АЙТИБАСТИОН

ИНТЕГРИРУЕМАЯ ПЛАТФОРМА ДЛЯ КОНТРОЛЯ ИНФОРМАЦИОННОГО ОБМЕНА: КАК «СИНОНИКС» СТАЛ ЧАСТЬЮ ОПЕРАЦИОННЫХ ПРОЦЕССОВ

Родин Константин
Заместитель директора
по развитию бизнеса

www.it-bastion.com

АЙТИБАСТИОН

ОСНОВА ДЛЯ АВТОМАТИЗАЦИИ ПРИ ПЕРЕДАЧЕ ДАННЫХ

АЙТИБАСТИОН

ОСНОВА ДЛЯ АВТОМАТИЗАЦИИ
ПРИ ПЕРЕДАЧЕ ДАННЫХ

АЙТИБАСТИОН

«Безопасная автоматизация процесса» без доверия не работает, но доверие – это не слепая вера.

Это четкие правила, контролируемая среда и прозрачность.

КРИТЕРИИ ДОВЕРИЯ В РАМКАХ БЕЗОПАСНОЙ АВТОМАТИЗАЦИИ ПРОЦЕССА

АЙТИБАСТИОН

01 «Нулевое» доверие к источнику и содержимому

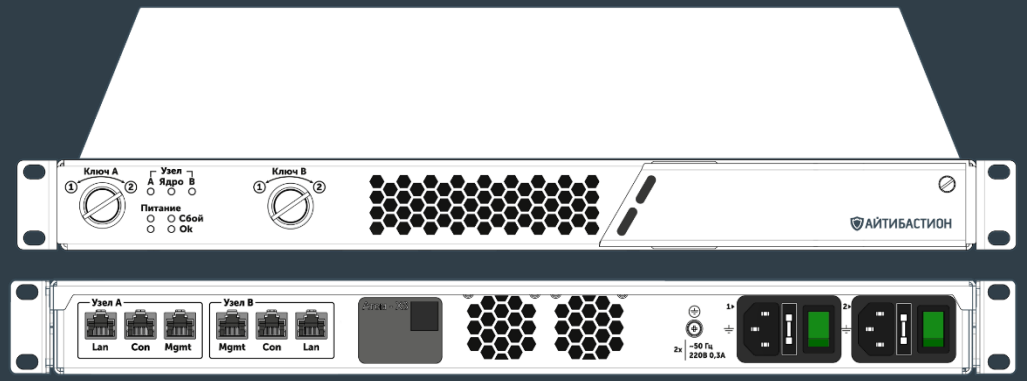
02 Доступ – не право, а привилегия через проверки и контроль

03 «Процесс» как объект контроля

www.it-bastion.com

«СИНОНИКС»
ИНСТРУМЕНТ СОЗДАНИЯ ДОВЕРИЯ

АЙТИБАСТИОН

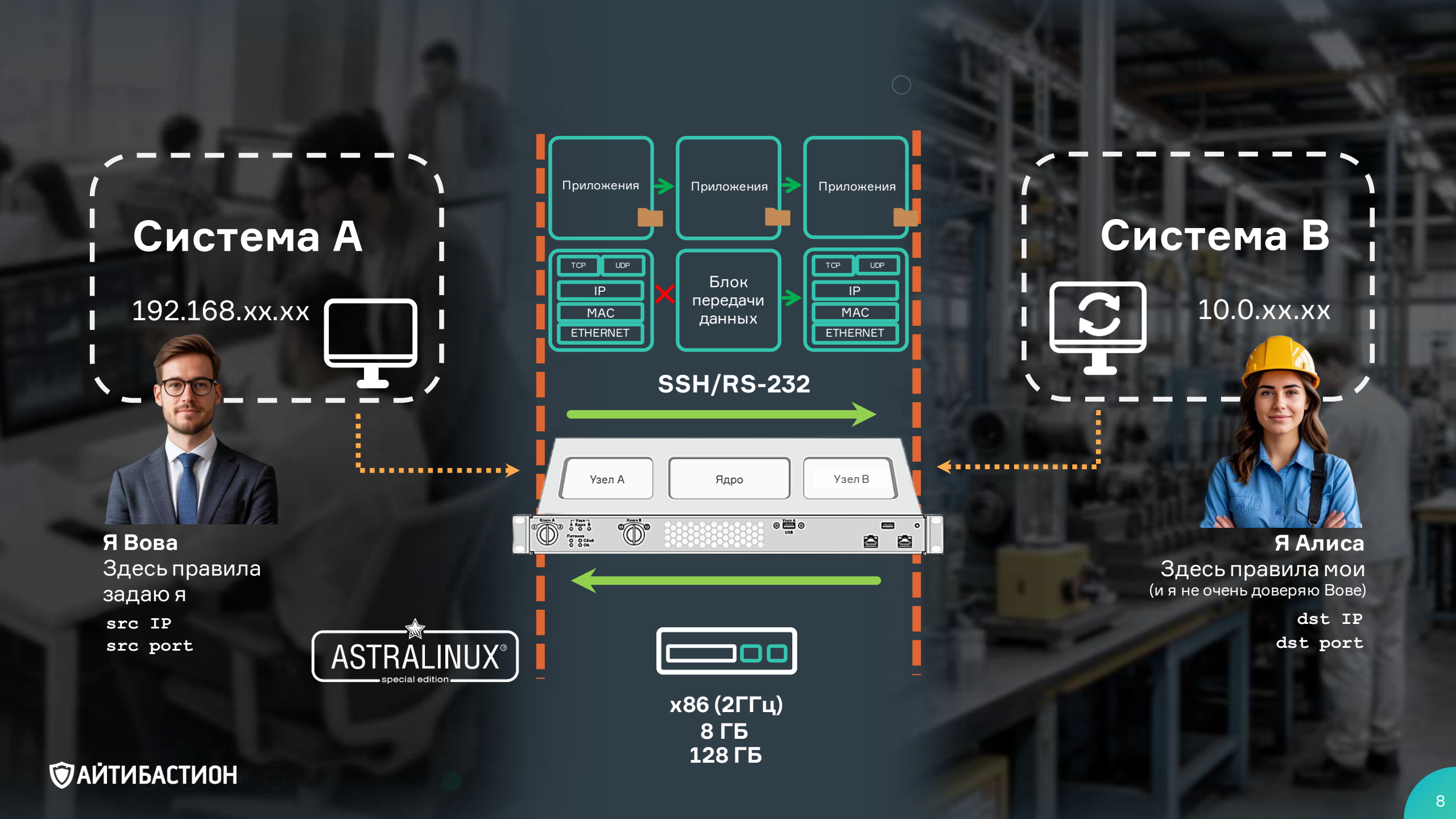


ПК «Синоникс» – система контроля информационного обмена. Решение позволяет организовать автоматизированную однонаправленную или двунаправленную передачу данных и файлов между узлами двух сетей, скрывая при этом информацию об их окружении.

«Синоникс» проектировался для:

1. **Управляемой передачи данных**
2. **Междоменного взаимодействия**
3. **Автоматизации процессов обмена**
4. **Существующей инфраструктуры заказчиков**
5. **Существующих процессов заказчиков**

www.it-bastion.com


Система А
192.168.xx.xx
Приложения
Приложения
Приложения
TCP
UDP
IP
MAC
ETHERNET
Блок передачи данных
TCP
UDP
IP
MAC
ETHERNET
SSH/RS-232
Узел А
Ядро
Узел В
Система В
10.0.xx.xx
Я Вова
Здесь правила задаю я
src IP
src port
Я Алиса
Здесь правила мои
(и я не очень доверяю Вове)
dst IP
dst port
ASTRALINUX
special edition
x86 (2ГГц)
8 ГБ
128 ГБ
АЙТИБАСТИОН

КОМБИНИРОВАННЫЙ РЕЖИМ

ПЕРЕДАЧА ДАННЫХ

- TCP, UDP, в т.ч. односторонняя
- Поддержка промышленных протоколов ModBus, MQTT
- Независимые политики для двух контуров
- Соединения точка-точка, изоляция окружения
- Поддержка работы с МЭ, NGFW и другим сетевым оборудованием

ПЕРЕДАЧА ФАЙЛОВ

- SFTP/FTP/SMB
- Автоматизация получение и передачи данных (PUSH/PULL)
- Выбор направления передачи
- Проверка типа, маски, размера, целостности
- Интеграция с ICAP-сервисами (DLP, Sandbox, AV, и др.)
- Встроенный антивирус
- Передача через внешние USB-накопители

АЙТИБАСТИОН

Система А

192.168.xx.xx

Я Вова
Здесь правила задаю я

TCP/UDP

Номера правил на обоих узлах должны совпадать

Режим работы на узлах должен быть разным

```
SynOS-A> transport show slots
transport set slot 1 protocol tcp mode collect ip 10.1.0.34 port 443
transport set slot 2 protocol tcp mode collect ip 10.1.0.34 port 75
transport set slot 3 protocol tcp mode collect ip 10.1.0.34 port 22
transport diode set slot 4 protocol udp mode exchange ip 10.0.128.75 port 515
```

Система В

10.0.xx.xx

Я Алиса
Здесь правила мои
(и я не очень доверяю Вове)

```
SynOS-B> transport show slots
transport set slot 1 protocol tcp mode exchange ip 192.168.0.5 port 443
transport set slot 2 protocol tcp mode exchange ip 192.168.0.5 port 3389
transport set slot 3 protocol tcp mode exchange ip 192.168.0.5 port 22
transport diode set slot 4 protocol udp mode collect ip 192.168.0.100 port 514
```

НОВЫЕ ПРОТОКОЛЫ

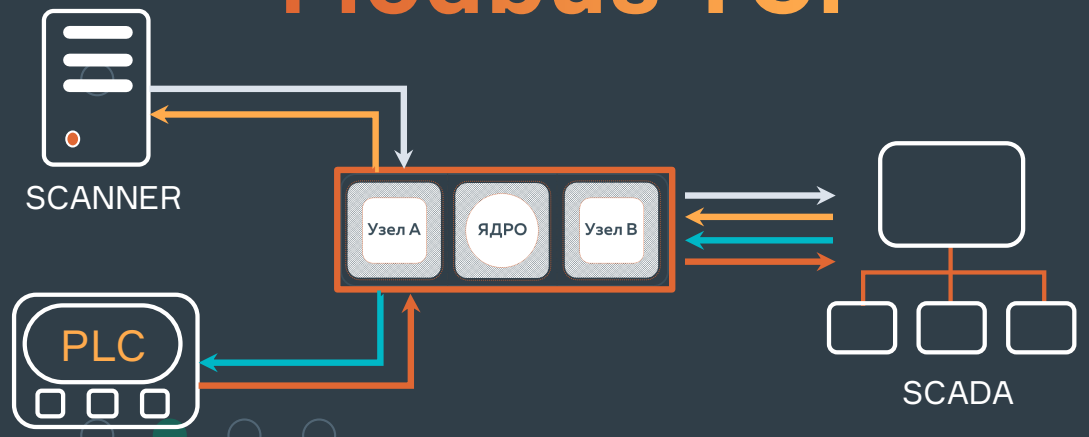
АЙТИБАСТИОН

MQTT

«Синоникс» может использоваться для передачи телеметрии производственной сети по промышленному протоколу MQTT.

Система обеспечивает обмен данными между внешними брокерами MQTT.

Modbus TCP



Интеграция «Синоникса» с промышленными устройствами от ПЛК и HMI до распределенной периферии. Это помогает передавать технологические данные на SCADA-системы.

Функционал будет полезен на предприятиях, работающих с системами автоматизации производства.

АЙТИБАСТИОН

Система А

192.168.xx.xx

Я Вова
Здесь правила задаю я

ОЛЬЗОВАТЕЛЬ
РАВИЛО
РОФИЛЬ

Подключение по SFTP

Направление: A->B / B->A, / A<->B

Проверки: размер, маска имени, целостность, ICAP

Система В

10.0.xx.xx

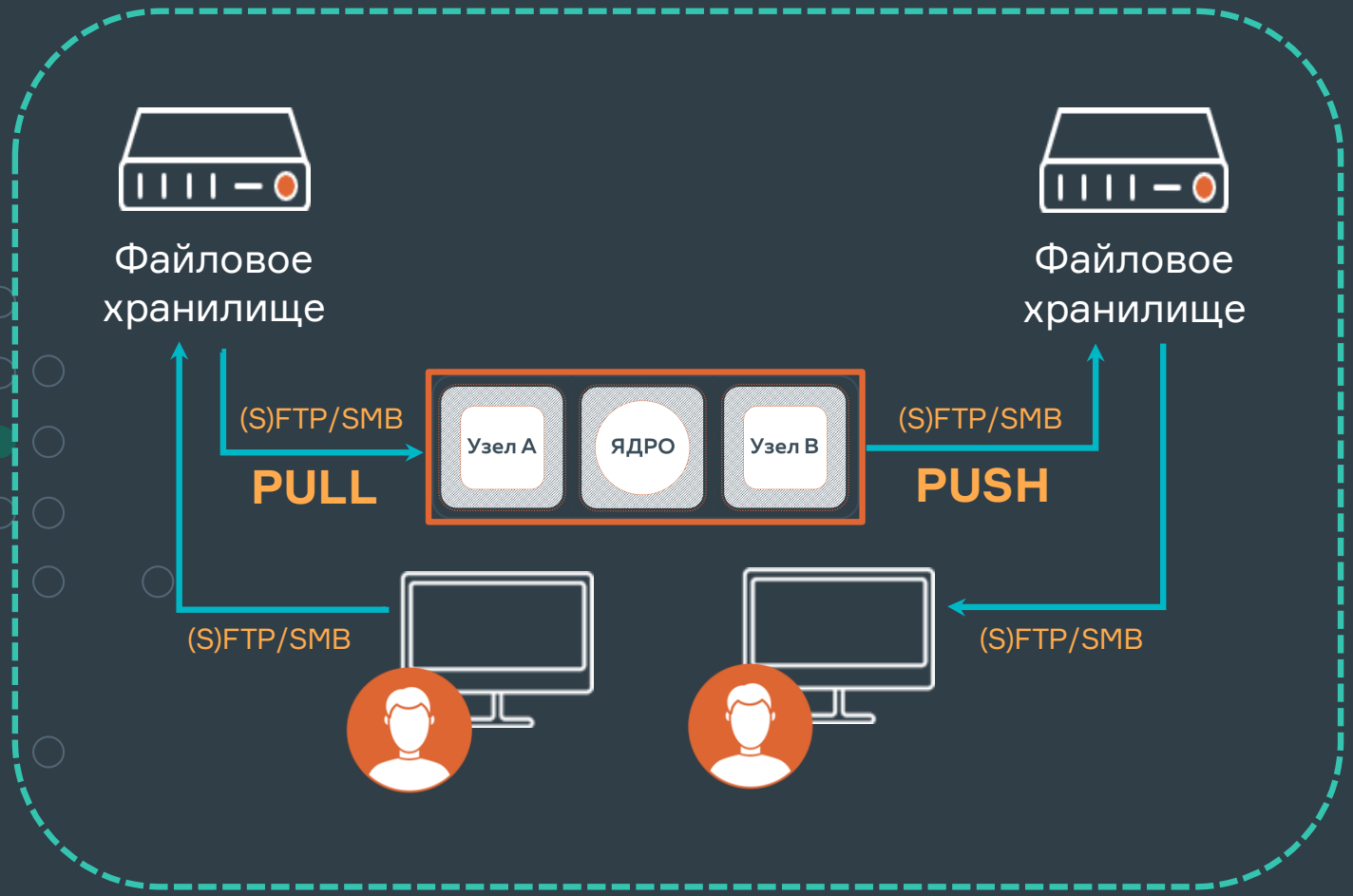
Я Алиса
Здесь правила мои
(и я не очень доверяю Вове)

Маска имени
Допустимый размер
Целостность
ICAP
и др...

ICAP

АВТОМАТИЗАЦИЯ ДОСТАВКИ ПО ПРОТОКОЛАМ SMB/(s)FTP

АЙТИБАСТИОН

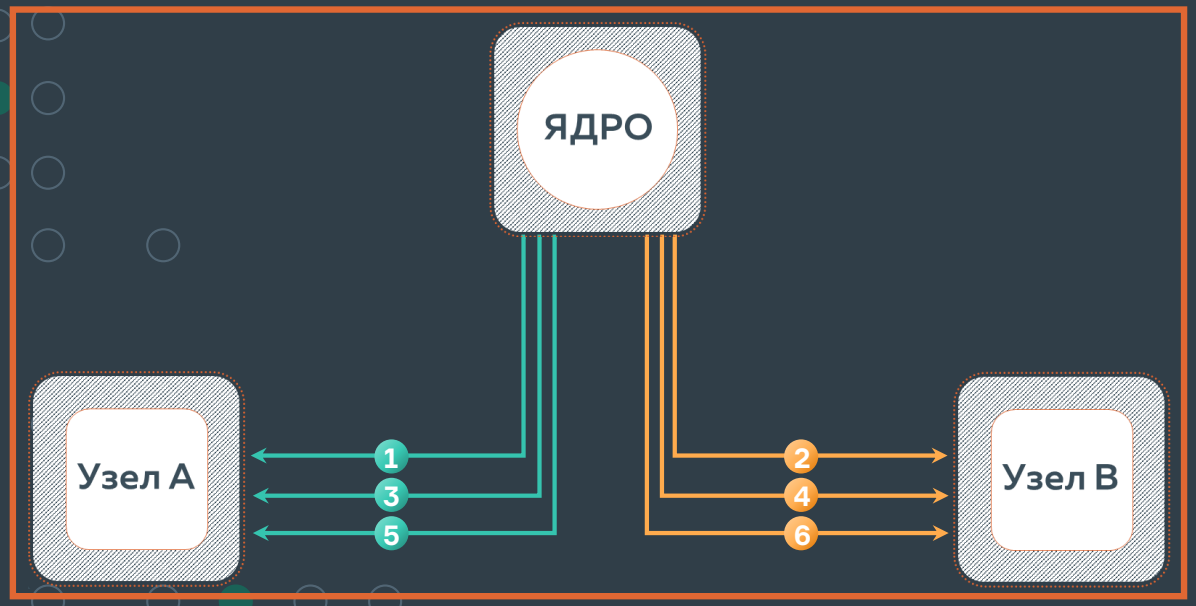


«Синоникс» благодаря новым режимам работы PUSH и PULL способен автоматически собирать данные из указанной директории и направлять в определенную директорию с другой стороны по запросу или расписанию, в том числе с использованием протоколов SMB и (s)FTP.

РЕЖИМ ТАМБУР

АЙТИБАСТИОН

Механизм безопасной передачи файлов, при котором Ядро «Синоникса» находится в изоляции от Узлов и связывается с ними только при наличии проверенной сессии передачи файлов.



Ядро по очереди «опрашивает» Узлы на наличие файловых сессий.

Ядро никогда не устанавливает соединение с двумя Узлами одновременно, что позволяет мансимально безопасно передавать информацию в конфиденциальные системы.

ДОПОЛНИТЕЛЬНЫЙ ФИЗИЧЕСКИЙ КОНТРОЛЬ

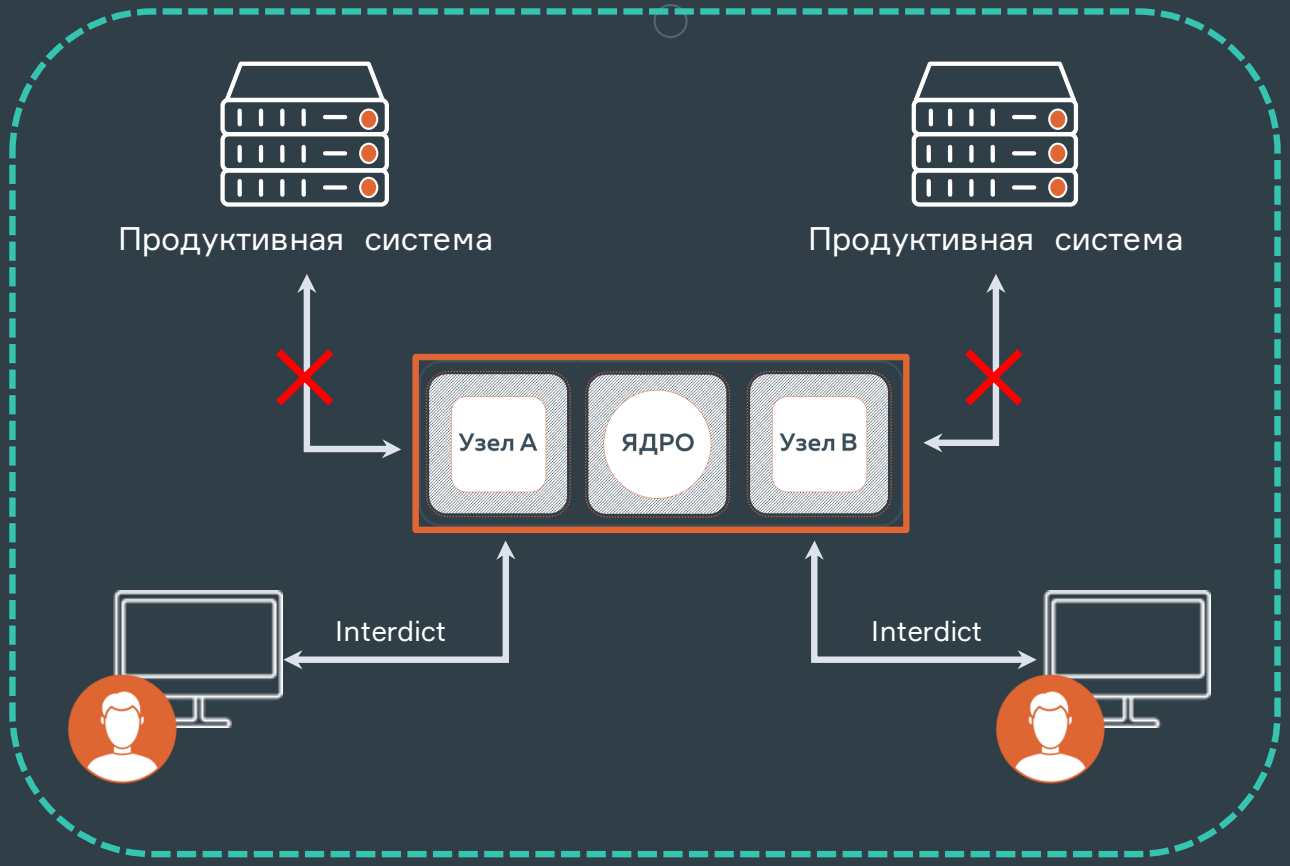
Дополнительный контроль обеспечивается с помощью физических пусковых ключей, разделяемых между сотрудниками, каждый из которых ответственен за свою сеть. Ключи разрешают или блокируют передачу данных через Синоникс путем полного отключения питания Ядра. При повороте одного из них, центральная плата отключается.

ПРОГРАММНЫЙ КЛЮЧ

АЙТИБАСТИОН

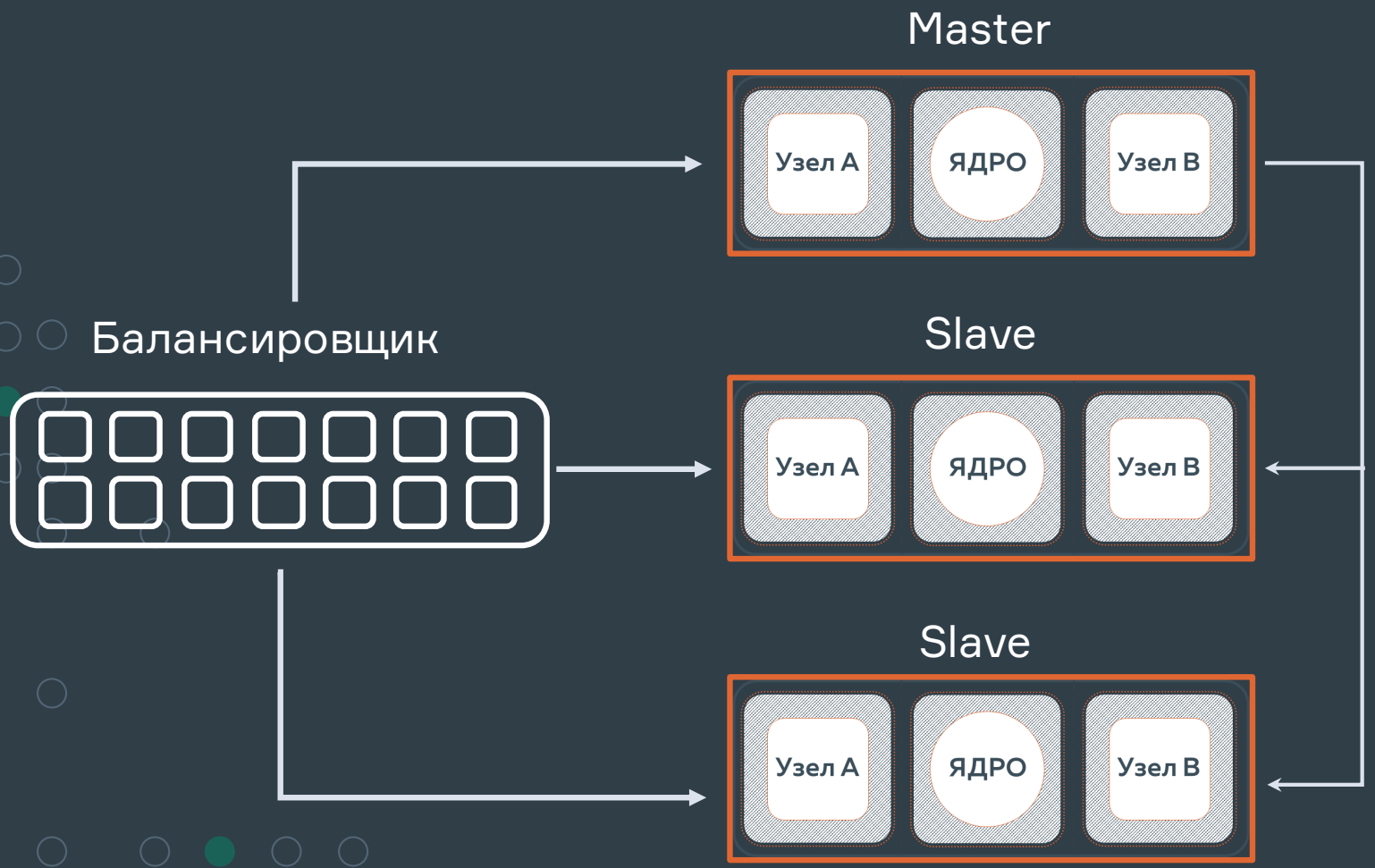
Администратор или оператор может запрещать обмен любыми данными из консоли.

Более гибкие настройки блокировок: отключение только одного режима передачи – либо данных, либо файлов.



ОТКАЗОУСТОЙЧИВОСТЬ И БАЛАНСИРОВКА ПОДКЛЮЧЕНИЙ

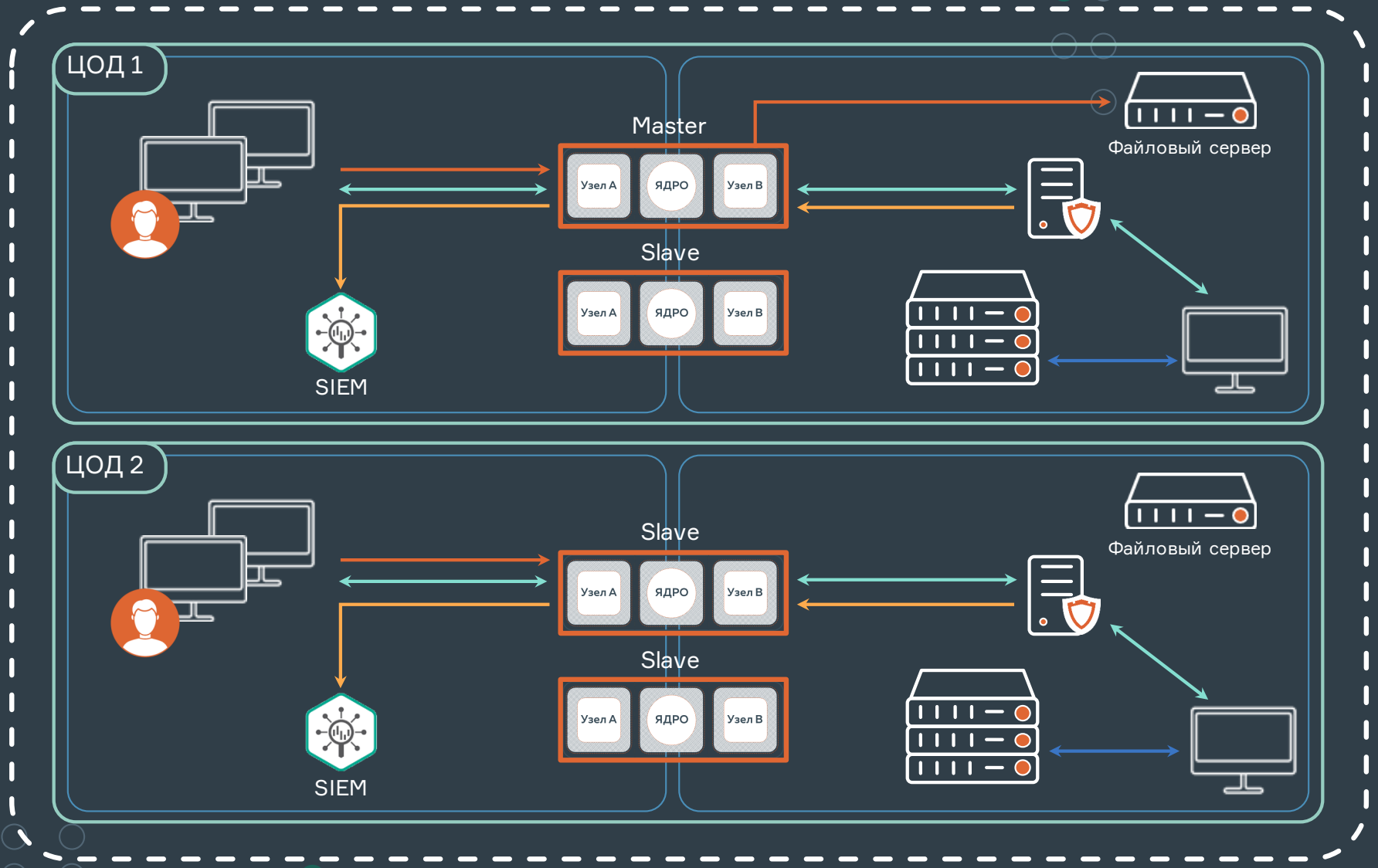
АЙТИБАСТИОН



- **DS Proxima**
- **HA Proxy**
- **Встроенный на узлах «Синоникса»**

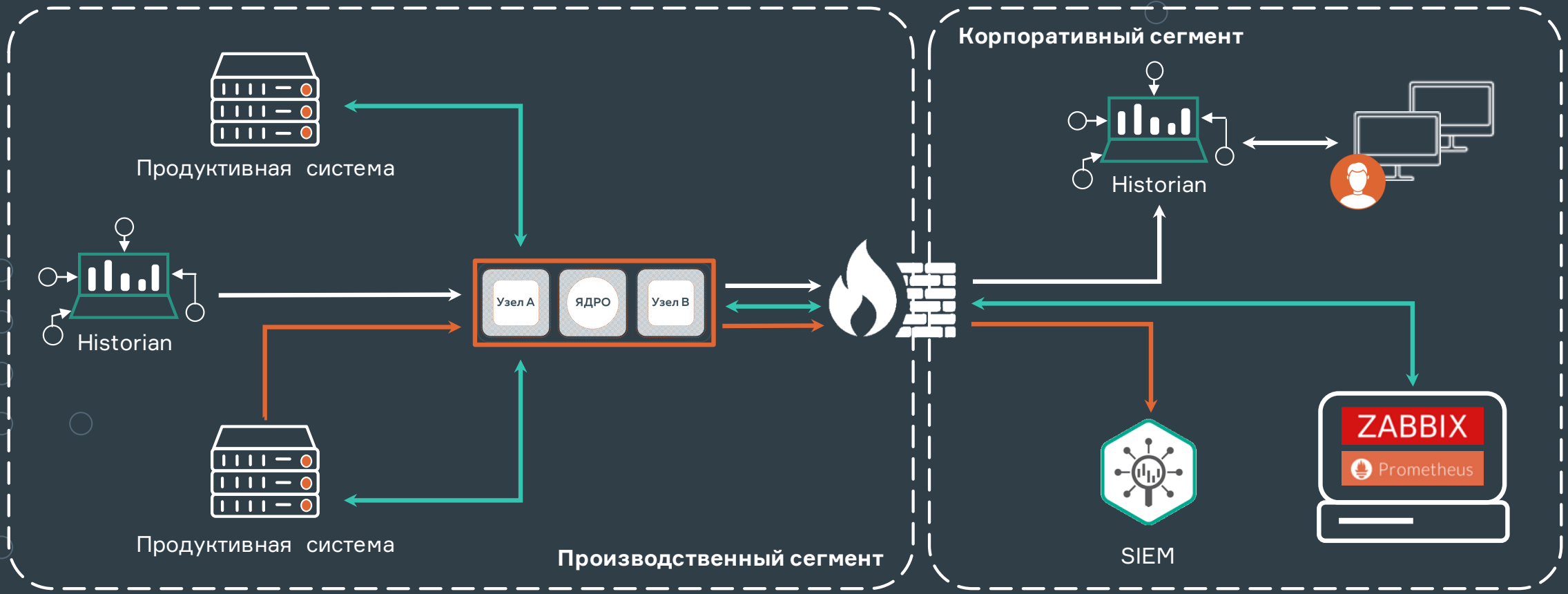
КАТАСТРОФОУСТОЙЧИВОСТЬ

АЙТИБАСТИОН



МОНИТОРИНГ СОСТОЯНИЯ ВО ВНЕШНИХ СИСТЕМАХ

АЙТИБАСТИОН

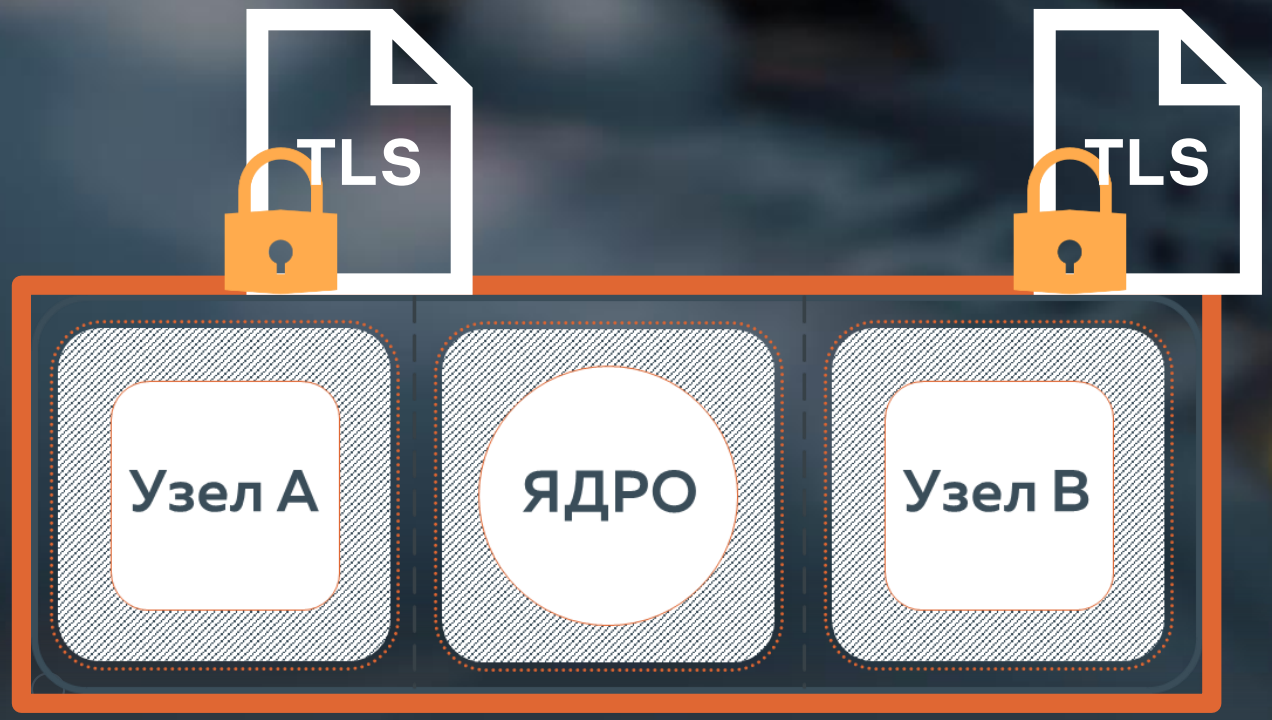


Сбор журналов (TCP/UDP)

Передача данных Historian

Передача данных мониторинговых систем (TCP)

ПОДДЕРЖКА
TLS

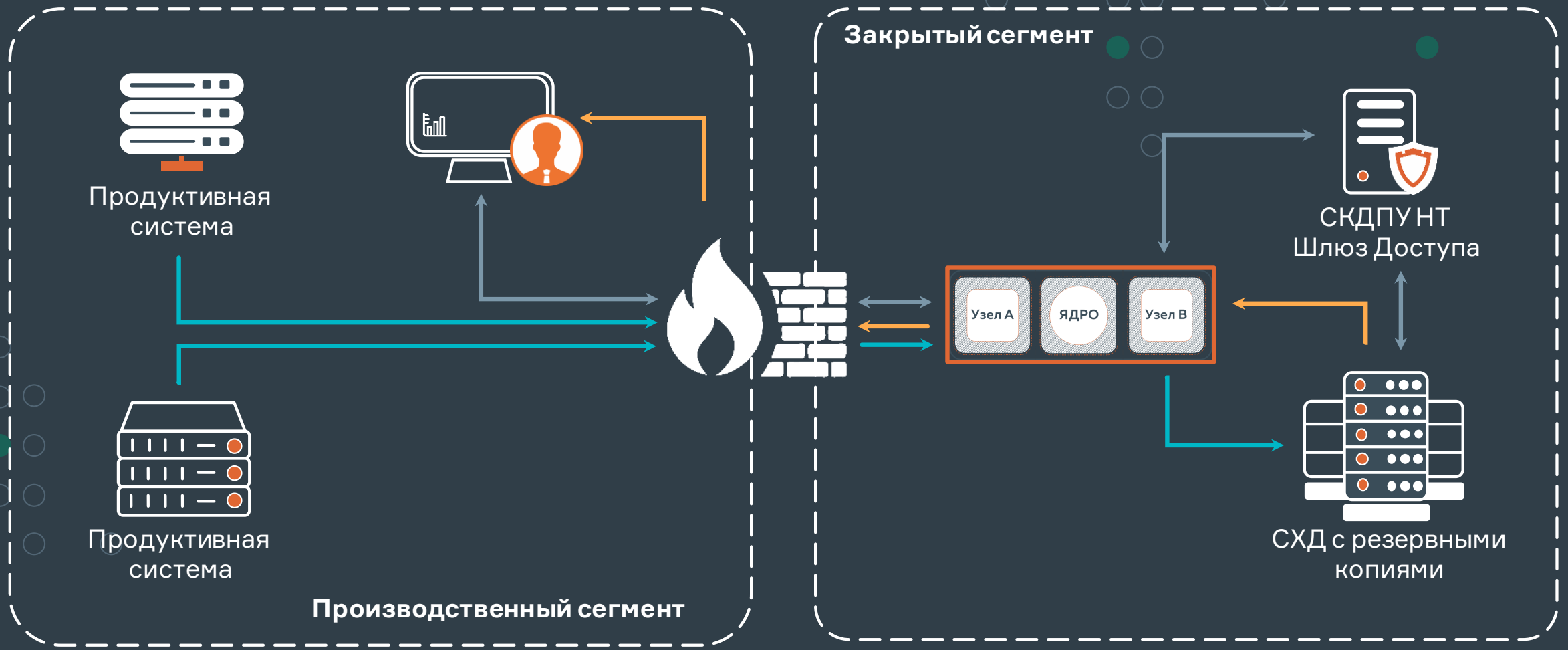


Загрузка сертификатов и ключей безопасности в настройки правил передачи данных для корректного взаимодействия с системами, требующих дополнительной защиты при соединении.

«СИНОНИКС»

Применим во всех сценариях, где обычно проектируют «классический» диод данных, и даже в большем их количестве

АЙТИБАСТИОН



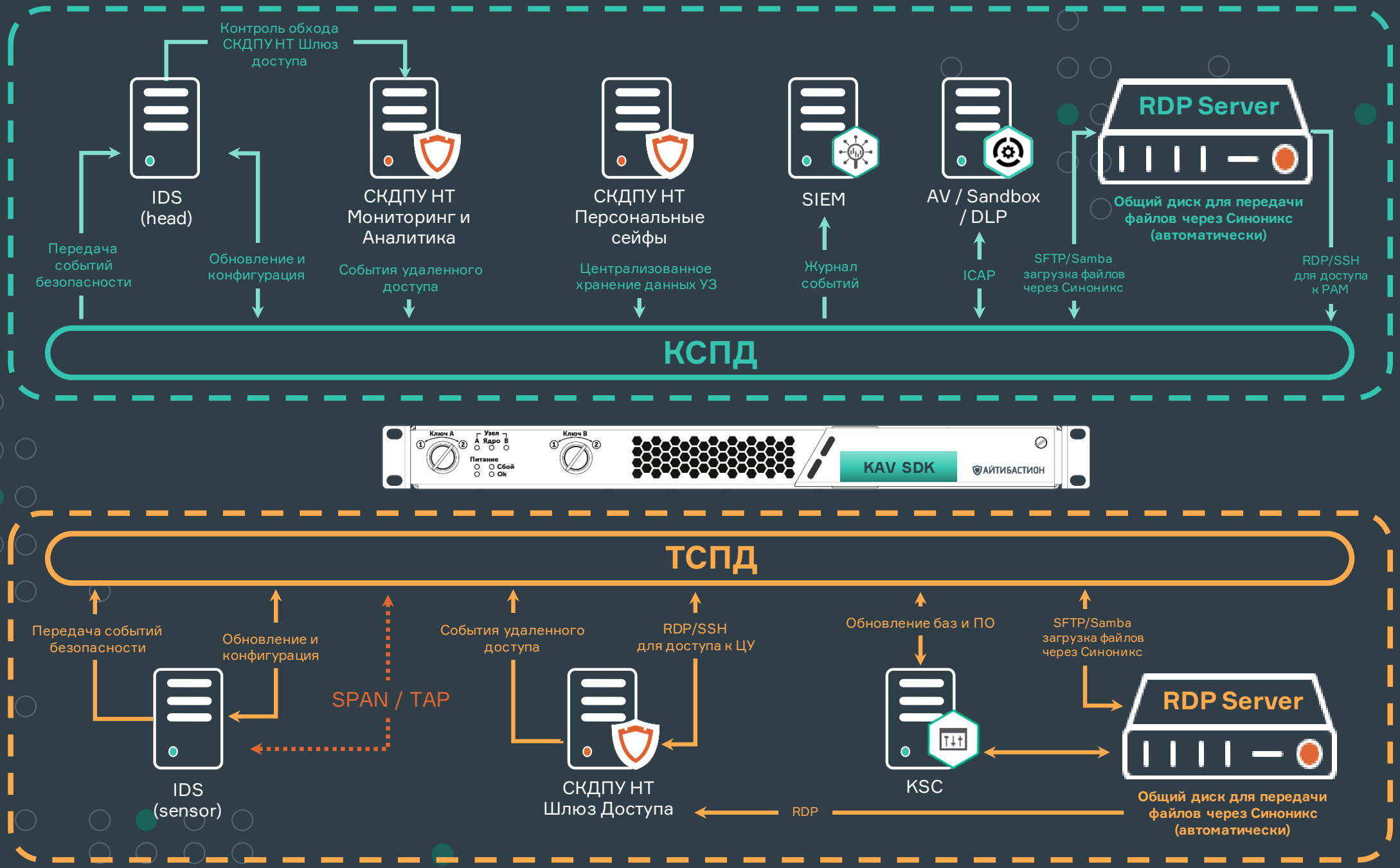
RDP/SSH
Доступ к СХД в закрытом сегменте через PAM-систему

TCP
Передача бэкапов на СХД в изолированный сегмент

Передача бэкапов, актуализация

АЙТИБАСТИОН

1. Изолирует системы на физическом уровне. Они остаются невидимыми друг для друга.
2. Реализует автоматизированную передачу данных как одностороннюю, так и двустороннюю с доставкой файлов.
3. Ограничивает количество взаимодействующих систем.
4. Согласование правил между системами.
5. Дополнительная физическая и программная блокировка.


Контроль обхода СКДПУ НТ Шлюз доступа
IDS (head)
СКДПУ НТ Мониторинг и Аналитика
СКДПУ НТ Персональные сейфы
SIEM
AV / Sandbox / DLP
RDP Server
Общий диск для передачи файлов через Синоникс (автоматически)
Передача событий безопасности
Обновление и конфигурация
События удаленного доступа
Централизованное хранение данных УЗ
Журнал событий
ICAP
SFTP/Samba загрузка файлов через Синоникс
RDP/SSH для доступа к PAM
КСПД
Ключ А
Узел
Ядро
Ключ В
Питание
Сбой
Ok
KAV SDK
АЙТИБАСТИОН
ТСПД
Передача событий безопасности
Обновление и конфигурация
SPAN / TAP
События удаленного доступа
RDP/SSH для доступа к ЦУ
Обновление баз и ПО
SFTP/Samba загрузка файлов через Синоникс
RDP Server
IDS (sensor)
СКДПУ НТ Шлюз Доступа
KSC
RDP
Общий диск для передачи файлов через Синоникс (автоматически)

КОНТРОЛЬ ПРИВИЛЕГИРОВАННОГО ДОСТУПА
РАМ-ПЛАТФОРМА СКДПУ НТ

АЙТИБАСТИОН

ШЛЮЗ ДОСТУПА

Контроль сессий,
запись событий доступа,
менеджер паролей,
двухфакторная аутентификация

Портал доступа

Единая точка доступа
к инфраструктуре шлюзов.
Удобная структурированная и
настраиваемая группировка
доступов

КАБИНЕТ ОПЕРАТОРА

Оптимизация управления
целевыми устройствами
и правилами доступа.
Разделение зон ответственности

АГРЕГАТОР ДОСТУПОВ

Автоматизированный перенос
данных авторизаций и политик
доступа к ресурсам из сторонних
систем в структуру Шлюза
доступа

МОНИТОРИНГ И АНАЛИТИКА

Мониторинг, отчетность
и статистика.
Поведенческий анализ
и детектирование аномалий.
Выявление инцидентов
и реагирование на них

АРХИВ АУДИТА

Централизованное хранение,
единая точка доступа и просмотра
видеозаписей
с разных Шлюзов доступа.
Увеличение скорости
расследования инцидентов.
Оптимизация хранения

ПЕРСОНАЛЬНЫЕ СЕЙФЫ

Корпоративный менеджер
секретов. Простой и удобный
способ хранения паролей, ключей
и сертификатов с возможностью
командной работы
с ними

www.it-bastion.com

АЙТИБАСТИОН

Благодарю за внимание!

Родин Константин
заместитель директора
по развитию бизнеса

k.rodin@it-bastion.com

+7 499 322 3667

it-bastion.com

www.it-bastion.com