udv|group

UDV DATAPK Industrial Kit 3.0

Комплексный подход к решению задач

UDV Group — это

200+
разработчиков

Распределённая команда
со штаб-квартирой
в Екатеринбурге

1500+
инсталляций

Проекты по защите АСУ ТП
и корпоративных сетей

10+
патентов

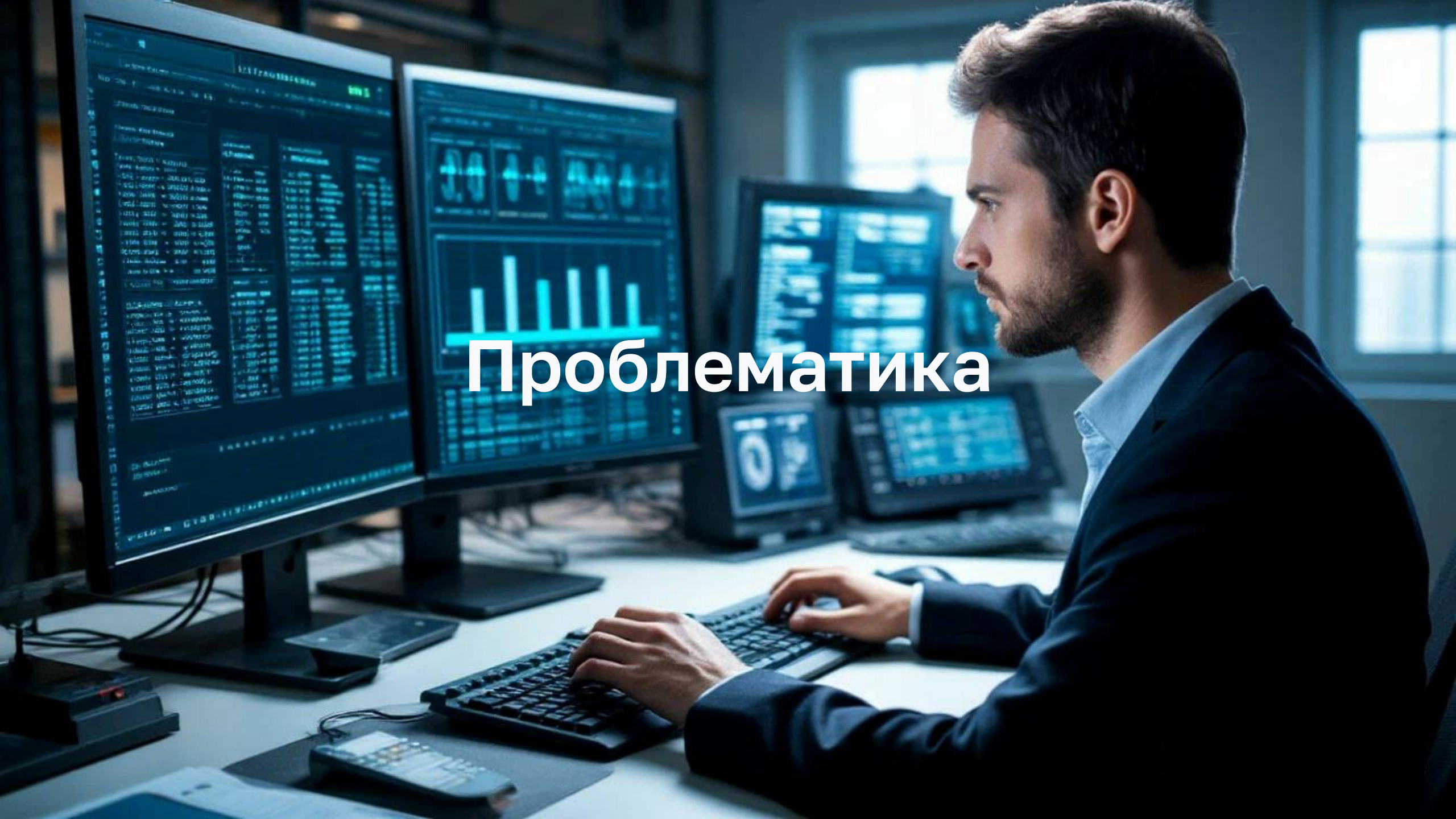
Собственный
исследовательский центр
в области
кибербезопасности

12
лет на рынке

Подтвержденный опыт
интеграции в крупных
предприятиях

UDV Group предоставляет
решения нацеленные на:

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


Проблематика

Бизнес-риски

Цифровизация
ставит технологические процессы в зависимость от корректной работы информационных систем

Умышленное нарушение
технологического процесса с помощью компьютерных средств — реальная угроза для бизнеса

Остановка производства

Техногенная катастрофа

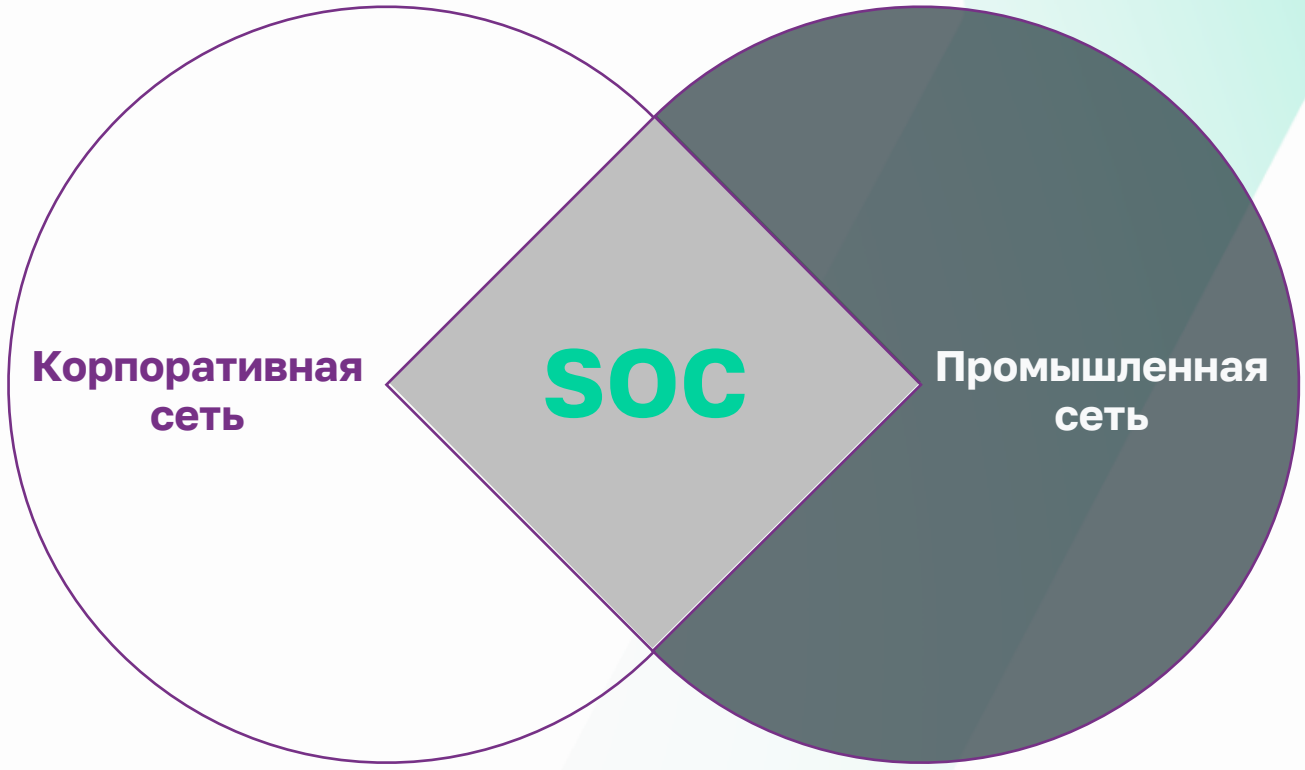
Мошенничество и саботаж

Брак

Кража технологий и секретов

Технологическая сеть — как объект защиты

- **АСУ ТП** — серая зона для большинства центров мониторинга
- **Нужен инструмент**, делающий происходящее в технологической сети прозрачным
- **Необходимы данные** о технологических аспектах работы для контроля бизнес-рисков



Перед нами поставили задачи...

Обнаружение атак в реальном времени и их предотвращение

Выявление уязвимостей и их устранение

Адаптация под изменения в инфраструктуре

Видимость сети АСУ ТП

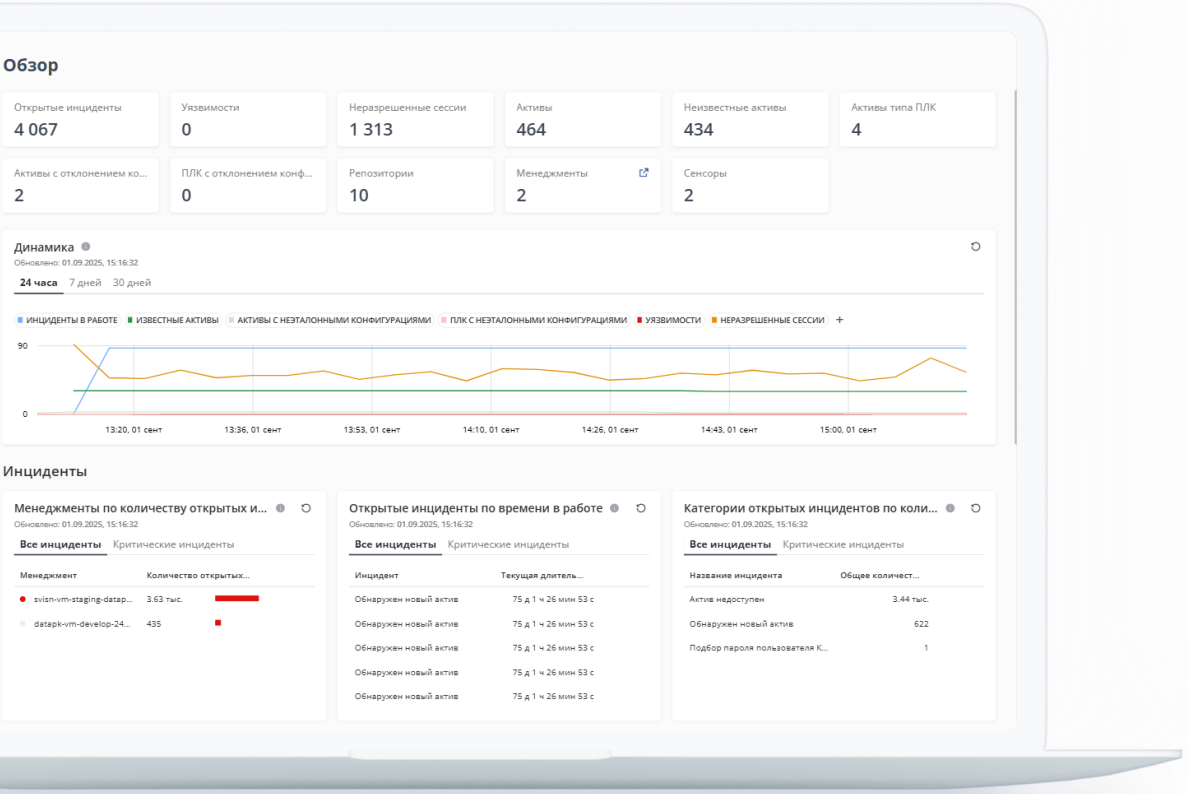
Компенсация нехватки кадров и опыта

Отслеживание изменений в конфигурациях

UDV DATAPK
Industrial Kit 3.0

UDV DATAPK Industrial Kit

Комплексная киберзащита АСУ ТП с полной видимостью атак,
угроз и выполнением требований законодательства



Решение использует целостный подход, что позволяет оптимизировать расходы на киберзащиту АСУ ТП:

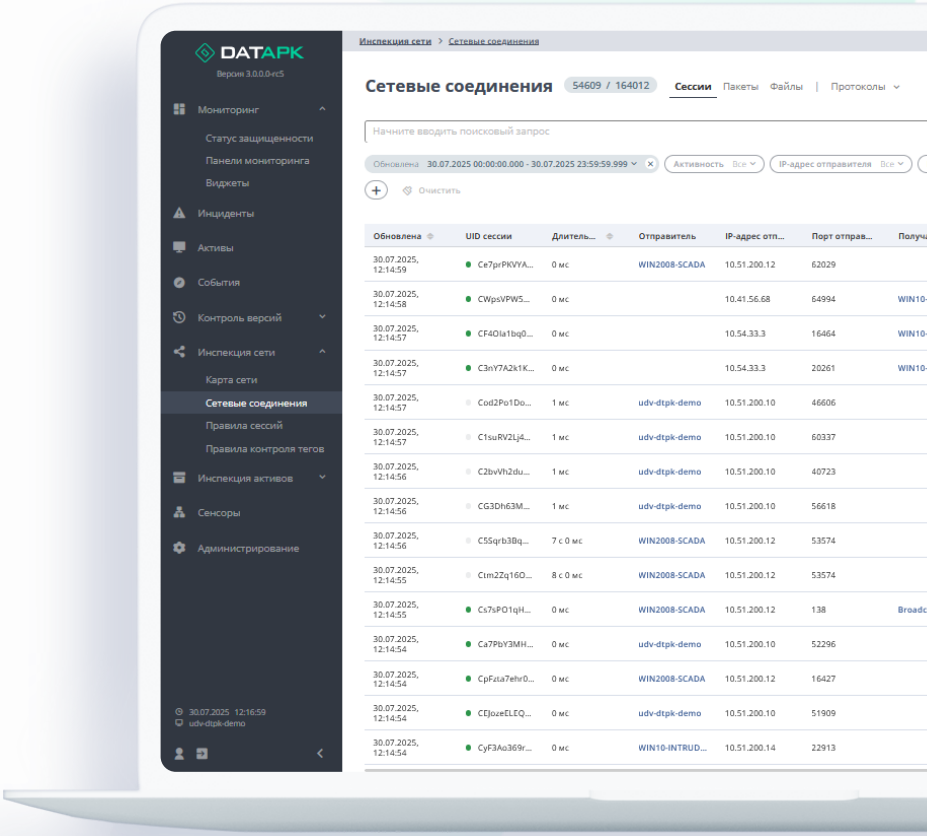
- Выявляет атаки и контролирует технологические процессы
- Обеспечивает соответствие конфигурационных параметров необходимым значениям
- Выявляет угрозы ИБ
- Собирает, обрабатывает, анализирует и отправляет события ИБ в другие системы
- Контролирует версии проектов ПЛК и восстанавливает исходный код проектов
- Выявляет аномалии в поведении ПЛК

UDV DATAPK Industrial Kit

Модуль Industrial NTA

Позволяет организациям выявлять атаки, проводить расследования и контролировать параметры технологических процессов

- Анализ копии сетевого трафика (SPAN, RSPAN, ERSPAN, TAP)
- Автоматическое создание правил сессий
- Выявление и инвентаризация всех активов
- Визуализация карты устройств в сети и сетевых соединений
- Обнаружение вторжений сигнатурными методами (IDS)
- Глубокая инспекция сетевых пакетов (DPI)
- Контроль параметров технологических процессов с помощью настраиваемых пользовательских правил
- Обнаружение атак, нелегитимных устройств в сети, несанкционированных сетевых соединений
- Выявление скрытых угроз ИБ, включая туннели и домены, сгенерированные алгоритмами (DGA), с помощью алгоритмов машинного обучения (ML)
- Определение техник и тактик, применяемых злоумышленником при реализации атаки
- Обнаружение файлов, передаваемых по сети, с возможностью их выгрузки для анализа
- Обновление правил обнаружения вторжений (IDS rules) без модификации программного кода
- Формирование инцидентов ИБ

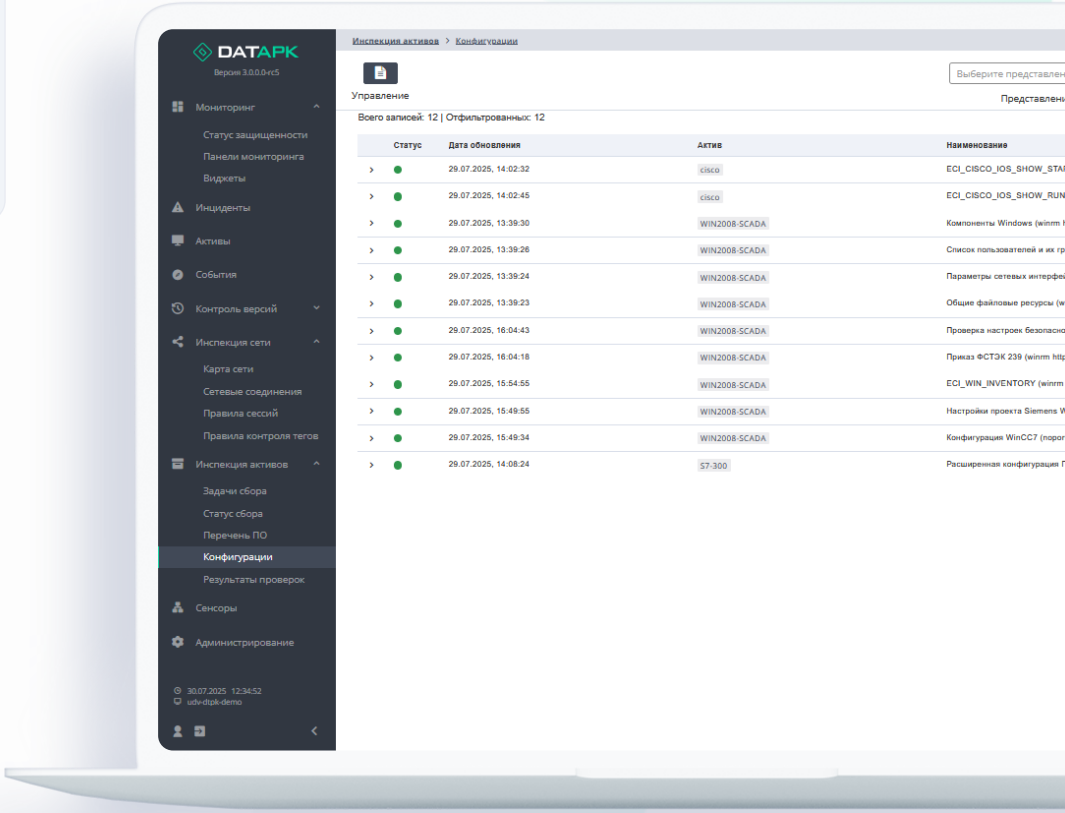


Управление конфигурациями устройств

Модуль Configuration Management

Позволяет инженерам АСУ ТП и специалистам по ИБ контролировать соответствие конфигурационных параметров необходимым значениям

- Сбор данных посредством общедоступных протоколов и интерфейсов компонентов АСУ ТП
- Контроль безопасных настроек и их неизменности, аудит изменений
- Контроль установленного на активах ПО
- Проверка соответствия требованиям ИБ
- Контроль неизменности программ на ПЛК
- Формирование инцидентов ИБ

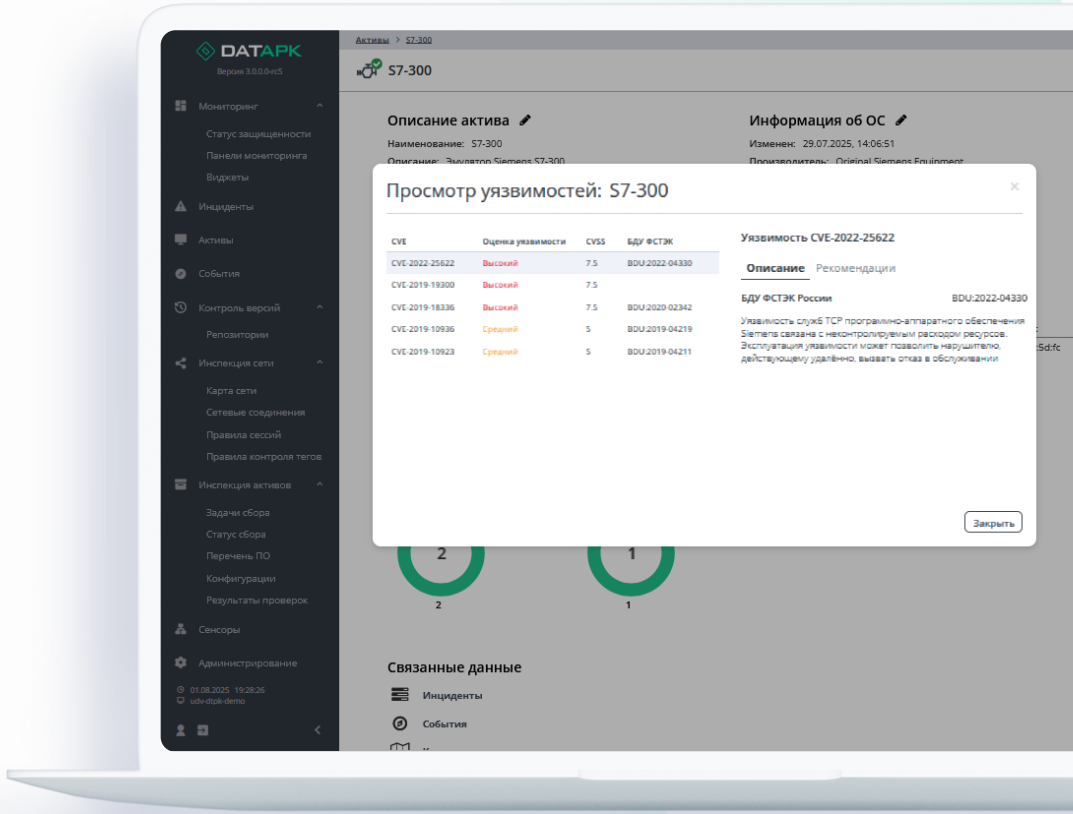


Управление уязвимостями

Модуль Vulnerability Management

Позволяет специалистам по ИБ проводить неинвазивный аудит защищенности АСУ ТП выявлять и устранять угрозы ИБ

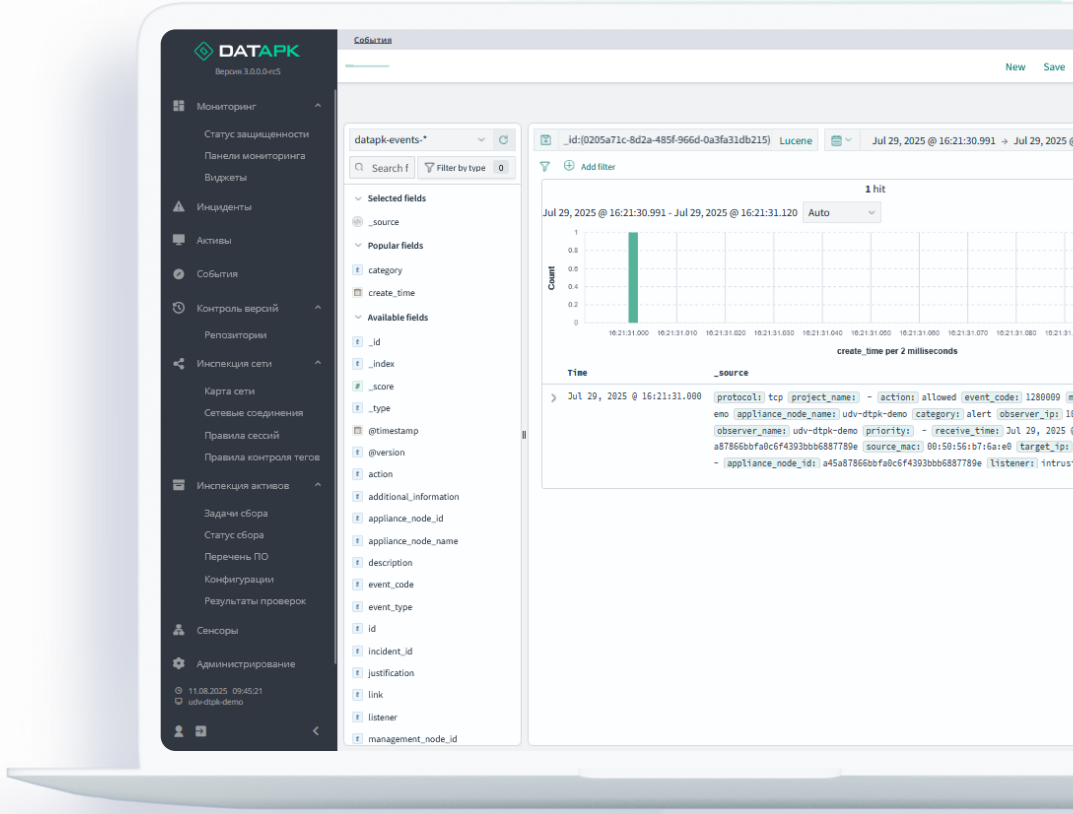
- Неинвазивный аудит информационной безопасности
- Проверка соответствия требованиям ИБ
- Технологии OVAL и CPE
- Возможность создания справочников сопоставления ПО
- Поддержка различных БДУ, включая БДУ ФСТЭК России
- Формирование инцидентов ИБ



Обработка и анализ событий

Модуль External Events Management

Предоставляет набор инструментов для обработки и анализа событий ИБ, собранных с внешних источников

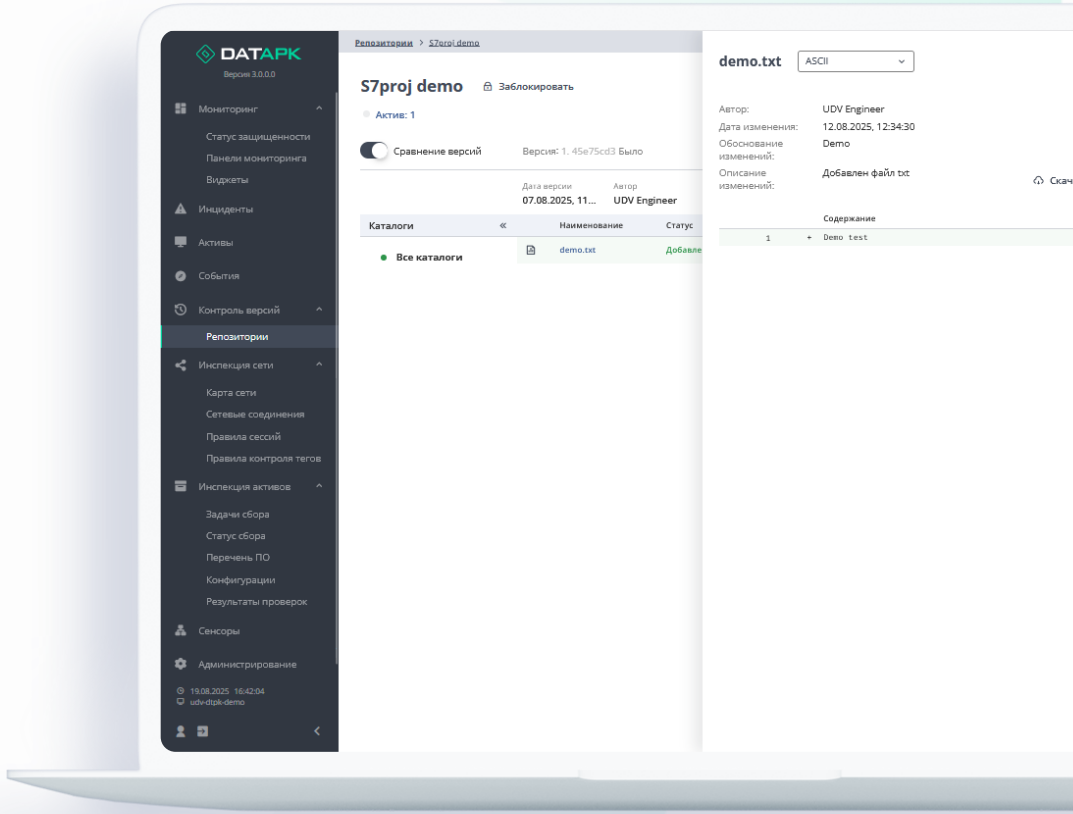


- Получение событий ИБ от различных источников
- Нормализация и корреляция событий ИБ
- Ретроспективный анализ событий ИБ
- Возможность настройки правил корреляции событий ИБ пользователем
- Преднастроенные и настраиваемые панели мониторинга
- Гибкие возможности для поиска и фильтрации внешних и внутренних событий ИБ
- Формирование инцидентов ИБ
- Возможность отправки событий и\или инцидентов ИБ в сторонние системы

Контроль версий проектов ПЛК

Модуль Version Control

Позволяет инженерам и программистам АСУ ТП централизованно управлять исходным кодом и проектами ПЛК



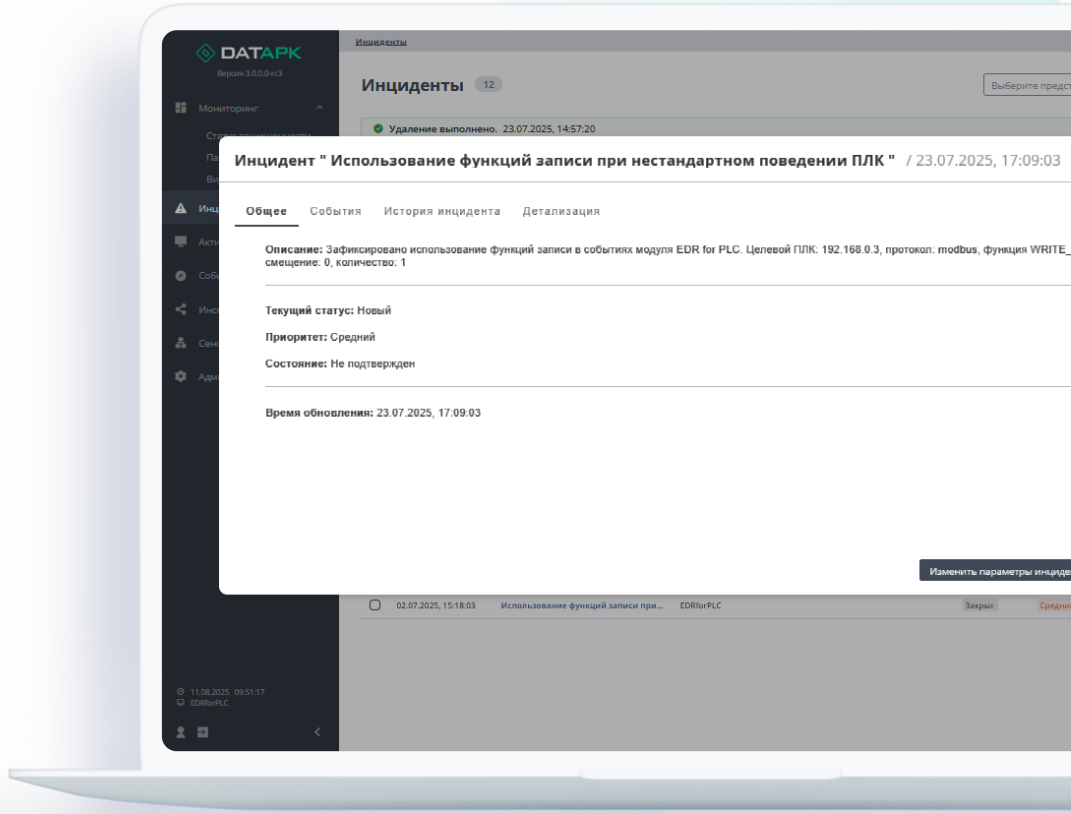
- Централизованное хранение исходного кода проектов ПЛК
- Контроль неизменности исходного кода проектов ПЛК
- Аудит изменений в исходном коде проектов ПЛК
- Отображение различий в исходном коде проектов ПЛК
- Восстановление версий исходного кода проектов ПЛК
- Непрерывная репликация проектов ПЛК на компонент Supervision
- Приложение, устанавливающееся на инженерную станцию
- Формирование инцидентов ИБ

Выявление аномалий в поведении ПЛК

Модуль ML for PLC

Позволяет организациям оперативно выявлять аномалии в поведении ПЛК посредством безагентного поведенческого анализа на основе машинного обучения

- Не использует агентов
- Независим от вендора ПЛК, версии прошивки и других факторов
- Отсутствие какого-либо негативного влияния на ПЛК
- Автоматизированное формирование эталонной модели поведения ПЛК на базе копии сетевого трафика
- Локальное обучение модели
- Возможность до-обучения модели
- Выявление аномалий в поведении ПЛК, которые не могут быть определены классическими DPI и SCADA-системами
- Формирование инцидентов ИБ
- Предоставление детализированной информации по выявленным инцидентам для определения первопричин аномалий



Реализация мер приказов №239 и №31 ФСТЭК России

UDV DATAPK Industrial Kit позволяет выполнить требования к организационным и техническим мерам проектирования и эксплуатации систем безопасности значимых объектов КИИ и защите АСУ ТП

ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов
ИАФ.2	Идентификация и аутентификация устройств
ИАФ.3	Управление идентификаторами
ИАФ.4	Управление средствами аутентификации
УПД.1	Управление учетными записями пользователей
УПД.4	Разделение полномочий (ролей) пользователей
УПД.5	Назначение минимально необходимых прав и привилегий
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему
УПД.9	Ограничение числа параллельных сеансов доступа
УПД.10	Блокирование сеанса доступа пользователя при неактивности
УПД.12	Управление атрибутами безопасности
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения
ЗНИ.7	Контроль подключения машинных носителей информации
АУД.1	Инвентаризация информационных ресурсов
АУД.2	Анализ уязвимостей и их устранение
АУД.4	Регистрация событий безопасности
АУД.5	Контроль и анализ сетевого трафика
АУД.6	Защита информации о событиях безопасности
АУД.7	Мониторинг безопасности
АУД.8	Реагирование на сбои при регистрации событий безопасности
АУД.9	Анализ действий отдельных пользователей
АУД.10	Проведение внутренних аудитов
СОВ.1	Обнаружение и предотвращение компьютерных атак
СОВ.2	Обновление базы решающих правил
ОЦЛ.1	Контроль целостности программного обеспечения
ОЦЛ.2	Контроль целостности информации
ОДТ.3	Контроль безотказного функционирования средств и систем
ОДТ.4	Резервное копирование информации
ЗИС.6	Управление сетевыми потоками
ЗИС.31	Защита от скрытых каналов передачи информации
ИНЦ.1	Выявление компьютерных инцидентов
ИНЦ.2	Информирование о компьютерных инцидентах
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах
УКФ.1	Идентификация объектов управления конфигурацией
УКФ.2	Управление изменениями
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения
УКФ.4	Контроль действий по внесению изменений
ОПО.4	Установка обновлений программного обеспечения
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации

Преимущества UDV DATAPK Industrial Kit

01 Отсутствие негативного влияния на АСУ ТП и технологические процессы

02 Сочетает функции нескольких классов решений ИБ

03 Возможности адаптации под индивидуальные потребности, в т.ч. непосредственными пользователями

04 Сертифицирован ФСТЭК России[1]

05 Совместим с компонентами АСУ ТП российских и зарубежных производителей

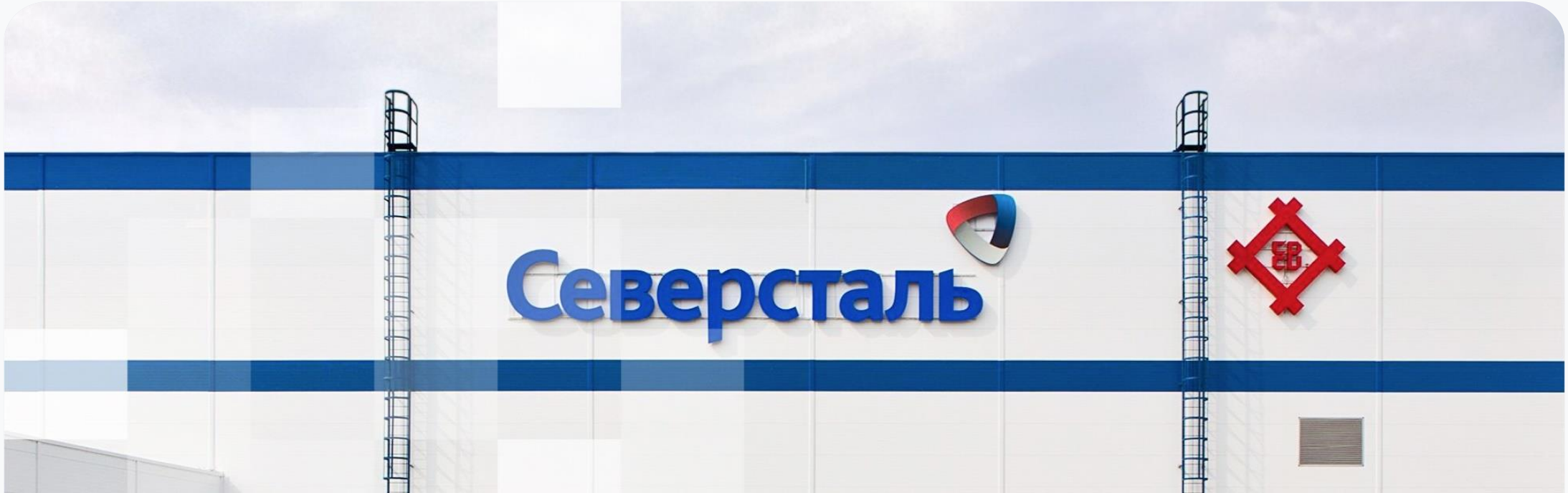
06 Модульная архитектура позволяет сократить расходы при ограниченных бюджетах

1. Сертификаты ФСТЭК России №4719 и №4451 по профилям защиты систем обнаружения вторжений уровня сети

Кейсы

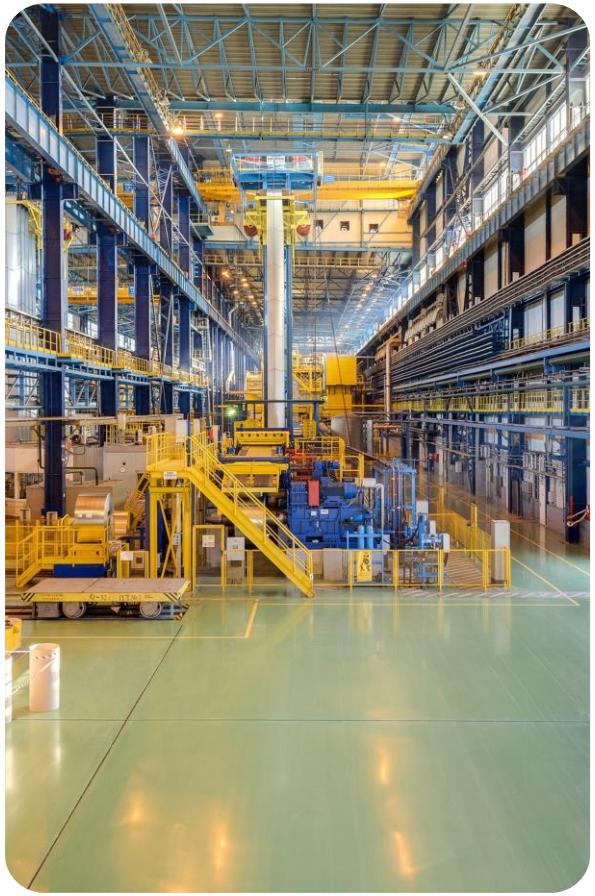
Система мониторинга ИБ для компании «Северсталь»

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.



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



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.

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

Экосистема решений UDV Group

Автоматизируют реагирование на инциденты и другие процессы ИБ, выстраивая целостную систему защиты информации в соответствии с требованиями регуляторов.

Комплексная платформа мониторинга функционирования распределённых автоматизированных систем

Защищают технологические сети от киберугроз, поддерживая бесперебойность производственных процессов.

Отсканируйте QR-код и загрузите буклет с описанием решений UDV Group в формате PDF

udv|group

udv|group

Остались вопросы?

Готовы обсудить ваши кейсы!

Контакты

commercial@udv.group

https://udv.group/

8-800-511-65-51