Создание зрелой системы обеспечения ИБ в АСУ ТП

Андрей Кудеров — руководитель отдела по развитию бизнеса с технологическими партнерами. Positive Technologies

Александр Карпенко — руководитель направлений защиты АСУ ТП и КИИ. Инфосистемы Джет

PRO автоматизацию

Особенности обеспечения ИБ промышленных предприятий

Особенности внедрения СЗИ в АСУ ТП — согласование с вендорами АСУ ТП, ожидание технологических окон

Территориальная распределенность и низкая доступность отдельных объектов

Смешение задач КИТСО и ИБ в ущерб последнему

Низкий уровень грамотности ИБ на местах

Санкции — особенности выбора и закупки средств защиты

Комплаенсный подход

ФСТЭК

- Проведение проверок (плановые и внеплановые) значимых объектов КИИ
- Ведение реестра значимых объектов КИИ
- Установка требований по безопасности
- Проверка результатов категорирования

ФСБ

- Координация деятельности субъектов КИИ по вопросам инцидентов (ГосСОПКА)
- Организация и проведение оценки безопасности КИИ
- Утверждение порядка, технических условий установки и эксплуатации средств, предназначенных для ГосСОПКА
- Другие функции в части ГосСОПКА

Дополнение такого подхода

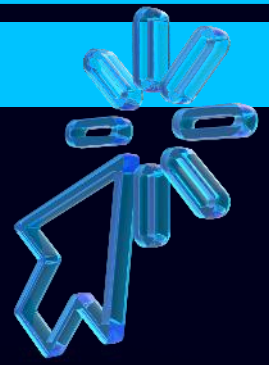
- Сложности по реализации процесса и своевременного устранения выявленных уязвимостей ИБ-компонентов АСУ
- Отсутствие поддержки производителем используемых аппаратных или программных компонентов АСУ ТП
- Недостаточное количество ресурсов для адекватной эксплуатации СОИБ АСУ ТП
- Отсутствие контроля цепочки поставок и доверенного взаимодействия с разработчиками ПО
- Недостаточный набор организационных и технических мер защиты для противодействия APT-атакам
- Харденинг операционных систем, СУБД, инфраструктурных сервисов затруднен, поскольку требует длительного тестирования изменений и встречает противодействие со стороны эксплуатационного персонала
- Часть наложенных средств защиты являются высокоинвазивными, в случае их несовместимости с аппаратным или программным обеспечением АСУ ТП приходится применять низкоэффективные компенсирующие меры

Абстракция комплексного подхода по уровням

Стратегический уровень

- **Анализ состояния ИБ АСУ ТП на уровне ИА**: проведение аудита верхнеуровневых процессов, изучение корреляции ИБ АСУ ТП и бизнес-целей
- **Систематизация подходов к защите:** разработка стратегии и дорожной карты, формирование целевой модели ИБ АСУ ТП

Тактический уровень

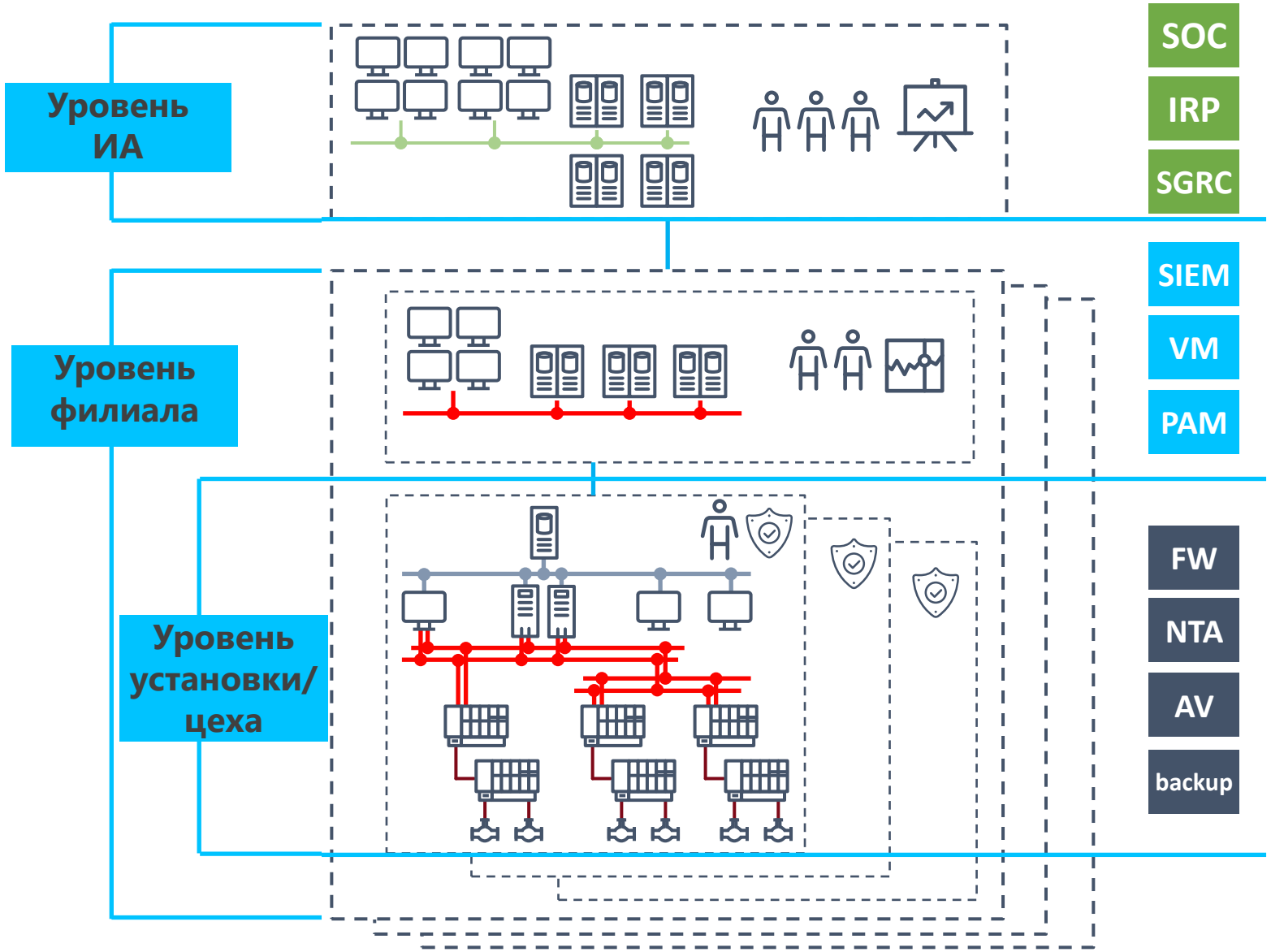


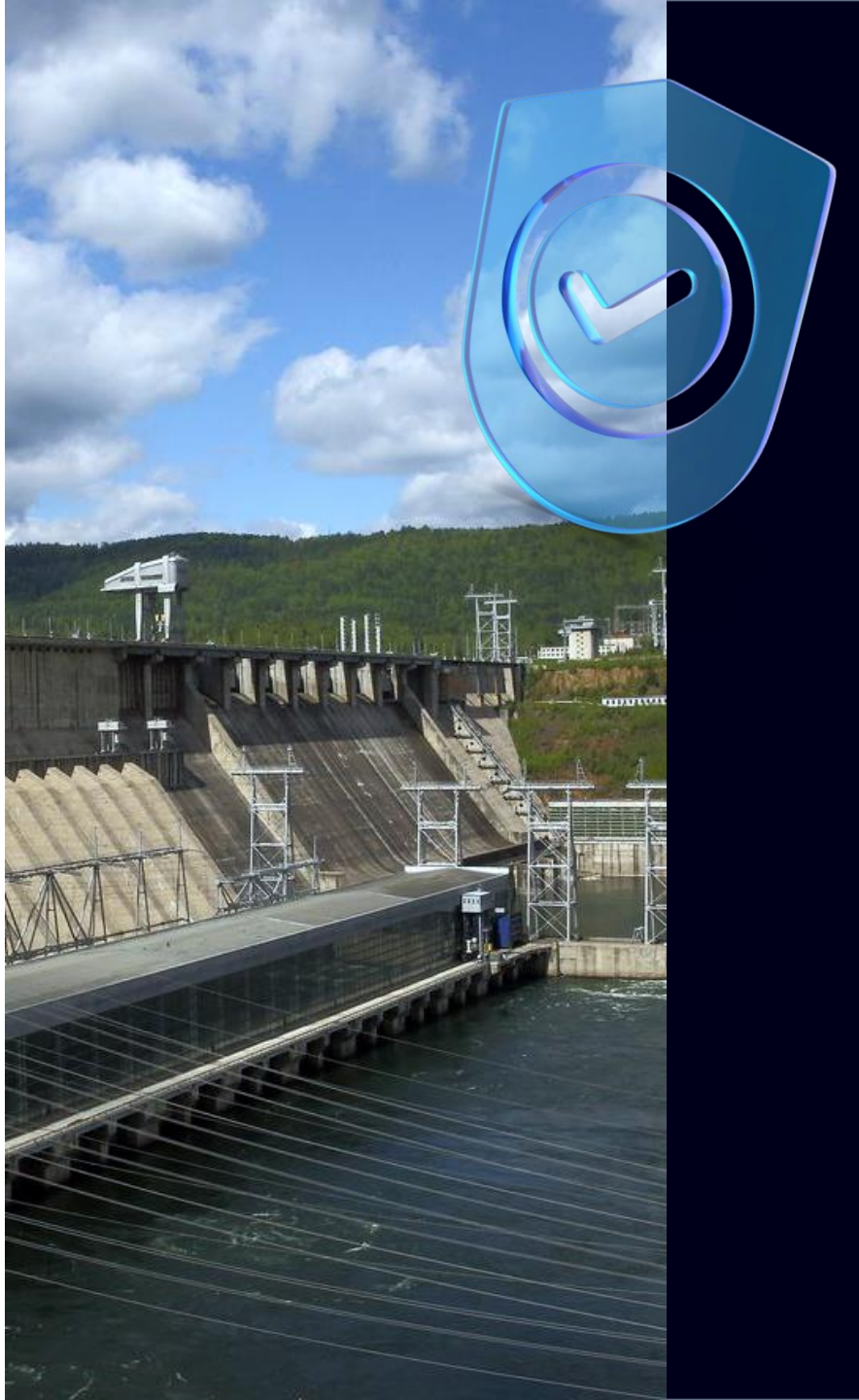
- **Анализ состояния ИБ АСУ ТП на уровне филиалов:** проведение тестов на проникновение для оценки реального уровня защищенности и инвентаризация типовых объектов
- **Формирование контура систем защиты:** разработка эскизных проектов для тестовых филиалов, формирование и тестирование наборов мер

Оперативный уровень

- **Повышение осведомленности на местах:** проведение обучений, киберучений
- **Аутсорсинг:** реализация оперативного мониторинга ИБ АСУ ТП

УРОВНИ СИСТЕМЫ ЗАЩИТЫ





Реализация механизмов защиты на Alpha.Platform

Харденинг прикладного ПО

Корректные компенсирующие меры

Реализация дополнительных мер защиты

Буду рад ответить на вопросы

@ALEXKRPENKO

Александр Карпенко
Руководитель направлений защиты АСУ ТП и КИИ
Инфосистемы Джет

Обеспечиваем практическую кибербезопасность

22 года
опыта исследований и разработок

2700+
сотрудников в компании: инженеров по ИБ, разработчиков, аналитиков и других специалистов

1200+
экспертов по кибербезопасности и разработке ПО

200+
обнаруженных уязвимостей нулевого дня в год

250+
аудитов безопасности корпоративных систем проводим ежегодно

50%
всех уязвимостей в промышленности и телекоме обнаружили наши эксперты

- Создаем продукты и решения
- Проводим аудит безопасности
- Расследуем инциденты
- Исследуем угрозы

Проблемы безопасности в Промышленных инфраструктурах

По данным Positive Technologies*, в среднем на промышленном предприятии выявляется до шести грубых нарушений, таких как:

- Непроектные АРМ, в том числе с выходом в интернет
- Незащищенные точки доступа
- Неконтролируемый, в т.ч. удаленный доступ к ресурсам технологической сети
- Неавторизованные каналы связи, отсутствие сегментации сети
- Отсутствие обновлений ПО и баз правил обнаружения
- Использование паролей по умолчанию и общих учетных записей пользователей

* Каждое нарушение несет в себе риски кибербезопасности

PT ICS — комплексное решение для защиты АСУ ТП

PT ISIM	Глубокий анализ трафика в промышленных ИТ-инфраструктурах, IIoT-средах, DICOM-системах и сетях
MaxPatrol SIEM	Для SOC: сбор и анализ событий безопасности с прикладного уровня систем АСУ ТП — серверов SCADA, контроллеров, АРМ
MaxPatrol VM	Выявление уязвимостей в промышленных системах и управление процессом их устранения
PT Sandbox	Поведенческий анализ и антивирусная проверка файлов из трафика и с рабочих станций
MaxPatrol EDR	Обнаружение целевых и сложных угроз на рабочих станциях и серверах
PT NGWF	Межсетевой экран нового поколения, сочетающий в себе производительность, надежность и простоту эксплуатации

Мониторинг событий безопасности Альфа платформы

- Поддержка протокола для разбора сетевого трафика
- Подмена или попытка изменить конфигурацию проекта сервера данных
- Попытка подменить файл, содержащий пароль для подключения к серверу данных
- Фиксация остановки сервера данных
- Попытка подменять файл конфигурации сервера данных
- Обнаружение изменений конфигурации Alpha.Security, Alpha.HMI, Alpha.Security.Configurator
- Обнаружение изменений файлов базы данных Alpha.Historian

Мониторинг событий безопасности Альфа платформы

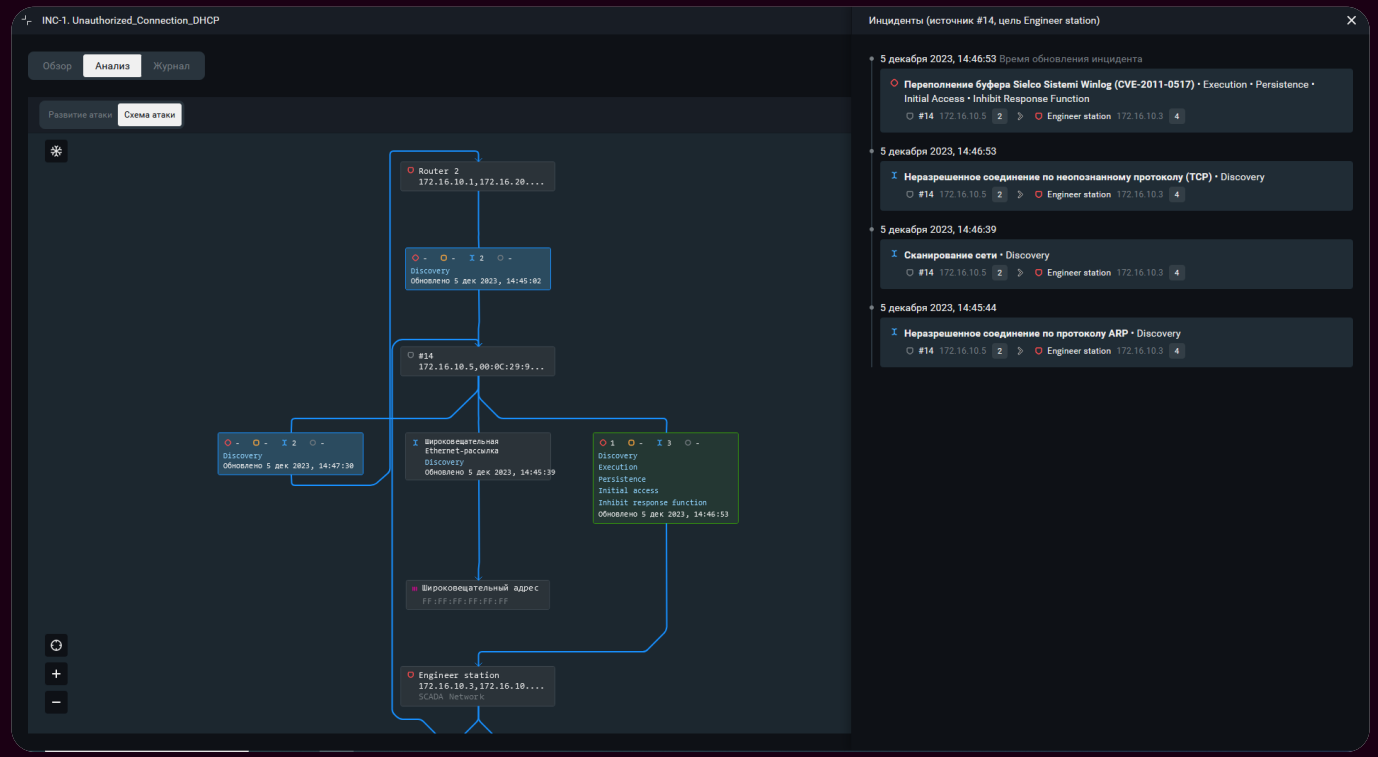
- ❑ Обнаружение изменения требований к паролю в Alpha.Security.Configurator по умолчанию
- ❑ Обнаружение изменения конфигурации Alpha.Security
- ❑ Обнаружение изменения исполняемых файлов Альфа платформы
- ❑ Обнаружение запуска процесса среды разработки Alpha.HMI
- ❑ Обнаружение завершения процесса среды визуализации Alpha.HMI
- ❑ Изменение или удаление логов
- ❑ Копирование файлов проекта

PT ISIM — основной инструмент для обеспечения киберустойчивости промышленных инфраструктур

PT ISIM — промышленная NTA-система

- Разбирает трафик общесетевых и промышленных протоколов на периметре и внутри сети
- Выявляет атаки и потенциально опасные действия
- Предоставляет информацию для расследования инцидентов

PT ISIM контролирует защищенность технологической сети, позволяет вовремя распознать угрозы кибербезопасности и предотвратить ущерб для предприятия



Какие задачи решает PT ISIM

Наблюдаемость и контроль изменений

технологической сети дают возможность повысить киберустойчивость инфраструктуры

Мониторинг безопасности

позволяет предотвращать опасные технологические нарушения

Обнаружение и анализ угроз

помогают защищать сеть и поддерживать непрерывность технологических и бизнес-процессов

Обеспечивает инвентаризацию технологической инфраструктуры и контроль изменений

Выявляет аномалии и события безопасности в технологическом трафике

Обнаруживает эксплуатацию уязвимостей и другие техники злоумышленников

Детектирует опасные технологические команды

Обнаруживает ВПО и отправляет подозрительные файлы на анализ

Помогает соблюдать требования регулирующих организаций

За примерами ходить недалеко

Нефтебаза

Слив из хранилища и вывоз десятка автовозов с нефтепродуктами

Сокрытие следов в SCADA

экономический ущерб

АЭС

До 20 разновидностей ВПО в системе контроля радиационного фона атомного энергоблока

Потенциальный ущерб государству, населению, экологии

Центр переработки ТБО

Незаконный ввоз и разгрузка ТБО на территорию центра.
Доступ к системе СКУД у водителей с незадекларированным грузом.
Разгрузка в обход систем контроля

экономический ущерб

Нефтепровод

Получение неучтенных остатков нефти при транспортировке
Слив и вывоз с территории ППН неучтенных остатков

экономический ущерб

Металлургический комбинат

Сотрудник в нерабочее время удаленно отключил ПАЗ и взял управление козловым краном.

Фатальный ущерб производству, пострадавший специалист на площадке

экономический ущерб

гибель человека

Positive Technologies в промышленности

Нефтегаз	SOC в трех крупнейших нефтегазовых компаниях
Металлургия	Три горнодобывающих и два металлургических предприятия SOC в одной из крупнейших металлургических компаний
Традиционная генерация	Более 60 электростанций SOC в двух энергокомпаниях
Гидрогенерация	30+ гидроэлектростанций SOC в двух генерирующих компаниях
Электрические сети	20+ подстанций 220/110 кВ SOC в трех электросетевых компаниях
Непромышленные инженерные системы	Дата-центр в национальном телеком-провайдере Крупнейший спортивный объект
Транспорт	100+ объектов железнодорожной транспортной инфраструктуры по всей стране

PT ISIM
Страница на сайте
ptsecurity.com

PT ICS
Подписывайтесь
на телеграм-канал
продукта

Спасибо!