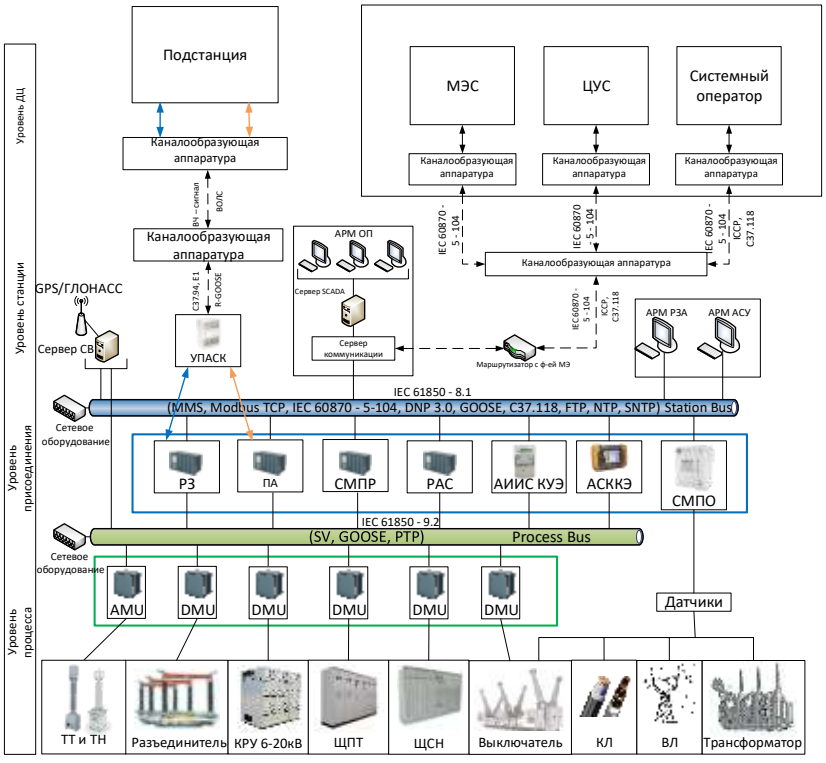
- О подрядчиках, осуществляющих наладку и эксплуатацию
- О том, что самая большая проблема – эксплуатация (т. е. люди)
- О системах удаленного мониторинга чего-либо кем-либо (турбины, процессы)

«Отцы-основатели»

- От сети всегда исходит угроза. Весь сетевой трафик не доверенный, его происхождение и источник не важны
- Внутренние и внешние угрозы всегда присутствуют
- Внутренняя сеть не равно доверенная сеть
- Каждое устройство, пользователь, информационный поток должны быть идентифицированы и аутентифицированы

Ростелеком
Солар

Основа реализации концепции цифровой трансформации



Цифровая подстанция

Автоматизированная подстанция, оснащенная взаимодействующими в режиме единого времени цифровыми информационными и управляющими системами и функционирующая без присутствия постоянного дежурного персонала.

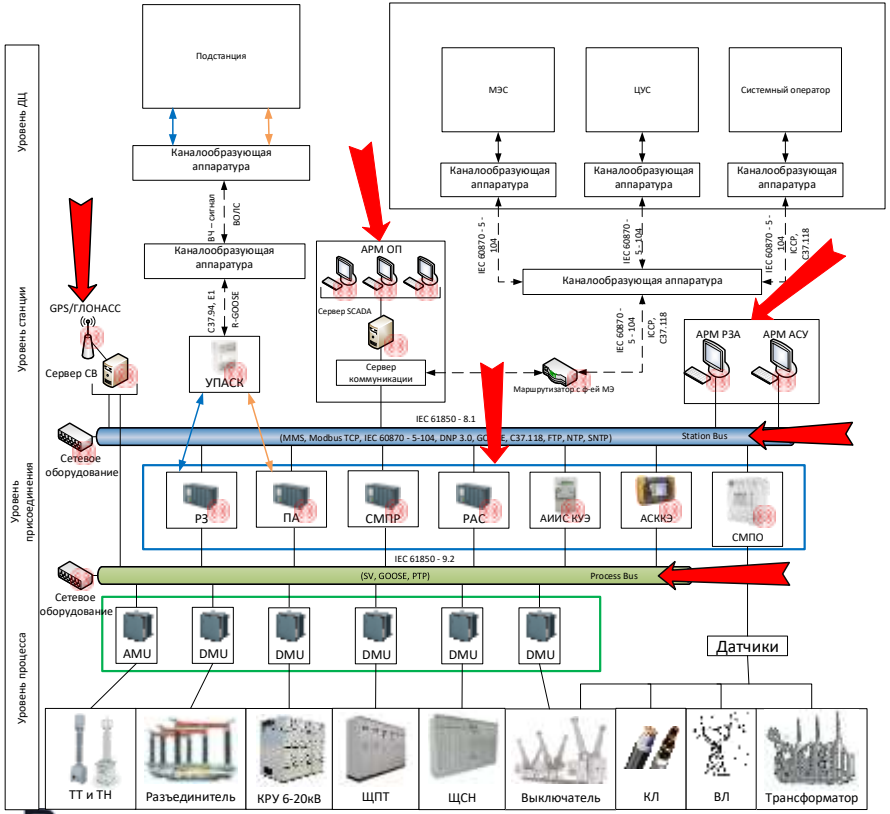
СТО 34.01.-21-004-2019 «Цифровой питающий центр»

Под «цифровой» подстанцией (ЦПС) понимается подстанция с высоким уровнем автоматизации управления, в которой практически все процессы информационного обмена между элементами ПС, обмена с внешними системами, а также управления работой ПС осуществляются в цифровом виде на основе протоколов МЭК.

Ростелеком Солар

IEC

Модель угроз ЦПС



Виды возможных атак

- GPS/ГЛОНАСС Spoofing
- GOOSE Spoofing
- MITM MMS
- MITM МЭК 60870 - 5 – 104
- Brute Force
- Риски успешных APT с ущербом кибер- и физическим характеристикам ЦПС и SmartGrids (ААС ЕЭС, цифровым сетям)

Возможные векторы воздействия

Атаки на Endpoints

Атаки на протоколы

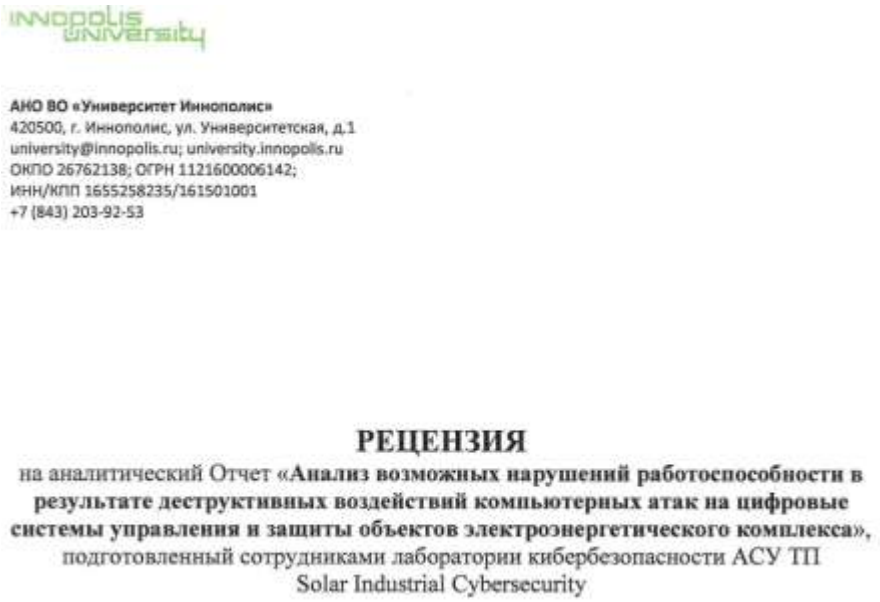
Ростелеком
Солар

Актуальные угрозы или история одного НИР

Результаты исследования отражают экспертную позицию авторского коллектива.

Наиболее значимый практический результат работы – это следующий вывод: нарушение устойчивости функционирования объектов электроэнергетики с высоким уровнем цифровизации вторичных систем из-за воздействия на них кибератак возможно.

Достигнутый результат заставляет по иному воспринимать риски цифровой трансформации электроэнергетической отрасли.



innopolis university

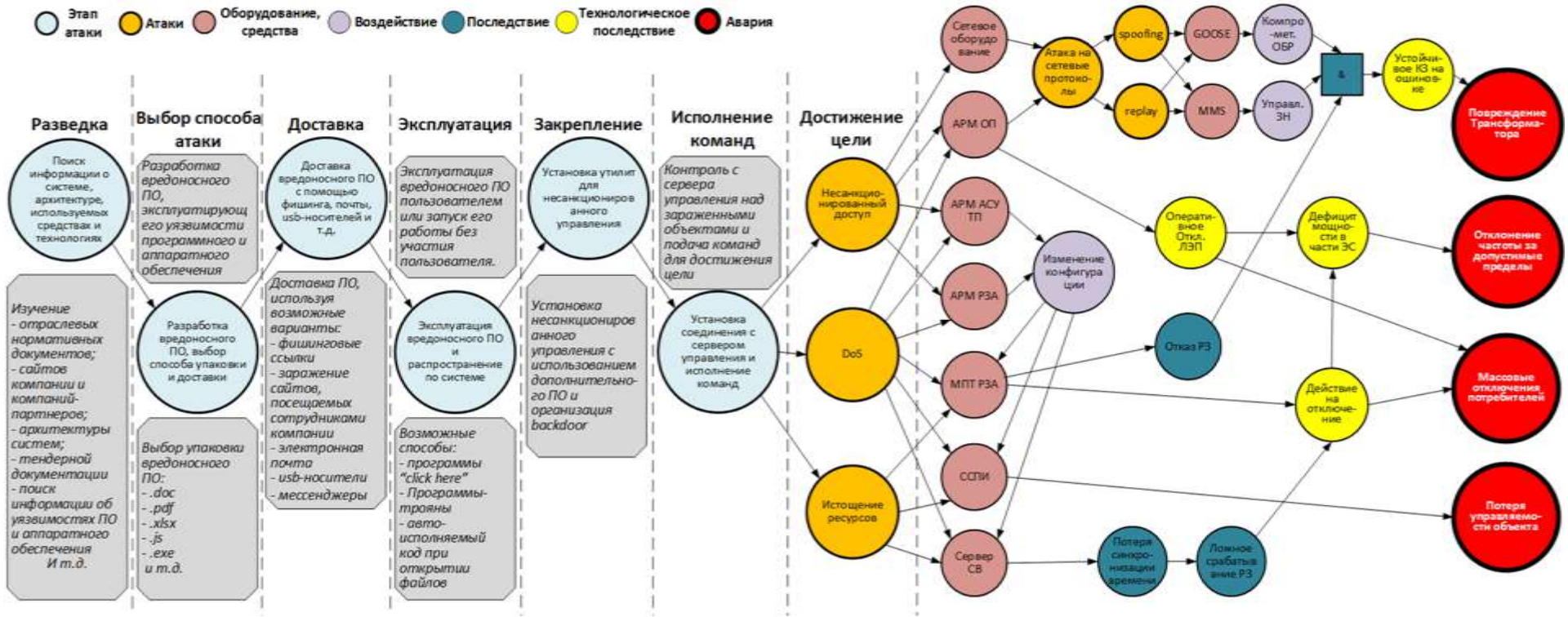
АНО ВО «Университет Иннополис»
420500, г. Иннополис, ул. Университетская, д.1
university@innopolis.ru; university.innopolis.ru
ОКПО 26762138; ОГРН 1121600006142;
ИНН/КПП 1655258235/161501001
+7 (843) 203-92-53

РЕЦЕНЗИЯ

на аналитический Отчет «**Анализ возможных нарушений работоспособности в результате деструктивных воздействий компьютерных атак на цифровые системы управления и защиты объектов электроэнергетического комплекса**», подготовленный сотрудниками лаборатории кибербезопасности АСУ ТП Solar Industrial Cybersecurity

Ростелеком
Солар

Результаты развития принципов моделирования угроз



Ростелеком Солар

Исследование Лаборатории кибербезопасности АСУ ТП «Анализ возможных нарушений работоспособности в результате деструктивных воздействий компьютерных атак на цифровые системы управления и защиты объектов электроэнергетического комплекса».

Глобальные тренды кибербезопасности

- Следование лучшим практикам или заявление производителей АСУ/АСУ ТП/РЗА о соответствии нормативно-техническим и нормативно-правовым требованиям.
  - NERC CIP и FERC Order No. 693
  - IEC 62351 Security Standards for the Power System Information Infrastructure
  - IEEE 1686-2013 IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities
  - ISO 27001 is a specification for an information security management system (ISMS)
  - IEC 62443 Industrial communication networks - Network and system security. Security for industrial automation and control systems
  - IEC 62541 OPC Unified Architecture standard series
- Разработка и предложение на рынке систем автоматизации, построенных по принципу Secure by Design, Built-in Security, Security for safety.
- Со стороны глобальных вендоров систем автоматизации сформировано комплексное предложение для западного и североамериканского рынков по обеспечению кибербезопасности объектов и систем заказчиков: продукты, сервисы.
- Повышение экспертного интереса к SecaaS, Cloud iSOC.

Ростелеком
Солар

Проблемы сохраняются

72%

уязвимостей — критического и высокого уровней

CWE-327

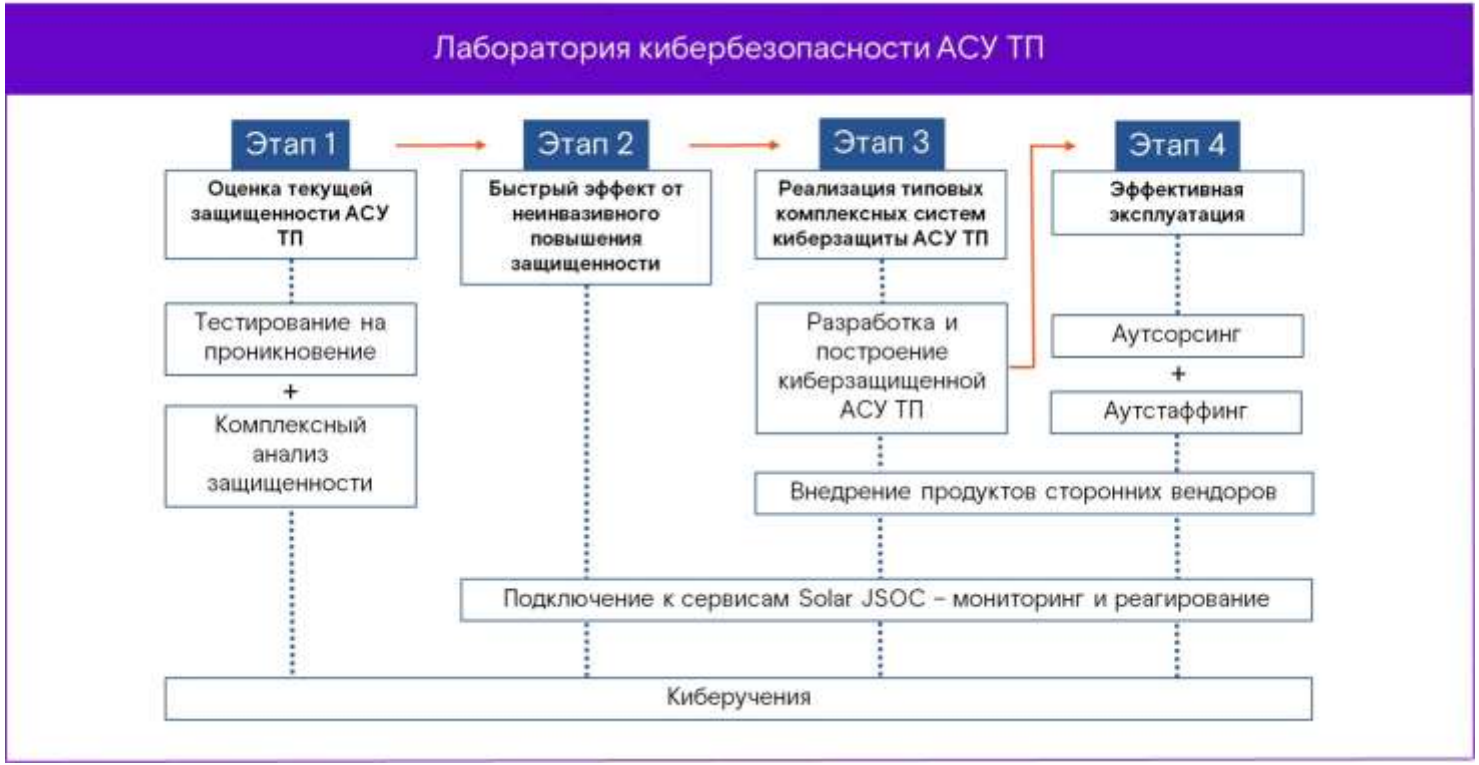
самая популярная уязвимость

Актуальная проблема: скорость реакции производителей

Балльная система не всегда позволяет корректно оценить критичность уязвимости

Ростелеком
Солар

Повышение киберзащищенности АСУ ТП



Ростелеком
Солар

Предпосылки. Варианты решения

Увеличение поверхности атаки

- Изменение архитектурных принципов построения ИС, АСУ ТП. «От пирамиды к mesh-сети»
- Появление новых активных взаимодействующих субъектов, например, просьюмеры в электроэнергетике
- Возрастающее количество угроз, вызванных ростом количества уязвимостей в прикладном и общесистемном ПО
- Развитие методов атак: преодоление периметра/компрометация периметровой защиты
- Применение технологий, уязвимых перед компьютерными атаками. Унификация и COST
  - ИКТ
  - Виртуализация/использование гипервизоров на ПЛК несколько операционных систем
  - Мультиагентные системы

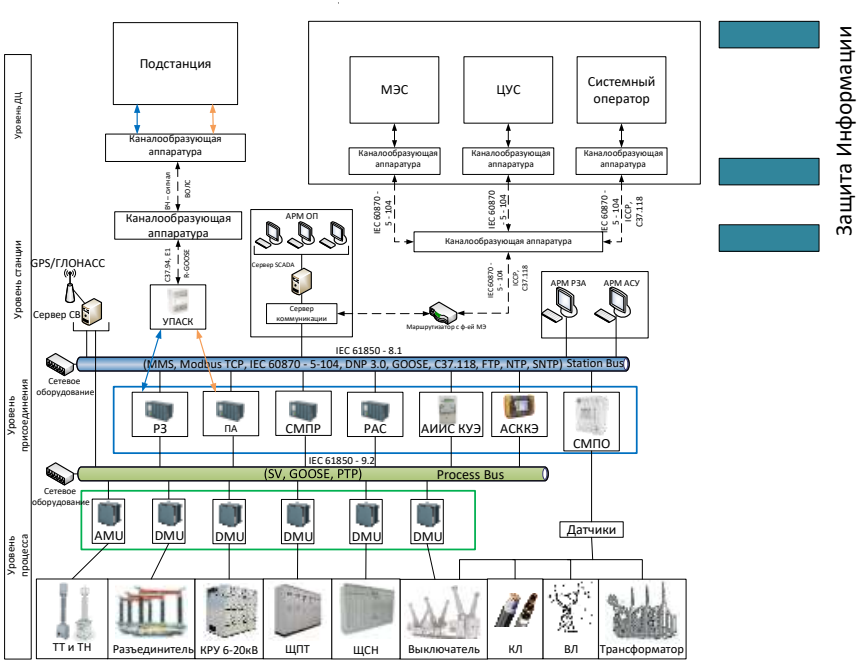
Реализация политики ZeroTrust

- **Сегодня.** Уменьшение поверхности атаки до максимально достижимого
- **Завтра.** В пределе переход к архитектуре с нулевым доверием

Ростелеком
Солар

Что делать?

Сегодня – снизить уровень риска до достижимо низкого

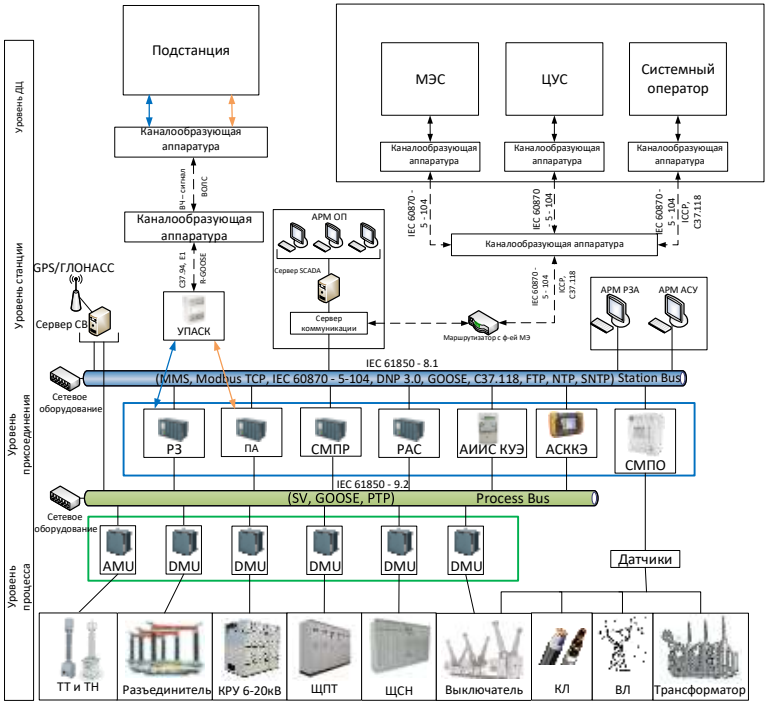


- Закрыть периметр
- Повысить наблюдаемость – мониторинг состояния защищенности
- Применить положения МЭК 62443
- Сегментировать и внедрить элементы многоуровневой защиты

Ростелеком Солар

Что делать?

Завтра – добиться снижения уровня риска до приемлемого



- Реализовать на практике принцип многоуровневой защиты
- Эффективно комбинировать применение наложенных и встроенных СЗИ
- Реализовать модель безопасности на уровне объекта (ЦПС)
- Реализовать модели безопасности на уровне каждого типа EndPoint: АРМ, сервер, терминал РЗА, контроллер присоединения, активное сетевое оборудование всех уровней и т.д.
- Доверенные коммуникации
- Внедрить практики безопасной разработки (SDL)
- Разработать и внедрить методики оценки соответствия

Ростелеком Солар

ЗАВТРА. Разработка доверенных систем технологического уровня

- Российские CPU и микроконтроллеры
- Доверенные операционные системы
- Аутентификация устройства
- Аутентификация пользователя устройств
- Доверенная загрузка устройства
- Доверенные обновления
- Встроенный МЭ
- Логирование событий безопасности
- Контроль целостности ПО устройства
- Защищенные протоколы обмена (TLS, защищенный 104-й, OPC UA и т.д.)
- Обеспечение неотказуемости для данных, передаваемых устройством
- Удаленная аттестация устройства

Выводы

1. Системы должны разрабатываться с учетом анализа угроз функциональной надежности и информационной безопасности.
2. Реализация концепции Secure by design (встроенных средств защиты информации в промышленных системах автоматизации) и требований безопасной разработки выглядит наиболее перспективно с учетом необходимости удовлетворять требования по функциональной надежности и безопасности, наличия требований по быстродействию телекоммуникационных протоколов и оптимальности затрат.
3. Формирование комплексного предложения по кибербезопасности IIoT возможно на основе сформированных экосистемных партнерств.

Ростелеком
Солар

Вопросы реализации киберзащищенной цифровой подстанции на основе российских технологий

Владимир Карантаев

Руководитель направления
«Кибербезопасность АСУ ТП»

E-mail: v.karantaev@rt-solar.ru

Ростелеком
Солар