АЙТИБАСТИОН

СЛОЖНОЕ ПРОСТО:
АВТОМАТИЗАЦИЯ ТИПОВЫХ ЗАДАЧ ОБЪЕКТОВ АСУ ТП С ТОЧКИ ЗРЕНИЯ ИБ

КОНСТАНТИН РОДИН
руководитель отдела
развития продуктов

Как взаимодействуют ваши сети?

Как взаимодействуют ваши сети?

Как передаются данные?

Как взаимодействуют ваши сети?

Как передаются данные?

Процесс удобен или «какой есть»?

АНОНИМНЫЙ ОПРОС

АЙТИБАСТИОН

https://clck.ru/39NHaD

www.it-bastion.com

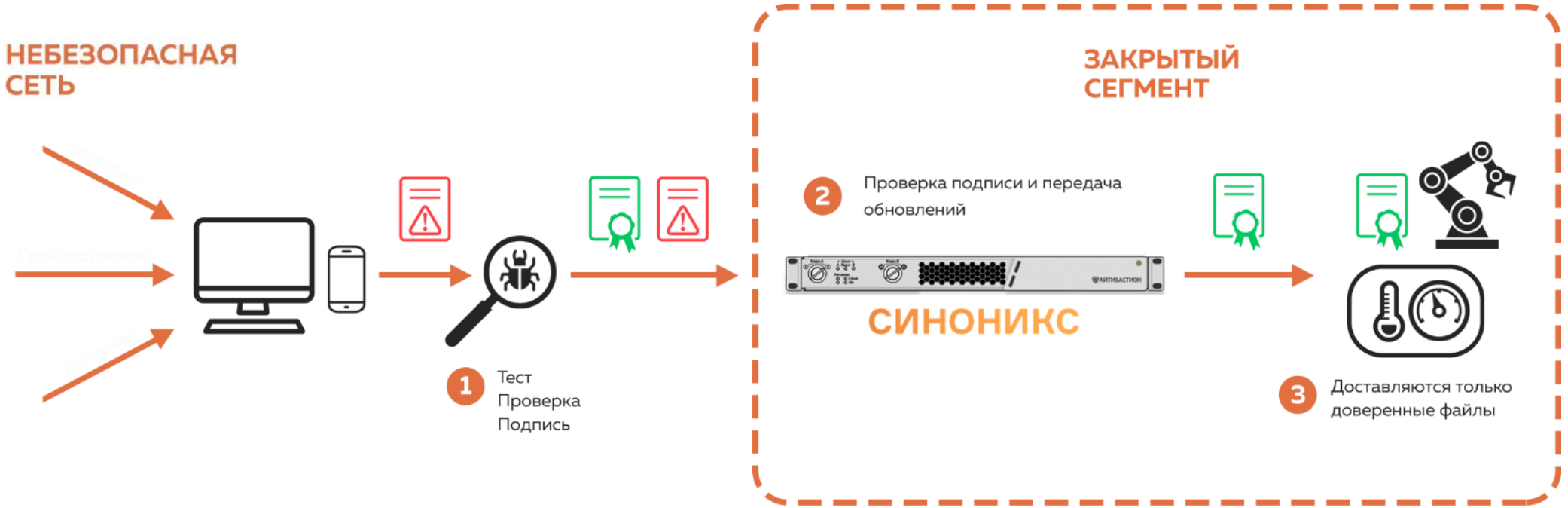
«КУРЬЕРСКИЙ» ОБМЕН ФАЙЛАМИ

АЙТИБАСТИОН

- «Человек с флешкой»
- Один компьютер с двумя сетевыми
- Что-то своё…

АВТОМАТИЗИРОВАННЫЙ ОБМЕН ФАЙЛАМИ

АЙТИБАСТИОН

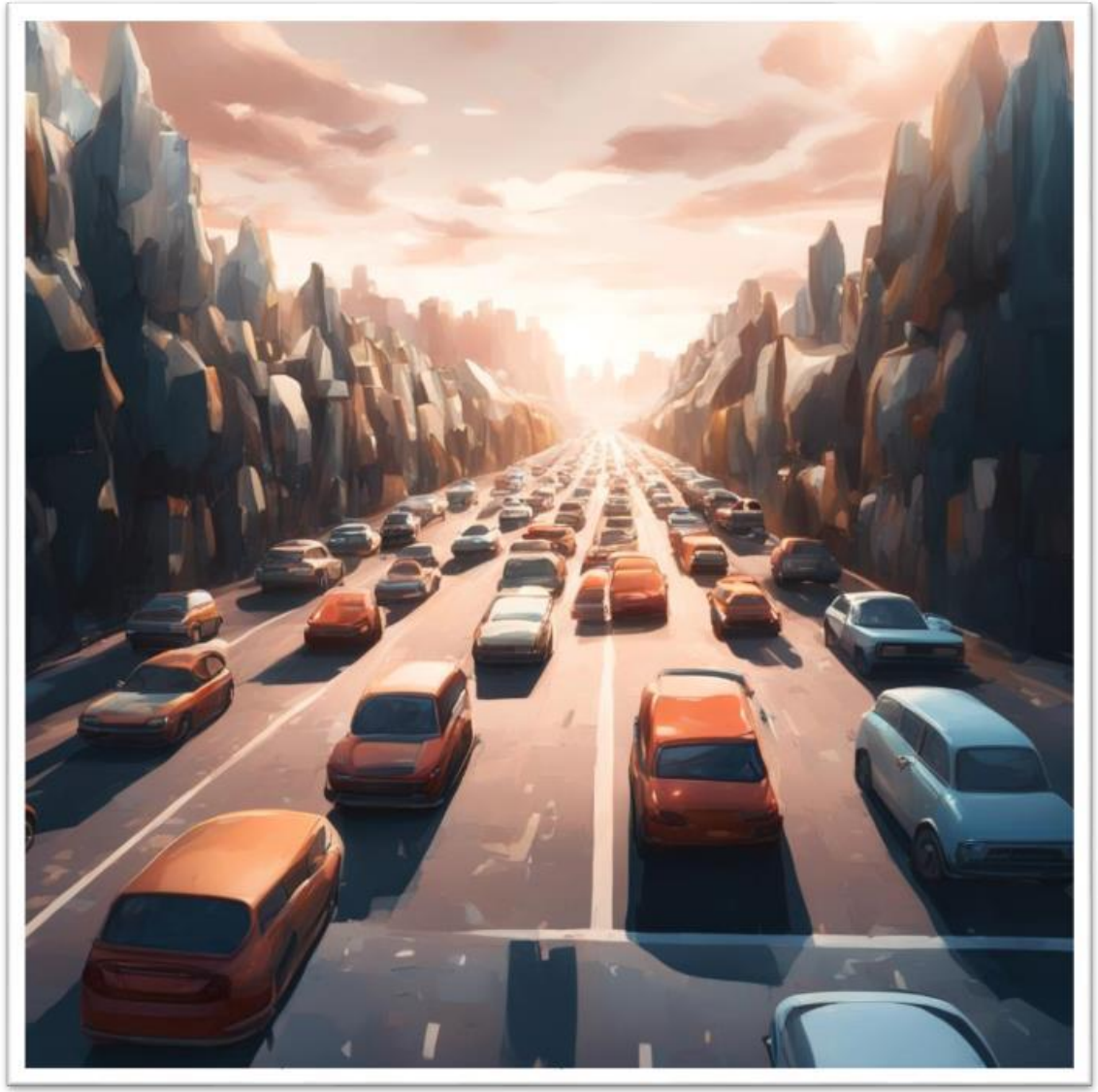


- Протокол обмена – SFTP
- Выбор направления передачи и «встречная» проверка объекта
- Проверка маски, ЭЦП
- Интеграция с ICAP-сервисами (DLP, Sandbox, AV и др.)

ПЕРЕДАЧА ДАННЫХ
ИЗ ИЗОЛИРОВАННОГО СЕГМЕНТА

АЙТИБАСТИОН

- «Стопка» NGFW
- «Стопка» диодов данных
- «Включили и выключили»



www.it-bastion.com

СЕГМЕНТАЦИЯ И КОНТРОЛЬ ПЕРЕДАЧИ ДАННЫХ ИЗ ИЗОЛИРОВАННОГО СЕГМЕНТА

АЙТИБАСТИОН

- TCP, UDP, в т.ч. однонаправленная
- Независимые политики для 2-х контуров
- Нейтрализация сетевых атак за счет «пересборки» пакетов
- Отсутствие прямой сетевой связности
- Скорость до 1 Гб/с
- Поддержка работы с МЭ, NGFW и другим сетевым оборудованием

ЖИВЫЕ ПРИМЕРЫ ИСПОЛЬЗОВАНИЯ СИНОНИКС

АЙТИБАСТИОН

1. Сбор данных производственной информации Historian из сегмента АСУ ТП

2. Синхронизация системного времени в сегменте АСУ ТП

3. Доступ к серверу корпоративных лицензий ПО на АРМ и серверах в сегменте АСУ ТП

4. Безопасный обмен между серверами Kaspersky Security Center

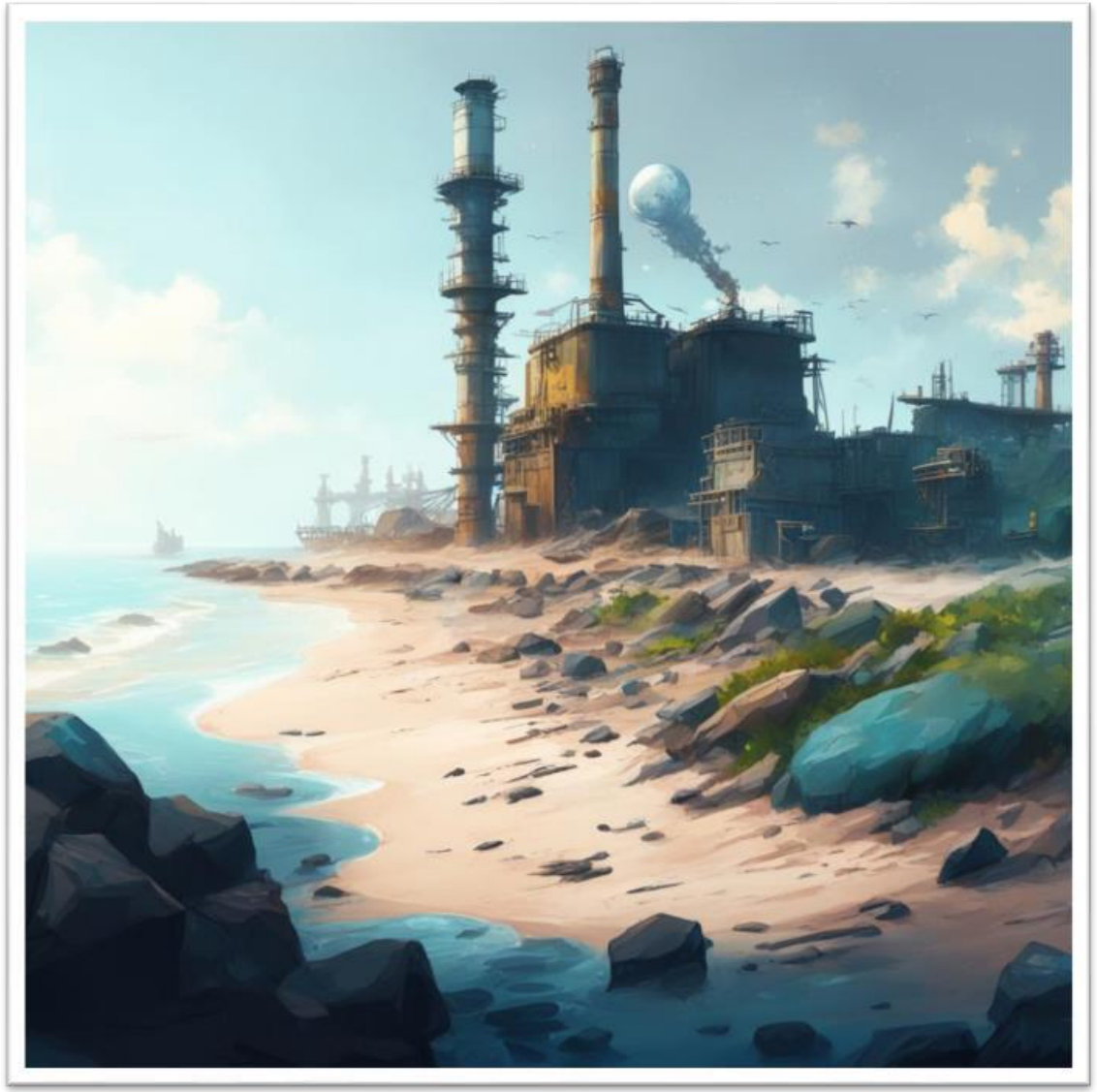
ЖИВЫЕ ПРИМЕРЫ ИСПОЛЬЗОВАНИЯ СИНОНИКС

АЙТИБАСТИОН

1. Передача событий в PT MaxPatrol SIEM от Kaspersky ICS, PT ISIM и ИС АСУ ТП

2. Передача обновлений и прошивок в закрытый сегмент сети с автоматической проверкой в Kaspersky ScanEngine

3. Доступ привилегированного персонала к объекту через СКДПУ НТ

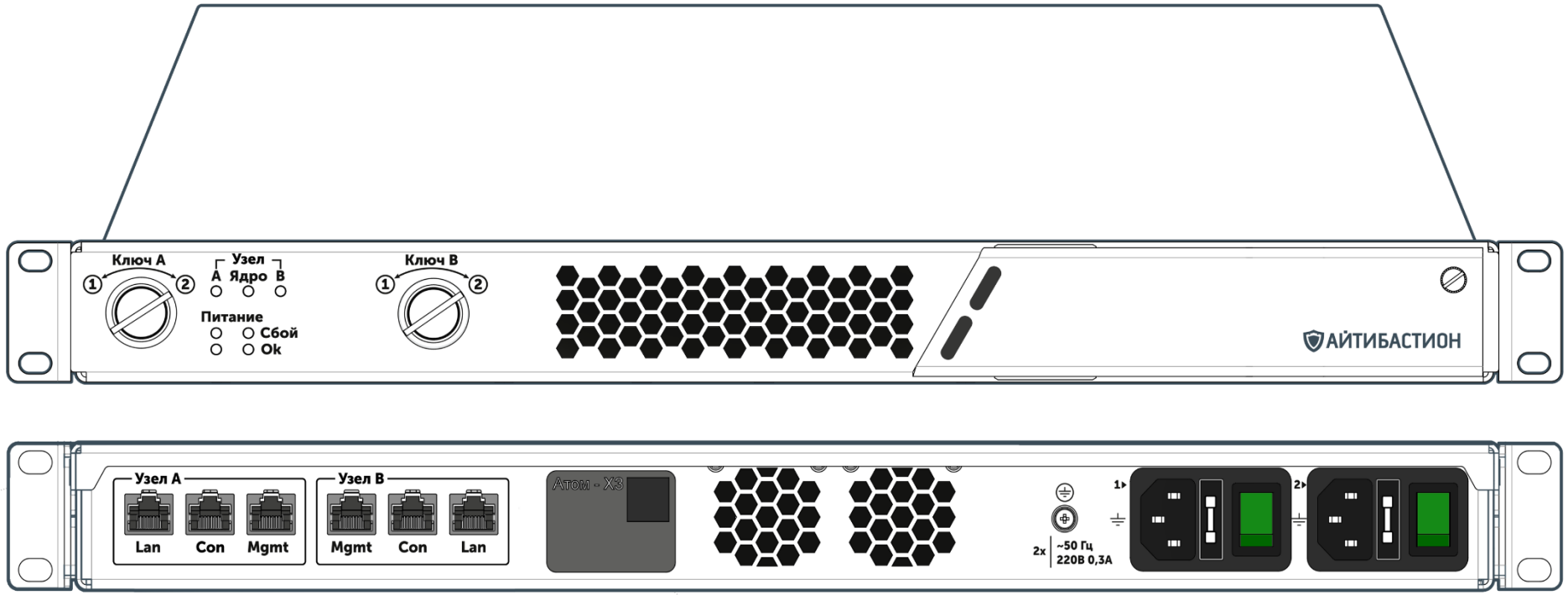


www.it-bastion.com

ШЛЮЗ БЕЗОПАСНОГО ОБЪЕДИНЕНИЯ СЕТЕЙ СИНОНИКС

АЙТИБАСТИОН

Синоникс - шлюз безопасного объединения изолированных сетей, который позволяет передавать данные и файлы между ними, при этом сохраняя безопасность каждого из объединяемых сегментов и обеспечивая сокрытие данных об их архитектуре.



ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ
ПАК СИНОНИКС

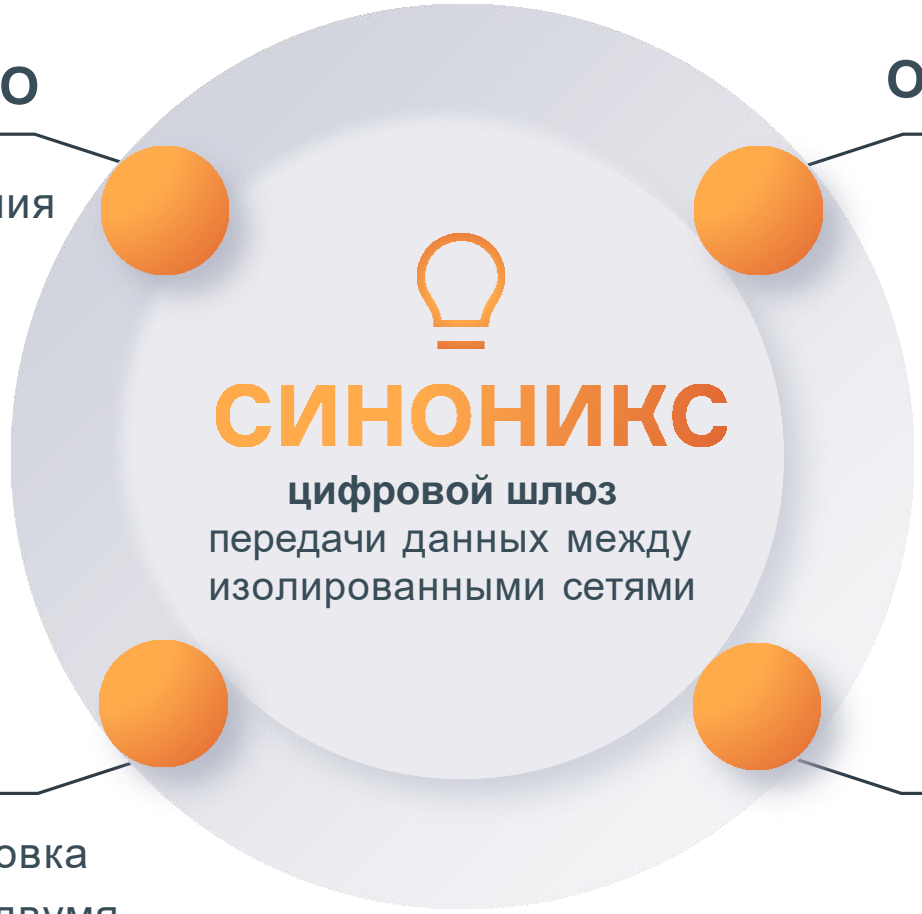
АЙТИБАСТИОН

ПРОИЗВОДСТВО

На базе оборудования отечественного производства

ОБОРУДОВАНИЕ

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



КОНТРОЛЬ

Физическая блокировка работы устройства двумя «пусковыми» ключами

СКОРОСТЬ

до 1 Гб/с

КЛЮЧЕВЫЕ ЗАДАЧИ СИНОНИКС

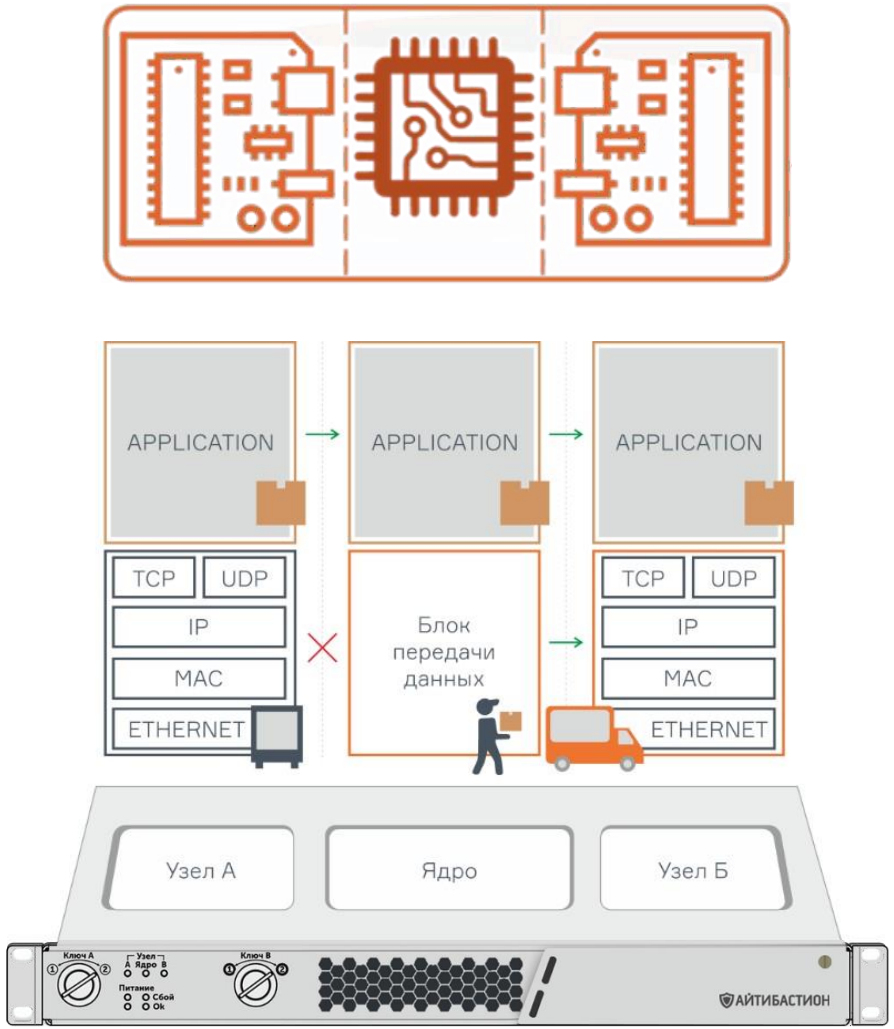
АЙТИБАСТИОН

Изоляция сетей на физическом уровне

Передача данных **в режиме «точка-точка»** как в одну, так и в обе стороны по протоколам TCP и UDP **с сохранением «воздушного зазора»**

Валидация файлов при передаче

Встроенный файловый шлюз, реализующий проверки маски, размера, **ЭЦП объектов** с возможностью внешней **валидации по ICAP** (AV, Sandbox, DLP и др.)



КЛЮЧЕВЫЕ ЗАДАЧИ СИНОНИКС

АЙТИБАСТИОН

Разграничение зон ответственности

Разделение интерфейсов управления между двумя ответственными для подтверждения прохождения данных.

Несогласованные с обоих сторон **правила игнорируются**

Физический контроль передачи

Физическая блокировка передачи «пусковыми» ключами, возможность запрета удаленного управления с доступом к **конфигурированию** только **через консоль RS-232**

СИНОНИКС
ТЕХНОЛОГИЧЕСКИЕ ПАРТНЕРЫ

АЙТИБАСТИОН

Антивирусы

kaspersky

Dr.WEB

МЭ/NGFW

КОД безопасности

UserGate

с•терра®

DLP

INFOWATCH®

SOLAR

и другие решения

www.it-bastion.com

Как взаимодействуют ваши сети?

Как передаются данные?

Процесс удобен или «какой есть»?

Спасибо за внимание!

АЙТИБАСТИОН

Константин Родин
Руководитель отдела развития продуктов

k.rodin@it-bastion.com

+7 916 560 50 66

it-bastion.com