Выявление уязвимостей и НДВ в компонентах АСУ ТП и IIoT

Лабораторные исследования компонентов АСУ ТП и промышленного Интернета вещей для своевременного выявления уязвимостей и недекларированных возможностей

rt-solar.ru

rt.ru

Ростелеком
Солар

Угрозы информационной безопасности АСУ ТП и IIoT

Автоматизированные системы управления технологическими процессами (АСУ ТП) и промышленный Интернет вещей (IIoT) — области, кибербезопасность которых вызывает активный интерес и озабоченность представителей промышленности и государства. Количество уязвимостей в этой сфере постоянно растет, а риски — чрезвычайно высоки.

Ситуацию усугубляет ряд других факторов:

- «Размытие» периметра из-за растущей популярности IIoT-технологий
- Увеличение связанности технологических сетей с корпоративными и сетями общего пользования
- Рост зависимости от уязвимых ИТ-технологий, хорошо изученных злоумышленниками
- Повышение сложности и многокомпонентности атак
- Появление методик и ПО, разработанных специально для атак на компоненты АСУ ТП и IIoT
- Вовлечение в злонамеренную деятельность структур с обширными финансовыми и человеческими ресурсами

700+

уязвимостей выявлено в компонентах АСУ ТП и IIoT за 2017-2018 гг.

50%

обнаруженных уязвимостей — высокой критичности

56%

промышленных предприятий, использующих системы SCADA/ICS, сообщили о кибератаках в 2017 году

Данные: «Ростелеком-Солар», Fortinet, 2019

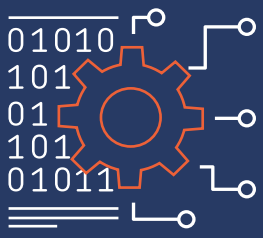
Государственное регулирование

Защита АСУ ТП и IIoT — вопрос, вызывающий обеспокоенность на самом высоком государственном уровне. Структура нормативно-правового регулирования включает следующие документы:

- **Доктрина информационной безопасности Российской Федерации:** указ Президента РФ № 646
- **ФЗ № 187-ФЗ** «О безопасности критической информационной инфраструктуры Российской Федерации»
- **ФЗ № 194-ФЗ** «О внесении изменений в Уголовный кодекс Российской Федерации...»
- **ФЗ № 193-ФЗ** «О внесении изменений в отдельные законодательные акты...»
- **ГОСТ Р 56939-2016** «Разработка безопасного ПО»
- **Приказ ФСТЭК России № 239 от 25.12.2017** «Об утверждении Требований по обеспечению безопасности значимых объектов критической инфраструктуры Российской Федерации (в редакции Приказа ФСТЭК России от 26 марта 2019 г. **№ 60**)»
- **Приказ ФСТЭК России № 31 от 14.03.2014** «Об утверждении Требований к обеспечению защиты информации в АСУ ТП»
- **Методический документ** «Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении», **ФСТЭК России, 2019 г.**

За несоблюдение требований законодательства Российской Федерации грозит административная и даже уголовная ответственность.

Уникальность



«Лаборатория кибербезопасности АСУ ТП» — это корпоративный центр компетенций для сбора, систематизации, распространения, приумножения знаний и лучших практик по обеспечению кибербезопасности систем промышленной автоматизации. Эксперты компании обладают реальным опытом разработки и внедрения проектов по защите АСУ ТП и являются одними из лидеров в рейтинге исследователей БДУ ФСТЭК России.

Решение

«Лаборатория кибербезопасности АСУ ТП» компании «Ростелеком-Солар» предлагает услуги по практическому исследованию безопасности компонентов АСУ ТП и IIoT для выявления известных и неизвестных ранее (0-day) уязвимостей и недекларированных возможностей.

Глубокий уровень анализа защищенности АСУ ТП/IIoT-систем

Широкий спектр методик инструментального и ручного анализа

Анализ компонентов АСУ ТП и IIoT с исходным кодом и без него

«Ростелеком-Солар» располагает собственными специализированными для АСУ ТП и IIoT методическими наработками, лабораторной базой и опытом. В своей работе компания придерживается принципа «координированного раскрытия информации» для предотвращения неконтролируемого разглашения информации об уязвимостях и повышения прозрачности и прогнозируемости процесса работы с ними.

Ключевые особенности

Специализация на компонентах АСУ ТП и IIoT

Собственные методики и лабораторная база

Команда исследователей с многолетним подтвержденным опытом

- Применение политики «координированного раскрытия информации» и большой опыт совместной работы с производителями, регуляторами отрасли (такими как ФСТЭК России) и командами реагирования на компьютерные инциденты

- Поиск уязвимостей прикладного общесистемного программного обеспечения
  - серверы SCADA, OPC, Historian
  - АРМ, HMI-панели
  - инженерное и сервисное ПО
  - прошивки сетевого оборудования, АСУ ТП и IIoT-устройств
  - облачные сервисы, веб-порталы, IIoT-платформы
  - беспроводные устройства
  - контроллеры АСУ ТП
  - и др.

«Ростелеком-Солар» оказывает методическую помощь в организации процессов работы с уязвимостями и гармоничного встраивания услуги в процессы разработки безопасного ПО.

Этапы работы

Подписание договора о неразглашении

Подготовка ТЗ и подписание договора

Подготовка плана, оборудования и стендов

Исследования безопасности компонентов

Подготовка отчета о найденных уязвимостях

Опционально: координация уязвимостей

Экспертиза

Одни из лидеров в рейтинге исследователей БДУ ФСТЭК России

100+ уязвимостей, опубликованных с российскими и международными командами реагирования на компьютерные инциденты

250+ выявленных уязвимостей в компонентах АСУ ТП

Большой опыт совместной работы по уязвимостям с производителями, регуляторами и независимыми командами реагирования на компьютерные инциденты

Десятки выявленных уязвимостей высокого и критического уровней (8+ по шкале CVSSv3)

Реальный опыт разработки и внедрения проектов по защите АСУ ТП

Услуги «Ростелеком-Солар» по защите АСУ ТП

- Приведение организации в соответствие с требованиями 187-ФЗ «О безопасности КИИ РФ»
- Кибербезопасность АСУ ТП
- Проведение киберучений для владельцев АСУ ТП и субъектов КИИ
- Подключение к сервисам Solar JSOC для АСУ ТП
- Выявление уязвимостей и НДВ в компонентах АСУ ТП и IIoT
- Комплексный анализ защищенности АСУ ТП
- Тестирование на проникновение АСУ ТП и IIoT

Узнать подробнее или заказать сервис

presale@rt-solar.ru

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».

Ростелеком Солар

info@rt-solar.ru rt.ru rt-solar.ru

+7 (499) 755-07-70

S.9.09.BR.ICS.VUL.01