

Проведение киберучений для владельцев АСУ ТП и субъектов КИИ

На предприятиях проводят разные тренировки и учения, в том числе и киберучения — тренировки по отражению кибератак на объекты критической информационной инфраструктуры и предприятия, использующие АСУ ТП. Необходимость киберучений диктуется как рисками компьютерных атак, так и требованиями регуляторов, в частности Приказа ФСТЭК России № 239.

81%

киберучений
проходит в Европе
и Северной Америке

57%

составил рост
числа киберучений
в странах Евросоюза

1200+

экспертов участвовали
в масштабных киберучениях
Locked Shields 2019

Решаемые задачи



Повышение
осведомленности
об угрозах



Оценка готовности
персонала
к кибератакам



Моделирование
реакции на
инциденты ИБ



Рекомендации по
устранению выявленных
недостатков

Варианты киберучений

Штабные

- Типовые и реальные сценарии.
- Отработка разработанных сценариев «на бумаге».
- Планирование и проведение в короткие сроки.

Гибридные

- Типовые и реальные сценарии.
- Отработка разработанных сценариев «на бумаге» с возможностью демонстраций на стендах.
- Проверка технических навыков специалистов заказчика.

Полнофункциональные

- Реальные сценарии.
- Учения на реальных площадках и инфраструктуре заказчика.
- Эмуляция реальных компьютерных атак.
- Отработка сценариев «на бумаге» при невозможности демонстрации на оборудовании.

Преимущества услуги

- Гибкая адаптируемая модель оказания услуги.
- Соблюдение нормативно-правовых требований по безопасности объектов критической инфраструктуры.
- Возможность отработать координацию между производственными подразделениями заказчика и усовершенствовать процессы обеспечения безопасности.
- Уровни оказания услуги: от объектового до национального.
- Рекомендации по устранению выявленных недочетов.
- Возможность обучения и консалтинга по результатам киберучений.
- Отработка действий сотрудников в условиях, наиболее приближенных к «боевым», и повышение готовности к кибератакам.

Этапы оказания услуги



Услуги «Ростелеком-Солар» по защите АСУ ТП

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

Узнать подробнее или заказать услугу

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».