Система анализа и мониторинга состояния ИБ DATAPK

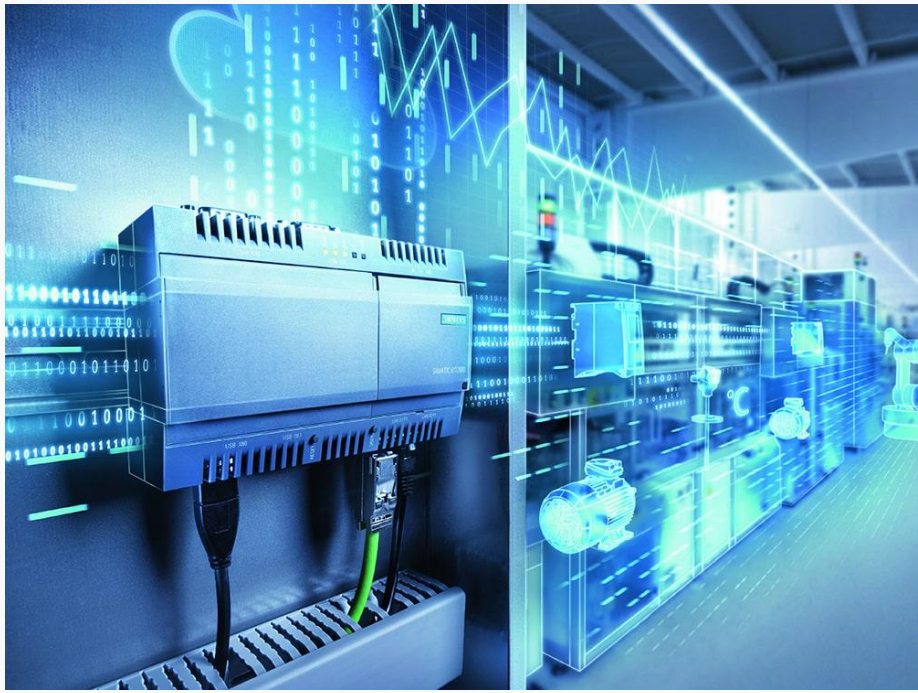
Тема 1. Общая информация. Подключение ПК DATAPK к инфраструктуре предприятия.

udv|group

Автоматизированная система управления технологическим процессом

АСУ ТП — это комплекс программных и технических средств, предназначенный для автоматизации управления технологическим оборудованием на предприятиях. Может иметь связь с более глобальной Автоматизированной системой управления предприятием (АСУ П).

Типовые функции:
измерение физических сигналов, параметров;
контроль функционирования технических и программных средств;
формирование заданий на управление;
реализация управления и т. д.



Автоматизированная система управления технологическим процессом

Под АСУ ТП обычно понимается целостное решение, обеспечивающее автоматизацию основных операций технологического процесса на производстве **в целом** или **каком-то его участке**, выпускающем **относительно завершенное изделие**.

Виды автоматических систем с программным управлением

Отличие АСУ ТП от других информационных систем

Сравнительный анализ информационных (IT) систем и АСУ ТП.

Сравниваемая характеристика	ИТ система	АСУ ТП
Требования к функционированию	Не является системой реального времени. Время реакции не всегда критично. Задержки и потеря данных могут быть приемлемыми. Менее критичные функции в аварийных ситуациях. Управление доступом определяется требованиями к ИБ.	Является системой реального времени. Время реакции критично. Задержки и потеря данных неприемлемы. Критична реакция в аварийных ситуациях. Управление доступом должно осуществляться, но не препятствовать функциям посредством человека-машинного интерфейса.
Требования к надежности и готовности	Перезагрузка является приемлемой. Дефициты готовности иногда могут быть приемлемыми, в зависимости от эксплуатационных требований.	Перезагрузка является неприемлема из-за требований к готовности. Требования к готовности, как правило, требуют внедрения резервирования. Планово-предупредительные работы планируются заранее. Высокая готовность требует всестороннего предварительного тестирования.
Требования к управлению рисками	Управление рисками относится, в первую очередь, к управлению данными. Первостепенное значение имеет конфиденциальность и целостность данных. Отказоустойчивость менее важна, поскольку кратковременный простой не является основным риском. Основным риском является задержка бизнес-операций.	Управление рисками относится, в первую очередь, к управлению физическими процессами. Первостепенное значение имеет безопасность людей, вытекающая из безопасности физических процессов. Отказоустойчивость имеет важное значение, даже кратковременный простой может быть неприемлемым. Основным риском является несоответствие требованиям регуляторов, воздействие на окружающую среду, жизнь и здоровье людей.

Отличие АСУ ТП от других информационных систем

Сравнительный анализ информационных (IT) систем и АСУ ТП.

Сравниваемая характеристика	ИТ система	АСУ ТП
Операционные системы	Используются ОС общего назначения. Обновления для ОС могут устанавливаться автоматически.	Нарду с ОС общего назначения, используются специализированные ОС, в том числе без встроенных функций ИБ. Изменения ПО тщательно контролируются и выполняются, как правило, поставщиками ПО, из-за специализированных алгоритмов управления и влияния на конфигурацию аппаратных средств, а также значительных затрат на лицензирование изменений.
Ограничения системных ресурсов	Системы имеют достаточно вычислительных ресурсов для добавления дополнительных приложений, связанных с обеспечением ИБ.	Системы разработаны для поддержки промышленных процессов и могут не иметь достаточно памяти или вычислительных ресурсов для поддержки функций безопасности.
Коммуникации	Применяются стандартные коммуникационные протоколы. Применятся в основном уже существующие сети. Применяются типовые сетевые решения.	Применяются специально разработанные (проприетарные) коммуникационные проколы. Часто прокладываются специальные сети. Сети базируются на различных типах медиа и могут требовать экспертных инженерных знаний.
Управление изменениями	Изменения ПО выполняются периодически под управлением политики и процедур безопасности. Процедуры изменений ПО зачастую автоматизируются.	Изменения ПО должны быть протестированы, и должно быть подтверждено сохранение целостности системы после изменений. Остановки в работе системы должны быть спланированы заранее. АСУ ТП может использовать не поддерживаемое более ПО.

Отличие АСУ ТП от других информационных систем

Сравнительный анализ информационных (IT) систем и АСУ ТП.

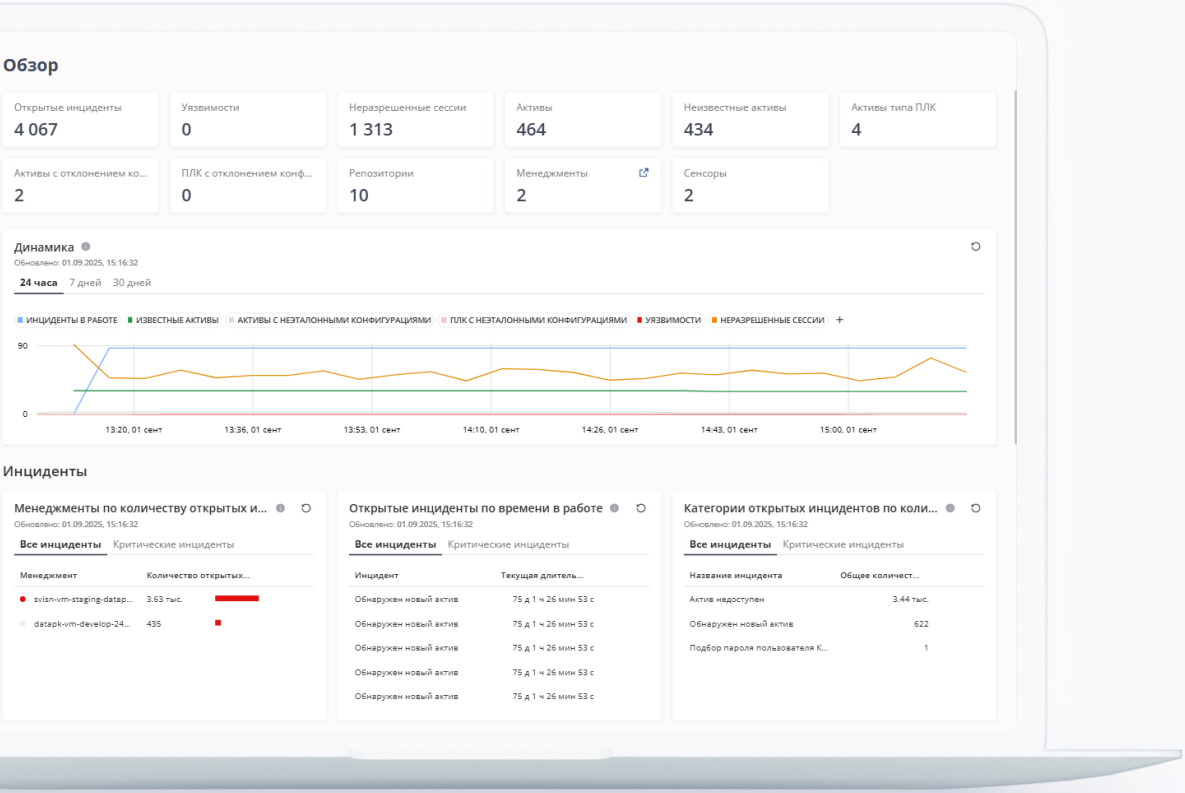
Сравниваемая характеристика	ИТ система	АСУ ТП
Поддержка эксплуатации	Может быть реализована различными поставщиками	Как правило, реализуется единственным поставщиком
Продолжительность эксплуатации	Типовая продолжительность жизненного цикла: 3-5 лет	Типовая продолжительность жизненного цикла: 10-15 лет, а некоторых объектов может доходить до 30 лет.
Физическое расположение компонентов	Компоненты обычно локализованы и к ним можно получить физический доступ	Компоненты могут быть изолированными , удаленными и с физически сложным доступом

Основные нормативные документы по ИБ АСУ ТП

- ФЗ от 26.07.2017 № 187-ФЗ «О безопасности КИИ РФ»
- Приказ ФСТЭК России №239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ»
- Приказ ФСТЭК России 31 от 14.03.2014 «Об утверждении Требований к обеспечению защиты информации в АСУ ТП …»

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

Производитель: ООО «СайберЛимфа» (входит в UDV Group)

Реестр российского ПО: запись № 4732 (CyberLympha DATAPK, UDV DATAPK Industrial Kit)

Сертификат ФСТЭК России: № 4719 (УД4, СОВ4, ЗБ)

Архитектура

Компоненты и их назначение

Supervision

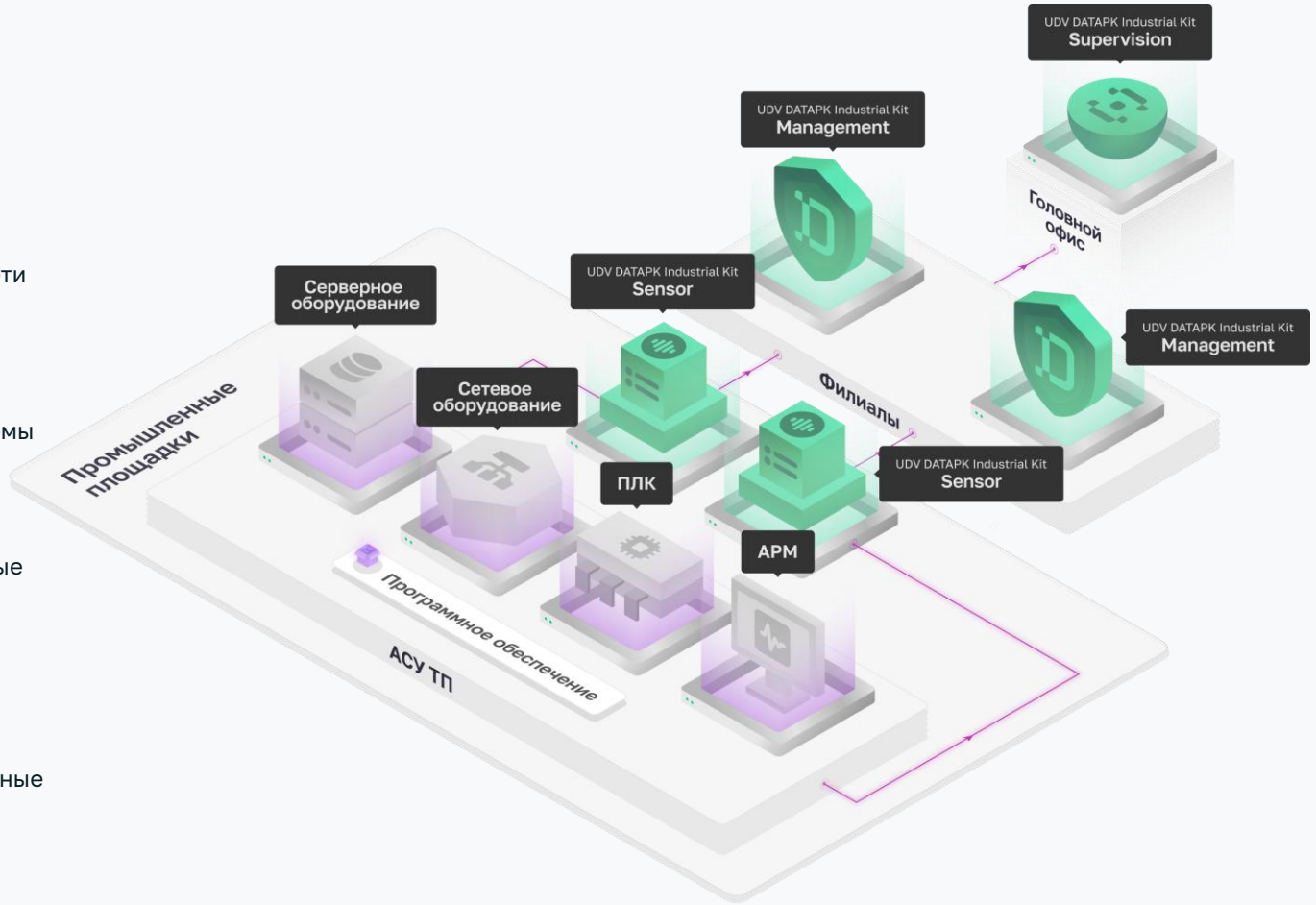
- Устанавливается в корпоративном или технологическом сегментах сети
- Получает данные от подключенных Management
- Предоставляет централизованную аналитическую информацию об общем состоянии защищённости АСУ ТП
- Осуществляет централизованное управление УЗ пользователей системы

Management

- Устанавливается в технологическом сегменте сети или за его пределами
- Получает данные от подключенных Sensor
- Осуществляет конфигурацию и администрирование связки Management + Sensor
- Осуществляет хранение обработанных данных
- Предоставляет детальные данные пользователю
- Предоставляет базовые панели мониторинга
- REST API для автоматизации
- Передает ключевые данные на Supervision

Sensor

- Устанавливается в технологическом сегменте сети
- Получает и хранит копию сетевого трафика
- Получает события ИБ от внешних источников
- Осуществляет сбор данных с активов
- Инициирует подключение к Management
- Передает пред-обработанные данные на Management



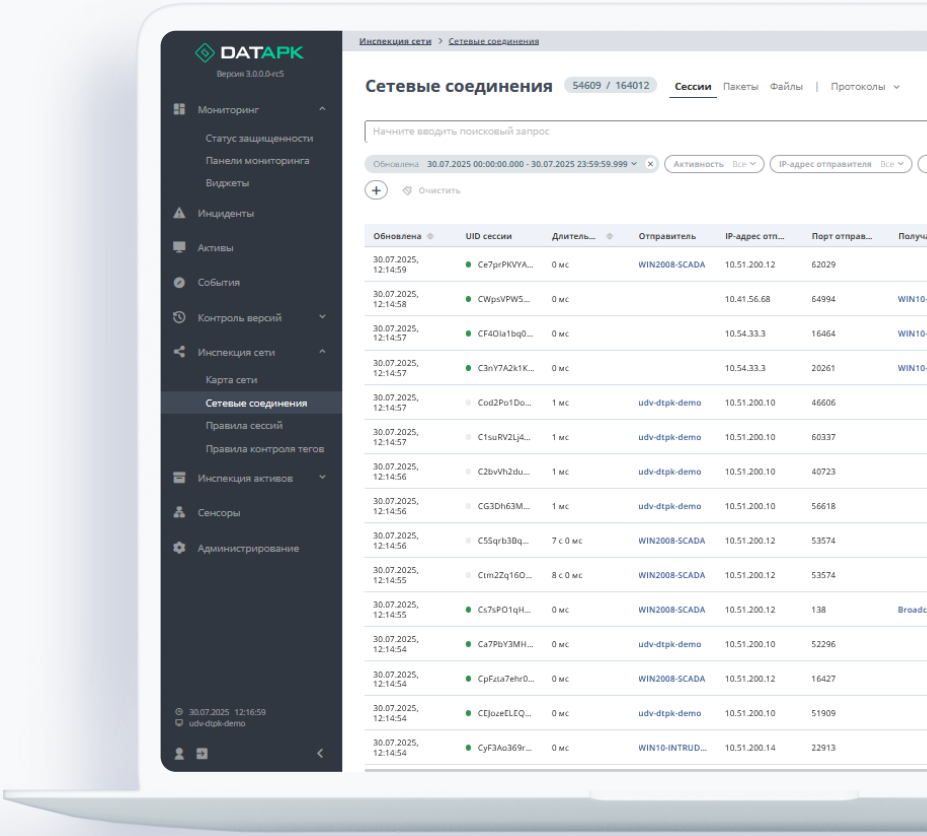
- **3 уровня иерархии (компонента)**: Supervision, Management, Sensor. Минимальная инсталляция – Management и хотя бы 1 Sensor
- **7 модулей (Core и еще 6 функциональных)**. Минимальная инсталляция – Core и хотя бы 1 модуль (с некоторыми нюансами)
- Supervision – всегда отдельная машина
- Management и 1 Sensor м.б. установлены на одной машине
- ОС: только **Альт СП Сервер 10.2** для всех 3 уровней (приобретается отдельно)

Анализ сетевого трафика

Модуль Industrial NTA (iNTA)

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



Сценарии использования

Модуль Industrial NTA (iNTA)

01 Непрерывная инвентаризация устройств и выявление скрытых активов

02 Обнаружение вторжений и скрытых действий злоумышленников

03 Анализ инцидентов ИБ и проведение расследований

04 Контроль параметров технологических процессов

05 Отслеживание управляющих команд

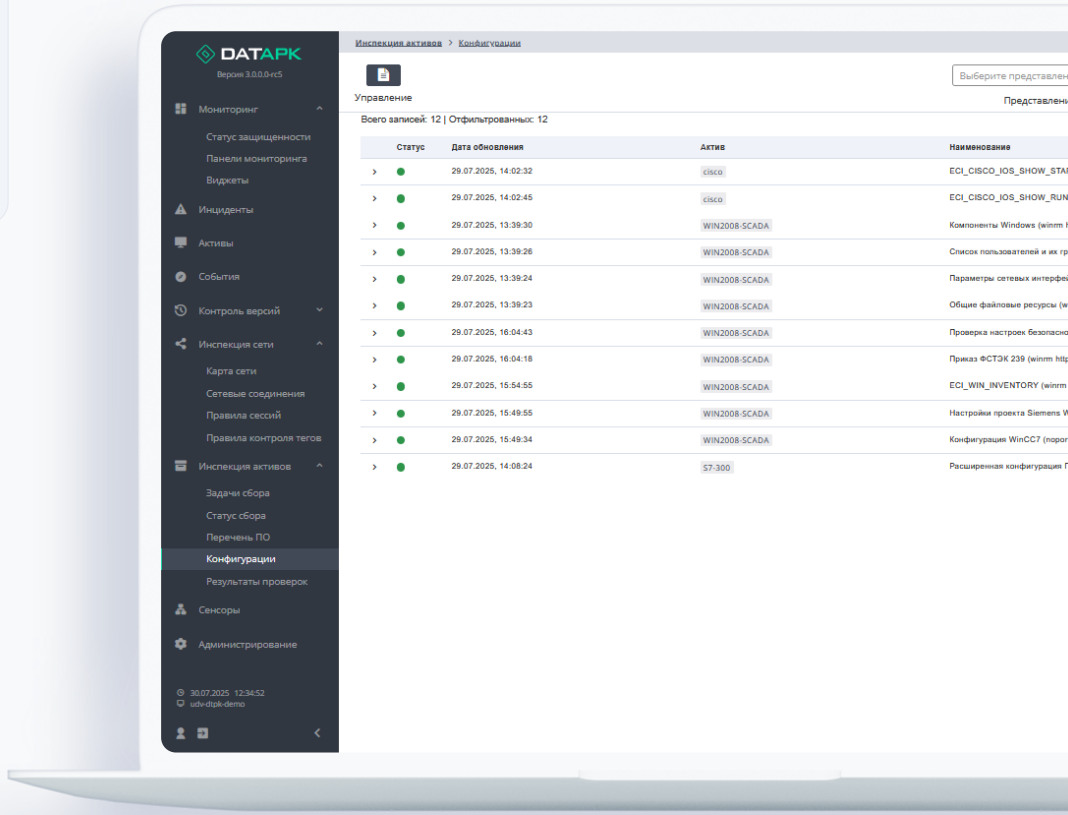
06 Анализ файлов, переданных по сети

Управление конфигурациями устройств

Модуль Configuration Management (CM)

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



Сценарии использования

Модуль Configuration Management (CM)

01 Анализ конфигурационных параметров инженерного оборудования, АРМ, серверов, СрЗИ и ПО

02 Аудит изменений конфигурационных параметров

03 Анализ инцидентов ИБ и проведение расследований

04 Проверка соответствия требованиям ИБ

05 Контроль установленного на активах ПО

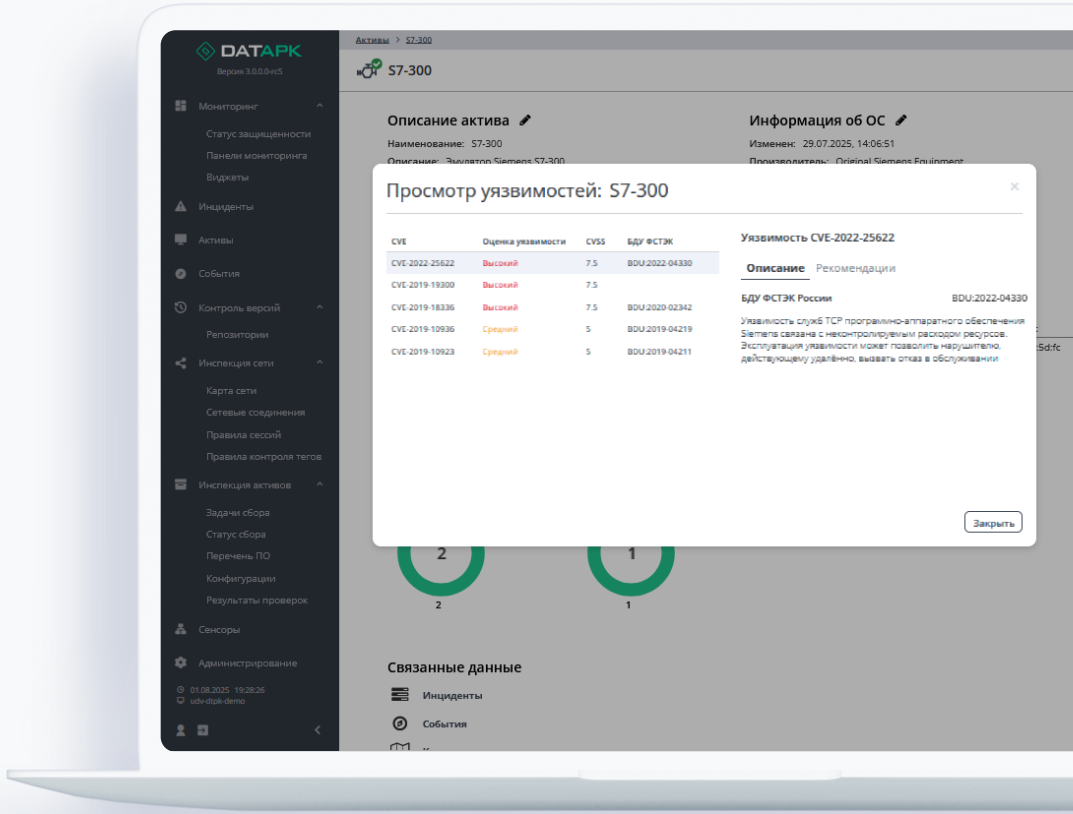
06 Автоматизация реагирования на изменения конфигурационных параметров

Управление уязвимостями

Модуль Vulnerability Management (VM)

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



Сценарии использования

Модуль Vulnerability Management (VM)

01 Неинвазивный аудит ИБ АСУ ТП

02 Выявление уязвимостей в соответствии с БДУ ФСТЭК

03 Выявление уязвимостей в специфичных, редких активах

04 Проверка соответствия требованиям ИБ

05 Подтверждение устранения уязвимостей после установки обновлений

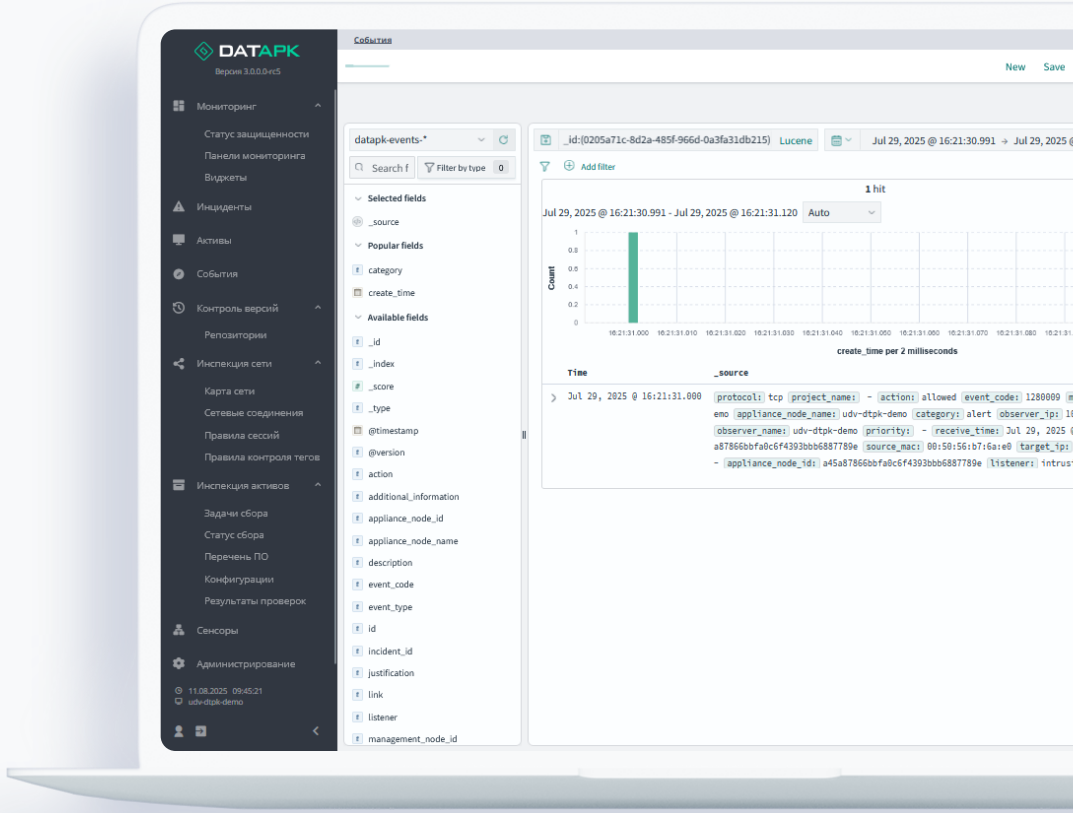
06 Минимизация рисков для цепочек поставок

Обработка и анализ событий

Модуль External Events Management (EEM)

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



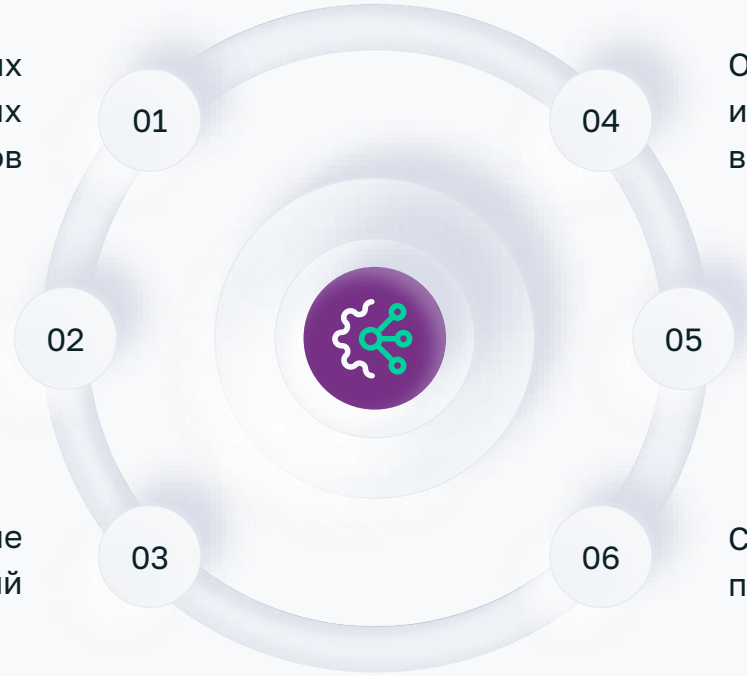
Сценарии использования

Модуль External Events Management (EEM)

01 Нормализация неструктурированных журналов и событий ИБ из различных источников

02 Корреляция событий ИБ и формирование инцидентов

03 Анализ инцидентов и проведение расследований



04 Отправка нормализованных и скоррелированных событий ИБ в сторонние системы, включая SIEM

05 Детальный поиск и визуализация событий ИБ

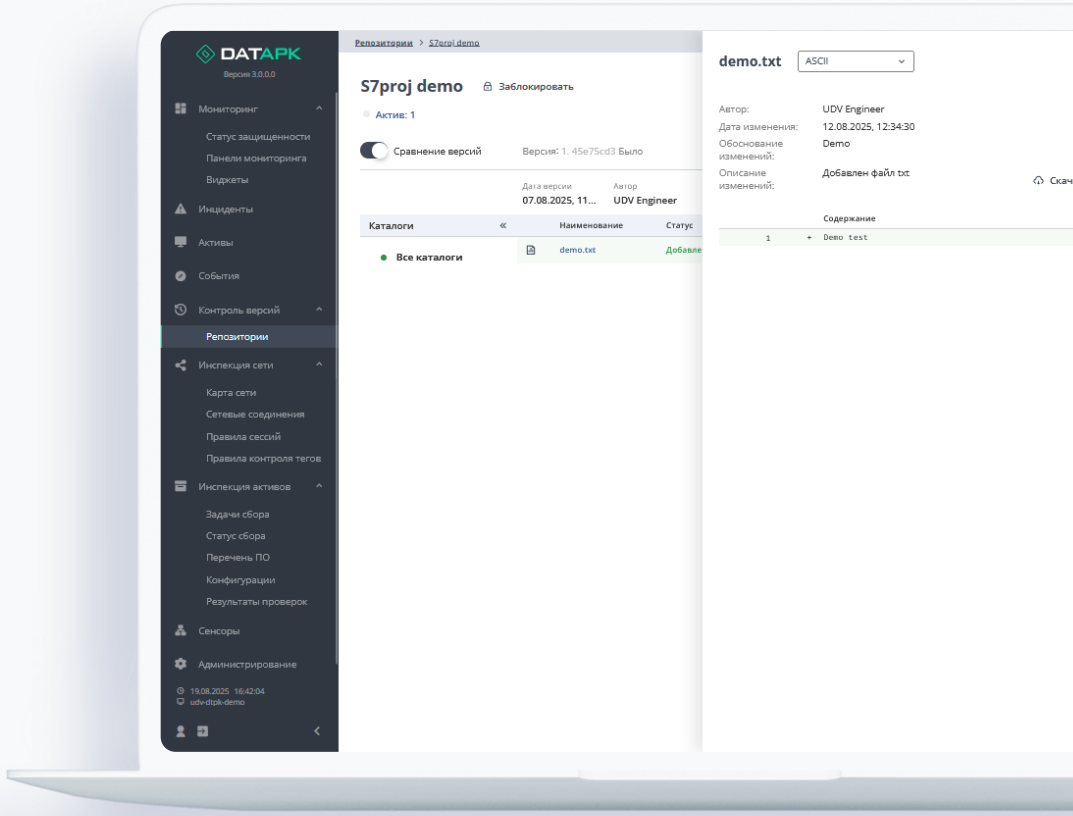
06 Создание собственных правил корреляции

Контроль версий проектов ПЛК

Модуль Version Control (VC)

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



Сценарии использования

Модуль Version Control (VC)

01 Централизованное и защищенное хранение исходного кода проектов ПЛК

02 Аудит изменений исходного кода проектов ПЛК

03 Анализ изменений в исходном коде проектов ПЛК

04 Восстановление исходного кода проектов ПЛК после катастроф

05 Безопасная разработка ПО для ПЛК

06 Контроль неизменности программ на ПЛК

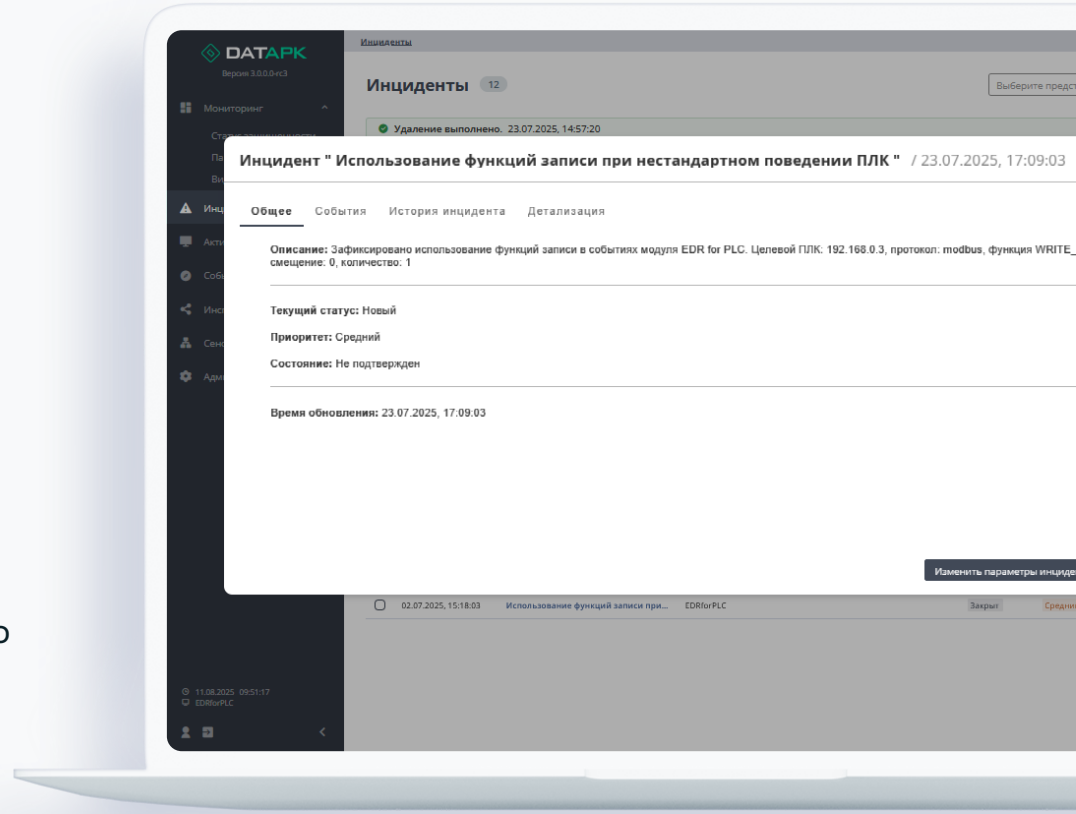
Выявление аномалий в поведении ПЛК

Модуль ML for PLC (EDR 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 дообучения 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



Сценарии использования

Модуль ML for PLC (EDR for PLC)

01 Выявление аномалий в сетевом трафике ПЛК

02 Выявление 0-day атак, не детектируемых классическими методами

03 Выявление нелегитимных изменений технологических процессов, не замечаемых SCADA

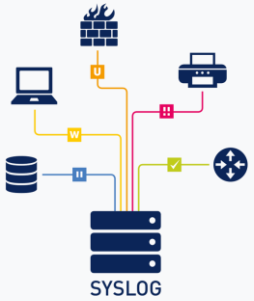
04 Анализ инцидентов ИБ и проведение расследований

05 Для экспертов по ИБ, не погруженных в специфику ПЛК

06 Цель — результативная ИБ АСУ ТП

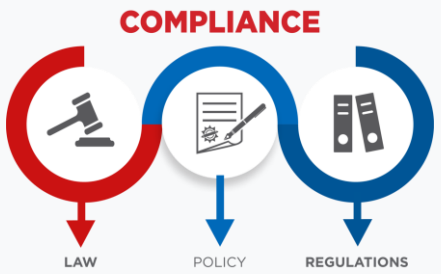
Режимы функционирования

Пассивный мониторинг



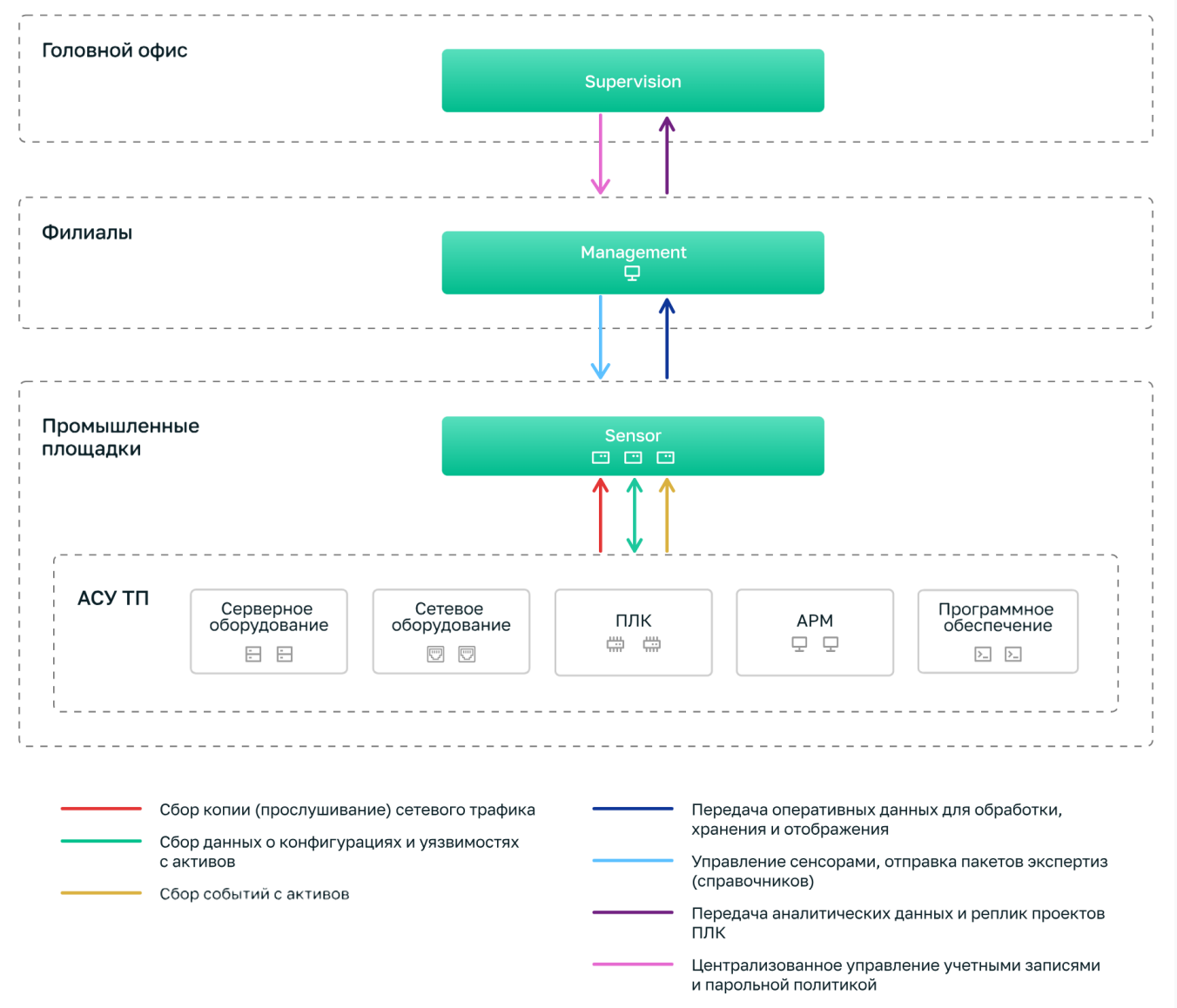
- Однонаправленное получение данных
- Прослушивание трафика (модуль iNTA, иногда дополнительно ML for PLC) и прием событий Syslog, SNMP Trap (EEM)

Режим опроса



- Получение конфигураций (CM) и событий (EEM)
- Взаимодействие в режиме «Запрос - Ответ» с использованием штатных механизмов активов (объектов защиты)
- Выявление уязвимостей и проверки на соответствие требованиям ИБ (VM в связке с CM)

Схема информационных потоков



Сетевые интерфейсы

Интерфейс управления
(активный интерфейс – везде)

Интерфейс для анализа сетевого трафика
(пассивный интерфейс – на уровне Sensor)

Интерфейс управления сервером
(iBMC, ILo)

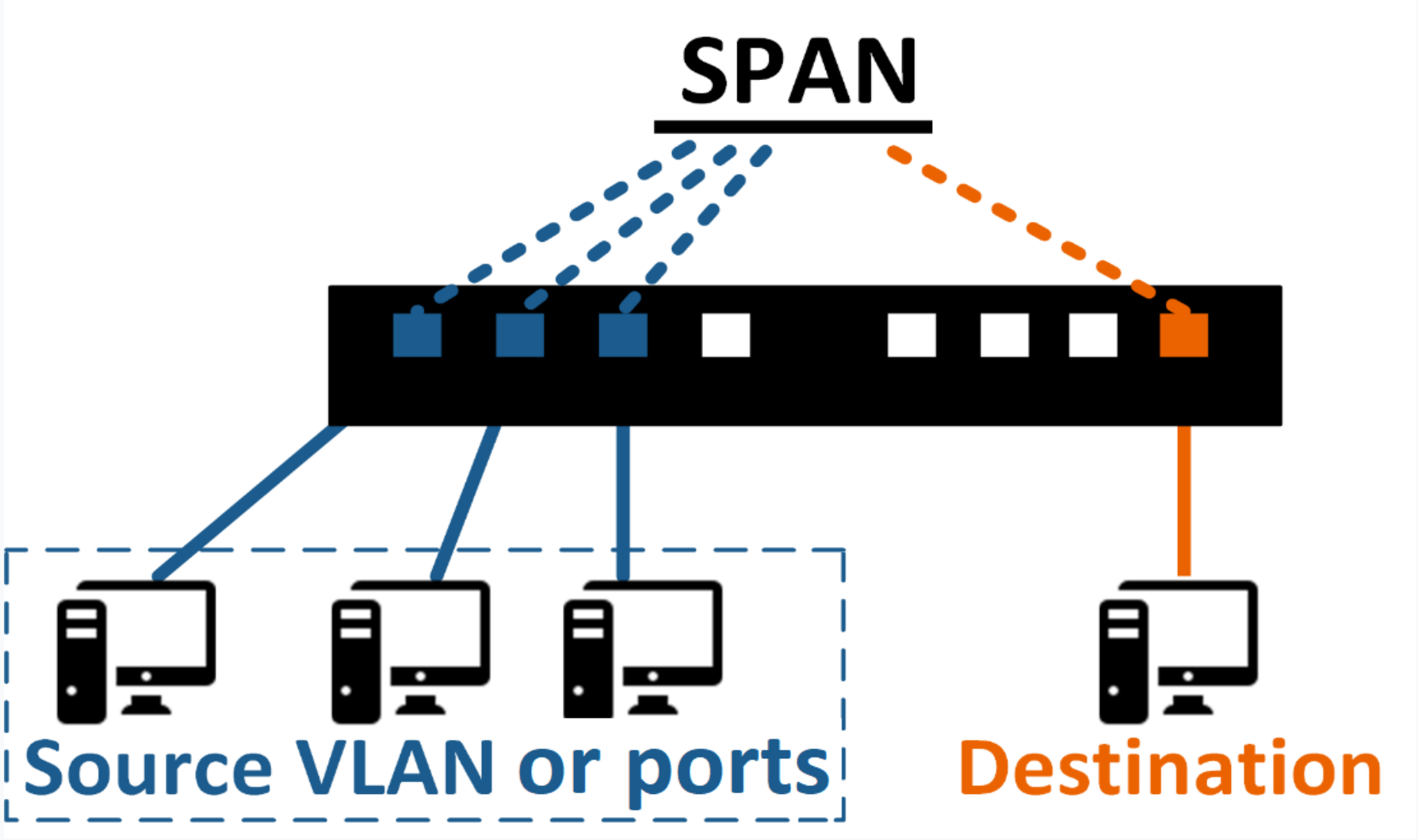
Размещение UDV DATAPK

- **уровень Sensor** – в ДМЗ или сети АСУ ТП, важно, чтобы сенсор получал копию трафика (модуль iNTA) и мог собирать конфигурации (CM), события (EEM). Для зеркалирования трафика нужен 1 или несколько слушающих интерфейсов. Если несколько – их надо объединить в bond средствами ОС. С активных интерфейсов не рекомендуется слушать трафик (за редким исключением). Нельзя объединять в bond одновременно пассивный и активный интерфейсы. На Sensor рекомендуем не более 100 активов в режиме опроса, не более 1 Гбит трафика.
- **уровень Management** – обычно в ДМЗ, он принимает данные от сенсоров и администрируется через web-интерфейс. Обычно рекомендуем на Management до 12-15 сенсоров. Поддерживается до 3000 EPS (событий в секунду на Management). Рекомендуется до 500 тыс. правил сессий, до 15 тыс. правил контроля тегов.
- **уровень Supervision** – обычно ДМЗ, он принимает данные со всех менеджментов (в 3.0 нельзя подключать нему более 19 уровней Management)
- для расчета системных требований есть информация в документации, а также калькулятор в xls

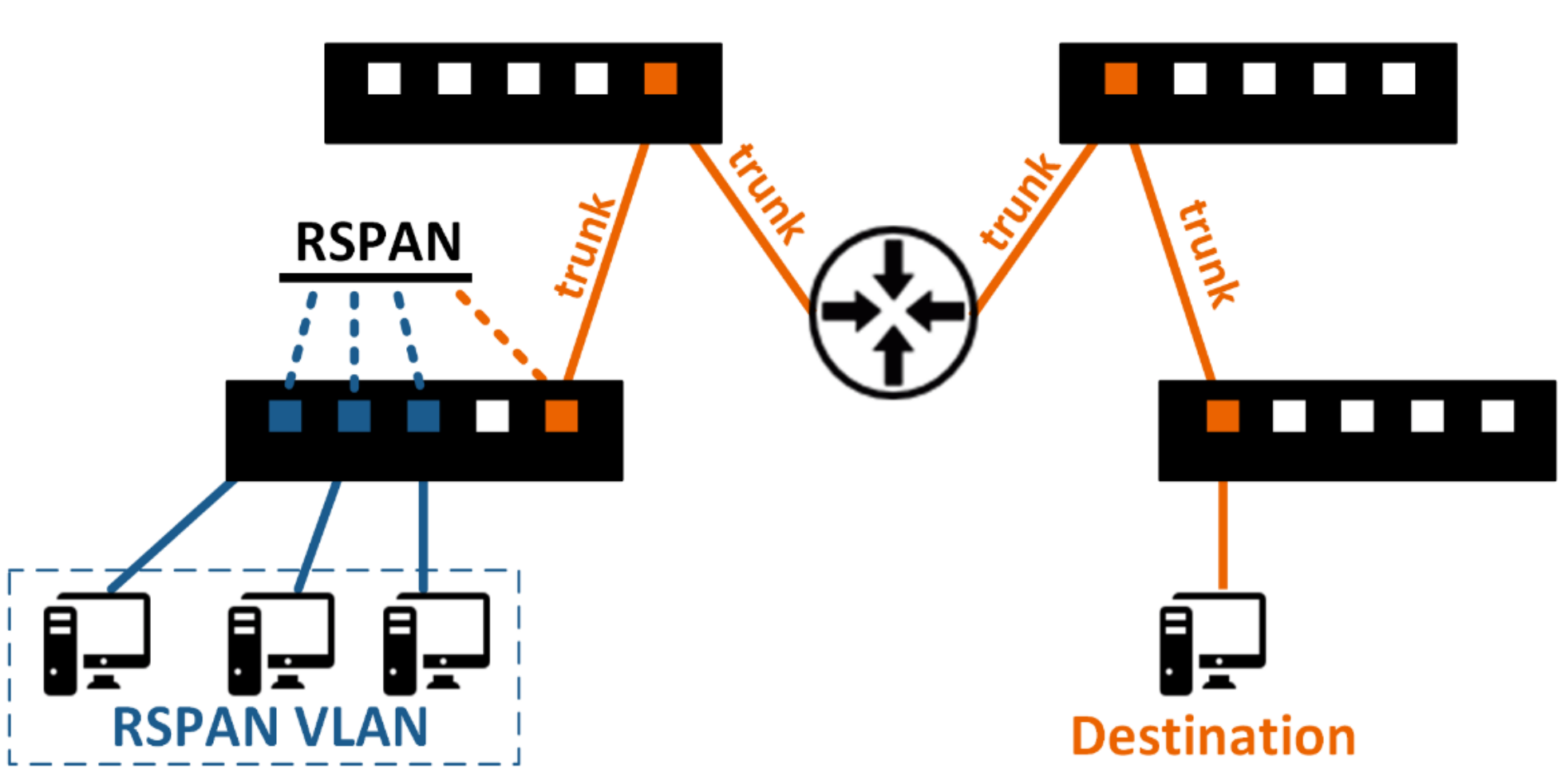
Архитектуру и сайзинг под проект необходимо согласовывать с производителем DATAPK

Варианты организации зеркалирования

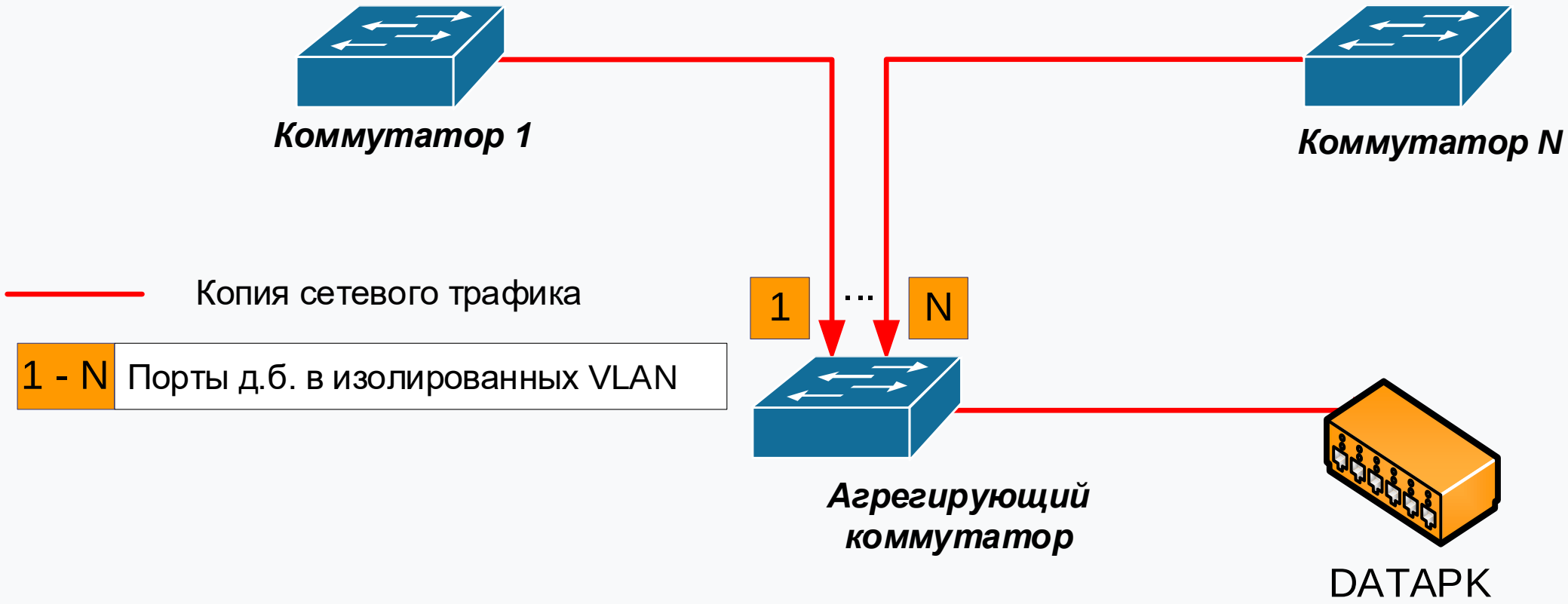
SPAN



RSPAN

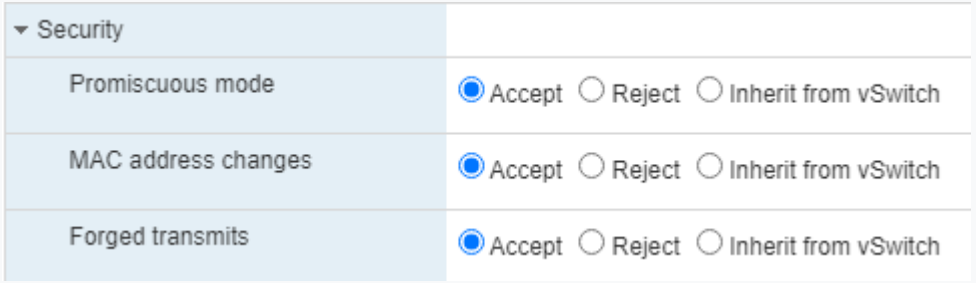


SPAN через агрегирующий коммутатор



Особенности зеркалирования в виртуальной инфраструктуре

Для зеркалирования трафика в виртуальной инфраструктуре необходимо активированы следующие настройки в порт-группах и виртуальных коммутаторах, используемых на стенде.



Базовые сетевые доступы

Источник трафика	Порт назначения	Узел назначения	Назначение трафика
АРМ административного персонала	TCP 443 (HTTPS) TCP 22 (SSH)	Требуемые DATAPK	Администрирование DATAPK (HPPPS – до Management, Supervision) ssh – для сервисного обслуживания (все уровни)
DATAPK	UDP 123 (NTP)	NTP-серверы	Синхронизация времени
DATAPK (Management, Supervision)	TCP 389 (LDAP) или TCP 636 (LDAPS)	LDAP-сервер	При использовании авторизации пользователей DATAPK через службу каталогов
DATAPK	TCP 53, UDP 53 (DNS)	DNS-серверы	Разрешение имен (при наличии серверов DNS)
DATAPK Sensor	TCP 16379, TCP 19091, TCP 15673 – Core (всегда) TCP 20085, TCP 20044, TCP 20104 – дополнительно при наличии iNTA	DATAPK Management	Взаимодействие Sensor и Management, Sensor всегда инициирует соединение (может находиться за NAT)
DATAPK Management	UDP 51820	DATAPK Supervision	Взаимодействие Management и Supervision
DATAPK Supervision	TCP 443 (HTTPS)	DATAPK Management	Подключение Management к Supervision

Сетевые доступы. Пассивный сбор событий

Источник трафика	Порт назначения	Узел назначения	Назначение трафика
ОЗ, поддерживающие передачу событий через стандарт syslog/snmp-trap	UDP 514 (syslog 3164) UDP 515 (syslog 5424) TCP 514 (syslog 3164 tcp) TCP 515 (syslog 5424 tcp) UDP 162 (snmp-trap)	DATAPK Sensor	Пассивный сбор событий от ОЗ (модуль EEM)

Сетевые доступы. Сбор данных в режиме опроса

Источник трафика	Порт назначения	Узел назначения	Назначение трафика
DATAPK Sensor	TCP 135 (MSRPC), TCP 139, TCP 445 (WINEXE), TCP 1024-5000 (MSRPC, XP), TCP 49152-65535 (MSRPC, Vista и новее), TCP 5985, TCP 5986 (WinRM), TCP 3306 (MySQL), TCP 1433 (MSSQL), TCP 5432 (PostgreSQL)	Объекты защиты (ОЗ) базе ОС Windows, СУБД	Взаимодействие с активами (режим опроса – модуль СМ, частично VM)
	TCP 22 (SSH), TCP 23 (telnet)	ОЗ на базе ОС Unix и для АСО	
	UDP 161 (SNMP) TCP 102 (S7) TCP 502 (Modbus, UMAS) TCP 44818 (EthernetIP) и др.	ПЛК, АСО	

Установка UDV DATAPK Industrial Kit

- DATAPK работает только на **ОС Альт СП Сервер 10.2**. Другие ОС (включая бесплатный Альт Сервер 10.2, загруженный по публичной ссылке) не подходят. ОС Альт СП надо приобретать отдельно. Для пилотных инсталляций необходимо запросить Альт СП у производителя. В UDV Group есть форма письма
- Установка возможна как на физическую, так и виртуальную машину с подходящими системными требованиями (учесть возможные нюансы с зеркалированием)
  * При выборе серверного оборудования необходимо убедиться, что ОС Альт СП Сервер устанавливается на данный сервер.
  * Для установки на ВМ, подходит любая среда виртуализация, которая поддерживает установку Альт СП Сервер. Тестировались среды виртуализации VMware, Proxmox, а так же другие на базе oVirt (zVirt, HOSTVM и пр.).
- Supervision – только отдельная машина. Management и 1 Sensor при необходимости могут быть установлены на 1 машину
- При установке рекомендуется заранее запланировать разметку дисков (в соответствии с документацией и планируемой нагрузкой) – в дальнейшем внести изменения в дисковые разделы будет затруднительно.
  * Обязательно выделять разделы для хранения сетевого трафика и извлеченных файлов на уровне Sensor – иначе ротация будет работать некорректно. Остальные разделы выделять не обязательно
- Установка сторонних инструментов и выполнение нетиповых настроек ОС (антивирус, расширенные настройки аудита ОС и пр.) не учитываются производителем DATAPK при подготовке сайзингов, поэтому необходимо все нетиповые настройки необходимо макетировать и согласовывать с UDV Group
- Работы по установке DATAPK могут косвенно повлиять на работу техпроцесса при отсутствии должной подготовки (поскольку подключается новое оборудование в сеть, вносятся изменения в топологию сети для зеркалирования трафика и пр.), поэтому необходимо с должным уровнем ответственности подходить к любым работам по внедрению и пилотированию

Начальная настройка UDV DATAPK Industrial Kit

- Убедиться, что интерфейс открывается, время синхронизировано, нужные модули установлены, компоненты Sensor полностью доступны
- Настроить ротацию данных и другие настройки в конфигурационных файлах
- Настроить доступы к UDV DATAPK в соответствии с требованиями организации (убрать простые пароли и пр.), создать учетные записи для представителей заказчика
- Для анализа трафика задать контролируемую сеть (иначе анализ будет неполный)
- Включить режим обучения (автоматическое создание правил сетевых сессий). После обучения провести аудит правил и перевести в боевой режим
- Инвентаризовать сетевые узлы, распределить по группам
- Выполнить тюнинг правил обнаружения вторжений, сетевых соединений, правил корреляции
- Настроить сбор конфигураций, событий, задать адекватные расписания опроса по согласованию с заказчиком
- Настроить и протестировать интеграцию со смежными системами (Syslog, SMTP), если это необходимо

Уникальность экземпляра DATAPK определяется по machine-id. Поэтому клонировать виртуальные машины с DATAPK можно только при условии обязательной смены machine-id после клонирования

Вопросы?

udv|group