kaspersky

Kaspersky Industrial Cybersecurity Conference 2020

Василий Шауро

Руководитель направления стратегического маркетинга, Emerson

#KasperskyICS

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

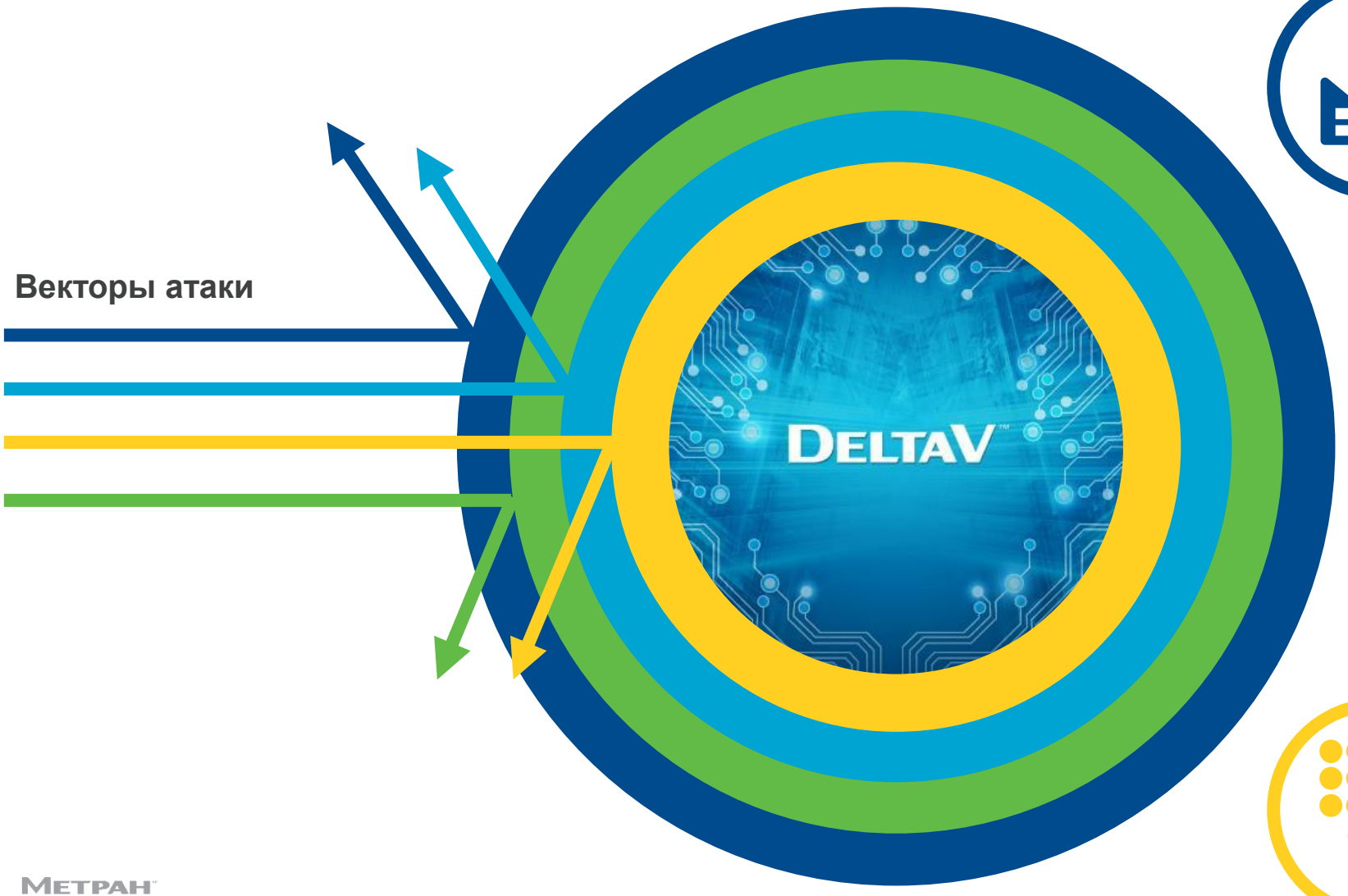
Система информационной безопасности АСУТП ДельтаВ

Sochi 2020
Василий Шауро, ООО Эмерсон
vasily.shauro@emerson.com

МЕТРАН™

EMERSON.

Информационная безопасность – слои защиты



Процедуры и политики

Технические и программные средства защиты

Поддержка и обслуживание

Тонкая настройка

Метран

EMERSON

Семь шагов эффективной защиты АСУТП

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

*Reference: Department of Homeland Security: Seven Steps to Effectively Defend Industrial Control Systems.

Процент инцидентов потенциально предотвращаемый каждой из стратегий

Метран

EMERSON

Семь шагов эффективной защиты АСУТП

1. Whitelisting и Endpoint.

Whitelisting приложений для системы DeltaV - останавливает случайное выполнение вредоносных программ. Файл не находящийся в «белом списке» на этом устройстве, не может быть выполнен. Endpoint Security для систем DeltaV обнаруживает и удаляет или помещает в карантин скрытые или спящие вредоносные программы (на базе Kaspersky KICS for Nodes).

2. Управление обновлениями и поддержание актуальных версий ПО

Автоматическое распространение обновлений при наличии и соблюдении политик и процедур гарантирует что Ваша защита не имеет известных уязвимостей. Для систем DeltaV доступно автоматическое распространение обновлений через систему Guardian Software Update Delivery Service (GSUDS)

3. Уменьшение потенциальной области атаки.

Набор политик при создании АСУТП рекомендованный для DeltaV

- Изолируйте сети управления технологическим процессом.
- Отключите все неиспользуемые службы в сети управления технологическим процессом.
- Используйте брандмауэры, где это возможно (не только для подключения к бизнес-сетям).
- Заблокируйте неиспользуемые порты и службы.
- Заблокируйте возможность изменения ППО в узлах АСУТП

Семь шагов эффективной защиты АСУТП

4. Защищенная среда

- Внедрите регулярные аудиты кибербезопасности.
- Сети АСУТП должны быть сегментированы.
- Возможность подключения съемных носителей отключена, до тех пор, пока это не понадобится.
- Неиспользуемые порты коммутаторов заблокированы.

5. Управление доступом

- В DeltaV встроены политики использования и разграничения прав пользователей.
- Используются независимые от корпоративной системы учетные записи.
- По возможности используется многофакторная аутентификация.

6. Мониторинг активности

- Информация о безопасности и управление событиями (SIEM).
- Отслеживание IP-трафика в сети управления на предмет вредоносных подключений и / или содержимого (на базе Kaspersky KICS for Networks).
- Встроенные средства для резервного копирования и восстановления.

Семь шагов эффективной защиты АСУТП

7. Внедрение удаленного защищенного доступа

- Отслеживайте и применяйте политики и процедуры удаленного доступа.
- Соединения настраиваются и разрешаются ICS.
- Активность подключений ограничена тем периодом, когда они необходимы.
- Используется многофакторная аутентификацию и «джамп сервера» для подключений, исходящих из бизнес-сетей и внешних VPN сетей.
- Используется платформа управления политиками безопасности, которая автоматизирует и обеспечивает безопасный доступ с учетом контекста к сетевым ресурсам.
    - Cisco Identity Services Engine (ISE) - это альтернативный сервис, предлагающий применение политик безопасности к любому удаленному устройству / пользователю, подключающемуся к ICS из локальной бизнес-сети или за пределами предприятия через VPN-соединение.

Технические средства защиты информации ПТК DeltaV. Коммутаторы DeltaV Smart Switch

Особенности

- Не используемые порты коммутатора блокируются нажатием одной кнопки (или по истечении 60 минут).
- Автоматическое определение некоторых man-in-the-middle атак.
- Диагностическая информация автоматически направляется на станции ПТК DeltaV.
- «Зеркалирование» входящего трафика выбранных портов коммутатора на выбранный порт для мониторинга с помощью средств анализа сетевого траффика таких как KICS for Networks.

Высокая степень защиты периметра технологической сети, лёгкое развёртывание, централизованное управление и мониторинг БЕЗ установки дополнительного ПО.

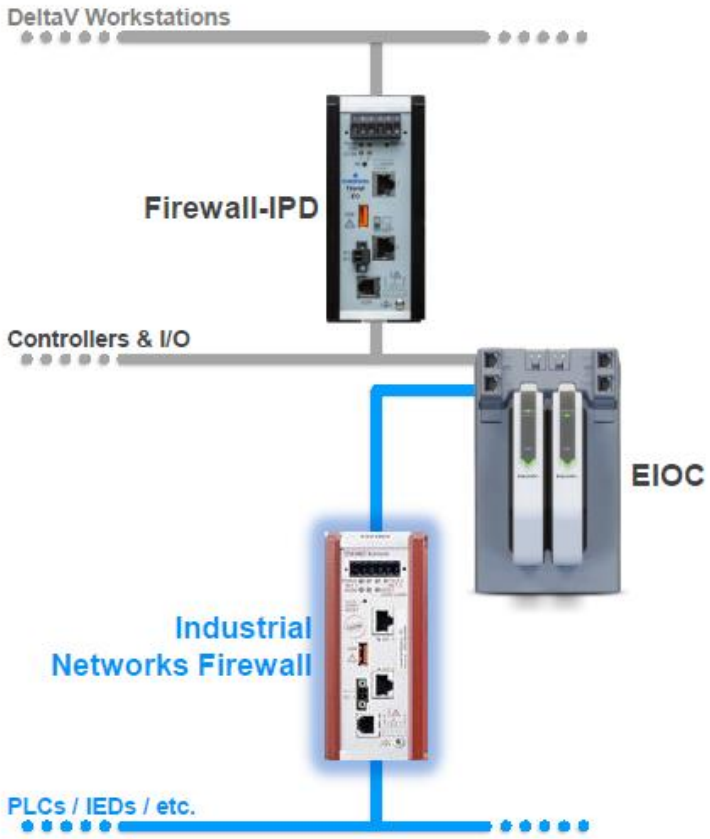
Технические средства защиты информации ПТК DeltaV. Промышленный межсетевой экран DeltaV Firewall-IPD

Особенности

- «Прозрачный» межсетевой экран.
- IPD – Средство предотвращения вторжений.
- Фильтрация команды «разблокировать» для узлов DeltaV уровня автоматизации L1.
- Фильтрация команды «разблокировать» для узлов SIS DeltaV.
- Доступен с медными и оптическими портами.
- Нативное решение для ПТК DeltaV, работающее «из коробки».

Новое комбинированное решение, сочетающее функциональные возможности Controller Firewall и SIS-IPD. Режим блокировки прохождения команд управляется «железным» дискретным сигналом.

Технические средства защиты информации ПТК DeltaV. Промышленный межсетевой экран Tofino Xenon



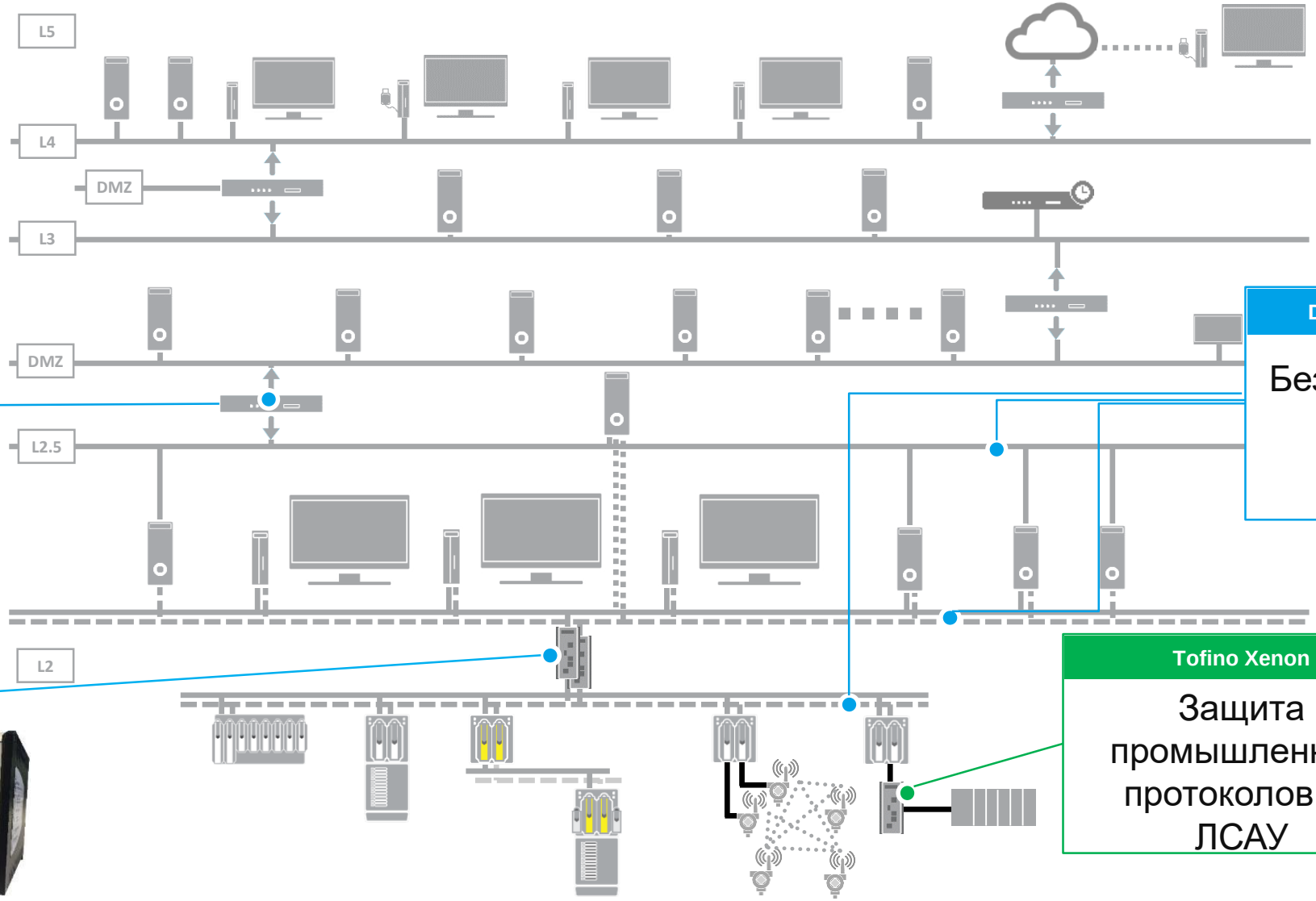
- Начиная с версии 13.3.1 в ПТК DeltaV, как дополнительный продукт, поддерживается промышленный межсетевой экран Tofino Xenon.
- Tofino Xenon рекомендуется использовать при интеграции ЛСАУ в ПТК DeltaV.

Особенности

- Выполнение функции межсетевого экранирования трафика.
- Поддержка более 125 IT и промышленных коммуникационных протоколов.
- Глубокий анализ пакетов (DPI) для протоколов Modbus TCP, EtherNet IP и OPC.

Настраивается с помощью интуитивно понятного графического интерфейса, конфигурирование не требует глубоких знаний в сфере IT.
Аналогично DeltaV Firewall-IPD имеет режим блокировки, управляемый «железным» дискретным сигналом.

Технические средства защиты информации ПТК DeltaV



Emerson Smart Firewall

Защита периметра сети ПТК DeltaV

DeltaV Smart Switches

Безопасность сети АСТУП

DeltaV Firewall-IPD

Защита сети контроллеров

Tofino Xenon

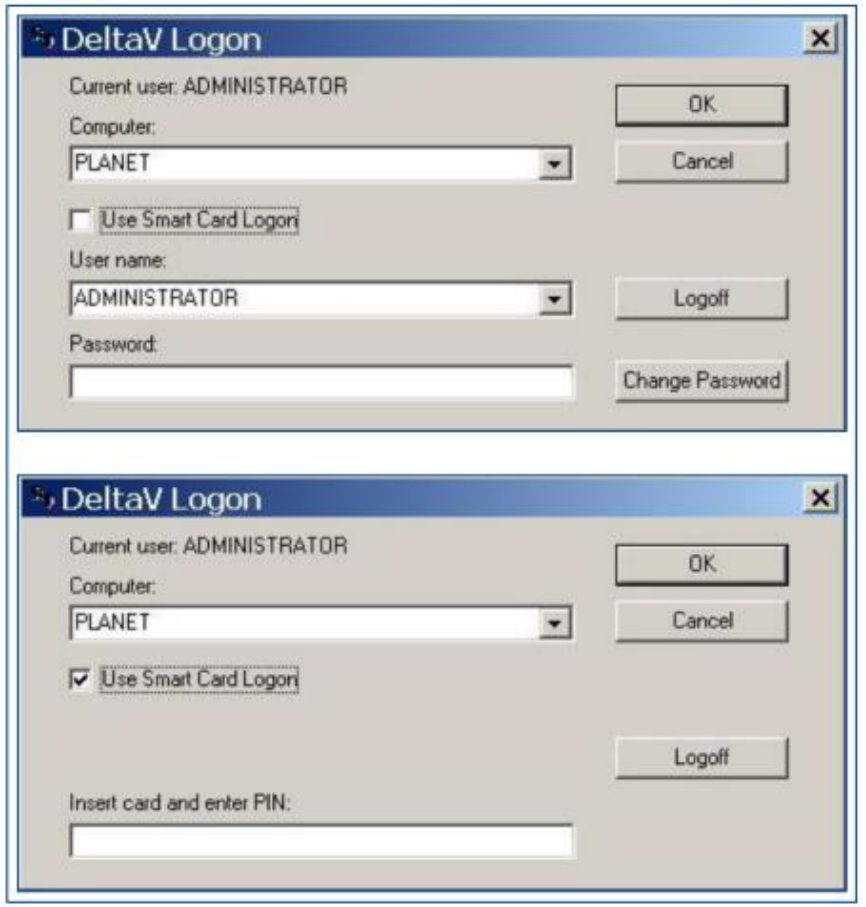
Защита промышленных протоколов от ЛСАУ

Метран

EMERSON

ГОСТ Р 56205-2014

Технические средства защиты информации ПТК DeltaV. 2-х факторная аутентификация

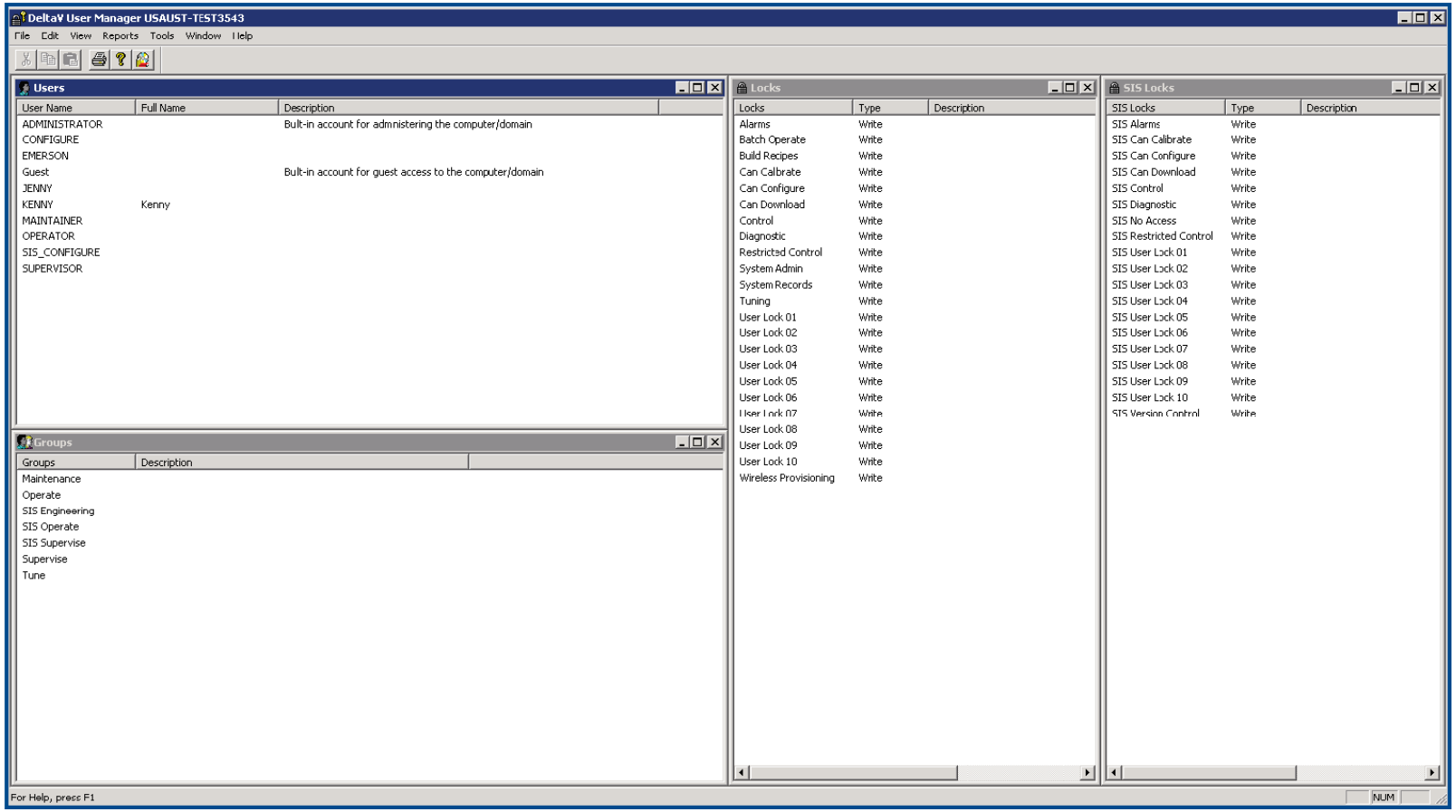


Двухфакторная Аутентификация с Применением совместимых с Windows Crypto API Smart Cards и Smart Card Readers

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.

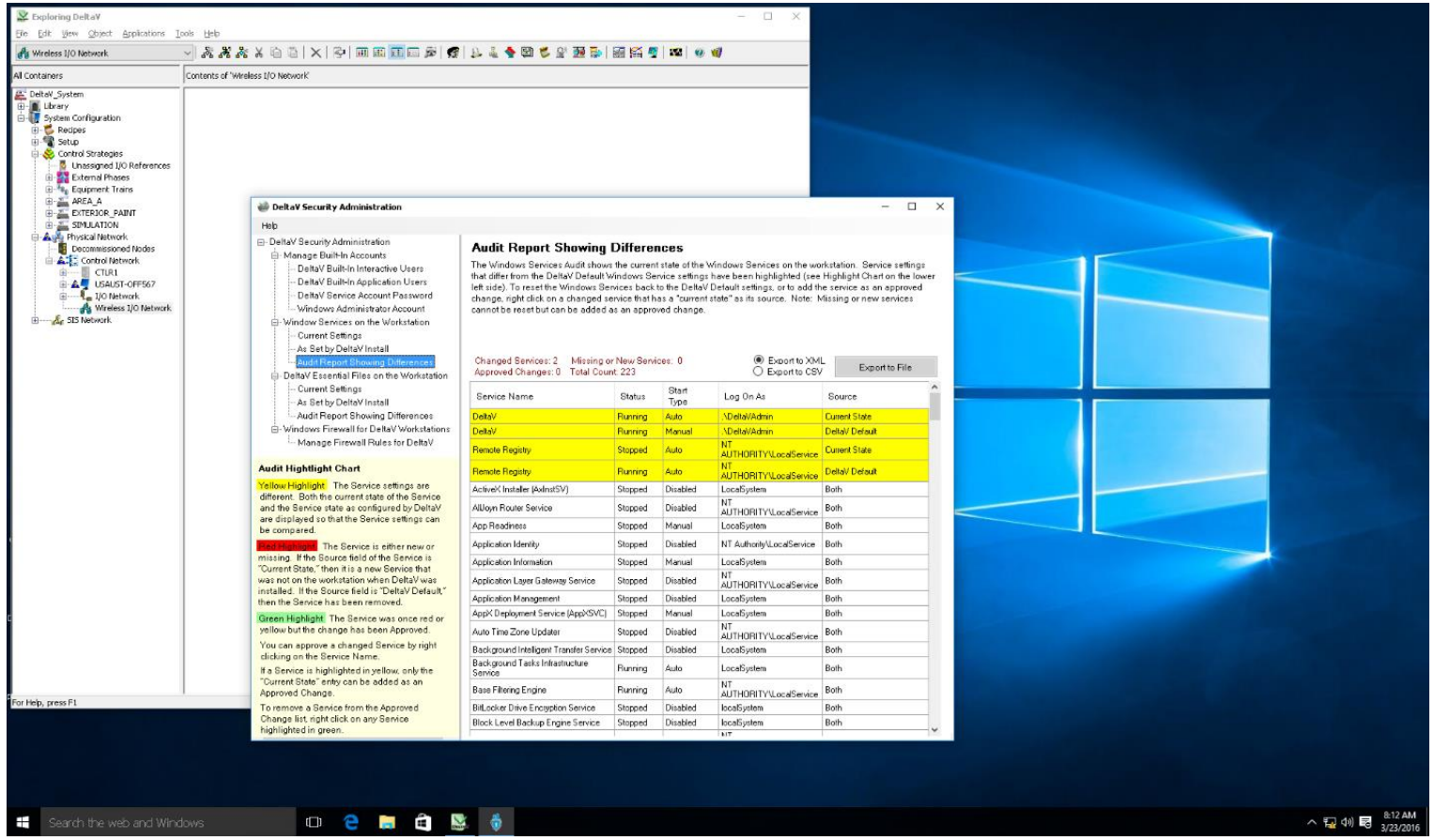


Программные средства защиты информации ПТК DeltaV. Приложение DeltaV Security Administration

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

Возможности

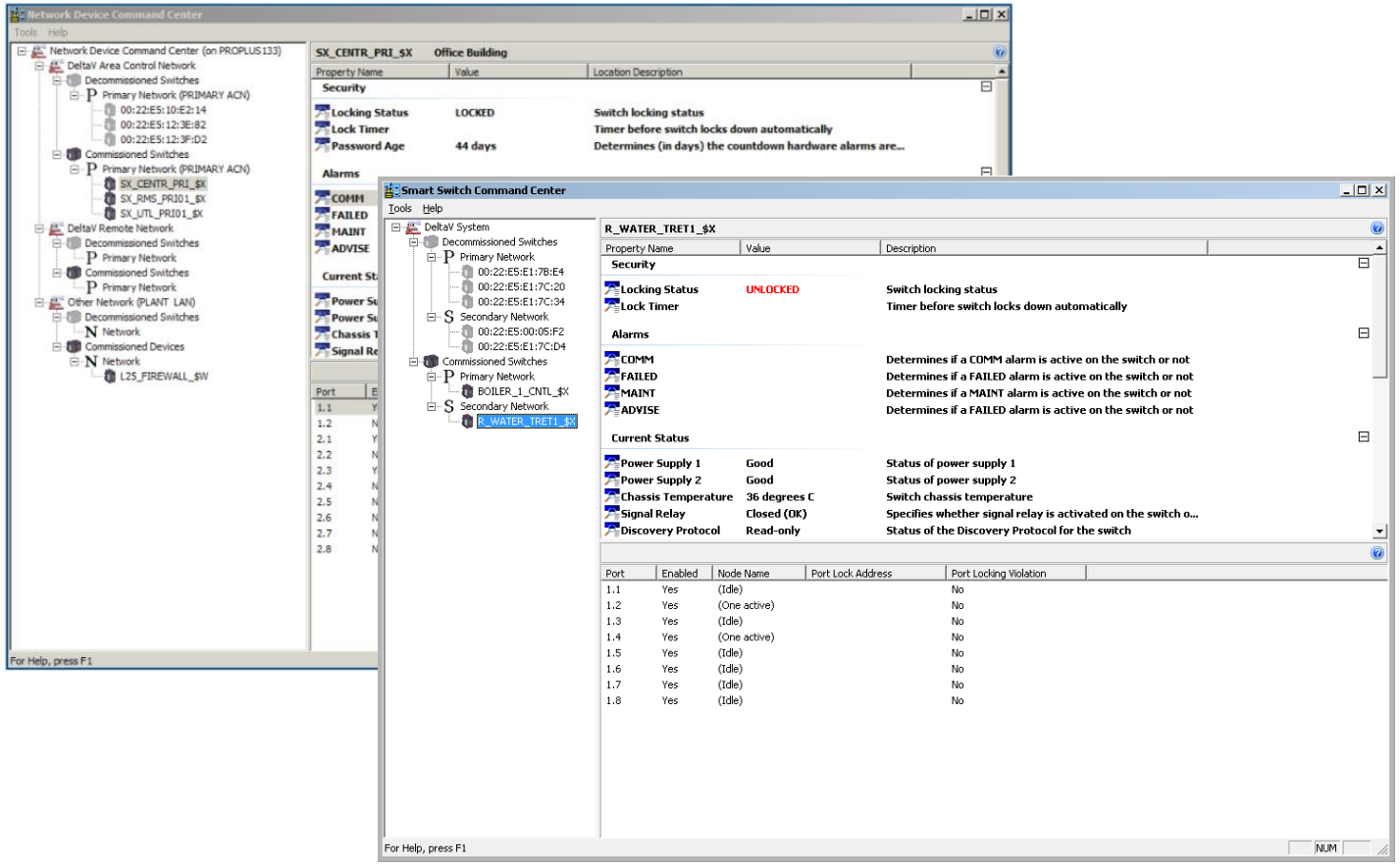
- Контроль состояния сервисов ОС Windows.
- Контроль целостности файлов специального ПО ПТК DeltaV.
- Интеграция с Windows Firewall.
- Управление встроенными аккаунтам.



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.



Приложение обеспечивает управление и мониторинг нативным оборудованием ПТК DeltaV.

Метран

EMERSON

Программные средства защиты информации ПТК DeltaV. Настройка встроенных механизмов защиты информации ОС Windows

Возможности

- Для ПТК DeltaV доступны параметры конфигурации настроек безопасности операционной системы Windows, подготовленные на основании бенчмарк-списков организации CIS.
- Конфигурирование настроек безопасности происходит в момент установки специального ПО ПТК DeltaV.
- Для применяемых параметров безопасности ОС Windows, существует подробное описание для приведения в соответствие с корпоративными стандартами заказчика.

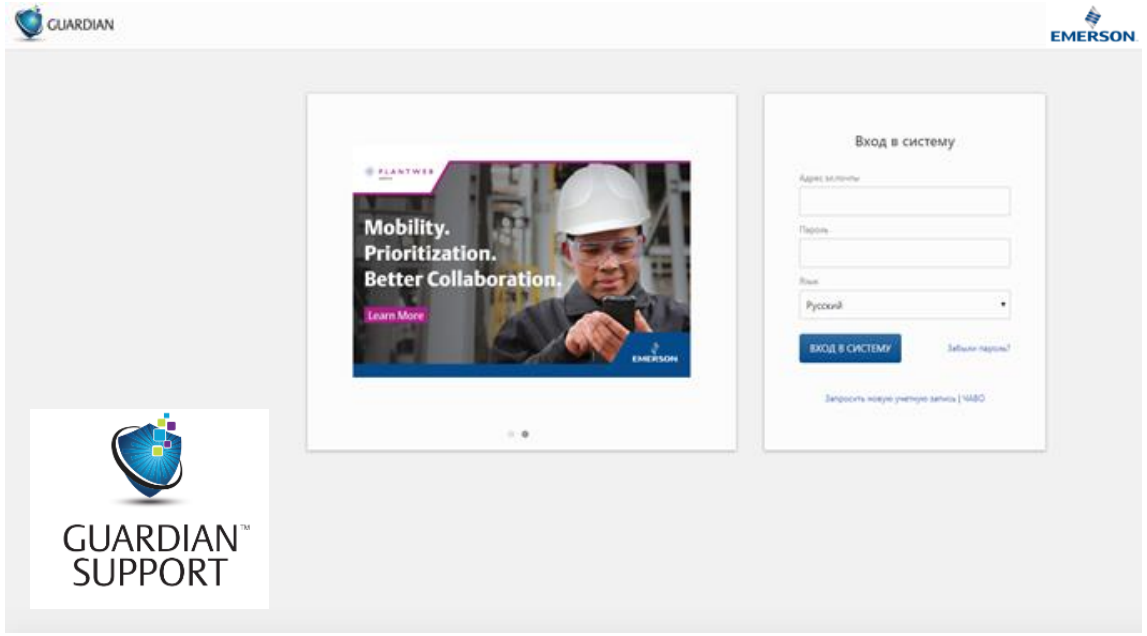
CIS® Center for Internet Security®

CIS Benchmarks™

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

Возможности

- Комплексная программа сервисного обслуживания и поддержки Guardian, включает в себя Guardian Software Update Delivery Service (GSUDS) – сервис получения обновлений и исправлений ПО ПТК DeltaV.
- Заказчики получают обновления для продуктов входящих в состав ПО ПТК DeltaV, предварительно прошедшие тестирование на совместимость со специальным ПО ПТК.
- Таким образом распространяются:
  - Обновления и исправления для ОС Windows.
  - Ссылки на обновления и исправления для антивирусного ПО.
  - Обновления и исправления для дополнительных продуктов ПТК DeltaV (таких как AMS Device Manger, AMS MHM и т.д.).

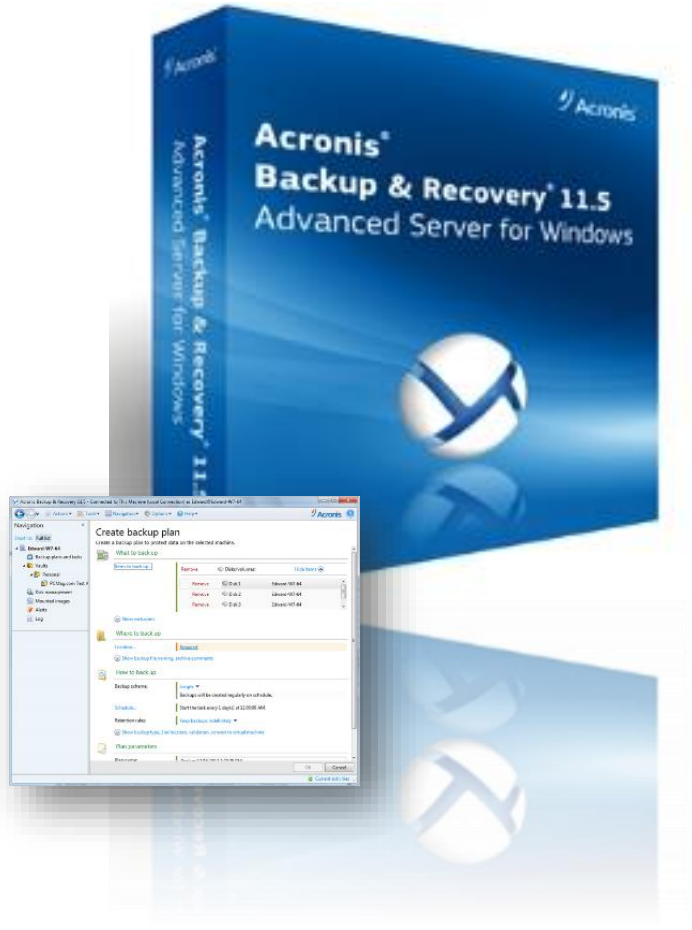


Программные средства защиты информации ПТК DeltaV. Программный продукт DeltaV Backup & Recovery

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.



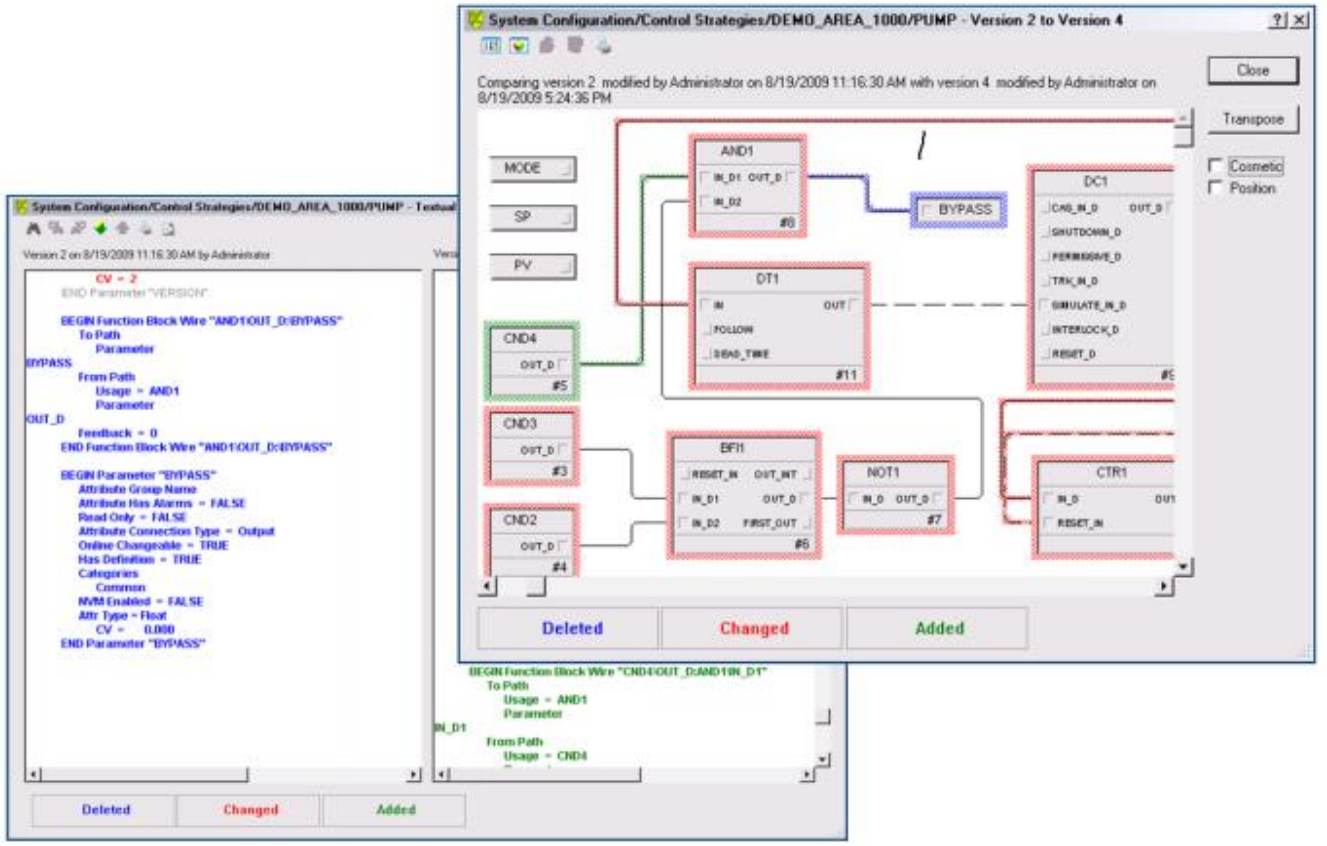
Восстановление из резервных копий

- 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. Контроль изменений

Возможности

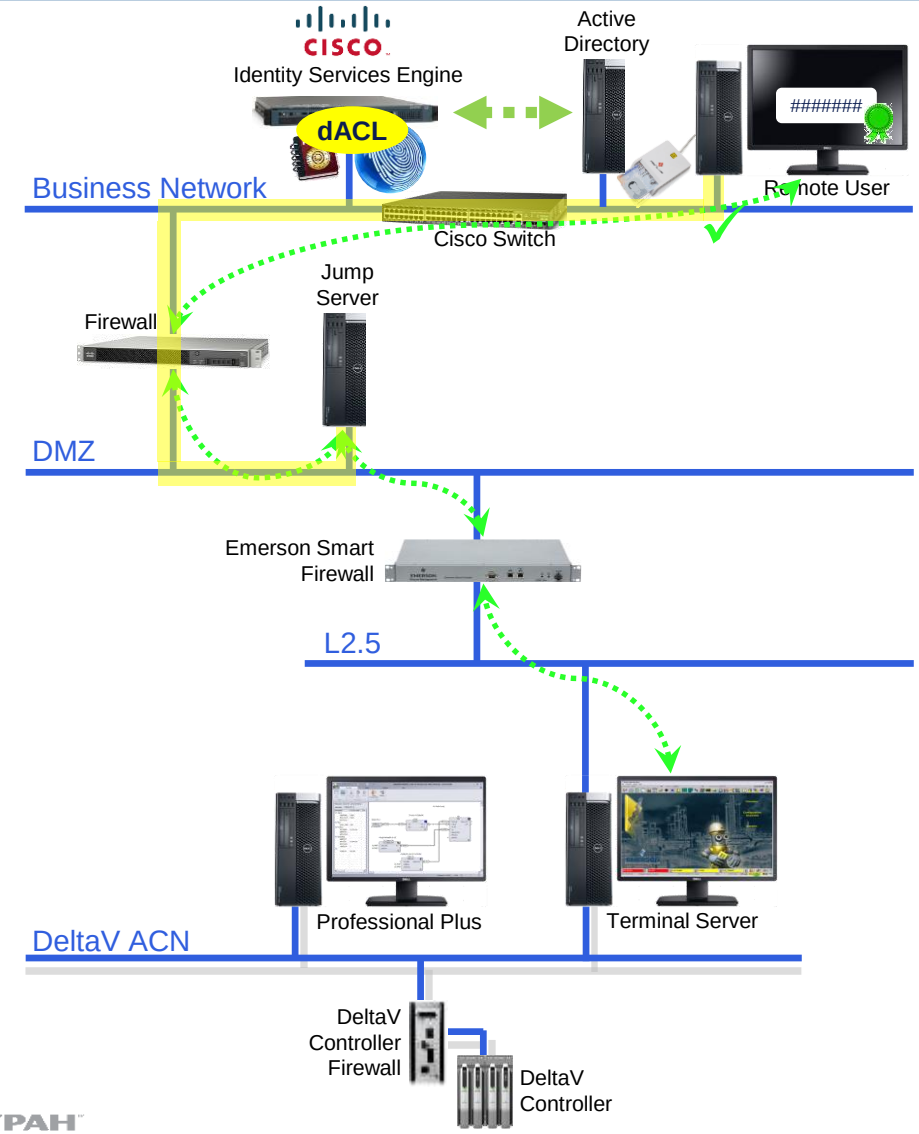
- Запись изменений конфигурации.
- Наглядное отображение изменений в конфигурации.
- Возможность отката к предыдущим версиям.
- Создание отчетов об изменениях.
- Отображение идентификаторов версий для загруженных элементов.
- Авторизация загрузки модулей ПАЗ (в зависимости от уровня SIL от 1 до 5 электронных подписей).
- Авторизация тестов ПАЗ (в зависимости от уровня SIL от 1 до 5 электронных подписей).
- Авторизация рецептов.



Метран

EMERSON

Защищенный удаленный доступ

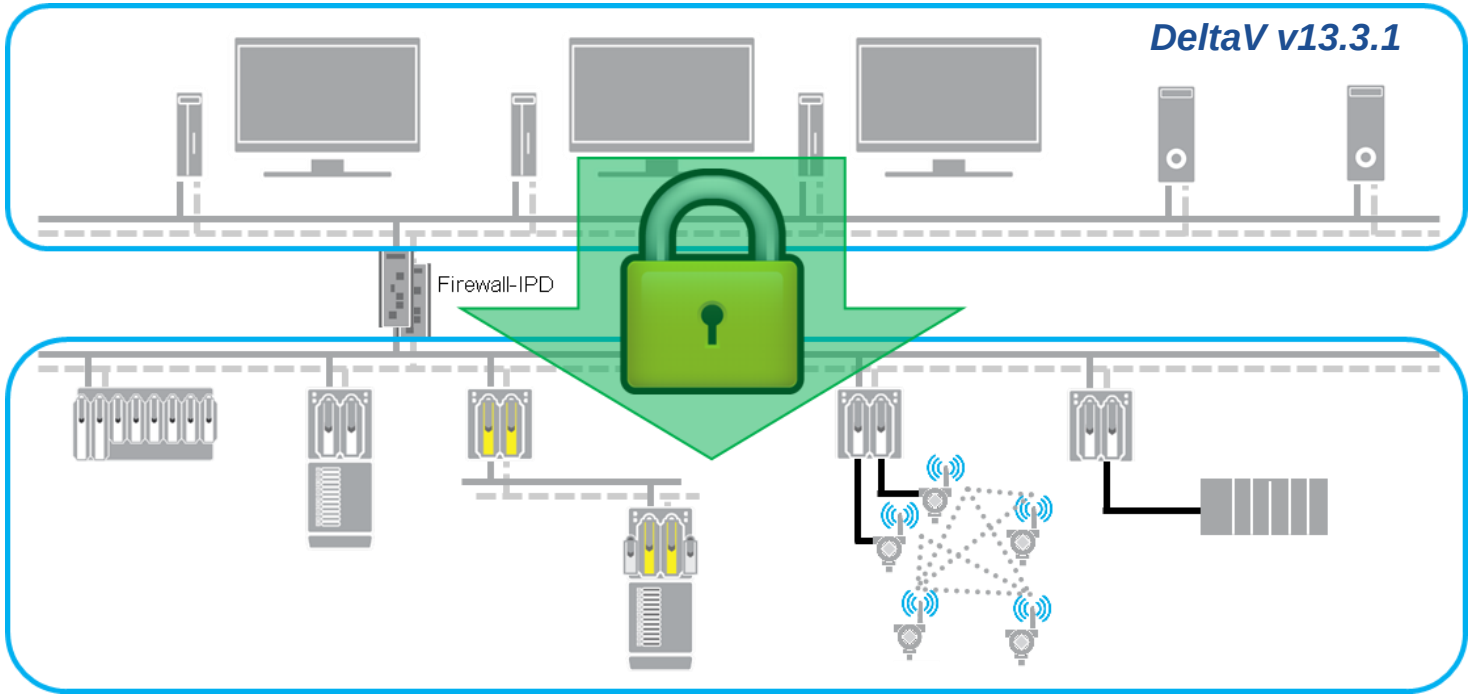


- Удаленный пользователь подключается из бизнес-сети.
- ISE применяет политики безопасности для новых устройств.
- Пользователь вводит учетные данные (двухфакторная аутентификация).
- ISE проверяет учетные данные с помощью Active Directory.
- ISE отправляет список управления доступом на коммутатор, к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

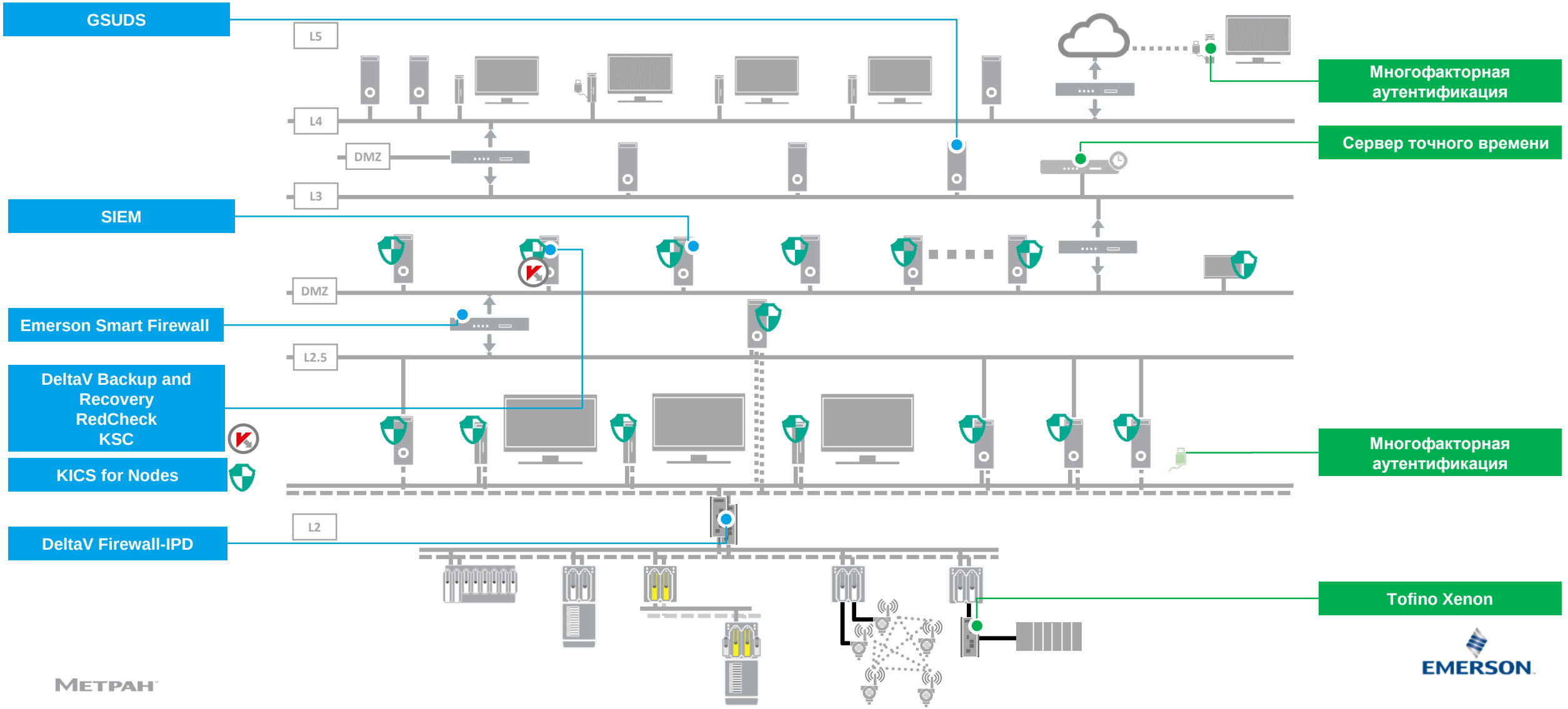
Технические средства защиты информации ПТК DeltaV. Команда блокировки для узлов ДельтаВ (Firewall-IPD)

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.



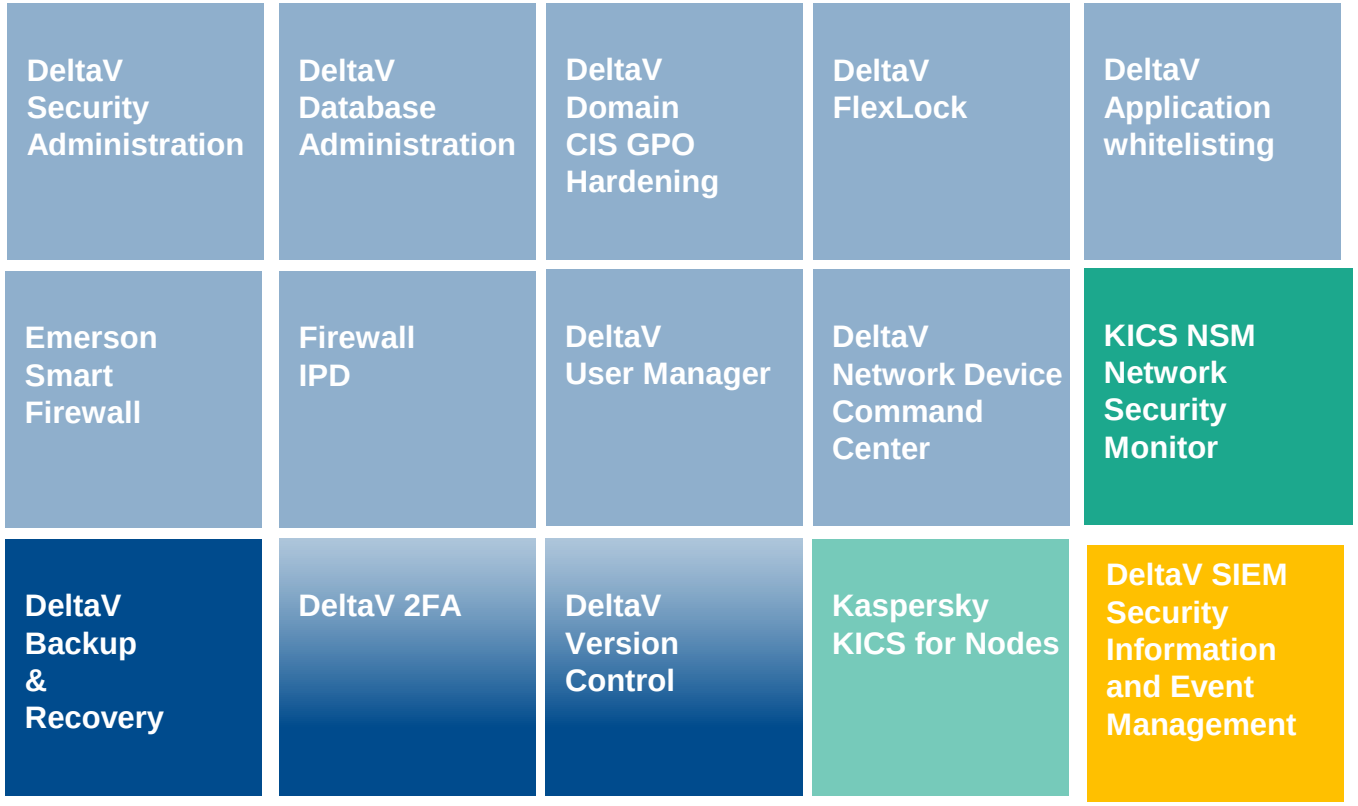
Архитектура решения по информационной безопасности



МЕТРАН

EMERSON

Бесшовное расширение системы киберзащиты АСУ



Совместимость Сертификаты и лицензии

- Лицензия на деятельность по технической защите конфиденциальной информации.
- Лицензия на деятельность по разработке и производству средств защиты конфиденциальной информации.
- Achilles level 2 сертификация большинства узлов, с версии 14.3.1
- Achilles level 2 для всей системы DeltaV 14.3.1 в процессе
- ISA SSA Level 1
- ISA SDLA
- Совместимость с KICS for nodes для версий 13.3.1, 14.3.1. RUS
- Совместимость с KICS for networks


СЕРИЯ КИ 0278 НОМЕР 013987

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ЛИЦЕНЗИЯ

НА ДЕЯТЕЛЬНОСТЬ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Регистрационный номер 3200 от 21 марта 2017 г.

Лицензия предоставлена Обществу с ограниченной ответственностью «Эмерсон» (ООО «Эмерсон») ОГРН 1027739864943, ИНН 7705130530

Адрес места нахождения: 115054, г. Москва, ул. Дубининская, д. 53, строение 5

Адрес места осуществления лицензируемого вида деятельности: 454003, г. Челябинск, пр-кт Новоградский, д. 15, строение 2

Перечень работ и услуг, на которые распространяется настоящая лицензия:

контроль защищенности конфиденциальной информации от несанкционированного доступа и его модификации в средствах и системах информатизации;

проектирование в защищенном исполнении: средств и систем информатизации; помещений со средствами (системами), подлежащими защите; защищаемых помещений;

установка, монтаж, испытания, ремонт средств защиты информации (программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации).

Лицензия предоставлена на основании приказа ФСТЭК России от 21 марта 2017 г. № 141-л

Лицензия действует бессрочно

Заместитель директора

А.Куц


СЕРИЯ КИ 0134 НОМЕР 006680

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ЛИЦЕНЗИЯ

НА ДЕЯТЕЛЬНОСТЬ ПО РАЗРАБОТКЕ И ПРОИЗВОДСТВУ СРЕДСТВ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Регистрационный номер 1467 от 13 октября 2015 г.

Лицензия предоставлена Обществу с ограниченной ответственностью «Эмерсон» (ООО «Эмерсон») ОГРН 1027739864943, ИНН 7705130530

Адрес места нахождения: 115054, г. Москва, ул. Дубининская, д. 53, стр. 5

Адрес места осуществления лицензируемого вида деятельности: 115054, г. Москва, ул. Дубининская, д. 53, стр. 5

Перечень работ, на которые распространяется настоящая лицензия:

разработка средств защиты конфиденциальной информации: программных (программно-технических) средств защиты информации; защищенных программных (программно-технических) средств обработки информации; программных (программно-технических) средств контроля защищенности информации;

производство средств защиты конфиденциальной информации: программных (программно-технических) средств защиты информации; защищенных программных (программно-технических) средств обработки информации; программных (программно-технических) средств контроля защищенности информации.

Лицензия предоставлена на основании приказа ФСТЭК России от 13 октября 2015 г. № 399-л

Лицензия действует бессрочно

Заместитель директора

м.п.

А.Куц

Спасибо за внимание!

DeltaV™

Информационная безопасность

ВОПРОСЫ?