Ростелеком
Солар

Новая парадигма кибербезопасности объектов КИИ и АСУ ТП

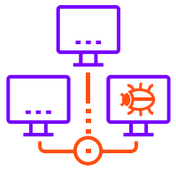
Виталий Сиянов, менеджер по развитию бизнеса «Solar Интеграция»

Ландшафт киберугроз промышленных компаний

Рост количества атак
через подрядчиков

Размытие периметра и незакрытые
уязвимости на периметре

Фишинг, смишинг и вишинг
продолжают набирать обороты



Отсутствие реальной сегментации
блока АСУ ТП

5 550 атак на предприятия ТЭК –
зафиксировано за первые шесть месяцев 2021
года по данным Solar JSOC

Каждая десятая ИТ-инфраструктура ТЭК
заражена вирусом

Постоянный DDoS на ИТ-инфраструктуру,
в том числе сегмент АСУ ТП

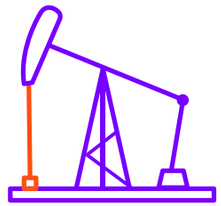
Сменился вектор атак с доставки
шифровальщиков в инфраструктуру
на целенаправленные атаки

Количество атак за последние три месяца увеличилось минимум вдвое

Ростелеком
Солар

Решаемые задачи промышленных предприятий

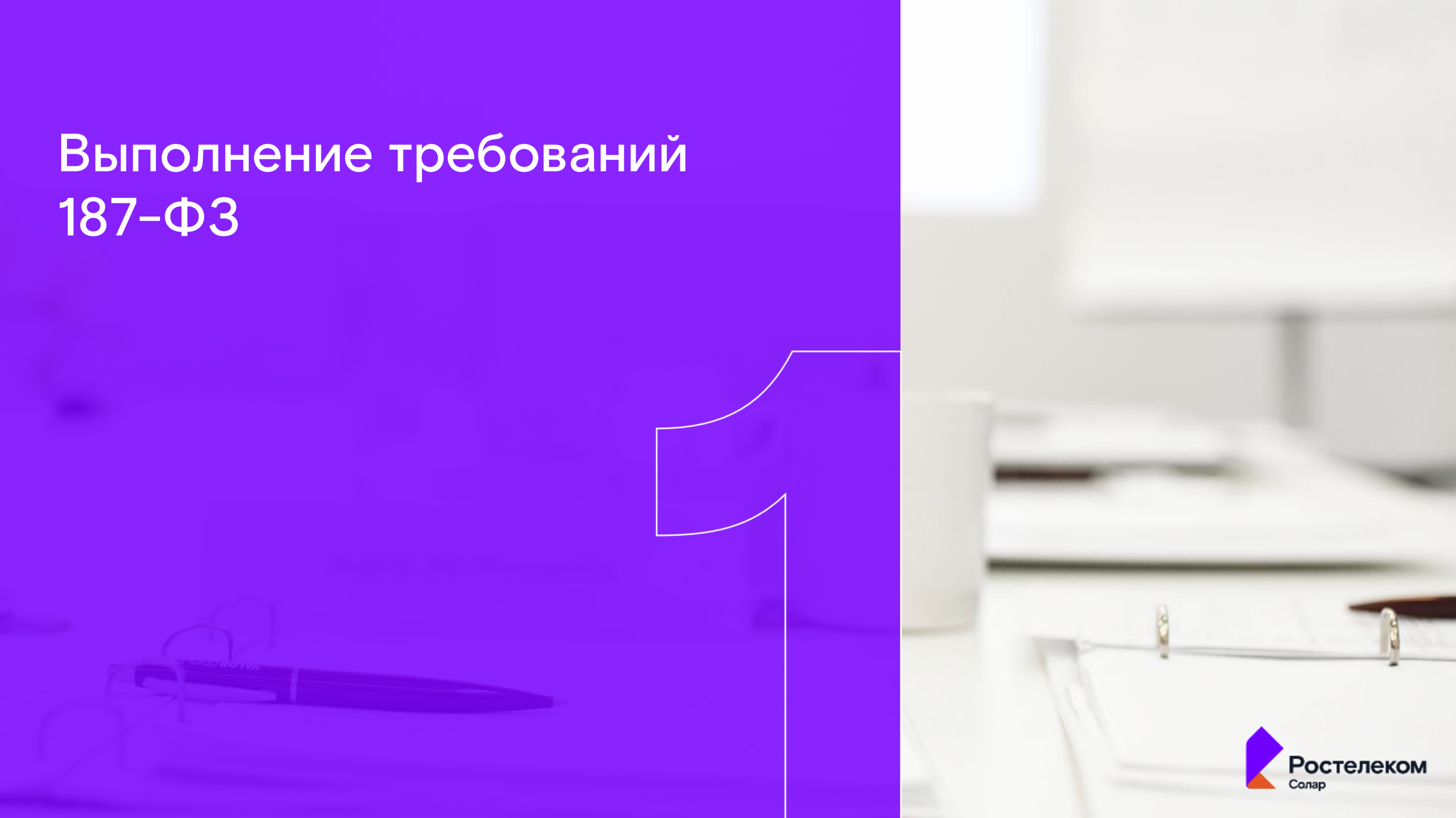
Выполнение требований 187-ФЗ



Обеспечение кибербезопасности АСУ ТП

Ростелеком Солар

Выполнение требований 187-ФЗ



Ростелеком
Солар

Административная и уголовная ответственность:

до 500 000 руб.
штраф за нарушение требований для юридических лиц

до 50 000 руб.
штраф за нарушение требований для должностных лиц

Приостановка деятельности
организации, если требования не исполняются

до 10 лет
лишения свободы, если произошел инцидент (уголовная ответственность)

Ответственность за невыполнение 187-ФЗ

187-ФЗ «О безопасности КИИ»
Регулирует вопросы, связанные с защитой объектов критической информационной инфраструктуры в 13 отраслях

Подзаконные нормативные акты

(17 нормативно-правовых актов)

Описывают вопросы, связанные с категорированием объектов КИИ, созданием системы безопасности значимых объектов КИИ, взаимодействием с ГосСОПКА

Ростелеком Солар

Состав услуг для выполнения 187-ФЗ

1. Категорирование объектов КИИ
2. Оценка соответствия систем безопасности объектов КИИ
3. Создание систем безопасности значимых объектов КИИ:
   - Формирование требований к системе безопасности значимых объектов КИИ
   - Проектирование системы безопасности для значимых объектов КИИ
   - Интеграция решений для защиты значимых объектов КИИ
4. Организация взаимодействия субъектов КИИ с ГосСОПКА
5. Сопровождение системы безопасности в процессе эксплуатации

Ростелеком Солар

План выполнения требований 187-ФЗ

Категорирование объектов КИИ

- Создание комиссии по категорированию объектов КИИ
- Определение перечня процессов, выявление критических
- Разработка перечня объектов КИИ, подлежащих категорированию
- Определение угроз безопасности для объектов КИИ
- Определение категории значимости для объектов КИИ
- Подготовка сведений о категорировании объектов КИИ

Разработка мероприятий по взаимодействию с ГосСОПКА

- Разработка регламента информирования НКЦКИ
- Организация взаимодействия с НКЦКИ

Создание системы безопасности значимого объекта КИИ

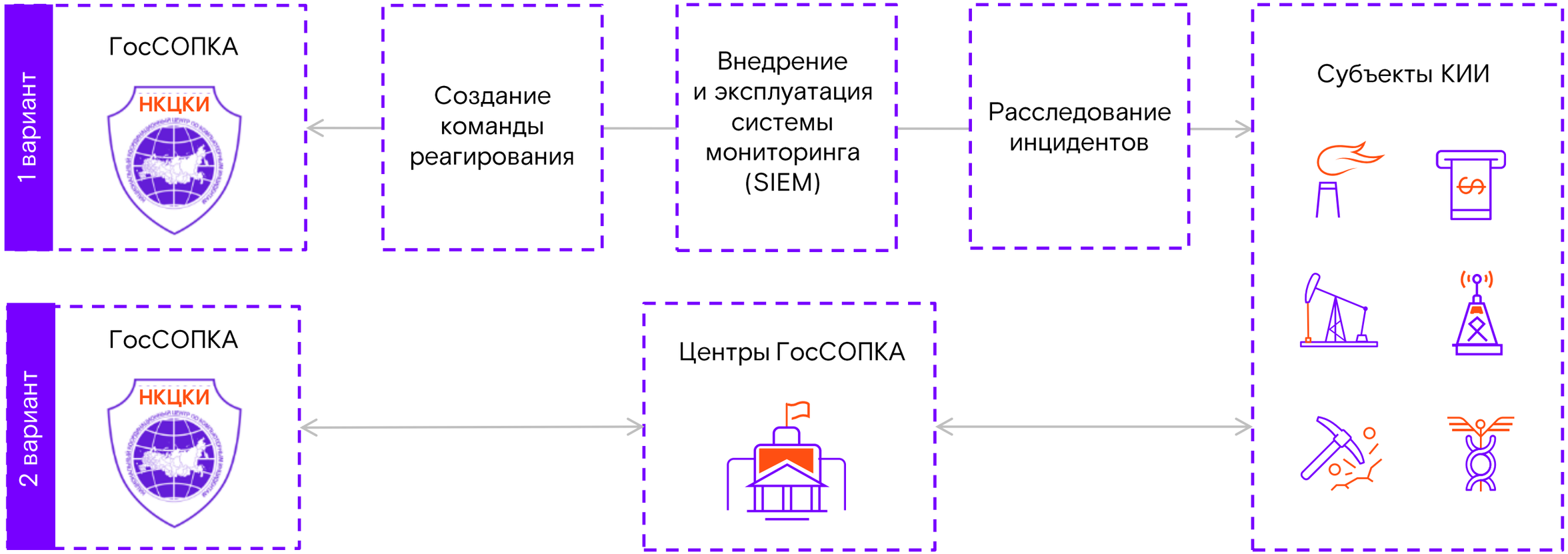
- Разработка и утверждение распоряжения о создании системы безопасности значимого объекта КИИ
- Установление требований к обеспечению безопасности значимого объекта КИИ
- Разработка орг- и техмер по обеспечению безопасности
- Внедрение орг- и техмер по обеспечению безопасности значимого объекта КИИ, ввод в действие

Обеспечение безопасности значимого объекта КИИ в ходе его эксплуатации

Обеспечение безопасности значимого объекта КИИ при выводе его из эксплуатации

Ростелеком Солар

Организация взаимодействия субъектов КИИ с ГосСОПКА



Ростелеком Солар

Обеспечение кибербезопасности АСУ ТП

2

Необходимость обеспечения безопасности промышленных предприятий

Взлом электрозарядных станций

Производитель оставил в контролере закладку для скрытого доступа через интернет. В результате взлома на экранах заправках появлялись нецензурные сообщения

2022 г.

Атака на нефтяную компанию

Атаке хакеров подверглась национальная нефтедобывающая компания Саудовской Аравии. Цель атаки – нарушение поставок нефти и газа на местный и международный рынки

2021 г.

Кибератака шифровальщика

В мае была приостановлена транспортировка топлива по Colonial Pipeline из-за кибератаки с использованием шифровальщика DarkSide

2021 г.

Атака нефтяной компании

В декабре вирус Shamoon атаковал итальянскую нефтяную компанию Saipem, «зачистив» 300 серверов и около 100 компьютеров на Ближнем Востоке, в Индии, Шотландии и Италии 2018

2018 г.

Заражение вирусом

В декабре стало известно о заражении вредоносным ПО инфраструктуры нефтяной компании Petrofac

2018 г.

Ростелеком Солар

Состав услуг для обеспечения кибербезопасности АСУ ТП

1. Комплексный анализ защищенности:
   - Тестирование на проникновение (включая выявление уязвимостей и НДВ)
   - Экспертный аудит (обследование инфраструктуры)
2. Разработка стратегии и концепции повышения защищенности
3. Создание системы обеспечения кибербезопасности
4. Мониторинг АСУ ТП
5. Киберучения АСУ ТП

Ростелеком Солар

Создание системы обеспечения кибербезопасности АСУ ТП

Анализ трафика, СОВ	Контроль привилегированных пользователей	Настройка МСЭ и правил межсетевого экранирования	Сегментация сети, организация ДМЗ, выделение зоны систем кибербезопасности
Защита конечных узлов	Защита от таргетированных атак	Средства мониторинга и управления инцидентами кибербезопасности	Настройка встроенных механизмов безопасности АСУ ТП и промышленной сети

КОД безопасности · infotecs · UserGate · s•terra · TIONIX · kaspersky · PT POSITIVE TECHNOLOGIES

INDEED ID · SafeInspect · IT Bastion · REDCheck · R-Vision · SECURITY VISION · КИБЕРПРОТЕКТ

Указ Президента № 166 от 30 марта 2022 г. «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»

Ростелеком Солар

Мониторинг АСУ ТП

- Анализ событий (SIEM) + анализ сетевого трафика (СОВ)
- Две схемы подключения на выбор: облачная и гибридная
- В качестве источников событий подключаются: АРМ, серверы, сетевое оборудование, СЗИ
- Организация взаимодействия с ГосСОПКА
- Набор сценариев детектирования разного уровня в зависимости от пожеланий заказчика

Анализ событий кибербезопасности на узлах

Анализ сетевого трафика в технологическом сегменте

Ростелеком Солар

Киберучения АСУ ТП

Киберполигон для отработки службами ИБ сценариев реагирования на кибератаки и их последствия

Техническая инфраструктура с настоящим отраслевым оборудованием

Специализированный программный комплекс для проведения киберучений

Уникальная методика обучения специалистов с учетом их знаний и специфики отрасли

На киберполигоне **эмулируется типовая инфраструктура выбранной отрасли,** включая сетевую часть, конкретные сервисы, приложения, инструменты, что позволяет:

- На практике освоить лучшие средства и методы защиты информации
- Подготовиться к реальным актуальным атакам
- Научиться защищаться от атак в реальном времени
- Объективно оценить уровень знаний специалистов
- Выявить и закрыть уязвимости инфраструктуры

Ростелеком Солар

Преимущества работы с «Ростелеком-Солар» в области защиты объектов КИИ и АСУ ТП

01 Комплексная защита АСУ ТП: построение комплексных систем кибербезопасности, подключение к ГосСОПКА, мониторинг инцидентов, проведение киберучений

02 Большой опыт в реализации комплексных проектов в компаниях из разных отраслей

03 Регулярное участие в экспертных группах, инициированных ФСТЭК России для разработки методических документов

04 Лаборатория кибербезопасности АСУ ТП: анализ СрЗИ, проверка на совместимость, аналитика, проведение пентестов, поиск уязвимостей

05 Доступ к Национальному киберполигону – уникальной площадке для отработки навыков защиты от киберугроз

06 Лидер рейтинга исследователей БДУ ФСТЭК России: передана информация о более 115 уязвимостях, связанных с компонентами АСУ ТП за два года*

*Данные актуальны на июль 2021 года.

Ростелеком Солар

Комплексный подход к защите корпоративного сегмента

Ростелеком
Солар

Архитектура ИБ. Технические меры защиты

Мониторинг и управление	Мониторинг и реагирование на инциденты ИБ (SIEM)	Управление кибербезопасностью (IRP, FWM)			
Защита web	Защита от DDoS-атак	Защита веб-приложений (WAF)	Анализ кода	**Защита корпоративных сервисов**	
Защита данных	Защита баз данных (DAM)	Защита данных на файловых хранилищах (DAG)	Защита от утечек информации (DLP)	Защита от продвинутых угроз	**Защита конечных станций**
Управление доступом	Управление правами доступа (IdM)	Многофакторная аутентификация (MFA)	Управление привилегированными пользователями (PAM)	Защита почты	Продвинутая защита конечных станций (EDR)
Защита ИТ-инфраструктуры	Антивирусная защита серверов и рабочих станций	Защита от НСД	Анализ защищённости	Защита среды виртуализации	Защита мобильных устройств (MDM)
Защита сети и периметра	Сегментирование и DMZ	Межсетевое экранирование (FW)	Обнаружение вторжений (IPS)	Криптографическая защита каналов связи	

Ростелеком Солар

Создание комплексных систем кибербезопасности

Комплексный подход к проектированию, созданию, эксплуатации и сопровождению систем безопасности на всех этапах их жизненного цикла

Консалтинг

- Формирование концепции и стратегии кибербезопасности
- Решение нетиповых задач

Анализ

- Обследование и аудит
- Практический анализ защищенности
- Оценка соответствия требованиям регуляторов
- Анализ рисков

Формирование требований

- Моделирование угроз
- Разработка технического задания
- Разработка roadmap развития кибербезопасности

Проектирование

- Проектирование системы кибербезопасности
- Разработка рабочей документации

Интеграция

- Внедрение СЗИ и настройка политик безопасности
- Настройка смежных систем
- Внедрение организационных мер защиты информации

Выстраивание процессов

- Разработка регламентов
- Выстраивание процессов управления изменениями
- Разработка ролевой модели и политики разграничения доступа к ресурсам

Сопровождение

- Техническая поддержка и эксплуатация СЗИ
- Аналитическая поддержка процессов кибербезопасности
- Актуализация документации

Ростелеком Солар

Решения и услуги Solar Интеграция

Экспертный консалтинг и комплексный аудит

- Комплексный аудит
- Анализ и оценка рисков
- Разработка стратегии и политики кибербезопасности
- Выстраивание процессов кибербезопасности

Защита периметра и ИТ-инфраструктуры

- Защита сети
- Криптографическая защита каналов связи
- Шлюз безопасности
- Защита от несанкционированного доступа
- Защита виртуализации
- Защита почты
- Защита от продвинутых угроз

Защита бизнес-приложений и данных

- Защита баз данных
- Защита данных на файловых хранилищах
- Шифрование дисков и носителей

Защита конечных станций и пользователей

- Защита рабочих станций и серверов от ВПО
- Продвинутая защита конечных станций
- Защищенный доступ с мобильных устройств

Защита онлайн-систем и веб-сервисов

- Защита от DDoS-атак
- Защита веб-приложений
- Анализ кода

Комплексный контроль защищенности

- Выявление и контроль уязвимостей
- Тестирование на проникновение

Управление доступом

- Управление правами доступа
- Многофакторная аутентификация
- Управление привилегированными пользователями

Управление кибербезопасностью

- Управление инцидентами
- Управление процессами
- Управление сетевой безопасностью

Кибербезопасность объектов КИИ и АСУ ТП

- Выполнение требований 187-ФЗ
- Обеспечение кибербезопасности АСУ ТП
- Мониторинг АСУ ТП
- Киберучения АСУ ТП

Обеспечение соответствия требованиям регуляторов

- Защита ПДн
- Защита ГИС
- Защита КИИ
- Защита финансовых организаций
- Защита КТ

Техническая поддержка и сопровождение 24/7

Ростелеком Солар

Ростелеком
Солар

Центральный офис

125009, Москва, Никитский переулок, 7с1

+7 (499) 755-07-70

solar@rt-solar.ru