# UDV DATAPK Industrial Kit

Комплекс решений для мониторинга состояния защищенности и оперативного обнаружения инцидентов ИБ в промышленных сетях

udv|group

# UDV Group — ведущий разработчик в области кибербезопасности

UDV Group предоставляет единый портфель решений для защиты технологических сетей, корпоративного сегмента и автоматизации в области объектовой безопасности:

- защита АСУ ТП и объектов КИИ
- мониторинг инфраструктуры
- реагирование на инциденты ИБ
- автоматизация работы SOC
- выполнение требований регуляторов

**200+**
разработчиков в штате

Распределённая команда
со штаб-квартирой в Екатеринбурге

**1000+**
инсталляций

Проекты по защите АСУ ТП
и корпоративных сетей

**10+**
патентов

Собственный исследовательский
центр в области кибербезопасности

**10**
лет на рынке

Подтвержденный опыт интеграции
в крупных предприятиях
нефтегазовой отрасли, энергетики,
металлургии и других

udv|group

# UDV DATAPK Industrial Kit

**UDV DATAPK Industrial Kit –** это комплексное решение для обеспечения ИБ АСУ ТП.

Решение позволяет быстро начать реагировать на угрозы без негативного влияния на защищаемые системы. Обеспечивает видимость ландшафта АСУ ТП, выявляет инциденты на ранних этапах и помогает выполнить требования регуляторов.

UDV DATAPK Industrial Kit использует целостный подход в рамках единого решения, что позволяет оптимизировать расходы на защиту АСУ ТП.

# Возможности UDV DATAPK Industrial Kit

## Industrial NTA + IDS
### Анализ сетевого трафика и обнаружение вторжений

- Анализ копии сетевого трафика (SPAN)
- Выявление и инвентаризация активов
- Визуализация карты устройств в сети и сетевых соединений
- Обнаружение атак, нелегитимных узлов, несанкционированных сетевых соединений
- Более 20 000 правил обнаружения «из коробки»
- Обновление правил обнаружения без модификации программного кода
- Формирование инцидентов ИБ

## Configuration Manager
### Управление конфигурациями

- Контроль безопасных настроек и их неизменности, аудит изменений
- Анализ соответствия требованиям ИБ
- Работа без использования агентов
- Использование стандартных общедоступных протоколов компонентов АСУ ТП
- Формирование инцидентов ИБ

# Возможности UDV DATAPK Industrial Kit

## Vulnerability Manager
### Управление уязвимостями

- Неинвазивный аудит безопасности без использования агентов
- Проверка соответствия требованиям (Compliance)
- Технологии OVAL и «CPE to CVE»
- Поддержка различных БДУ, включая ФСТЭК России
- Формирование инцидентов ИБ

## External Event Manager
### Управление внешними событиями

- Получение событий ИБ с различных источников
- Нормализация событий ИБ
- Корреляция событий ИБ
- Возможность настройки правил корреляции событий ИБ
- Отправка инцидентов ИБ в сторонние системы (syslog)
- Формирование инцидентов ИБ

# UDV DATAPK Industrial Kit

Комплексное решение для мониторинга состояния защищенности и оперативного обнаружения инцидентов ИБ в промышленных сетях

udvgroup

# Классы средств защиты информации

к которым относится UDV DATAPK Industrial Kit
в соответствии с Приказом №235 ФСТЭК России

Средство управления событиями

Система обнаружения вторжений

Средство анализа защищенности

udvgroup

# Больше чем СОВ для АСУ ТП

01

Замена нескольких разнородных решений единым комплексом, разработанным для промышленных предприятий

02

Выполнение требований регулятора и реализация мер 31 и 239 приказов ФСТЭК России

03

Обладает дополнительной функциональностью нескольких классов решений

04

Оптимизирует процессы управления ИБ в организации

# Режимы работы UDV DATAPK Industrial Kit

## Режим наблюдения

- Однонаправленное получение данных
- Прослушивание трафика
- Возможно подключение через диод данных, для гарантии отсутствия влияния на объекты защиты

## Режим запрос-ответ

- Взаимодействие с объектами защиты в режиме «запрос-ответ» с использованием штатных механизмов и протоколов
- Получение с объектов защиты данных о программном обеспечении, его версиях, патчах и конфигурациях
- Выявление уязвимостей и проверки на соответствие требованиям ИБ

| Функции | Режим наблюдения | Режим опроса |
|---|---|---|
| Сбор событий ИБ | ⊖ ✓ | ✓ |
| Обнаружение атак | ✓ | ✓ |
| Выявление сетевых аномалий | ✓ | ✓ |
| Сбор конфигураций | ⊖ | ✓ |
| Определение текущего состава ОЗ | ✓ | ✓ |
| Выявление изменений в составе ОЗ | ✓ | ✓ |
| Проверка ОЗ на наличие уязвимостей | ⊖ ✓ | ✓ |

udvgroup

# Архитектура UDV DATAPK Industrial Kit

## SUPERVISION

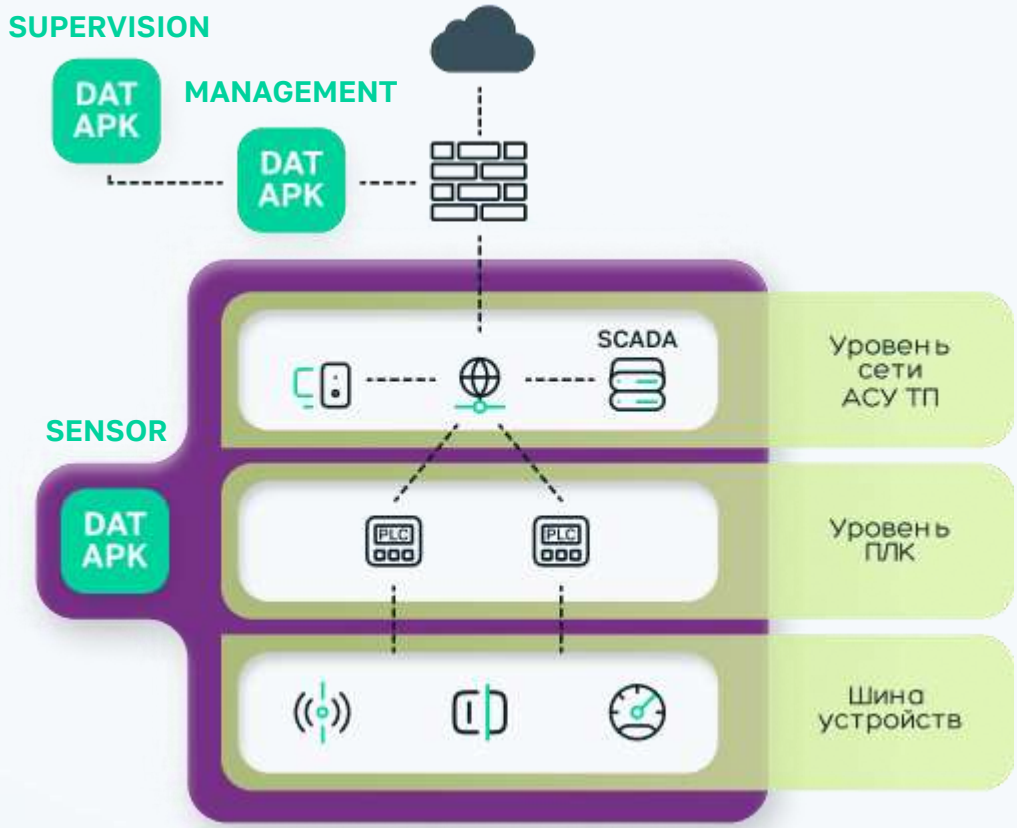
- Централизованная аналитика и отчетность для любой роли
- Централизованное управление всей системой

## MANAGEMENT

- Детализированное представление данных
- Базовые панели мониторинга и отчетность
- Конфигурация системы
- Управление сенсорами
- REST API для интеграции со сторонними системами

## SENSOR

- Получение данных, полученных от компонентов АСУ ТП, и передача на уровень Management
- Пассивный анализ копии сетевого трафика
- Активный сбор данных о конфигурациях, уязвимостях, и т.д.
- Получение событий из внешних источников (syslog)



# Преимущества UDV DATAPK Industrial Kit

01 Создан для АСУ ТП и учитывает все требования к средствам защиты информации

02 Реализует все необходимые возможности класса промышленных СОВ

03 Обладает дополнительной функциональностью нескольких классов решений

04 Сертифицирован ФСТЭК России[1]

05 Защищает значимые объекты КИИ в РФ[2]

06 Протестирован производителями АСУ ТП[3]

udvgroup

1 – Сертификат №4451 от 27.09.2021 ФСТЭК России по требованиям профиля защиты СОВ уровня сети, уровням доверия в соответствии с Приказом №76 от 2 июня 2020 года

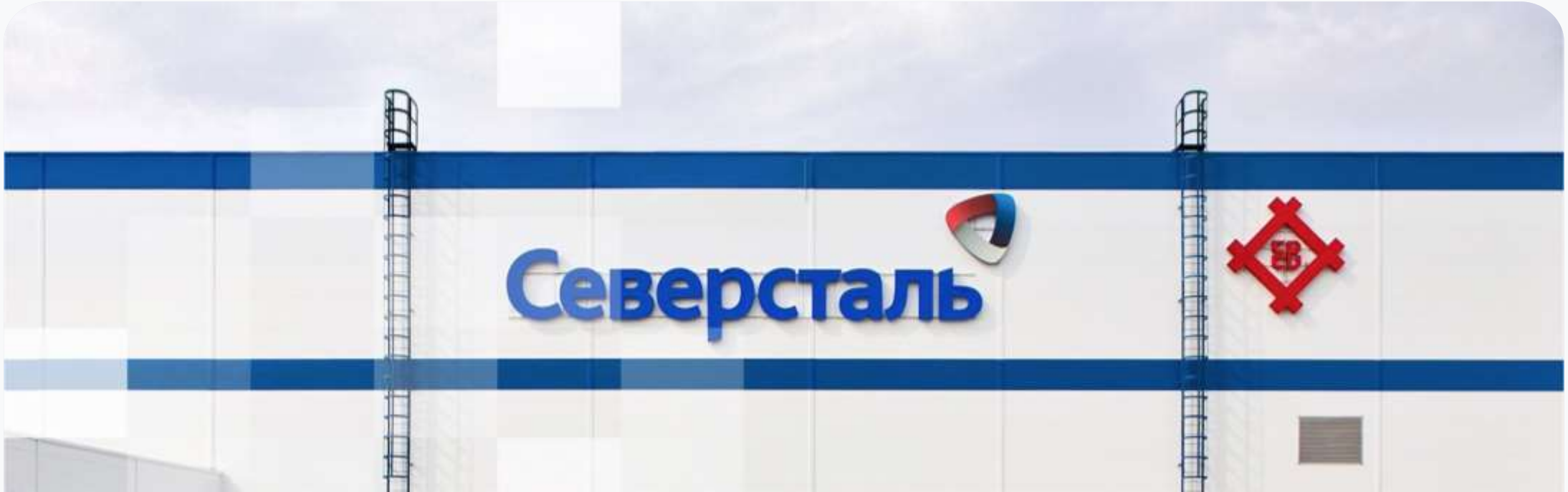
2 – «Северсталь» и УЦСБ завершили один из этапов построения системы защиты https://www.severstal.com/rus/media/news/document22118.phtml, информация о внедрениях на других предприятиях является конфиденциальной

3 – Schneider Electric и компания «СайберЛимфа» успешно завершили испытания совместимости программных комплексов https://www.se.com/ru/ru/about-us/newsroom/news/press-releases/, информация о тестировании с другими производителями предоставляется по запросу

# Кейсы внедрения

# Система мониторинга ИБ для компании «Северсталь»

Компания «Северсталь» — крупнейшее горно-металлургическое предприятие с крупными активами в разных странах. «Северсталь» производит десятки миллионов тонн различной металлопродукции — стали, чугуна, железной руды, осуществляя поставки в 69 стран мира.



# О проекте

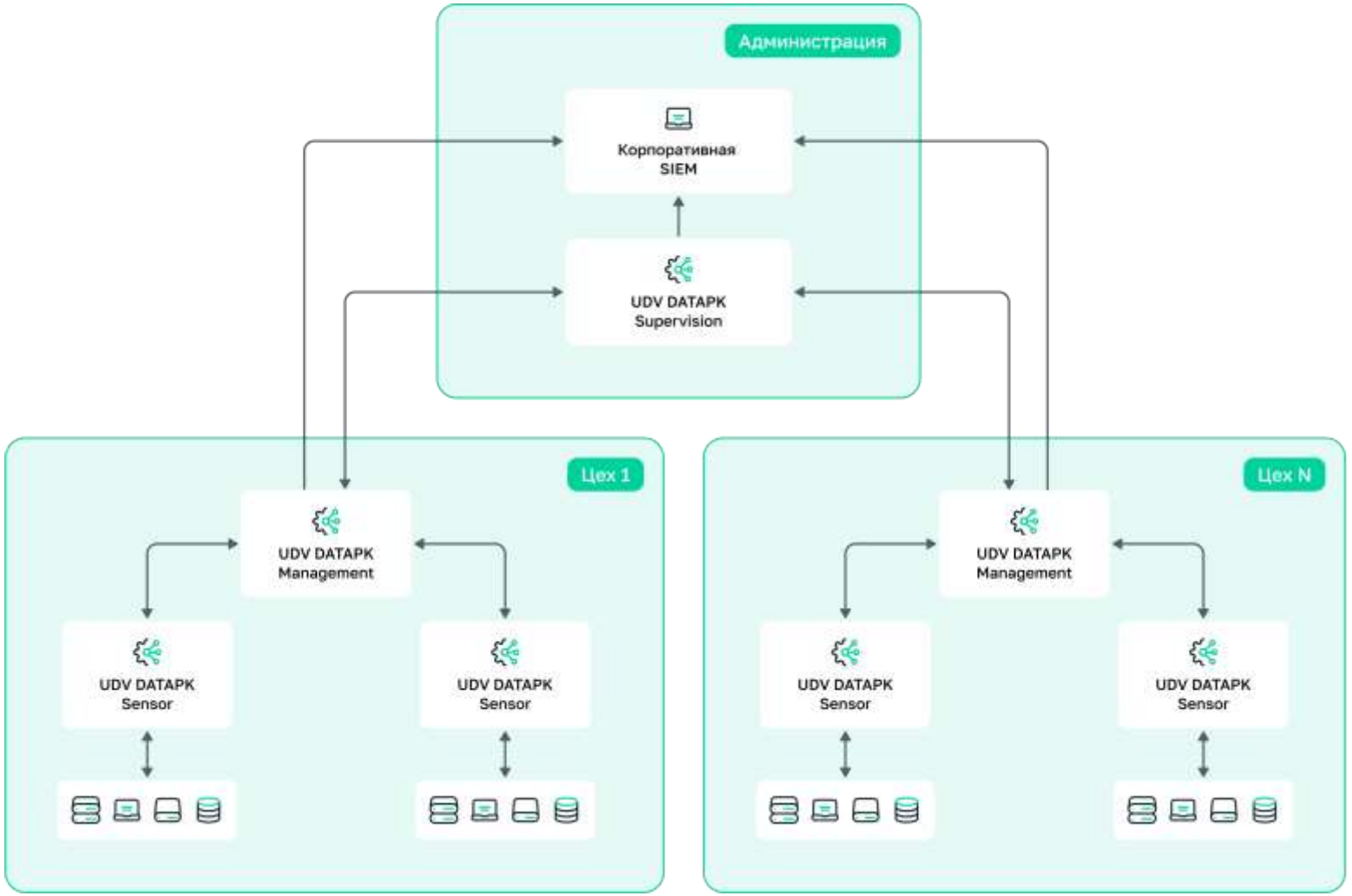
## Цель

Заказчику требовалось внедрить централизованную систему мониторинга информационной безопасности и защиты КИИ. Было необходимо обеспечить видимость конфигураций компонентов АСУ ТП, гибкий механизм корреляции событий ИБ и быструю реакцию на инциденты. Кроме того, на основании собственной экспертизы сотрудники «Северстали» сформировали список инцидентов для отслеживания, под который было необходимо адаптировать внедряемое решение.

**В качестве решения был внедрен комплекс**
**UDV DATAPK Industrial Kit, обеспечивающий:**

- Сбор событий безопасности с компонентов АСУ ТП
- Непрерывный контроль неизменности конфигураций компонентов АСУ ТП

# Схема внедрения



# Результаты внедрения

- Правила корреляции событий ИБ были адаптированы под требования заказчика, что помогло сократить количество инцидентов и устранить «белый шум» из уведомлений
- Конфигурации АСУ ТП приведены к соответствию стандартам организации
- Автоматизировано выявление аномалий
- Автоматизирована отправка данных в корпоративную SIEM-систему заказчика для дальнейшей обработки специалистами по ИБ

# Особенности проекта

01

## Распределенная организационная структура

Независимые подразделения отвечают за свою часть информационной безопасности (ИБ АСУ ТП, настройка узлов АСУ ТП, настройка сетевого оборудования и т.д.), что создает необходимость консолидирования данных от каждого из них при сохранении автономности.

02

## Совмещение локального и централизованного управления

Также были развернуты дополнительные сенсоры для обеспечения отказоустойчивости системы мониторинга ИБ. Новая система должна была учитывать интересы и приоритеты как филиалов, так и централизованной службы ИБ.

03

## Интеграция с корпоративным SOC

Необходимо было обеспечить совместимость с существующими ИБ-системами заказчика — в частности, отправку событий в SIEM.

# Система мониторинга безопасности для Ленинградской АЭС

ЛАЭС — уникальная атомная электростанция, которая производит более 55% потребляемой в регионе электрической энергии. Эта станция – единственная, где действуют энергоблоки двух разных типов – канальные уран-графитовые (РБМК) и водо-водяные (ВВЭР). ЛАЭС находится в Ленинградской области, в 40 километрах от Санкт-Петербурга, на побережье Финского залива.

# О проекте

## Цель

Основной целью проекта было проектирование и внедрение системы мониторинга безопасности объектов КИИ — специализированных промышленных систем управления изолированными энергосистемами. Также было необходимо интегрировать систему мониторинга с имеющимися на предприятии системами оповещения об инцидентах.

**В качестве решения был внедрен комплекс**

**UDV DATAPK Industrial Kit**

Он обеспечивает неинвазивный мониторинг сетевого трафика без влияния на работу АСУ ТП

# Результаты внедрения

- Внедрены системы мониторинга безопасности для уникальных технологических активов изолированных энергосистем
- Обеспечена видимость устройств и трафика, настроен сбор конфигураций
- Инженеры АСУ ТП получают своевременно информацию об уязвимостях и уведомления об инцидентах

# Особенности проекта

01

## Экосистема проприетарных сетевых протоколов и специфического программного обеспечения

В сети заказчика присутствовали специфические контроллеры и ряд проприетарных компонентов АСУ ТП. Решение DATAPK Industrial Kit было оперативно доработано под данные особенности.

02

## 10 комплексов UDV DATAPK Industrial Kit, выстроенных в двухуровневую иерархию для каждой энергосистемы

На энергоблоках были размещены компоненты уровней Management и Sensor. Также были развернуты дополнительные сенсоры для обеспечения отказоустойчивости системы мониторинга ИБ.

03

## Отсутствие выделенных специалистов ИБ

Изолированные системы на каждом из энергоблоков обслуживаются операторами АЭС без привлечения специалистов по информационной безопасности.

udv|group

# Спасибо!

## Закажите пилотный проект или персональную демонстрацию наших решений


Контакты

commercial@udv.group
8-800-511-65-51

Адрес

620100, г. Екатеринбург,
ул. Сибирский тракт, 12,
строение 7, этаж 4

Сайт

udv.group

Telegram

@udv_group