АЙТИБАСТИОН

АЙТИБАСТИОН

РЕШЕНИЕ ЗАДАЧ ИНФОРМАЦИОННОГО ОБМЕНА С ПОМОЩЬЮ СИНЕНИКС НА ПОНЯТНЫХ ПРИМЕРАХ

Гончарова Александра
Инженер поддержки продаж

АЙТИБАСТИОН

2014

ОСНОВАНИЕ КОМПАНИИ

10 лет на российском рынке информационной безопасности

300+

ПАРТНЕРОВ-ИНТЕГРАТОРОВ

Интеграции с компаниями, позволяющие выполнить квалифицированную помощь в реализации защиты инфраструктуры

250+

ЗАКАЗЧИКОВ И ПРОЕКТОВ

Присутствие во всех отраслях: от нефтяных компаний до футбольных клубов,
от небольших инфраструктур до геораспределенных площадок

АЙТИБАСТИОН

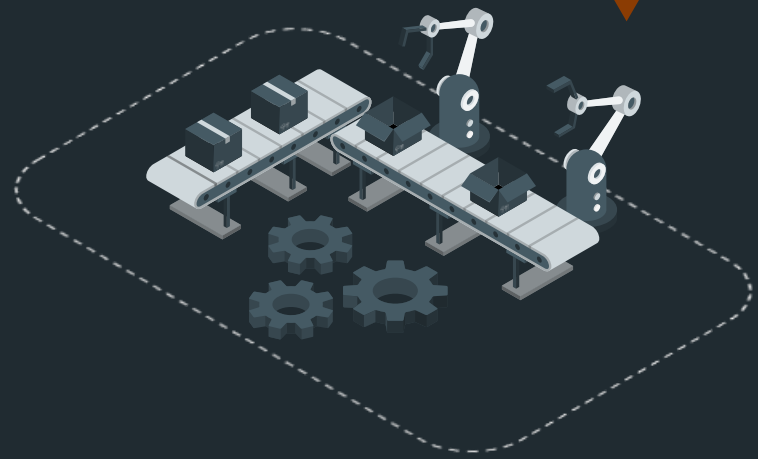
49,7 %

Рост российского рынка АСУ ТП в 2024 г.

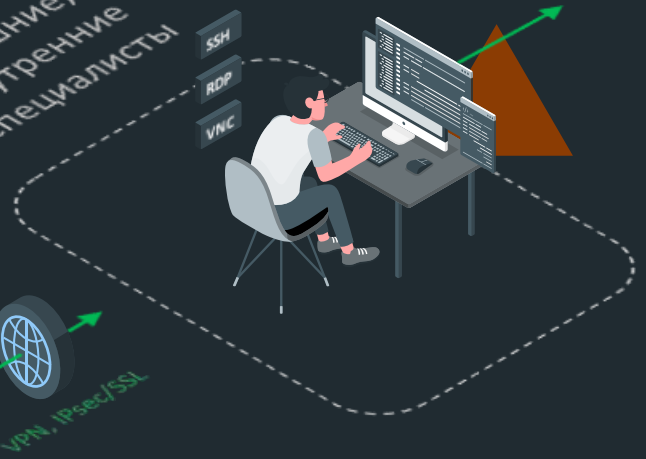
АЙТИБАСТИОН

1. Использование вредоносного программного обеспечения
2. Изменение статусов устройства АСУ ТП
3. Эксплуатация уязвимостей
4. Вмешательство в процесс загрузки и выгрузки файлов АСУ ТП
5. Компрометации учетных данных
6. Социальная инженерия

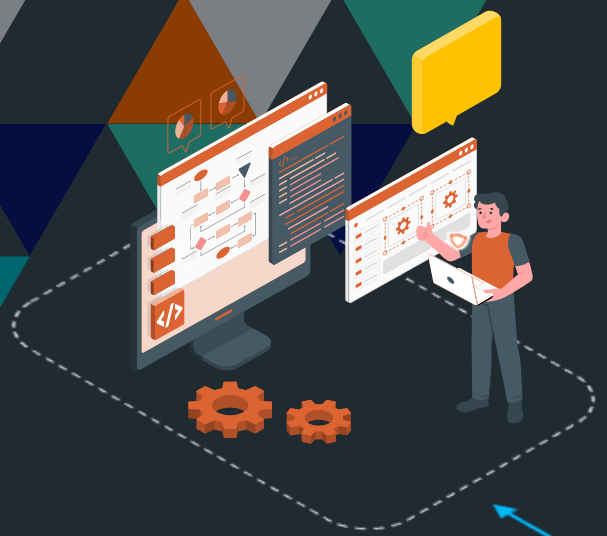
АЙТИБАСТИОН



Внешние, внутренние специалисты



АЙТИБАСТИОН



Передача в контур

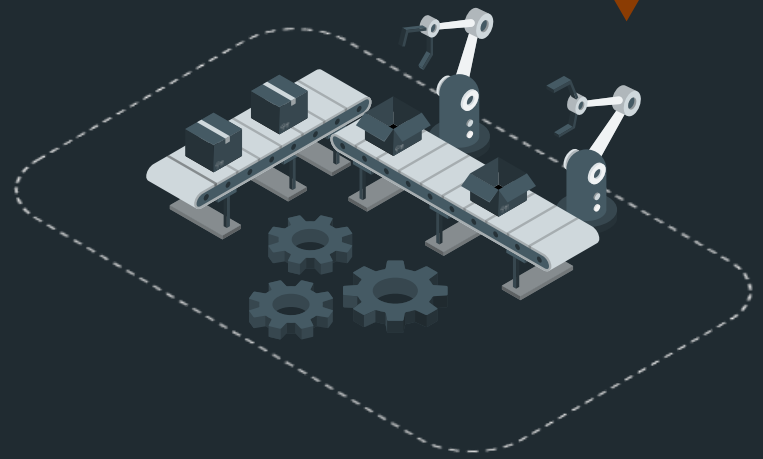
Обновление

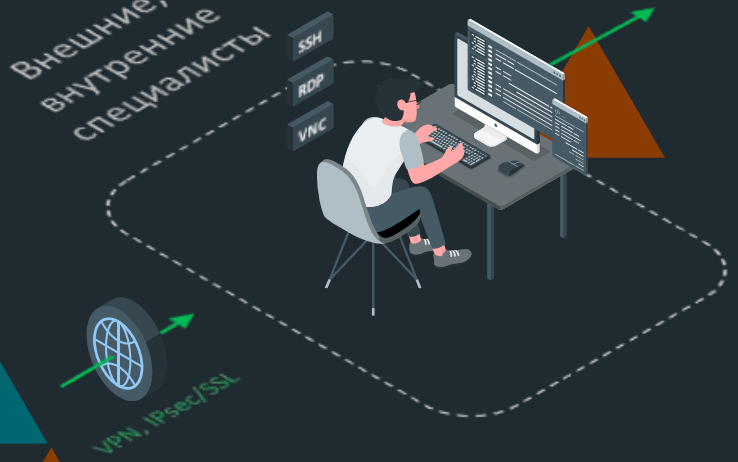
Настройка

Базы

Файлы

Иные данные





АЙТИБАСТИОН

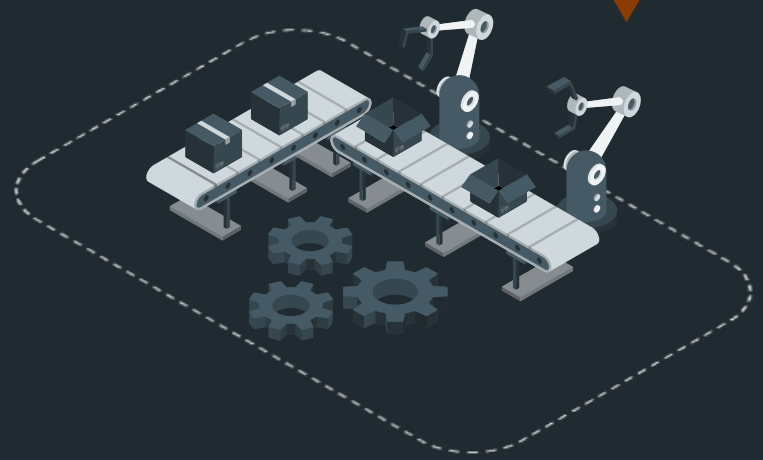
Передача из контура

Телеметрия

Логи

Базы

Иные данные



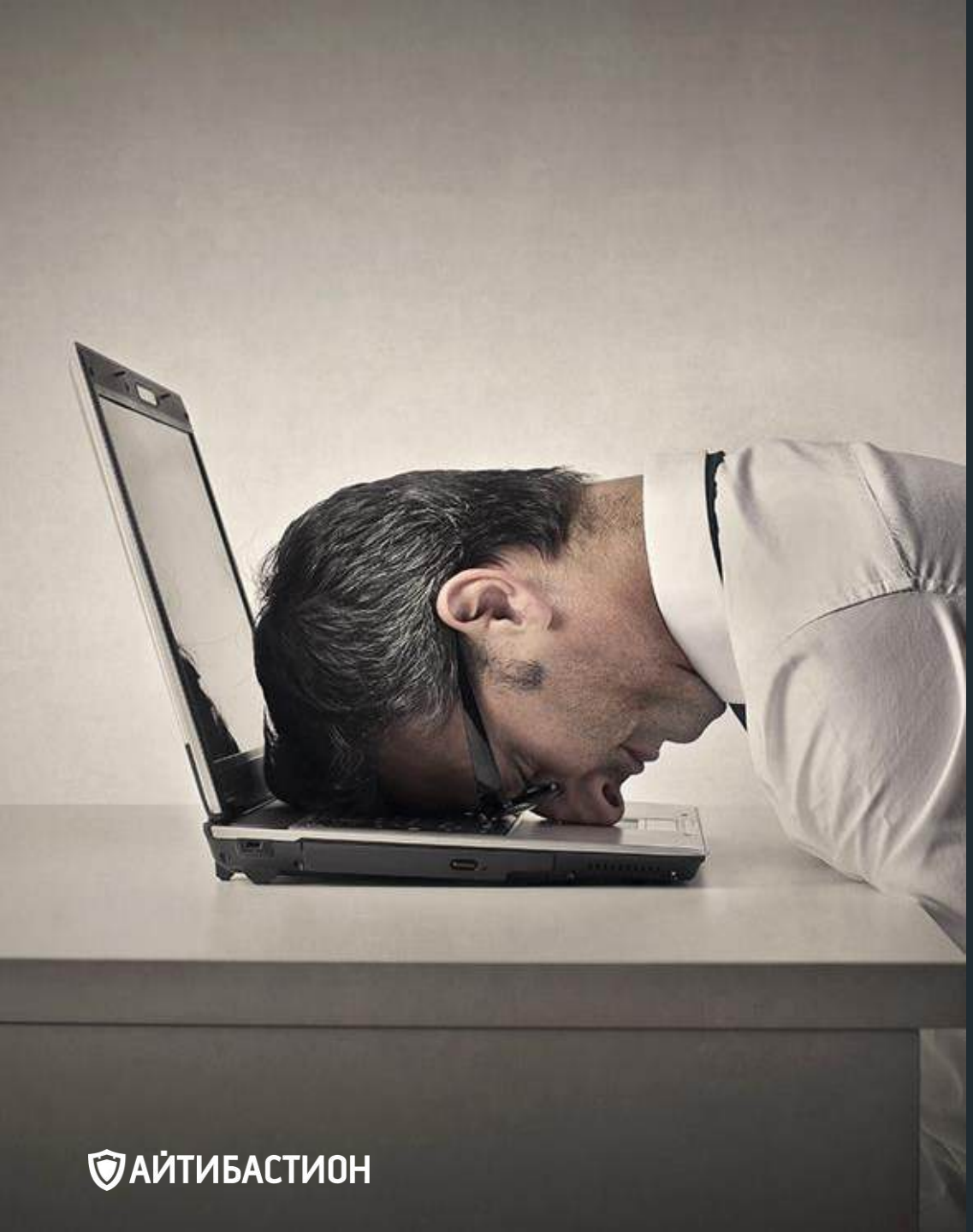
Внешние, внутренние специалисты

SSH

RDP

VNC

VPN, IPsec/SSL

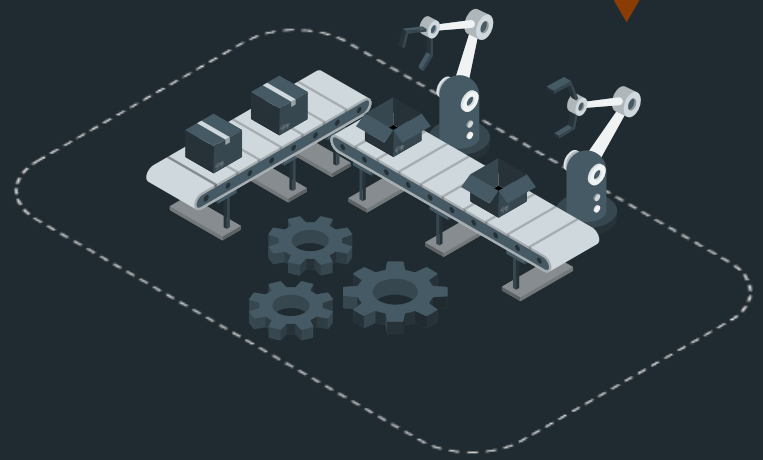


АЙТИБАСТИОН

- ТРУДОЗАТРАТЫ
- ВРЕМЯ
- АКТУАЛЬНОСТЬ
- БЕЗОПАСНОСТЬ

www.it-bastion.com

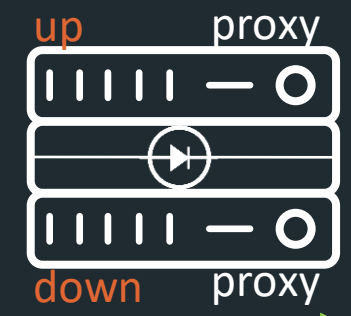
АЙТИБАСТИОН

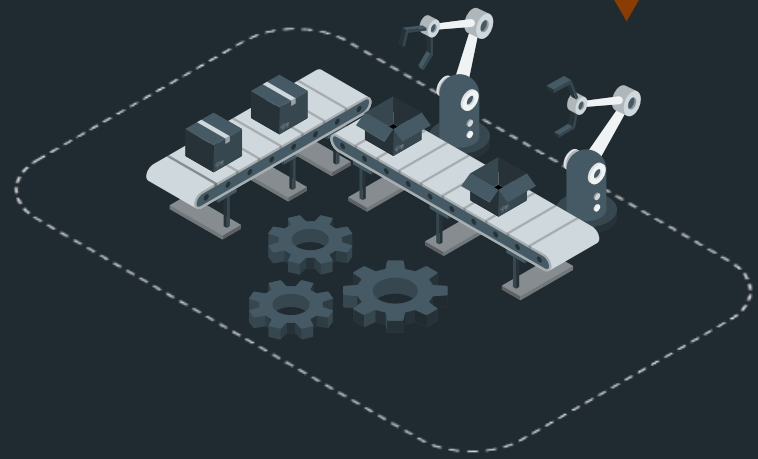


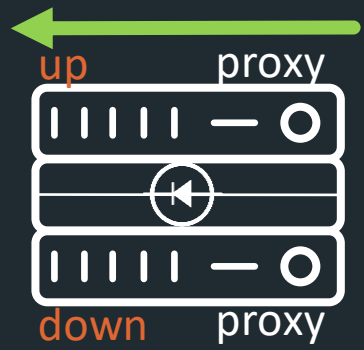
Внешние, внутренние специалисты

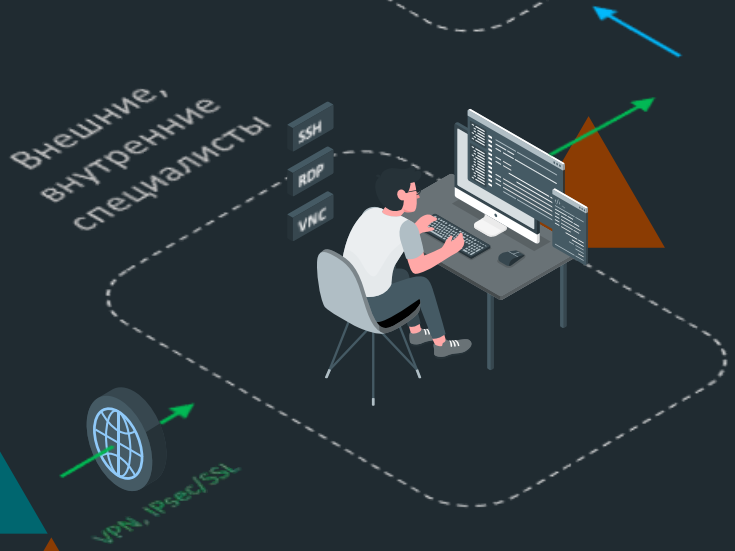
VPN, IPsec/SSL

АЙТИБАСТИОН



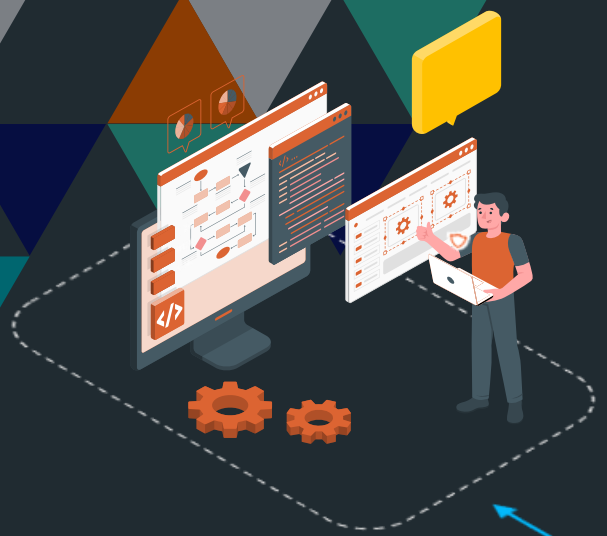


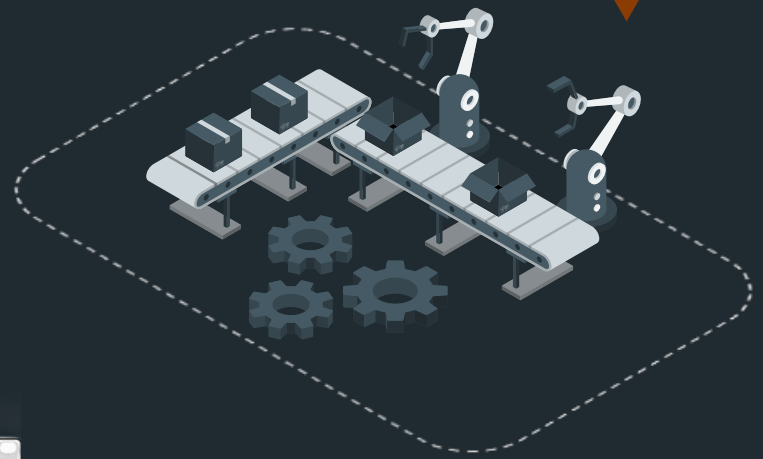




TCP?

АЙТИБАСТИОН





Узел А

Ядро

Узел Б

Внешние, внутренние специалисты

SSH

RDP

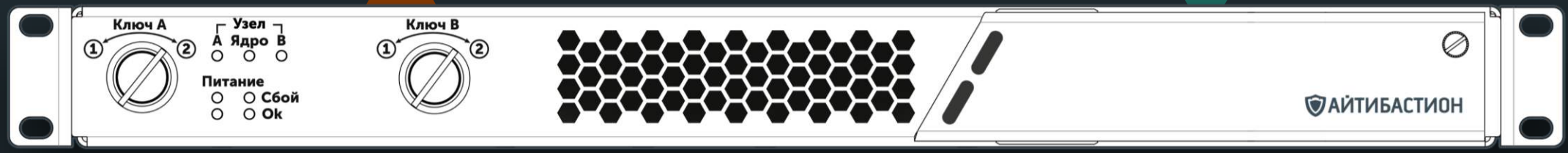
VNC

VPN, IPsec/SSL

АЙТИБАСТИОН

Система контроля информационного обмена

Позволяет организовать безопасный обмен информацией между узлами одной системы или разными системами, предотвращая распространение киберугроз и вредоносного взаимодействия между ними.



АЙТИБАСТИОН

ПЕРЕДАЧА ДАННЫХ

Передача данных между изначально ИЗОЛИРОВАННЫМИ системами со встроенной защитой от атак транспортного уровня

- TCP, UDP, в т.ч. Однонаправленная
- Независимые политики для двух контуров
- Физическая блокировка передачи данных
- Скорость до 1 Гб/с

ПЕРЕДАЧА ФАЙЛОВ

Передача файлов между изначально ИЗОЛИРОВАННЫМИ системами проверкой этих файлов на соответствие политикам передачи

- SFTP
- Проверка корректности ЭЦП, размера и маски файлов
- Внешняя валидация по ICAP (DLP, Sandbox, AV и др.)
- Автоматизация процесса доставки файлов

КОМБИНИРОВАННЫЙ РЕЖИМ

АЙТИБАСТИОН

ПРОИЗВОДСТВО

На базе оборудования отечественного производителя

ОБОРУДОВАНИЕ

Архитектура x86-64
Диск 128 ГБ
Форм-фактор 1U
ОС AstraLinux 1.7 SE

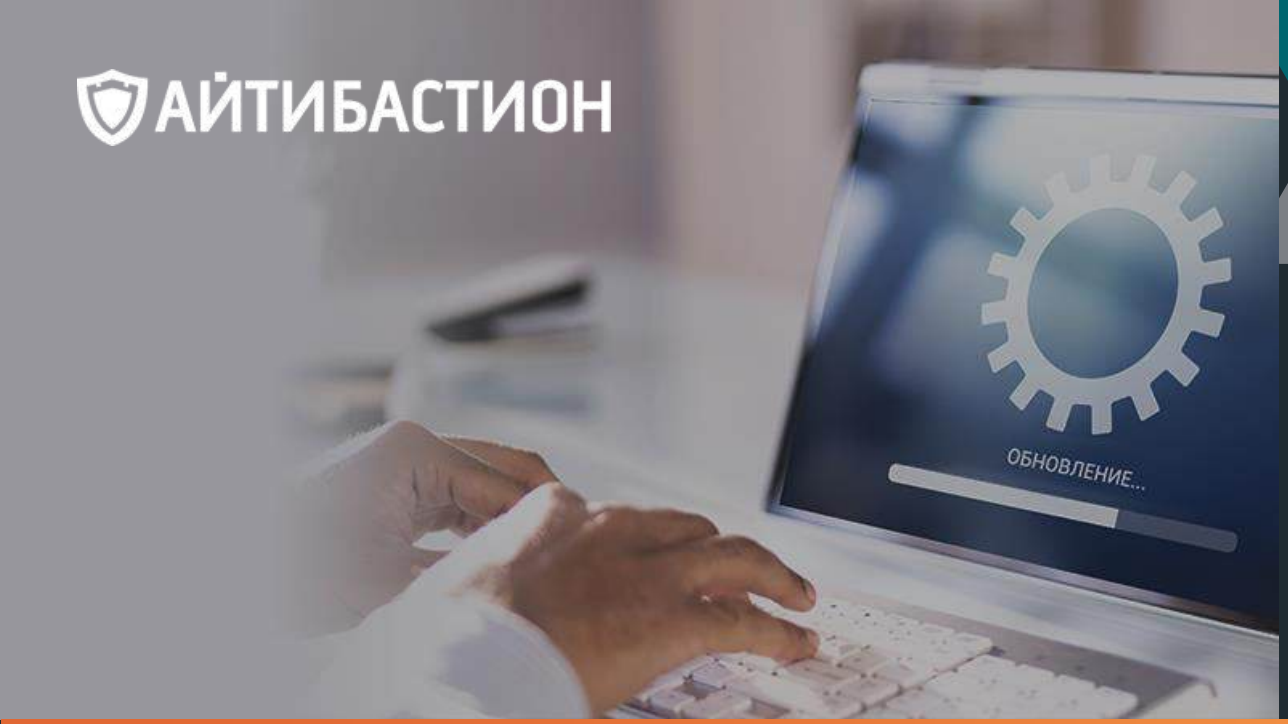
КОНТРОЛЬ

Дополнительная физическая блокировка

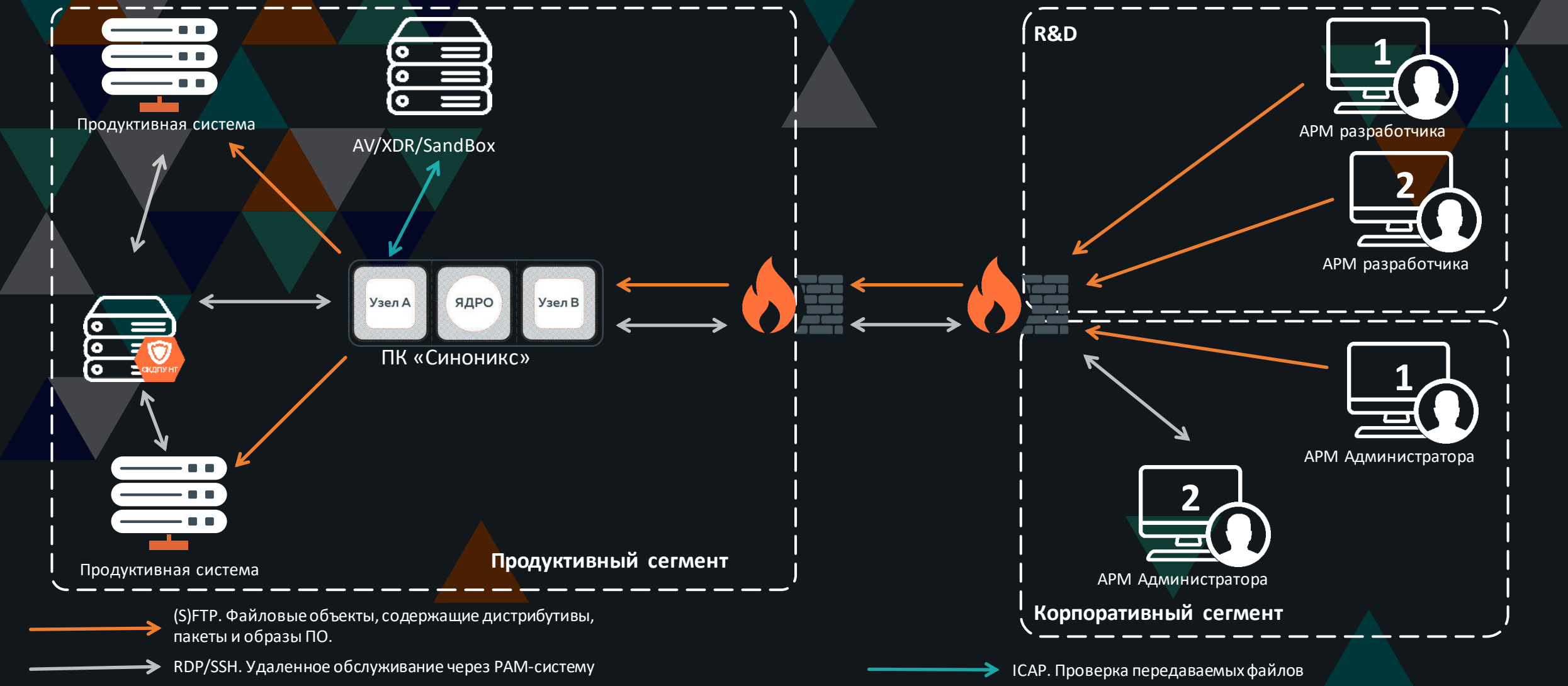
СКОРОСТЬ

до 1 Гб/с
до 256 каналов

АЙТИБАСТИОН

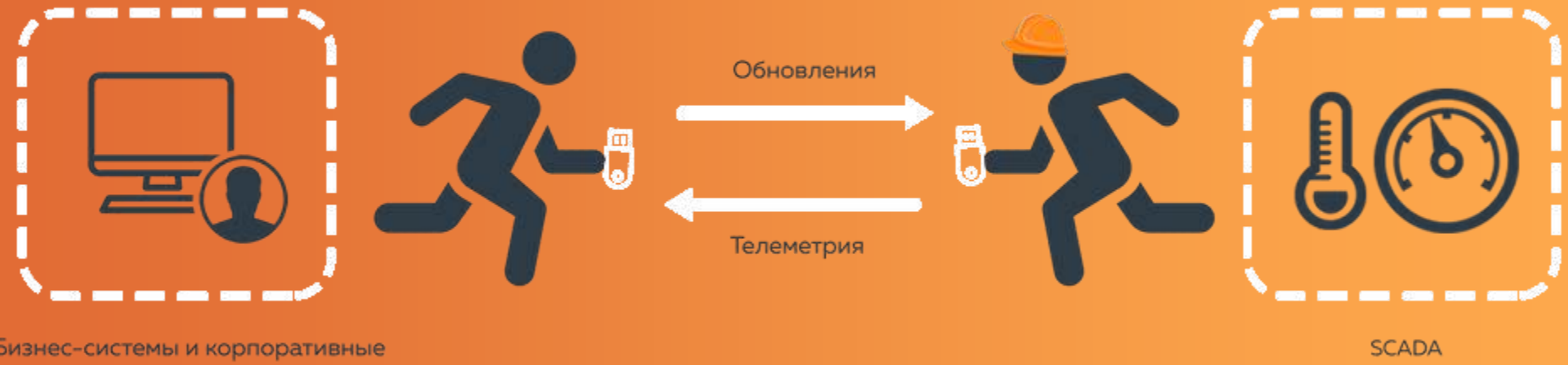


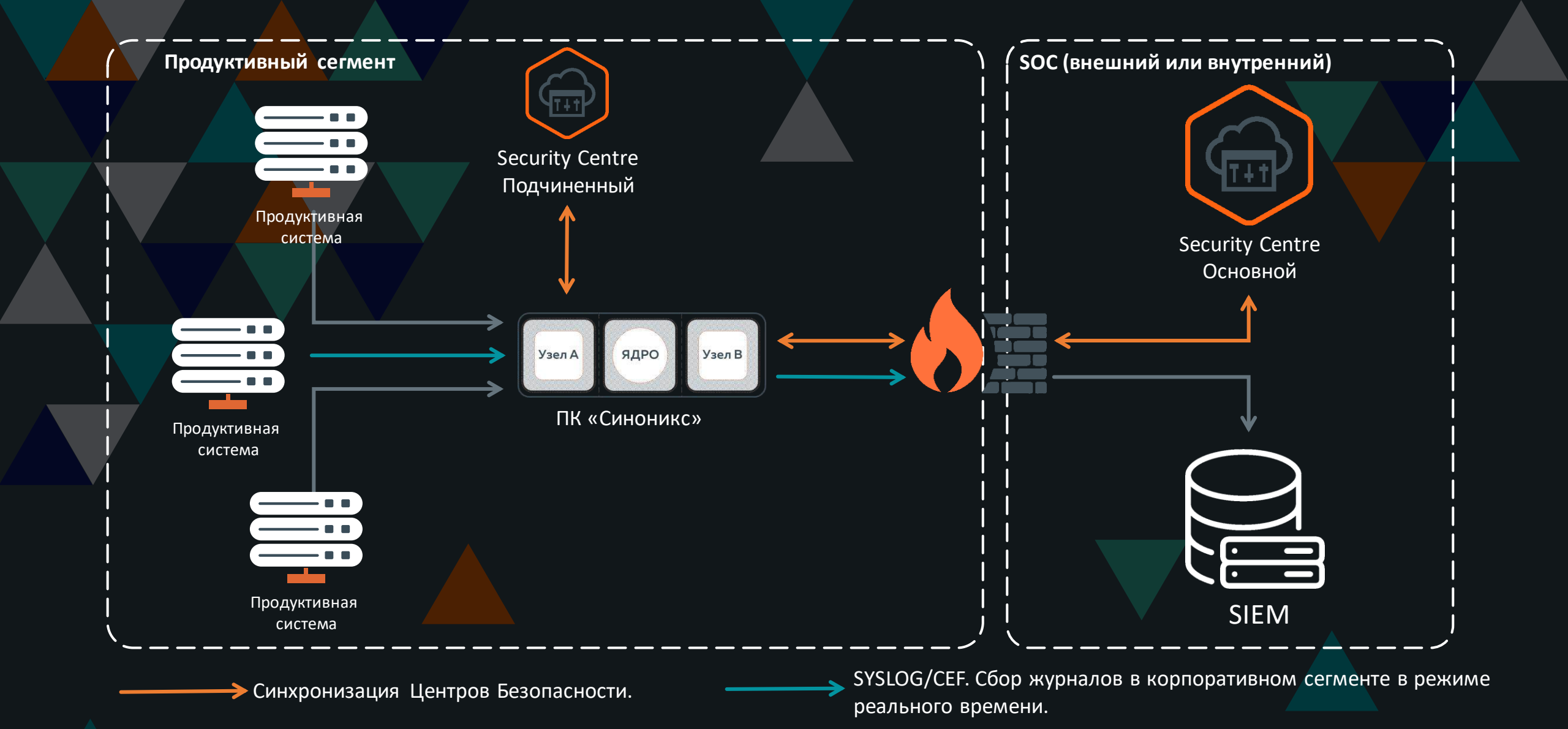
Обновление баз АВЗ в изолированных системах



После тестирования нового ПО **разработчики** могут в **передать файлы обновления** в продуктивный сегмент. Администраторы могут передавать загруженные от вендоров и интеграторов **дистрибутивы** обновлений. В процессе передачи файлы проходят различные проверки, в том числе по ICAP о внешние системы. После загрузки обновлений возможна **организация сеансов администрирования** через **PAM**-систему для установки обновлений и других операций, связанных с обслуживанием продуктивных систем.

Передача данных из изолированных систем





Сбор журналов с необходимых систем в продуктивном сегменте производится через **однонаправленные соединения**. Двусторонний канал организован **для синхронизации** основного и подчиненного центров безопасности для **управления всей инфраструктурой** из центральной консоли, а **также передачи обновлений** на подчиненный центр, откуда будут обновляться версии ПО и сигнатуры клиентов, работающих на конечных машинах.

АЙТИБАСТИОН

Система А

192.168.xx.xx

Приложения

Приложения

Приложения

TCP

UDP

IP

MAC

ETHERNET

Блок передачи данных

TCP

UDP

IP

MAC

ETHERNET

Система В

10.0.xx.xx

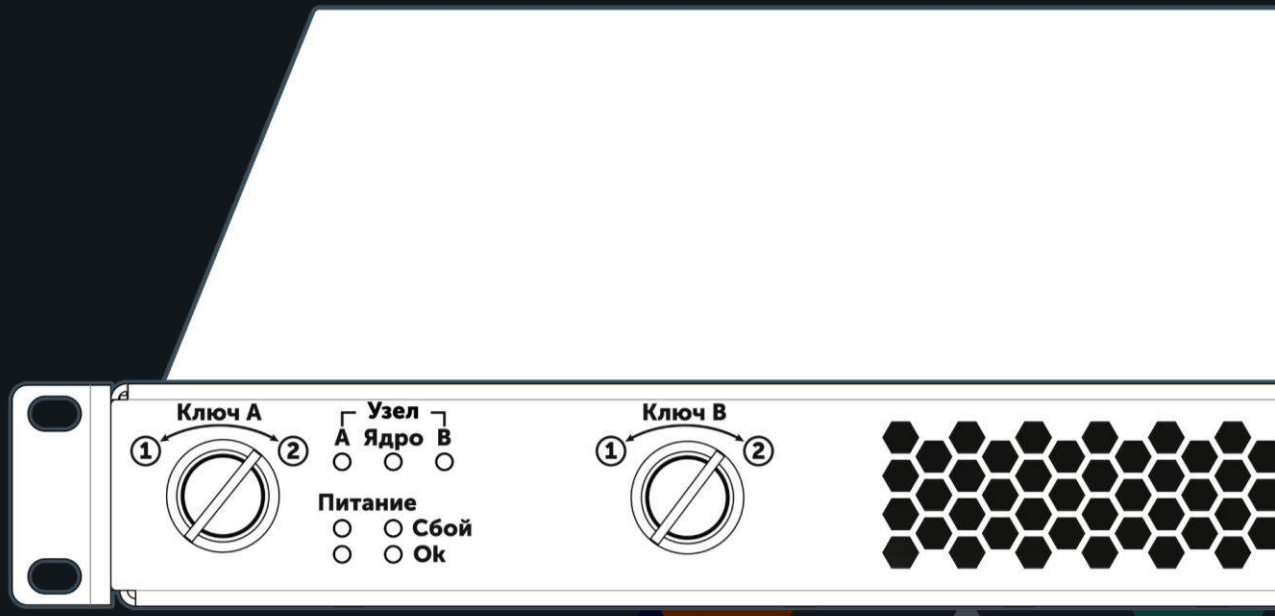
Я Ваня
Здесь правила задаю я

Я Петя
Здесь правила мои
(и я не очень доверяю Ване)

АЙТИБАСТИОН

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.



АЙТИБАСТИОН

• Изолирует системы на физическом уровне. Они остаются невидимыми друг для друга.

• Ограничивает количество взаимодействующих систем.

• Реализует автоматизированную передачу данных как одностороннюю, так и двустороннюю.

• Согласование правил между системами.

• Дополнительная физическая блокировка.

АЙТИБАСТИОН

Антивирусы

kaspersky

Dr.WEB

МЭ/NGFW

КОД безопасности

UserGate

с•терра®

DLP

INFOWATCH®

SOLAR

и другие решения

АЙТИБАСТИОН

Благодарю за внимание!

Гончарова Александра

a.goncharova@it-bastion.com

+7 499 322 3667

it-bastion.com