АЙТИБАСТИОН

www.it-bastion.com

2025

ЕСТЬ ЛИ УДАЛЕННЫЙ ДОСТУП В АСУ ТП?
КОНТРОЛЬ ДОСТУПА С ИСПОЛЬЗОВАНИЕМ СКДПУ НТ И ИЗОЛЯЦИЯ ЧЕРЕЗ ПК «СИНОНИКС»

Алексей Ширикалов

www.it-bastion.com

КОМПАНИЯ
АЙТИ БАСТИОН

АЙТИБАСТИОН

2014

300+

250+

>70%

ОСНОВАНИЕ КОМПАНИИ
10 лет на российском рынке информационной безопасности

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

ЗАКАЗЧИКОВ И ПРОЕКТОВ
Присутствие во всех отраслях от нефтяных компаний до футбольных клубов, от небольших офисов до георасределенных площадок

РАМ-РЫНКА РФ
Комплекс СКДПУ НТ решение, проверенное «в боях» и доказавшее свою эффективность, надежность и качество

ЕСТЬ ЛИ УДАЛЕННЫЙ ДОСТУП В АСУ ТП?

www.it-bastion.com

ЕСТЬ ЛИ УДАЛЕННЫЙ ДОСТУП В АСУ ТП?

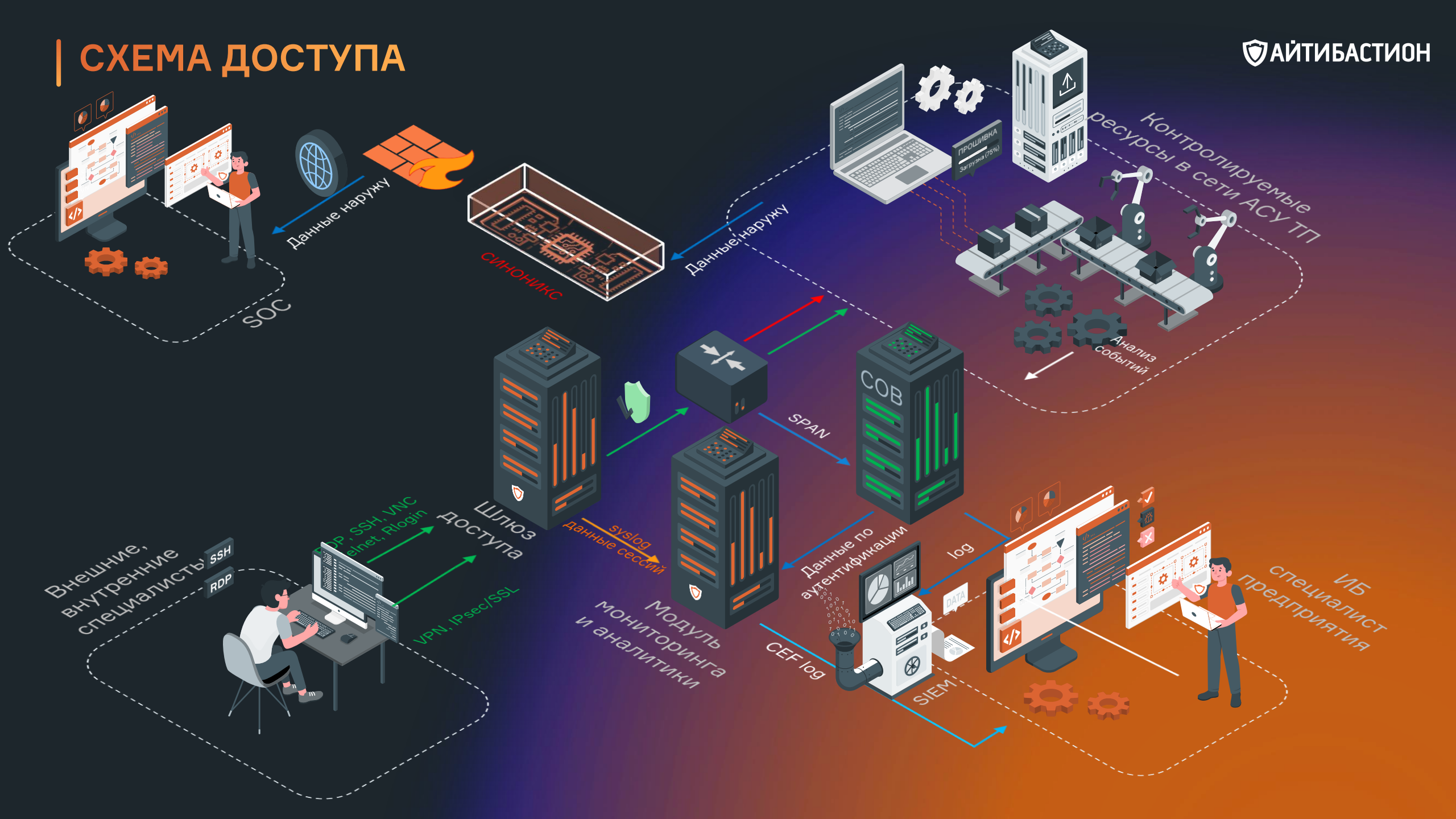
НЕТ!

СПАСИБО ЗА ВНИМАНИЕ!

www.it-bastion.com

СХЕМА ДОСТУПА

АЙТИБАСТИОН



ЧТО ТАКОЕ РАМ?

www.it-bastion.com

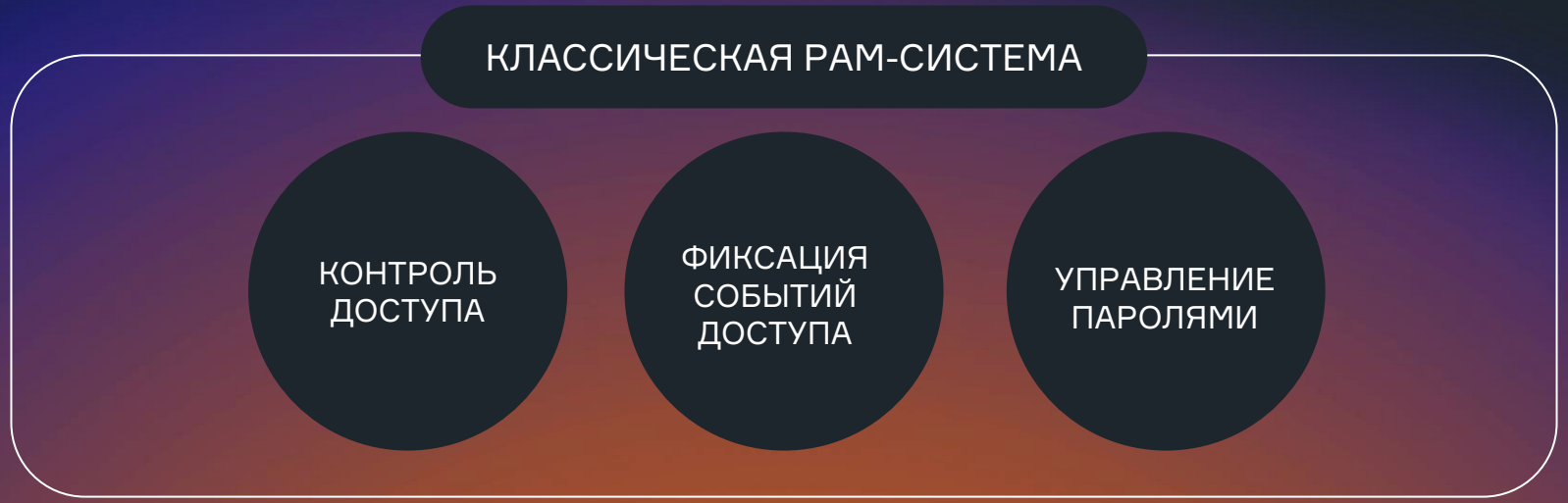
ЧТО ТАКОЕ PAM?

АЙТИБАСТИОН

Privileged Access Management (PAM) – Решение для отслеживания, обнаружения, предотвращения и расследования несанкционированного привилегированного доступа к критически важным ресурсам, которое тем самым помогает защитить организации от киберугроз

ПАМ В 2025 ЭТО:

АЙТИБАСТИОН



СКОПУ НТ

www.it-bastion.com

ПАМ В 2025 ЭТО:

АЙТИБАСТИОН

- РАСШИРЕННЫЙ КОНТРОЛЬ ДОСТУПА
- НЕПРЕРЫВНЫЙ МОНИТОИНГ
- УПРАВЛЕНИЕ СЕКРЕТАМИ И ИХ ХРАНЕНИЕ
- ВЫЯВЛЕНИЕ И ОБРАБОТКА ИНЦИДЕНТОВ
- ПОИСК И ВЫЯВЛЕНИЕ АНОМАЛИЙ
- РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

КОМПЛЕКСНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ

КЛАССИЧЕСКАЯ PAM-СИСТЕМА

- КОНТРОЛЬ ДОСТУПА
- ФИКСАЦИЯ СОБЫТИЙ ДОСТУПА
- УПРАВЛЕНИЕ ПАРОЛЯМИ

ОТЕЧЕСТВЕННЫЕ ОС и БД
СОВМЕСТИМОСТЬ С СКДПУ НТ

АЙТИБАСТИОН

1 Базовая ОС и БД

СКДПУ НТ работает под управлением ОС **Astra Linux SE** и БД **Postgres**

2 Совместимые ОС

СКДПУ НТ поддерживает работы с ОС **РедОС**, **Альт Линукс**, **Роса** и др. при использовании их в качестве пользовательской и целевой систем

3 Отсутствие агентов

СКДПУ НТ не требует установки агентов ни на АРМы пользователей, ни на целевые ресурсы

4 Формат поставки

СКДПУ НТ может поставляться как в формате **ПАК** так и в формате образа **виртуальной** машины

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

АЙТИБАСТИОН

Приказ ФСТЭК России
№ 31, № 17, № 21

Приказ ФСТЭК России
№239, №235

СТО БР (ИББС 1.4-2018)
п.6.4. Основное требование 3, п.6.7, п. 9.3

СТО БР (ИББС-1.0-2014)
раздел 7.4.3.

Указ президента РФ
№ 250

ФЗ-187
«О безопасности КИИ РФ»

GDPR и ФЗ 152

ГОСТ Р 57580.1—2017

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

АЙТИБАСТИОН

Включен в реестр отечественного ПО

Сертификат ФСТЭК УД-4

Сертификат МО РФ НДВ-2

РАМ-ПЛАТФОРМА СКДПУ НТ

АЙТИБАСТИОН

Шлюз доступа включает в себя:

- модуль контроля сессий;
- менеджер паролей;
- модуль отказоустойчивости и катастрофоустойчивости.

Мониторинг и аналитика включает в себя:

- модуль мониторинга и отчетности;
- модуль поведенческого анализа, включая детектирование аномалий, инцидентов, реагирование и расширенной статистики

Портал доступа

Кабинет оператора

СКДПУ НТ

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

АЙТИБАСТИОН

ЕДИНАЯ ТОЧКА ДОСТУПА

Единая точка доступа в инфраструктуру (SSO). Гибкая ролевая модель доступов с возможностью интеграции в существующую инфраструктуру (LDAP, AD, Radius)

ЗАПИСЬ СОБЫТИЙ ДОСТУПА

Полная запись видео и метаданных сессий с созданием долгосрочного архива. Клавиатурный ввод, буфер обмена, передача файлов, OCR, элементы интерфейсов, процессы, команды и т.д. А наличие сертификата ФСТЭК по УД-4 гарантирует неизменяемость данных для использовании их в качестве доказательно базы

УПРАВЛЕНИЕ ПАРОЛЯМИ

Управление паролями целевых учетных записей без необходимости установки агентов на целевые устройства по настраиваемым политикам

БЕЗ УСТАНОВКИ АГЕНТОВ

Подключение к ЦУ без необходимости установки агентов, что особенно важно при подключении к объектам КИИ

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

АЙТИБАСТИОН

КОНТРОЛЬ ПРИЛОЖЕНИЙ И УЗ В НИХ

Подключение к конечным приложениям без предоставления полного доступа с сокрытием УЗ от приложений.

ПРОСМОТР И ПРЕРЫВАНИЕ СЕССИЙ

Возможность не только контролировать сессию по её результату, но и видеть все действия в режиме реального времени. А в случае необходимости - блокировать сессию пользователя, предотвращая потенциальную угрозу.

РАБОТА ПО ЗАЯВКАМ С ВОЗМОЖНОСТЬЮ ПОДТВЕРЖДЕНИЯ ДОСТУПА

Возможность предоставления доступа по запросу как в момент подключения, так и заранее. Согласование доступа возможно с добавлением одного и более подтверждающих лиц.

КОНТРОЛЬ НА СТОРОНЕ ИС

Блокировка туннелей, доступа вне разрешенных диапазонов, запрет на запуск процессов и т.д.

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

АЙТИБАСТИОН

ПРОФИЛИРОВАНИЕ И ПОВЕДЕНЧЕСКИЙ АНАЛИЗ

Создание и ведение профилирования пользователей. Анализ всех действий в разрезе «пользователь-цель-действие», машинное обучение и математические модели.

ДЕТЕКТИРОВАНИЕ АНОМАЛИЙ

Предобработка, анализ и детектирование аномального поведения пользователей на основе профилирования и событий

ОТЧЕТЫ И СТАТИСТИКА

Обработка информации и её выдача в виде понятных отчетов от оперативных до сводных, в т.ч. для руководителей.

ОТКАЗОУСТОЙЧИВОСТЬ И МАСШТАБИРОВАНИЕ

Возможность построения действительно отказоустойчивых инсталляций, в т.ч. распределенных между городами и странами. Легкая возможность наращивать мощности как вертикально, так и горизонтально без привязки к территориальному расположению узлов.

СКДПУ НТ ИНТЕГРАЦИИ

АЙТИБАСТИОН

Реализация концепции взаимодополняемых ИТ- и ИБ-систем, где каждая система предоставляет другой профильные данные, обогащая модель событий и предоставляя человеку максимально полный перечень данных для быстрого и точечного реагирования на инциденты

СКДПУ НТ
ТЕХНОЛОГИЧЕСКИЕ ПАРТНЕРЫ

АЙТИБАСТИОН

ASTRA LINUX®

POSITIVE TECHNOLOGIES

kaspersky

INFOWATCH®

Пассворк

Rusiem

GIS
ГАЗИНФОРМ СЕРВИС

ROSA

CyberLympha®

РУТОКЕН

Аладдин

zVirt

alt linux

с•терра®

MULTIFACTOR

UserGate

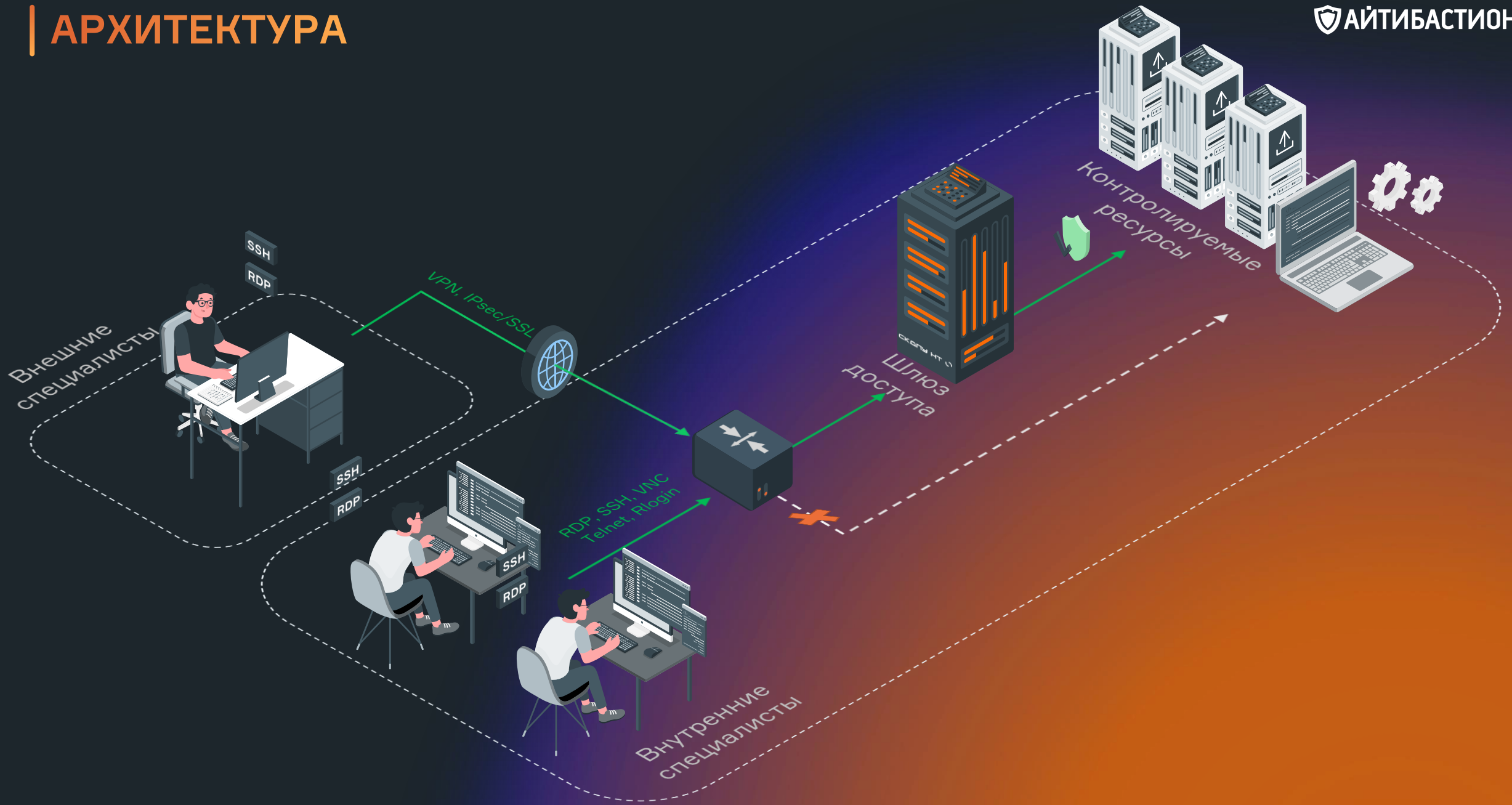
РЕДОС

КОД безопасности

и другие партнеры

АРХИТЕКТУРА

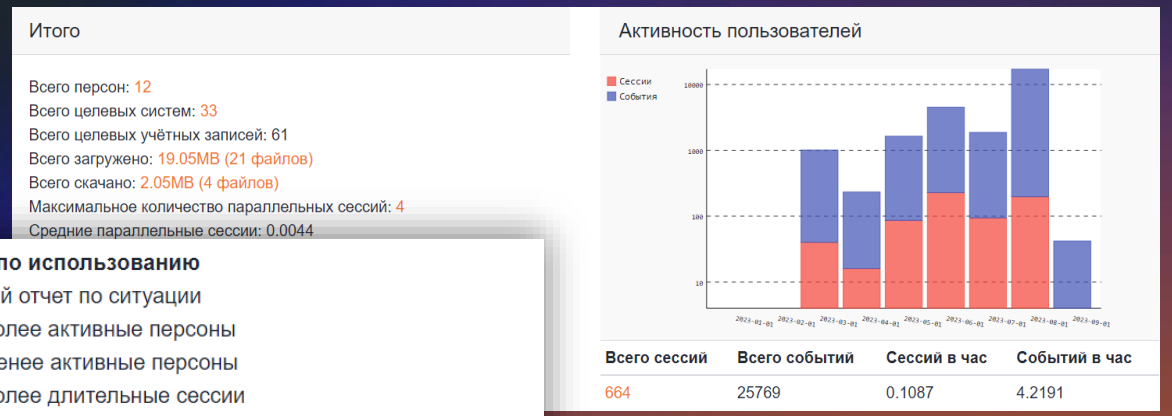
АЙТИБАСТИОН

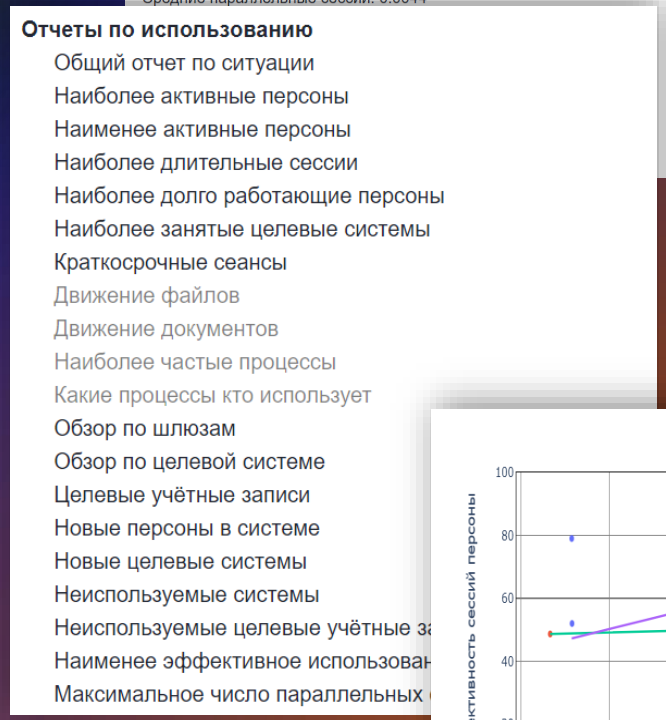


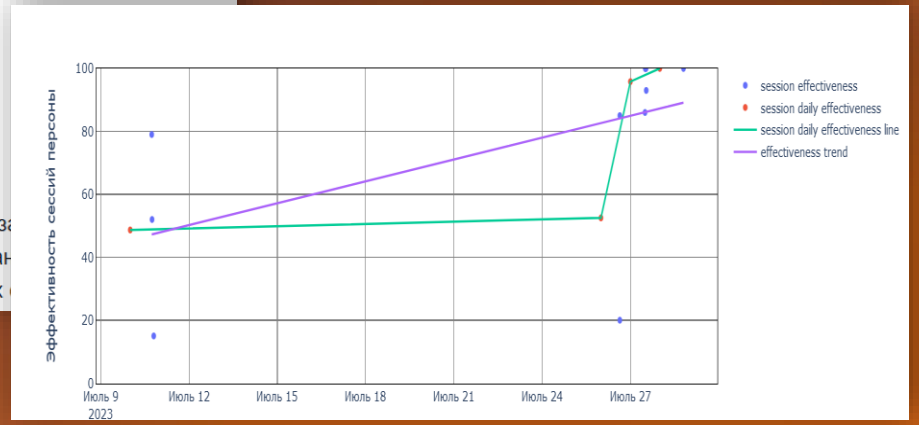
МОНИТОРИНГ И АНАЛИИТКА
РАМ-ПЛАТФОРМЫ СКДПУ НТ

АЙТИБАСТИОН

Система расширенной статистики, анализа и реагирования на потенциальные инциденты информационной безопасности в рамках сессий удаленного подключения.





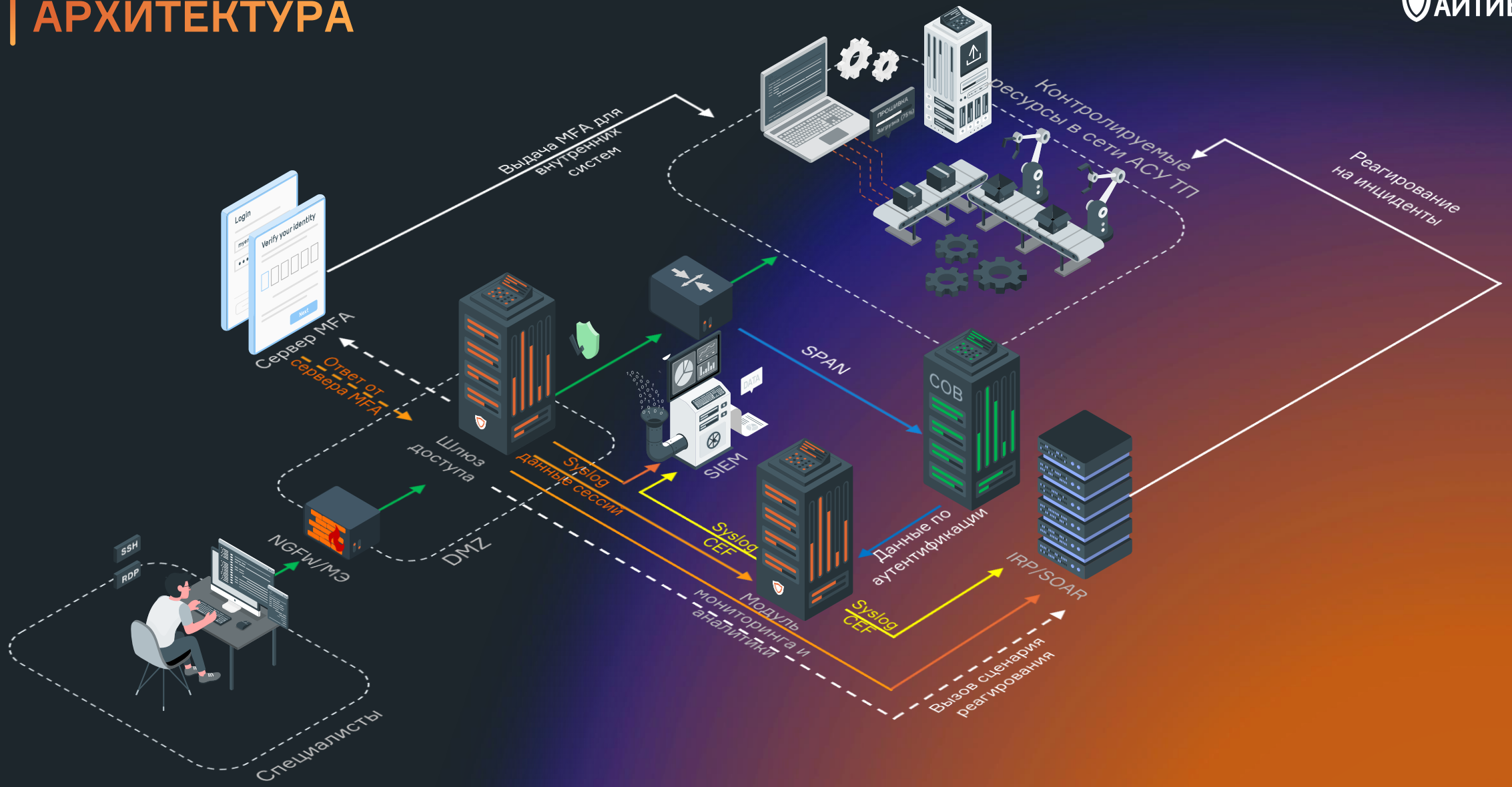


Основные возможности системы

- Мониторинг моно- и мультиинсталляций
- Полнотекстовый поиск
- Профилирование пользователей
- Поведенческий анализ и детектирование аномалий
- Реагирование на инциденты
- Автоматизируемая библиотека отчетности
- Интеграция и обмен информацией с ИТ и ИБ системами в контуре

АРХИТЕКТУРА

АЙТИБАСТИОН



ПОРТАЛ ДОСТУПА
РАМ-ПЛАТФОРМЫ СКДПУ НТ

АЙТИБАСТИОН

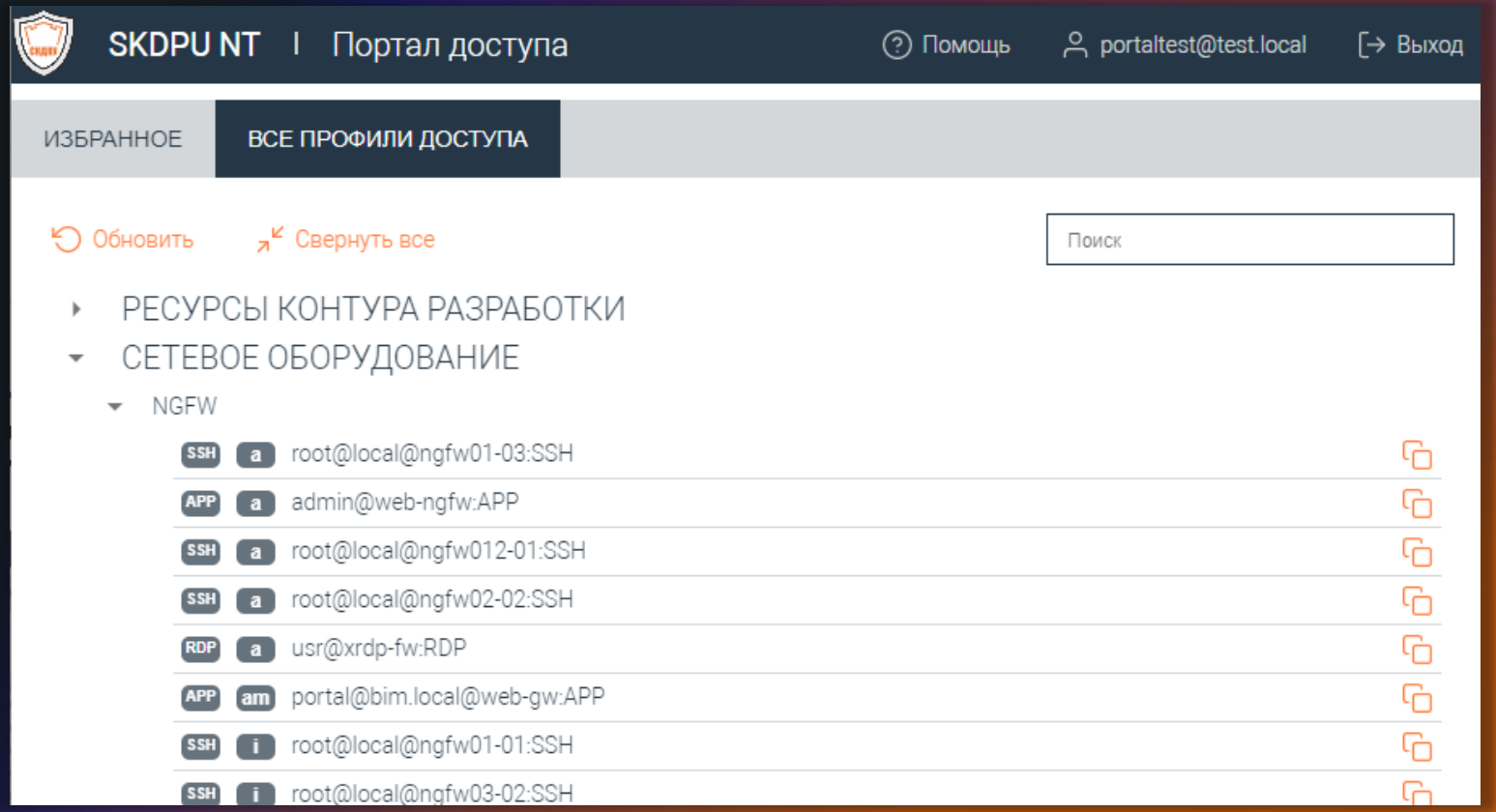
Быстрый и удобный доступ к ресурсам СКДПУ НТ
для всех типов пользователей и при любых размерах ИТ-инфраструктуры

ЕДИНЫЙ ДОСТУП

Единая точка доступа к инфраструктуре шлюзов доступа и запрашиваемым ресурсам в рамках виртуальной инфраструктуры

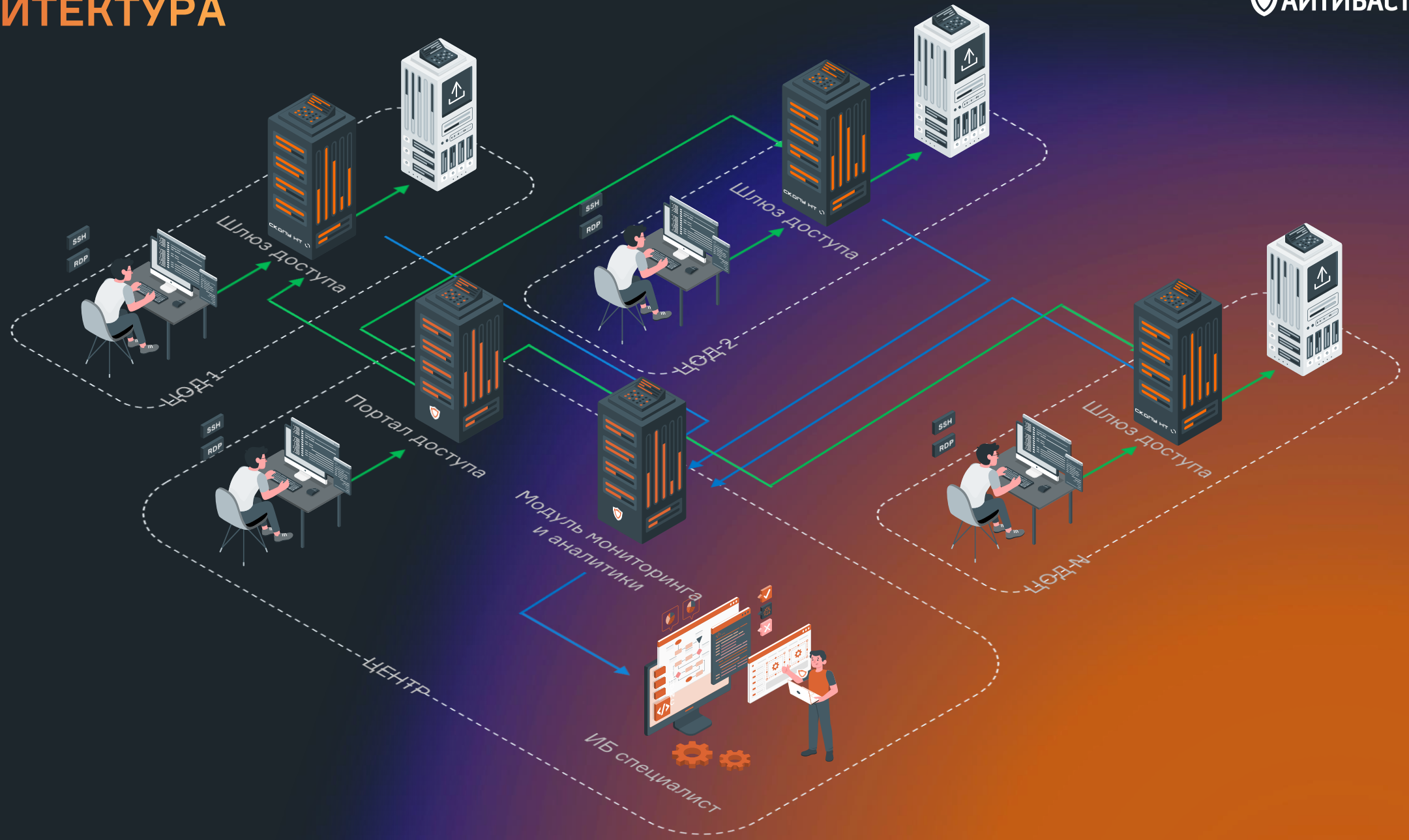
ЕДИНОЕ ОТОБРАЖЕНИЕ

Настраиваемая группировка доступов ко всем доступным ресурсам



АРХИТЕКТУРА

АЙТИБАСТИОН



КАБИНЕТ ОПЕРАТОРА
УПРАВЛЕНИЕ ЦЕЛЕВЫМИ РЕСУРСАМИ

АЙТИБАСТИОН

ОПТИМИЗАЦИЯ
Управления доступом

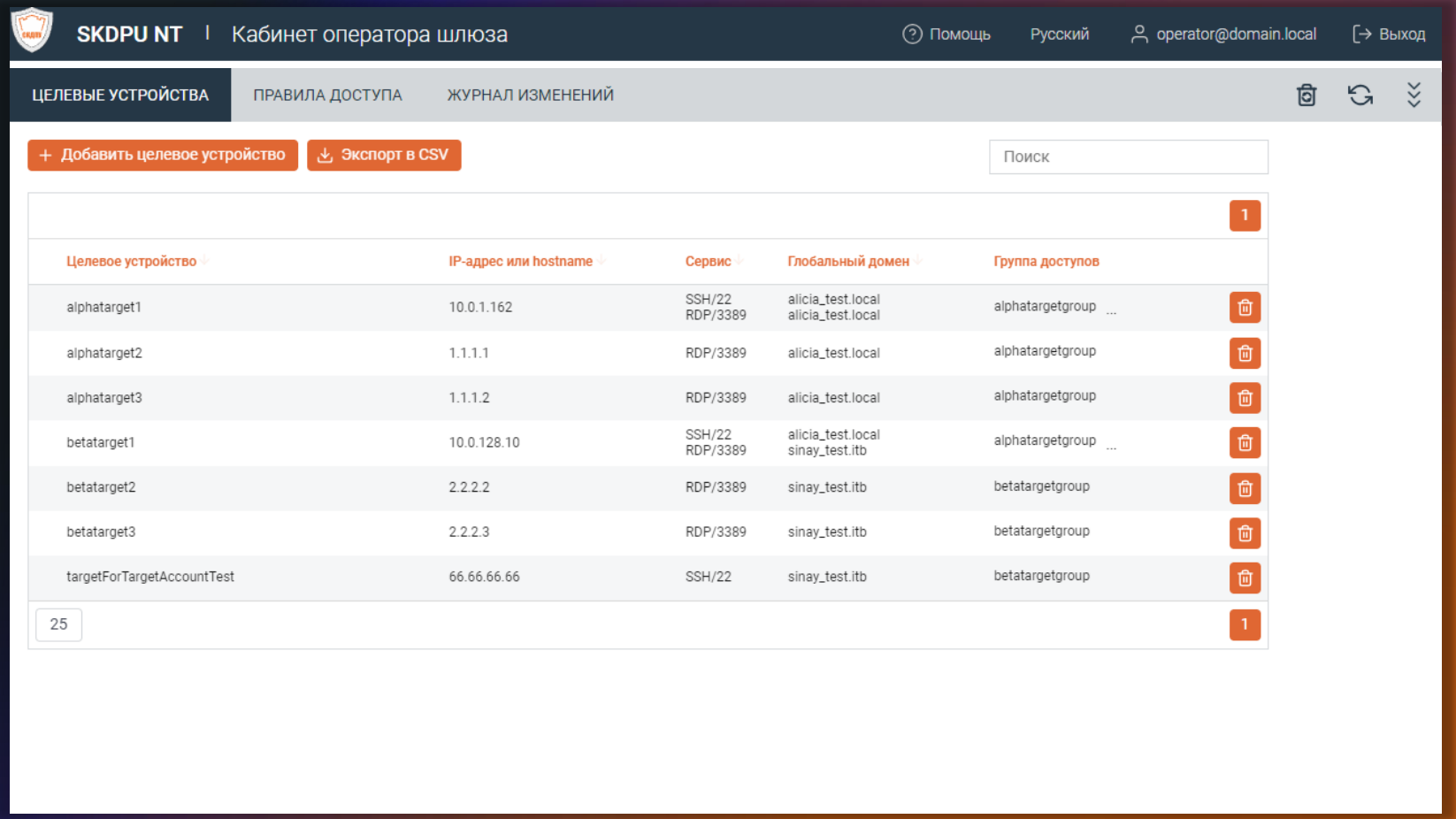
ПОВЫШЕНИЕ
Эффективности работы офицера ИБ

КОНТРОЛЬ
Критичных изменений

РАЗДЕЛЕНИЕ
Зон ответственности

МИНИМИЗАЦИЯ
Ошибочных доступов

ДЕЛЕГИРОВАНИЕ
Части полномочий



СИНЭНИКС

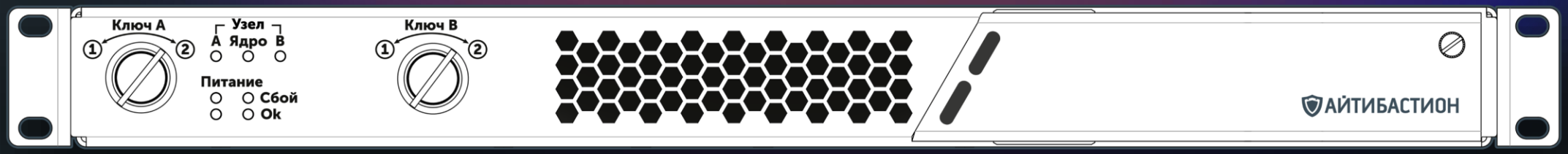
www.it-bastion.com

СИНОНИКС

АЙТИБАСТИОН

«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



ПЕРЕДАЧА ДАННЫХ

- TCP, UDP, в т.ч. Однонаправленная
- Независимые политики для двух контуров
- Скорость до 1 Гб/с
- Соединение «точка-точка»
- Поддержка работы с МЭ, NGFW и другим сетевым оборудованием

ПЕРЕДАЧА ФАЙЛОВ

- SFTP
- Двусторонняя/односторонняя с выбором направления
- Проверка маски имени, размера и контроль целостности
- Интеграция с ICAP-сервисами (DLP, Sandbox, AV и др.)
- Доставка файлов во внешние хранилища

СИНЕНИКС
КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

АЙТИБАСТИОН

ИЗОЛЯЦИЯ НА ФИЗИЧЕСКОМ УРОВНЕ

Архитектура и технологии решения обеспечивают автоматизированную контролируемую передачу данных в режиме «точка-точка», как в одну , так и в обе стороны по протоколам TCP и UDP без прямой связанности узлов.

ФИЗИЧЕСКИЙ КОНТРОЛЬ

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

РАЗГРАНИЧЕНИЕ ЗОН ОТВЕТСТВЕННОСТИ

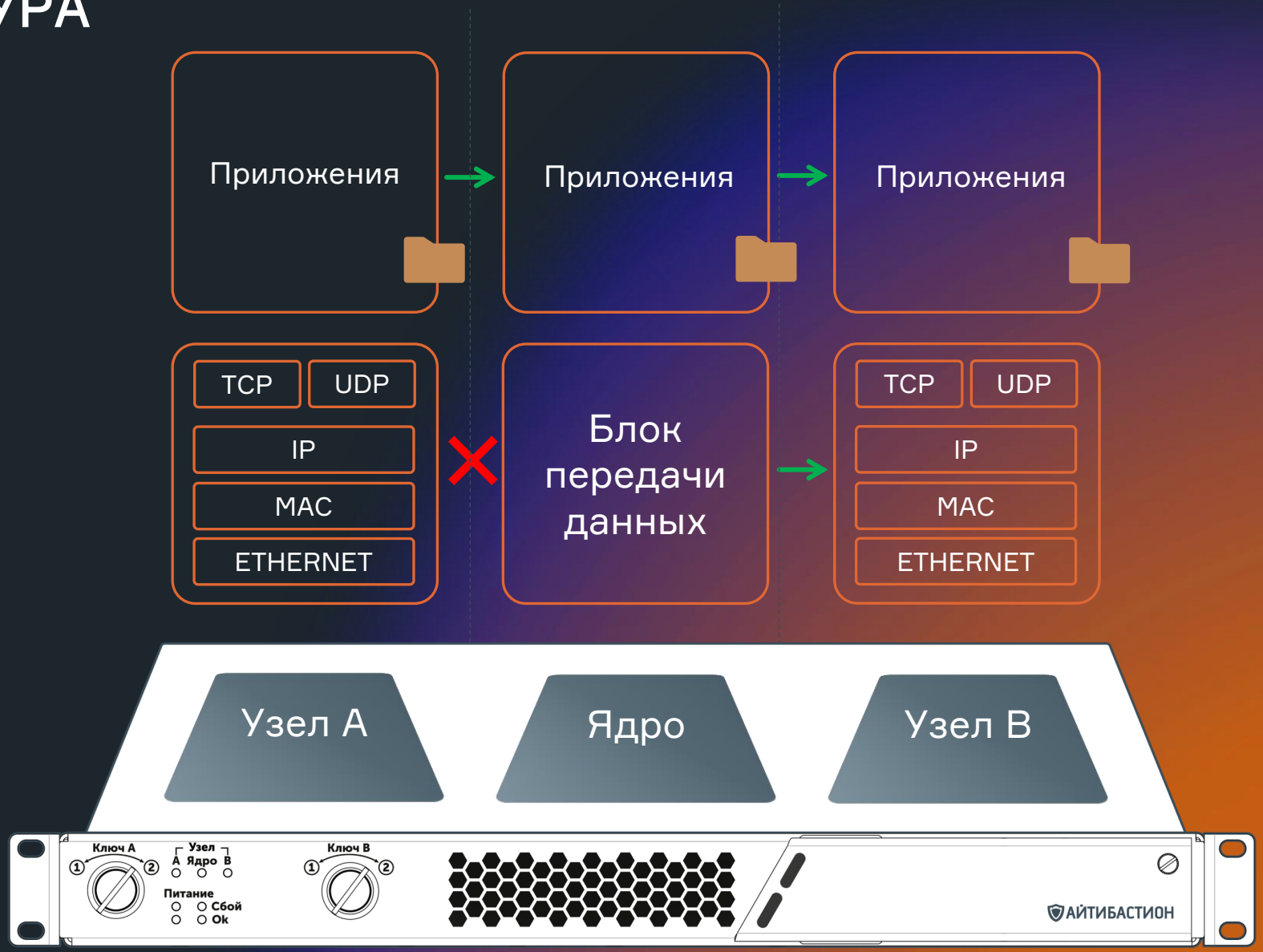
Встречный контроль, реализованный через управление двумя ответственными для подтверждения прохождения данных. Несогласованные с обеих сторон правила игнорируются.

ПРОВЕРКА ФАЙЛОВ ПЕРЕД ПЕРЕДАЧЕЙ

Проверка размера, маски, а также целостности передаваемых объектов. Имеет встроенные механизмы дополнительной верификации объектов во внешних системах средствами ICAP-протокола.

СИНЕНИКС
АРХИТЕКТУРА

АЙТИБАСТИОН

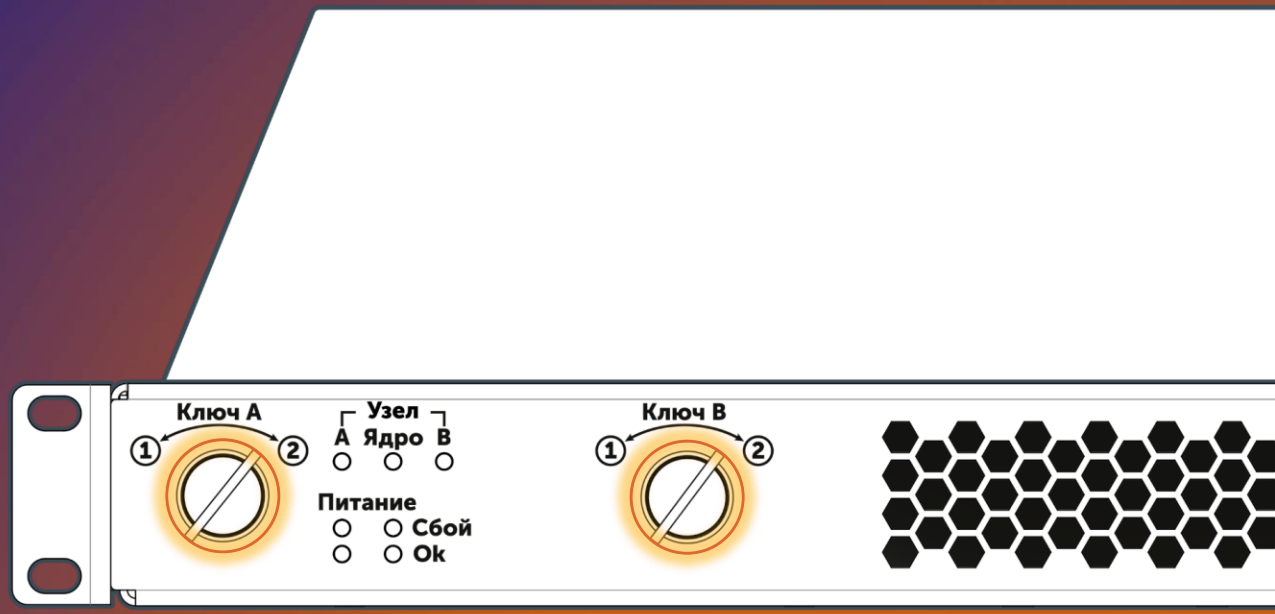


СИНОНИКС
АРХИТЕКТУРА

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.



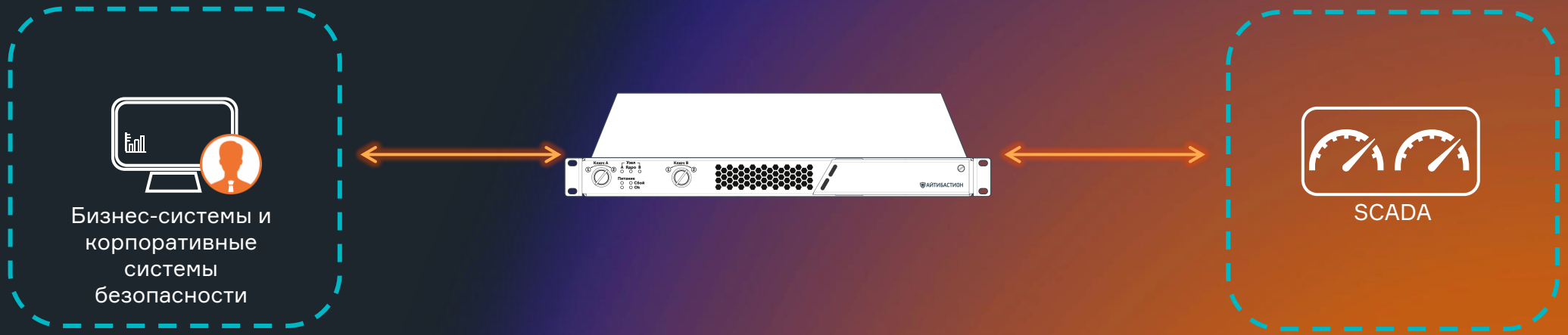
СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

www.it-bastion.com

СИНЕНИКС
СЦЕНАРИЙ №1

АЙТИБАСТИОН

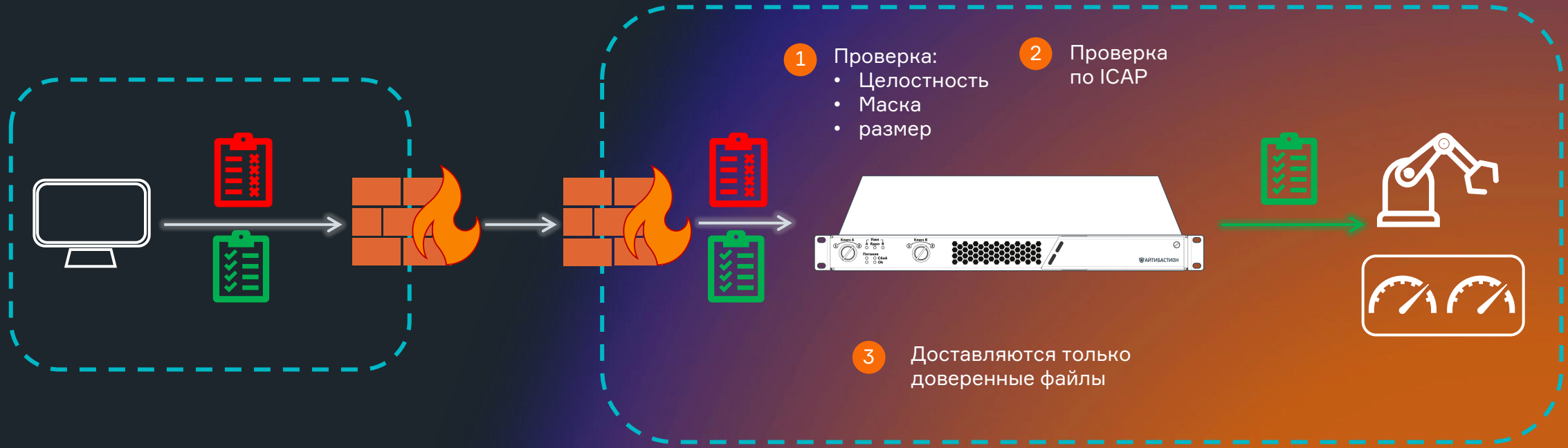
Задача: организовать непрерывный обмен данными между устройствами без сетевой связанности с сокрытием их окружения.



СИНЕНИКС
СЦЕНАРИЙ №2

АЙТИБАСТИОН

Задача: развернуть надежную автоматизированную систему для передачи обновлений к системам из разных сетей

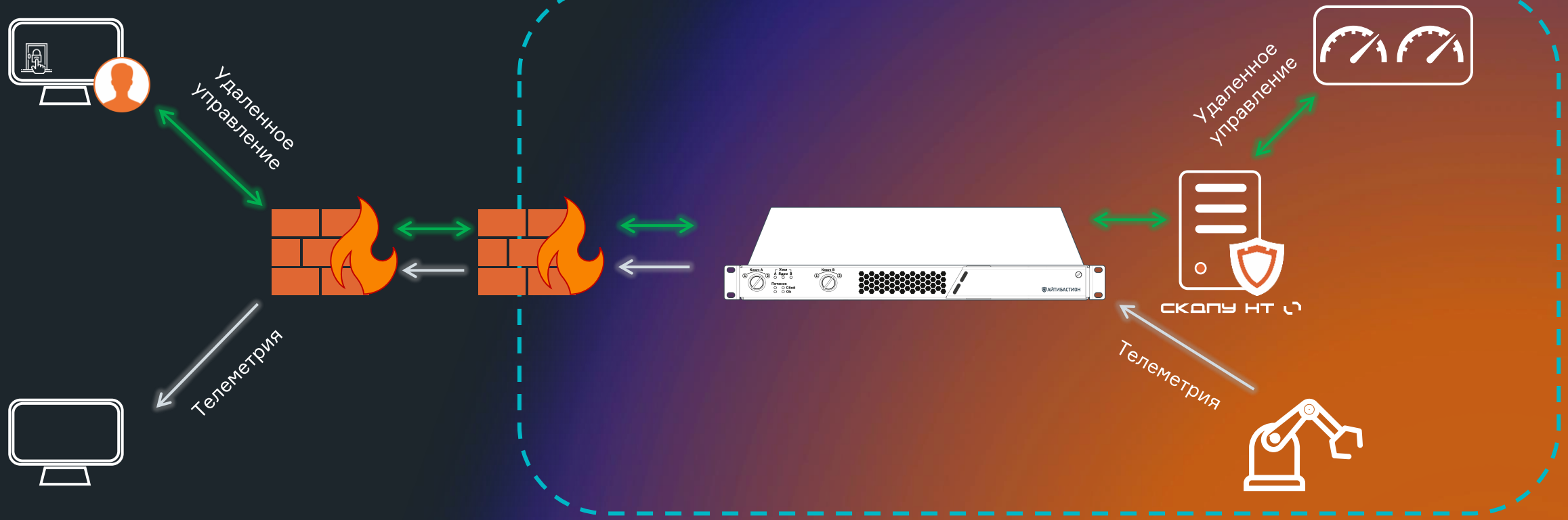


www.it-bastion.com

СИНЕНИКС
СЦЕНАРИЙ №3

АЙТИБАСТИОН

Задача: организовать передачу части данных со стороны одной из несвязанных систем и обеспечить контролируемый доступ к важным объектам средствами PAM-системы.



СИНЕНИКС
ТЕХНОЛОГИЧЕСКИЕ ПАРТНЕРЫ

АЙТИБАСТИОН

АНТИВИРУСЫ

kaspersky

Dr.WEB

МЭ/NGFW

КОД безопасности

UserGate

с•терра®

DLP

INFOWATCH®

SOLAR

и другие решения

www.it-bastion.com

АЙТИБАСТИОН

Спасибо за внимание!

a.shirikalov@it-bastion.com

+7 499 322 3667

it-bastion.com