kaspersky

Kaspersky Industrial Cybersecurity Conference 2021

Василий Шауро

Руководитель направления стратегического маркетинга, Emerson, Россия

#KasperskyICS

Чат конференции: https://kas.pr/kicscon

DELTAV™

Развитие кибербезопасности АСУТП в условиях цифровизации предприятий

Промышленная революция и влияние цифровизации

Эволюция промышленности

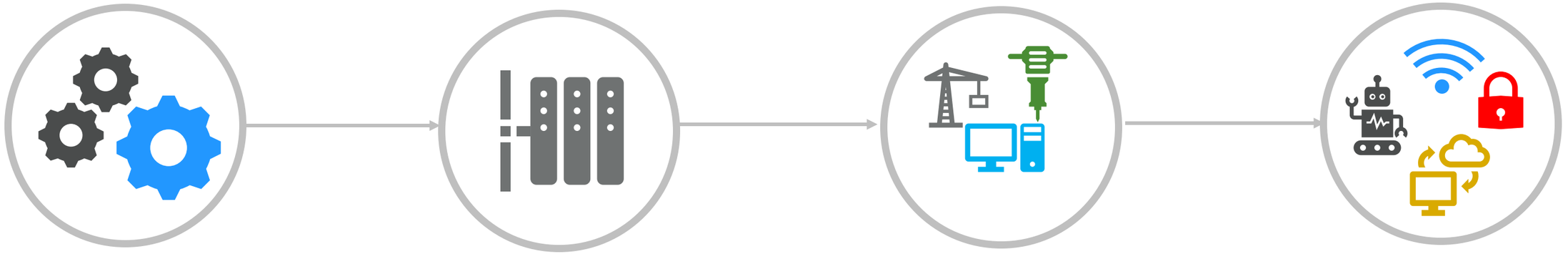
Механизация и внедрение парового двигателя

Массовые сборочные линии с использованием электроэнергии

Автоматизированное производство, компьютеры, IT-системы и робототехника

Умная фабрика. Автономные системы, IIOT, машинное обучение, кибербезопасность.

Industry 1.0 | **Industry 2.0** | **Industry 3.0** | **Industry 4.0**



Текущие тенденции рынка АСУТП

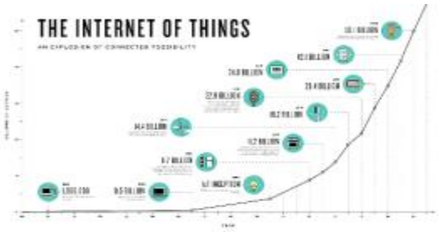
Производительность операций

Слияние ОТ и ИТ

Повышение вычислительных мощностей

Center for Operator Performance
An Industry/University Center for Excellence

IIoT & Big Data



Единая сеть устройств, работа с большими массивами данных, массовое внедрение внешних аналитических приложений

Кибербезопасность

«За последние 3 года вторжения в критически важную инфраструктуру увеличились в 17 раз».
Источник Министерство обороны США

Новые методы строительства заводов

Комплектно-блочные установки

Модульные заводы

Удаленное и сложное расположение заводов

Уменьшение количества персонала
Внедрение удаленного доступа
Внедрение удаленного управления

Облачные технологии

Виртуализация
Распределенные вычисления
Виртуальный стек ПЛК

Эволюция АСУТП – прошлое и настоящее

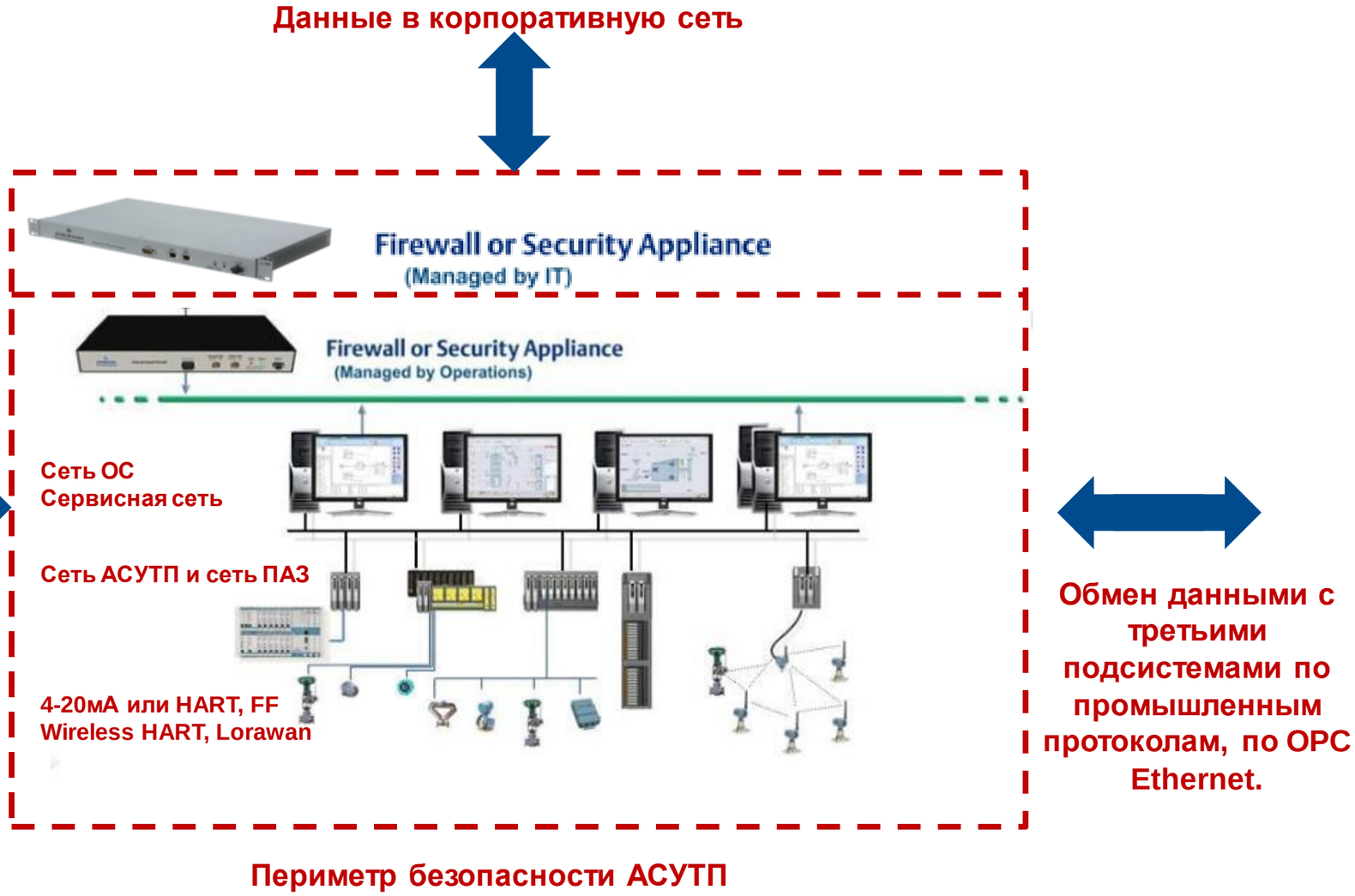
АСУТП в прошлом ОТ объект:

- **Обособленный объект с минимумом внешних связей.**
- **Полевой КИП не является частью сетевой инфраструктуры.**
- **Обмен с другими АСУТП происходит по промышленным протоколам.**
- **Обмен с сетью предприятия чаще всего однонаправленный.**
- **Специализированные ОС ПЛК АСУТП и ПАЗ.**

Эволюция АСУТП – настоящее и будущее

АСУТП сейчас на границе ИТ и ОТ:

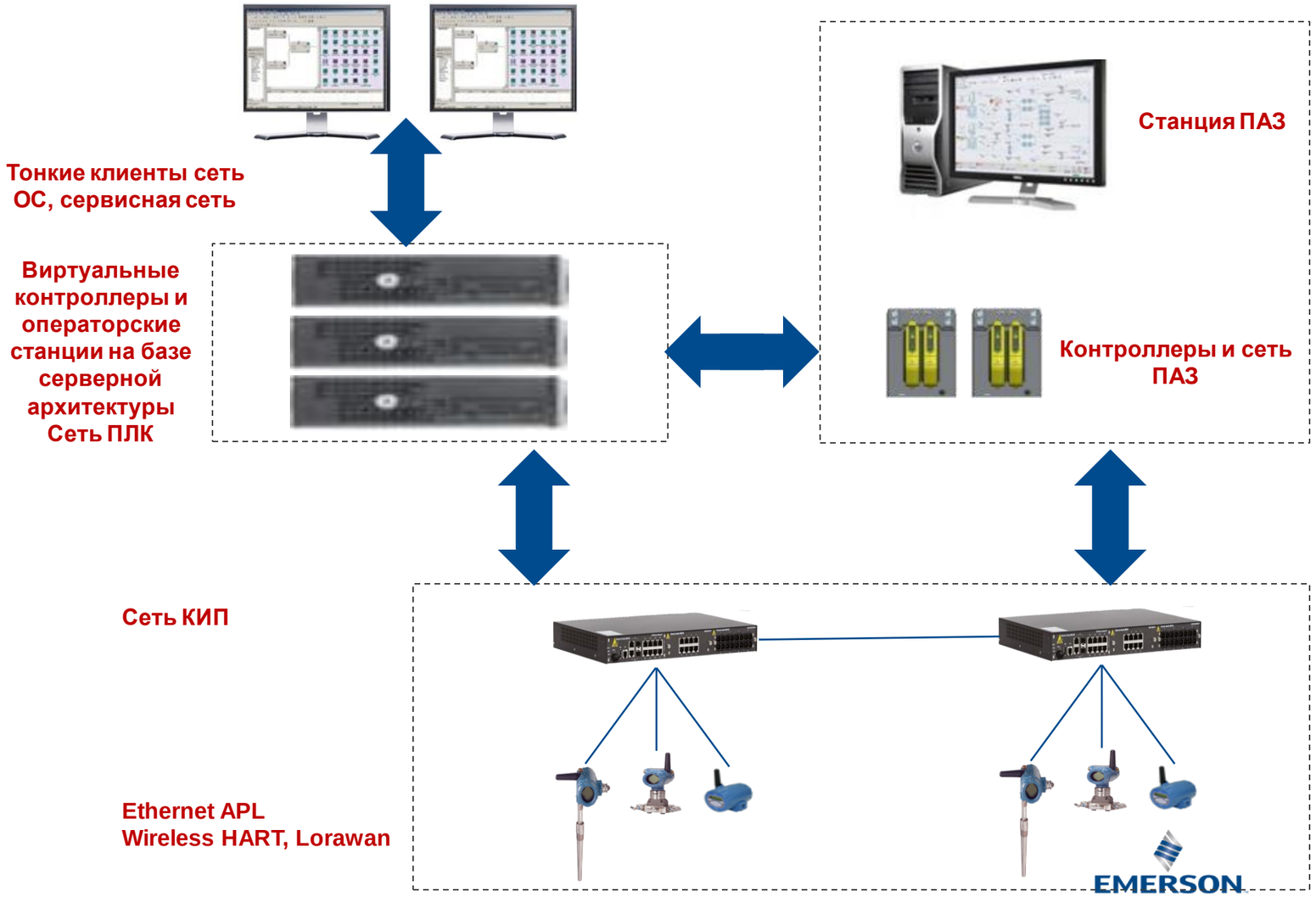
- Обособленный объект с большим количеством внешних связей.
- Полевой КИП частично является частью сетевой инфраструктуры.
- Обмен с другими АСУТП происходит как по промышленным протоколам так и по общераспространенным.
- Обмен с сетью предприятия двунаправленный.
- Специализированные ОС ПЛК АСУТП и ПАЗ.
- Сеть ПАЗ отделена от сети АСУТП.
- Возможен удаленный доступ.
- Присутствует сервисная сеть.



Эволюция АСУТП – потенциальное будущее 10-15 лет

АСУТП в будущем фактически ИТ объект:

- **Интегрированный объект с большим количеством внешних связей.**
- **КИП является частью сетевой инфраструктуры.**
- **Обмен с другими АСУТП происходит общераспространенным протоколам, IIOT.**
- **Обмен с сетью предприятия двунаправленный или интеграция в сеть.**
- **Стандартные ОС ПЛК АСУТП и специализированные для ПАЗ.**
-
- **ПАЗ отделен от АСУТП.**
- **Возможен удаленный доступ.**
- **Возможно удаленное управление серверы с виртуальными ПЛК могут находится не на объекте.**



ИТ и управление процессами: проблемы / различия

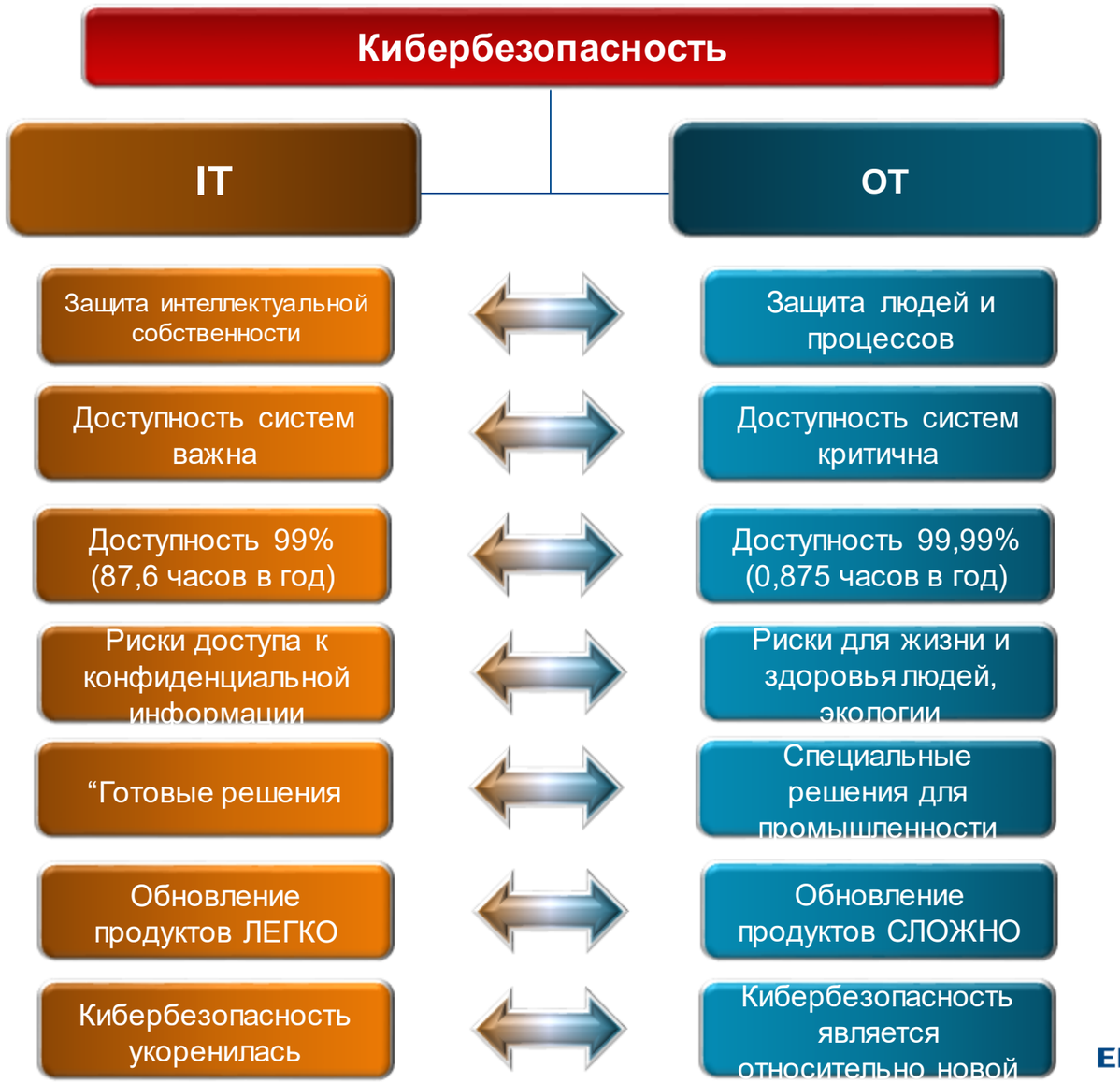
Ключевые различия в перспективах ИТ и ОТ:

Требования и ограничения в ОТ системах приводят к конкурирующим и часто конфликтующим решениям в области безопасности.

Различия в системах приводят к различным стратегии защиты, что увеличивает нагрузку на существующие службы предприятия.

Требования к системам различных производителей отличаются, что вызывает различия в том как механизмы безопасности реализуются и используются.

ИТ и ОТ:
нужны друг другу



Контрольный список кибербезопасности

- Сегментация сетей между ОТ и ИТ, и внутри сети АСУТП.
- Подключения к АСУ ТП должны осуществляться через сервисную сеть сеть L2.5.
- Контроллеры домена не должны быть подключены к сети служб.
- Разработана и применяется ОРД.
- Внедрена политика управления исправлениями и изменениями.
- Используется белый список приложений.
- Ограничена возможность (разрешения) пользователей устанавливать и запускать нежелательные программные приложения и применен принцип «Наименьших привилегий» ко всем системам и службам.
- Все рабочие станции АСУ ТП не имеют возможности несанкционированного подключения внешних устройств, а также заперты внутри шкафов.
- Используется план резервного копирования и восстановления данных для всей важной информации.
- Внедрена двухфакторная аутентификация.

Наиболее распространенные слабые места системы на разных этапах жизненного цикла системы

Ранг	По результаты оценки площадки	По отчетам об инцидентах	По анализам отчетов аудита
1	Управление учетными данными	Дизайн сети	Отсутствие или огрехи в документации
2	Настройки брандмауэра	Настройки брандмауэра	Слабый мониторинг событий
3	Дизайн сети	Слабый мониторинг событий	Разрешения, привилегии и контроль доступа

Мониторинг событий:

- Логи отсутствуют или не анализируются.
- Слабый контроль входящего и исходящего траффика.
- Нет анализа сетевого траффика.

Слабые правила брандмауэра:

- Доступ к определенным портам, настроен неправильно, открыты дополнительные порты.
- Правила брандмауэра, не адаптированы к трафику DCS.

Слабые стороны сетевого дизайна:

- Периметр безопасности не определен.
- Отсутствие сегментации сети.
- Отсутствие DMZ.
- Брандмауэры отсутствуют.
- Брандмауэр обходится.

Сложности при внедрении кибербезопасности АСУТП

- **Кто должен следить за кибербезопасностью АСУТП? Часто эта функция находится в серой зоне, между ИТ и ОТ. Чтобы кибербезопасность была эффективной, она должна быть разработана с помощью «видения» высшего уровня и скоординировано развернута на всем заводе или в организации.**
- **Бюджеты ИТ на кибербезопасность не всегда включают в себя АСУТП.**
- **Отдельные политики и процедуры для АСУТП не разрабатываются, а общие ИТ политики не применяются.**
- **Нет анализа первопричин инцидентов.**
- **Отсутствие надлежащей политики и процедур в отношении "портативных носителей".**
- **Анализ сетевого траффика не проводится.**
- **Проектирование сетей систем управления без учета требований информационной безопасности.**
- **«Плохое управление обновлениями» для приложений в сети АСУТП. Многие компании имеют развитый сервис обновления для своих бизнес-систем, но они не включают в себя АСУТП.**

Одно из решений расширить функционал АСУТП

Обеспечение информационной безопасности в АСУТП с помощью встроенных инструментов

Модуль аудита состояния элементов системы кибербезопасности

Модуль управления обновлениями в том числе антивирусной защиты

Аппаратные блокировки критических узлов, портов, служб.

Мониторинг целостности системы

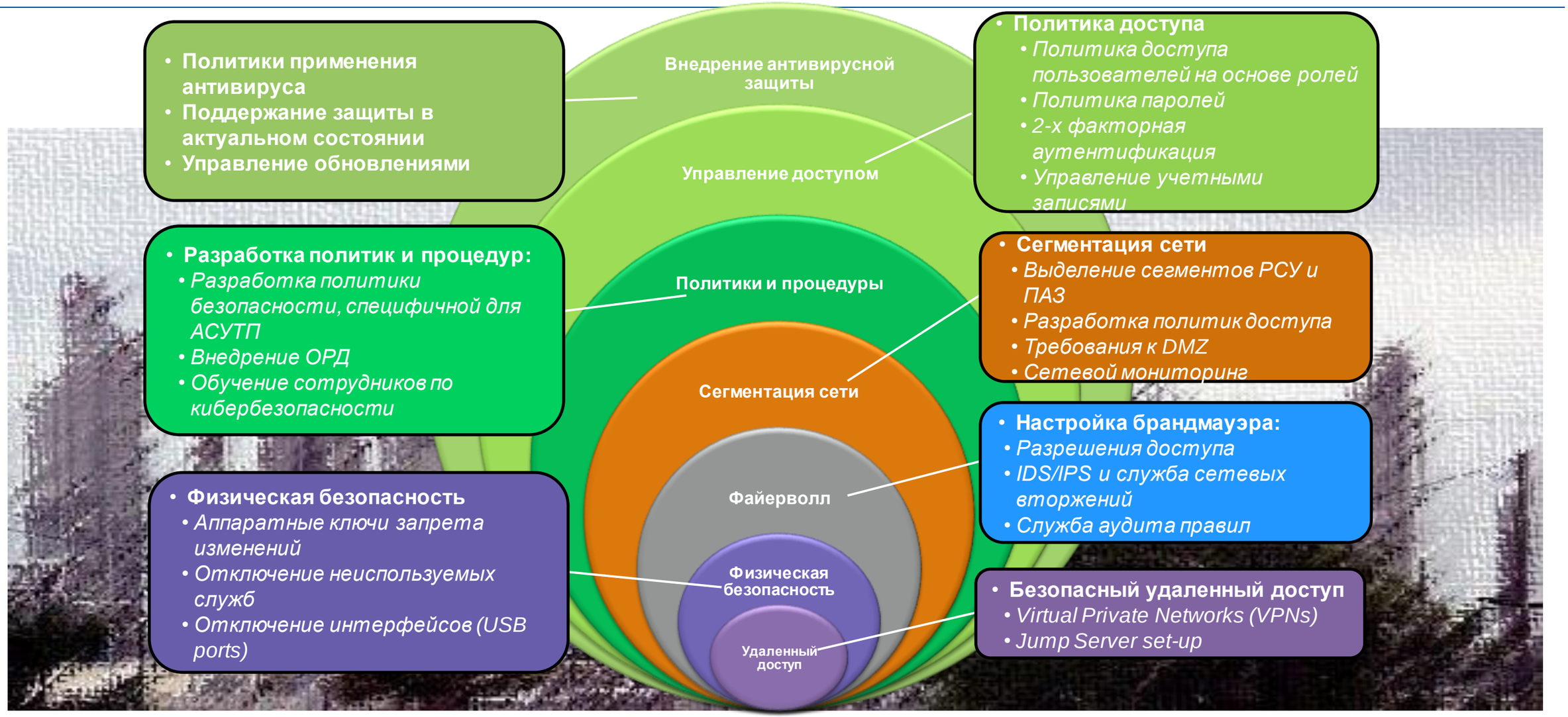
Резервное копирование

Модуль контроля доступа и 2-х факторная аутентификация

Защищенный удаленный доступ и защита USB портов

Используйте соответствующие наборы решений для управления этими рисками

Многоуровневая кибербезопасность



- **Политики применения антивируса**
- **Поддержание защиты в актуальном состоянии**
- **Управление обновлениями**

- **Политика доступа**
  - *Политика доступа пользователей на основе ролей*
  - *Политика паролей*
  - *2-х факторная аутентификация*
  - *Управление учетными записями*

- **Разработка политик и процедур:**
  - *Разработка политики безопасности, специфичной для АСУТП*
  - *Внедрение ОРД*
  - *Обучение сотрудников по кибербезопасности*

- **Сегментация сети**
  - *Выделение сегментов РСУ и ПАЗ*
  - *Разработка политик доступа*
  - *Требования к DMZ*
  - *Сетевой мониторинг*

- **Настройка брандмауэра:**
  - *Разрешения доступа*
  - *IDS/IPS и служба сетевых вторжений*
  - *Служба аудита правил*

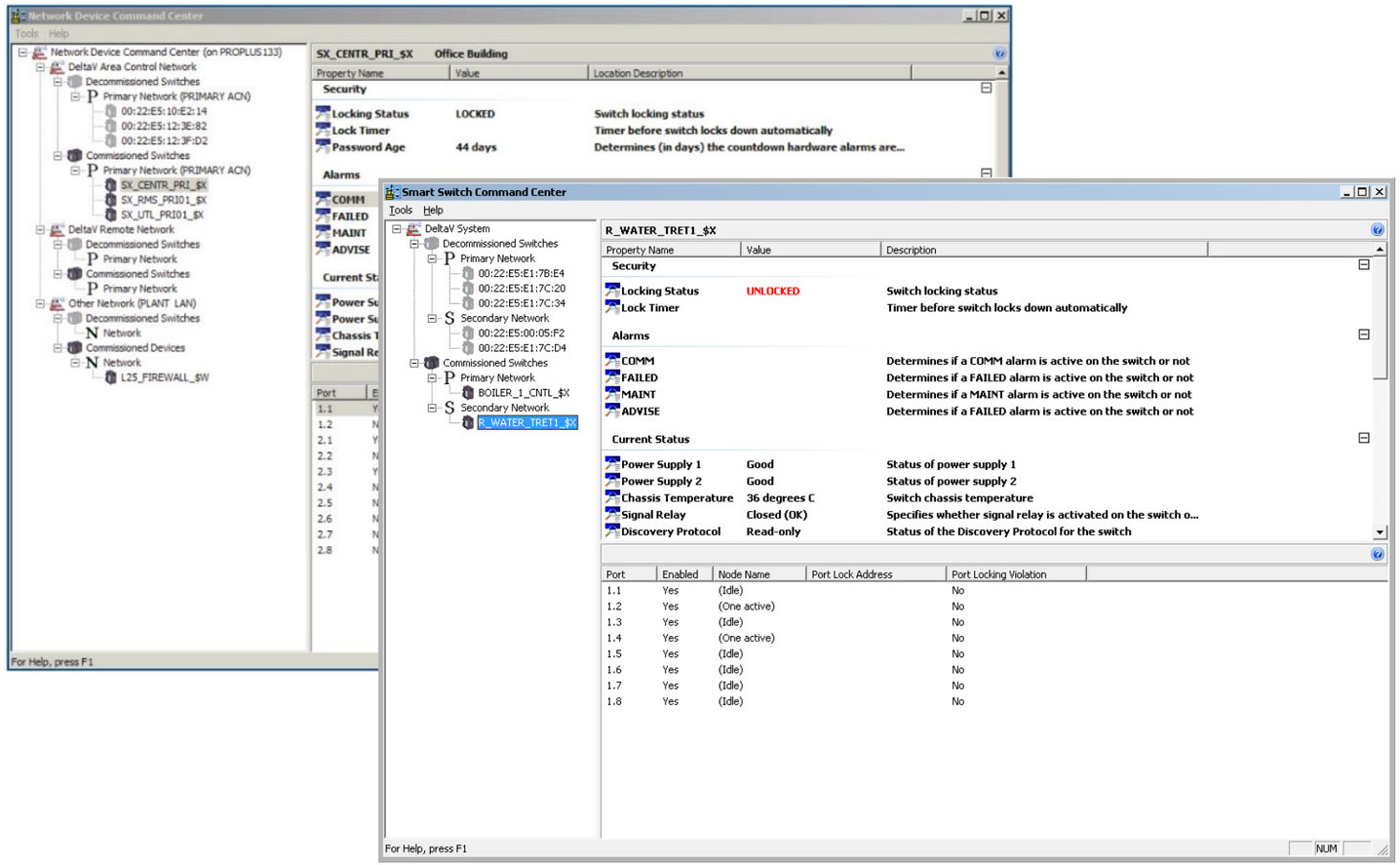
- **Физическая безопасность**
  - *Аппаратные ключи запрета изменений*
  - *Отключение неиспользуемых служб*
  - *Отключение интерфейсов (USB ports)*

- **Безопасный удаленный доступ**
  - *Virtual Private Networks (VPNs)*
  - *Jump Server set-up*

Программные средства защиты информации ПТК DeltaV. DeltaV Network Device Command Center

Возможности

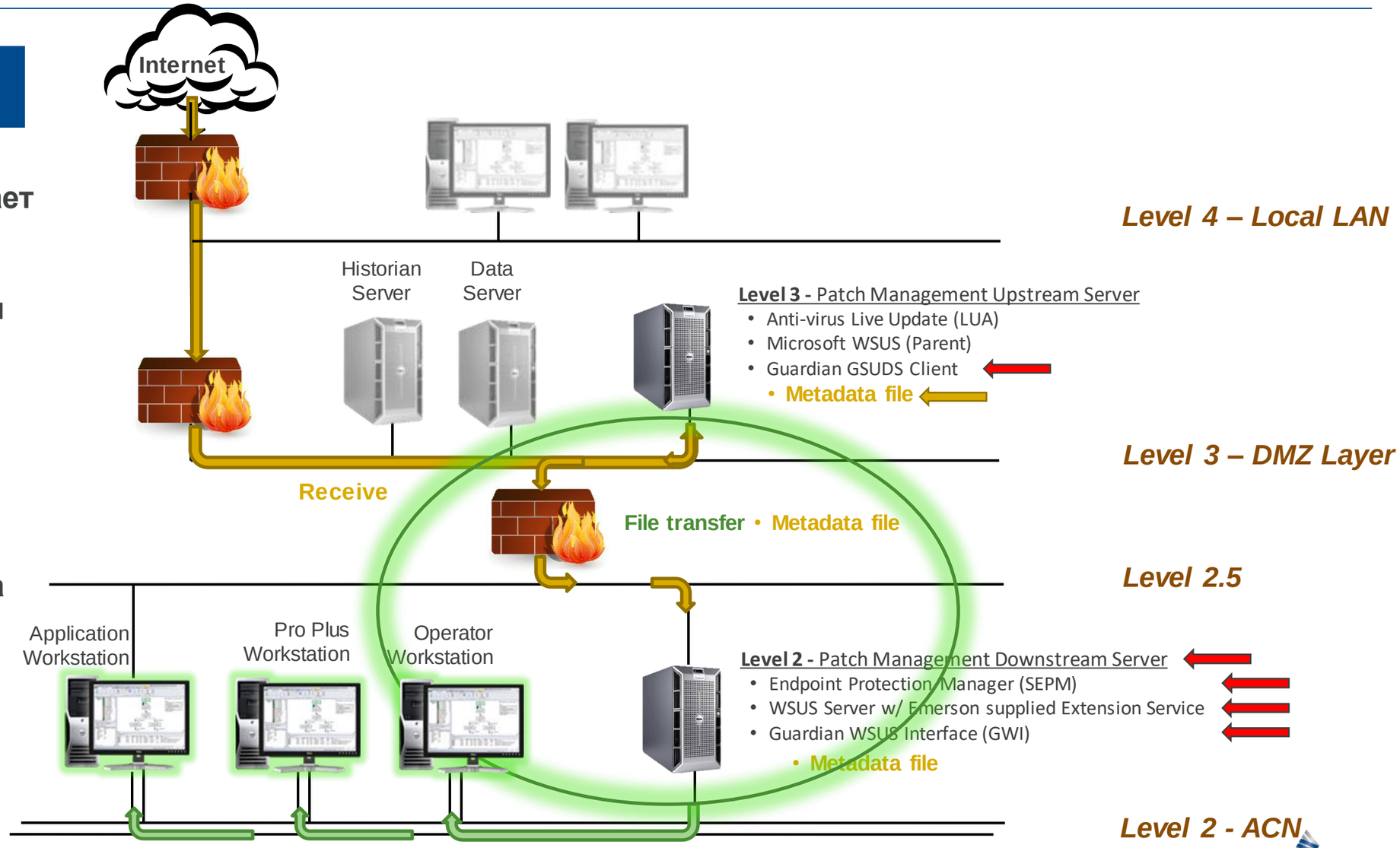
- Мониторинг состояния сетевого оборудования ПТК DeltaV (Smart Switch, Firewall-IPD, Emerson Firewall).
- Конфигурирование коммутаторов ПТК DeltaV (Smart Switch).
- Ведение статистики сетевой активности.
- Мониторинг событий безопасности.
- Ручная и автоматическая блокировка неиспользуемых портов коммутаторов.



Программные средства защиты информации ПТК DeltaV. Сервис распространения обновлений ПО в рамках программы техподдержки

Возможности

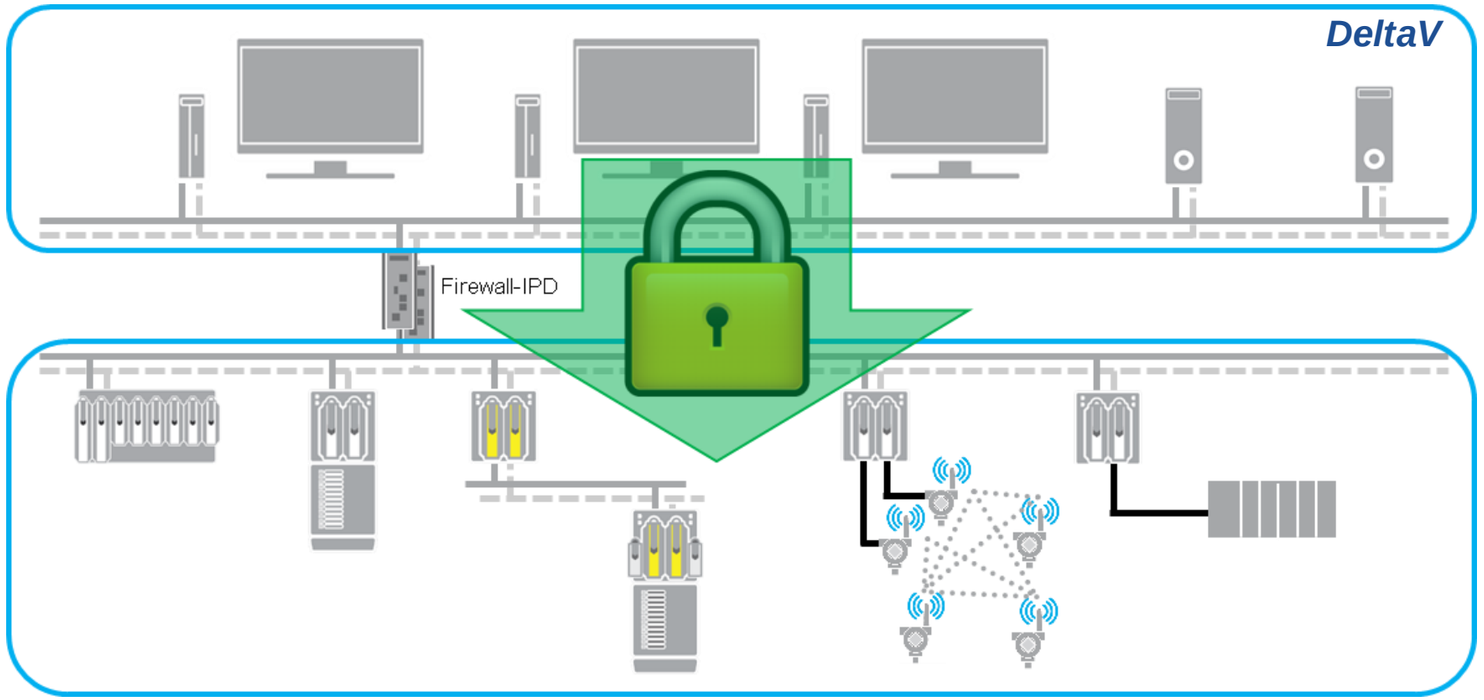
- Комплексная программа поддержки Guardian, включает в себя Guardian Software Update Delivery Service (GSUDS) – сервис получения обновлений и исправлений.
- Заказчики получают обновления для продуктов входящих в состав ПО ПТК DeltaV, предварительно прошедшие тестирование на совместимость со специальным ПО ПТК.
- Все обновления имеют специальный идентификационный ключ подтверждающий подлинность.



Технические средства защиты информации ПТК DeltaV. Команда блокировки для узлов ДельтаВ (Firewall-IPD)

Начиная с версии 13.3.1, узлы ПТК DeltaV (такие как Контроллеры, CIOC, WIOC) не принимают следующие команды, если находятся в защищённом режиме:

- **Загрузка.**
- **Вывод из работы.**
- **Обновление.**
- **Отладка.**

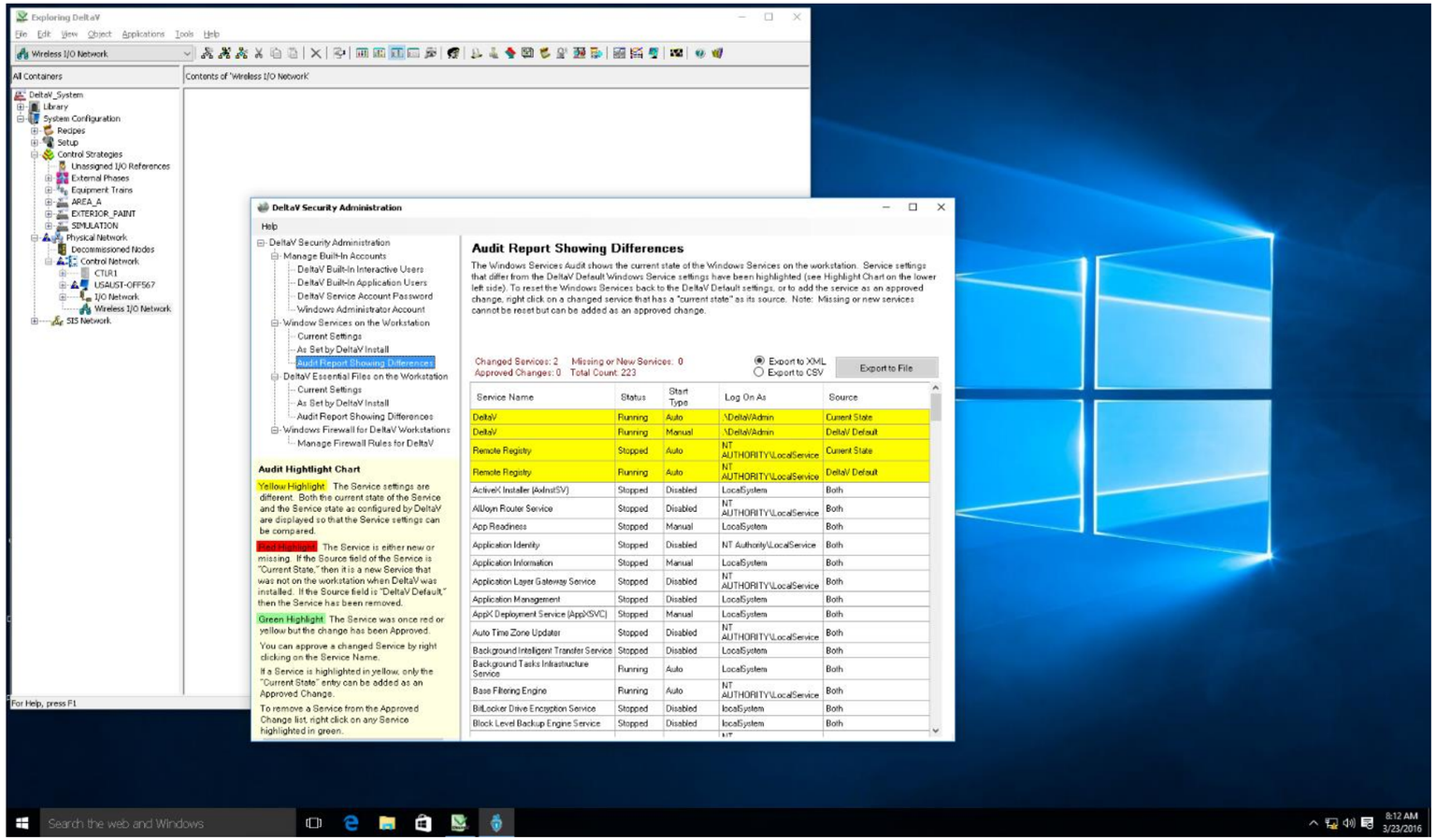


Программные средства защиты информации ПТК DeltaV. Приложение DeltaV Security Administration

В ПТК DeltaV 13.3.1 и выше доступно приложение для мониторинга состояния и настроек ПО ПТК.

Возможности

- **Контроль состояния сервисов ОС Windows.**
- **Идентификационные подписи файлов специального ПО ПТК DeltaV.**
- **Интеграция с Windows Firewall.**
- **Управление встроенными аккаунтам.**

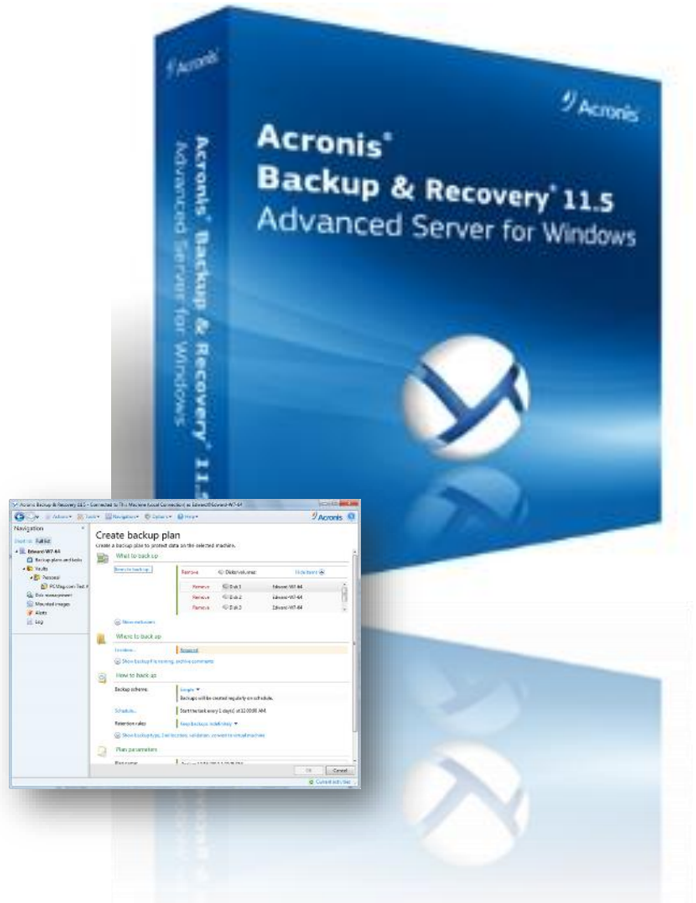


Программные средства защиты информации ПТК DeltaV. Программный продукт DeltaV Backup & Recovery

Решение компании Эмерсон для резервного копирования и восстановления информации ПТК DeltaV, основано на продукте компании Acronis (Acronis Backup & Recovery).

Резервное копирование

- **Позволяет производить резервное копирование на регулярной основе.**
- **Готовое решение для ПТК DeltaV.**
- **Обеспечивает централизованный, удалённый контроль за процессом резервного копирования и восстановления.**



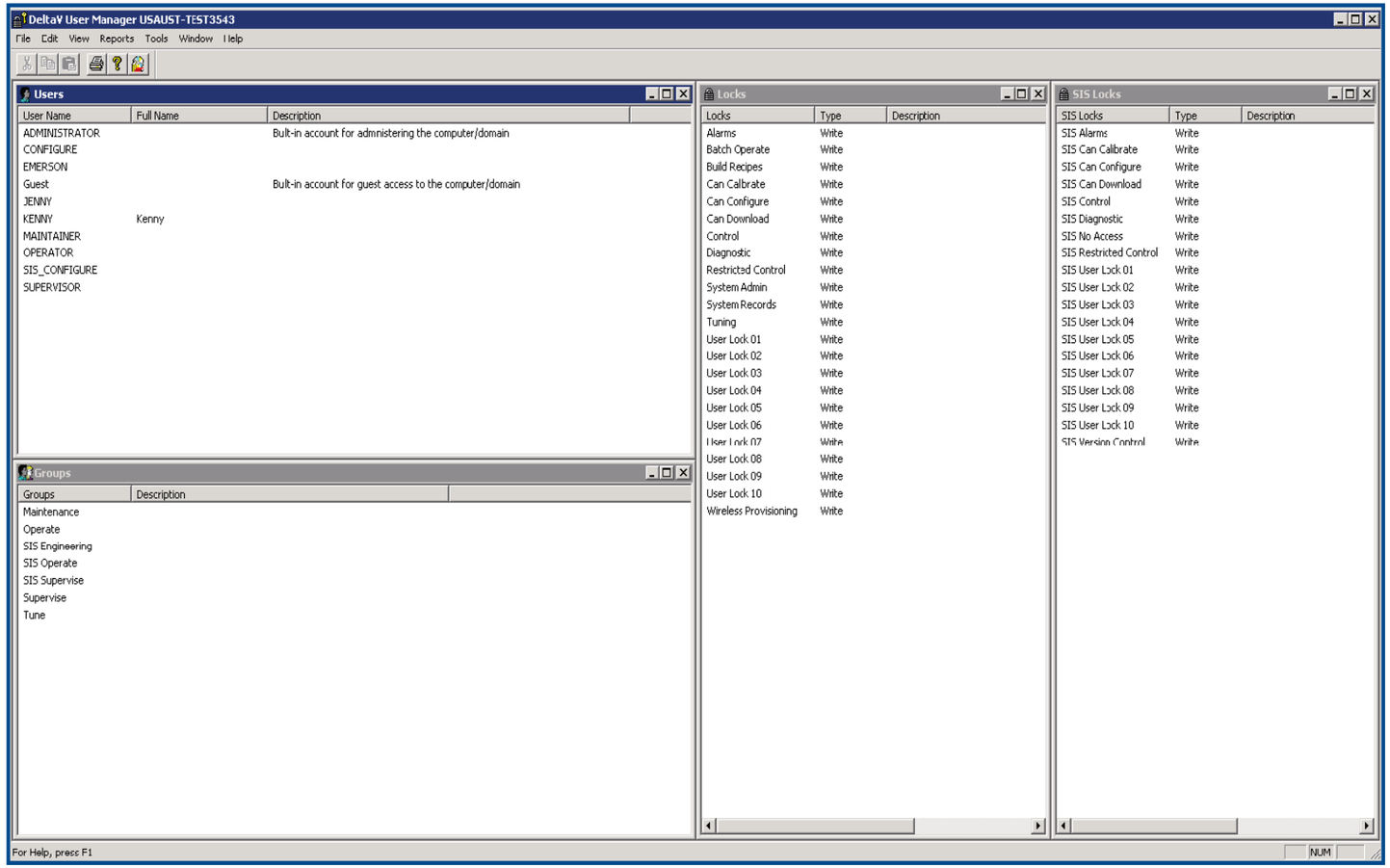
Восстановление из резервных копий

- **Решение для всех типов станций ПТК DeltaV.**
- **Поддержка режима Universal restore (восстановление на другом «железе» с заменой драйверов оборудования).**

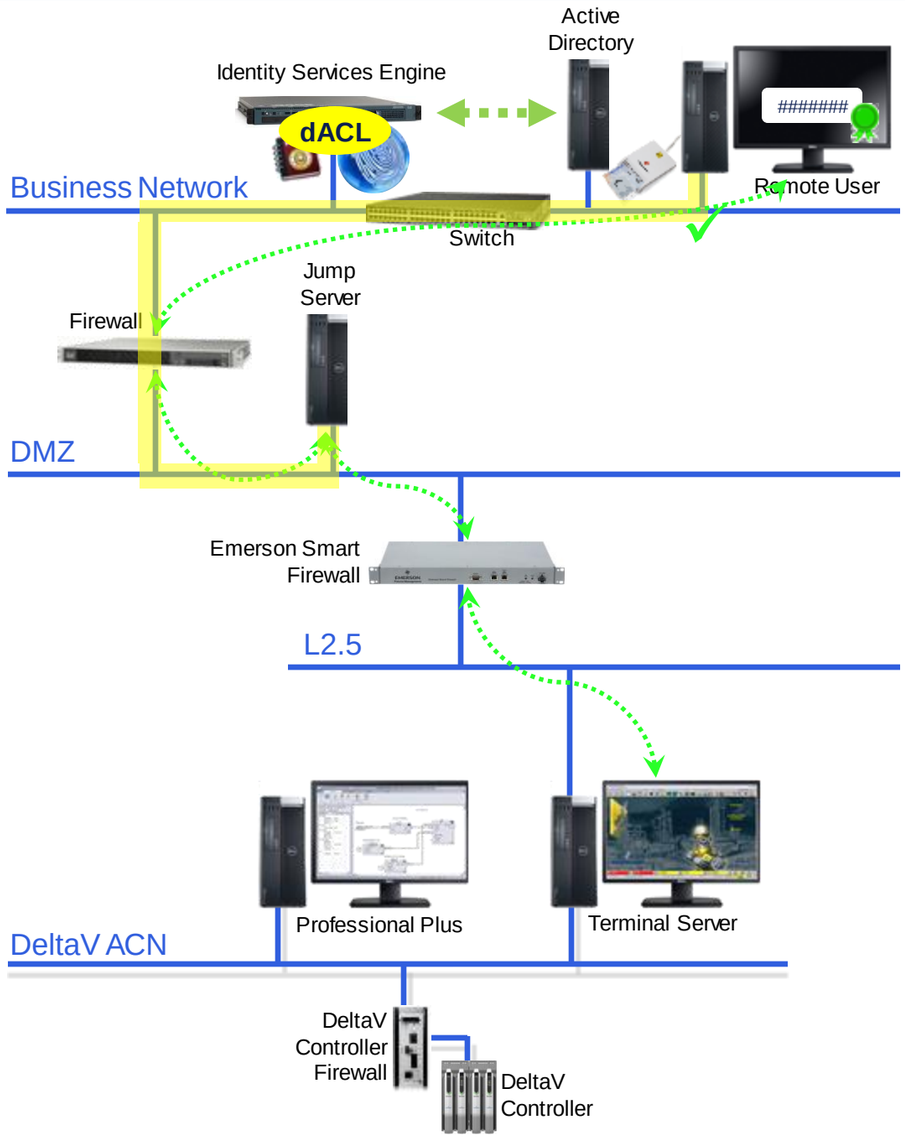
Программные средства защиты информации ПТК DeltaV. Приложение DeltaV User Manager

Возможности

- Интеграция с диспетчером пользователей ОС Windows.
- Управление группами пользователей.
- Управление правами доступа пользователей.
- Приложение может быть запущено на любой рабочей станции\сервере ПТК DeltaV.



Защищенный удаленный доступ с использованием сервиса идентификации



- Удаленный пользователь подключается из бизнес-сети.
- ISE применяет политики безопасности для новых устройств.
- Пользователь вводит учетные данные (двухфакторная аутентификация).
- ISE проверяет учетные данные с помощью Active Directory.
- ISE отправляет список управления доступом на коммутатор, к которому подключен удаленный пользователь.
- Согласно списку контроля доступа, пользователь заблокирован для «Сервер переходов».
- Пользователь устанавливает удаленный сеанс на прикладной рабочей станции с «сервера переходов».

Защита USB носителей информации

- Специальная станция проверки USB устройств.
- Прошедшие проверку устройства получают идентификатор позволяющий использование на станциях DeltaV.
- Небезопасные устройства маркируются и не будут распознаны станциями DeltaV.
- Позволяет настроить политику использования USB устройств на станциях АСУТП

Что такое управление кибербезопасностью DeltaV?

Оценка кибербезопасности
- Оценка и отчеты
- Анализ уязвимостей
- Рекомендации

Решения по кибербезопасности
- Автоматизированный сервис обновлений
- Whitelisting
- SIEM и анализ
- Мониторинг сетевого траффика
- Backup & Recovery
- Smart Firewalls, Smart switches и PLC Firewalls

Periodic Audits
- Годовой или полугодовой аудит
- Проверка действий по результатам предыдущего аудита
- Оценка текущего состояния на уязвимость к новым факторам угроз

Кибербезопасность АСУТП на примере DeltaV

HW / SW Solutions

Services

Антивирус KICS for Nodes	Внесение приложений в белый список	Автоматизированное обновление	Backup & Recovery
SIEM	Network scan KICS for Networks	USB Device Security	Безопасный удаленный доступ
Брандмауэры и коммутаторы DeltaV	NTP Сервер	Независимый контроллер домена DeltaV	Сетевое хранилище
Оценки безопасности	Создание отчетов	Разработка политик и процедур	Консалтинг и тестирование совместимости

Модульное и масштабируемое решение для ваших задач в кибербезопасности автоматизации!