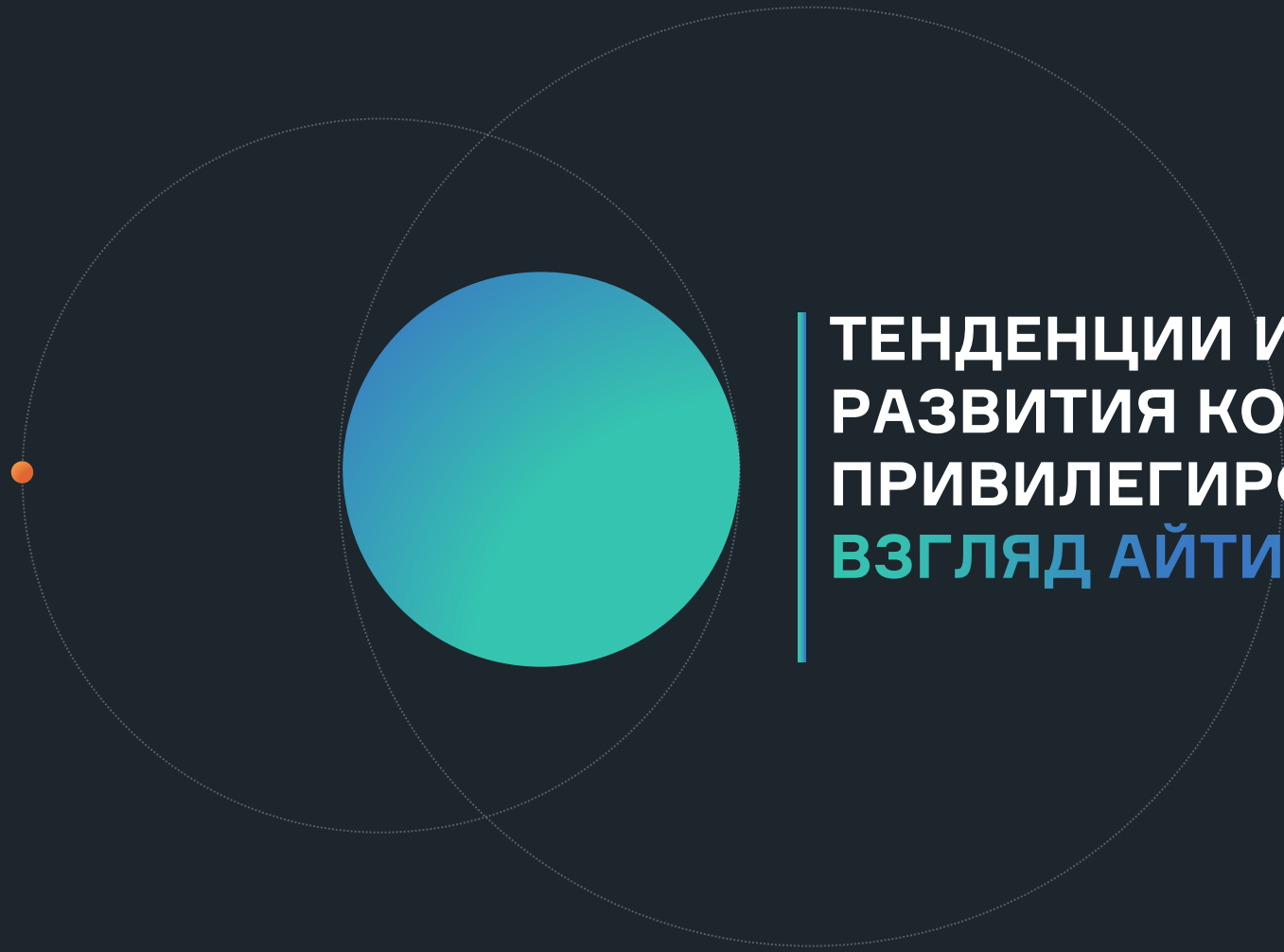
2024



ТЕНДЕНЦИИ И ПЕРСПЕКТИВЫ РАЗВИТИЯ КОНТРОЛЯ ПРИВИЛЕГИРОВАННОГО ДОСТУПА. ВЗГЛЯД АЙТИ БАСТИОН

АЛЕКСАНДР КАРПОВ

www.it-bastion.com

КОМПАНИЯ
АЙТИ БАСТИОН

АЙТИБАСТИОН

2014
ОСНОВАНИЕ КОМПАНИИ
10 лет на российском рынке информационной безопасности

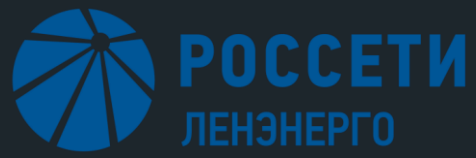
300+
ПАРТНЕРОВ-ИНТЕГРАТОРОВ
Интеграции с компаниями, позволяющие выполнить квалифицированную помощь в реализации защиты инфраструктуры

250+
ЗАКАЗЧИКОВ И ПРОЕКТОВ
Присутствие во всех отраслях от нефтяных компаний до футбольных клубов, от небольших офисов до геораспределенных площадок

>70%
РАМ-РЫНКА РФ
Комплекс СКДПУ НТ решение, проверенное «в боях» и доказавшее свою эффективность, надежность и качество

ЗАКАЗЧИКИ

АЙТИБАСТИОН

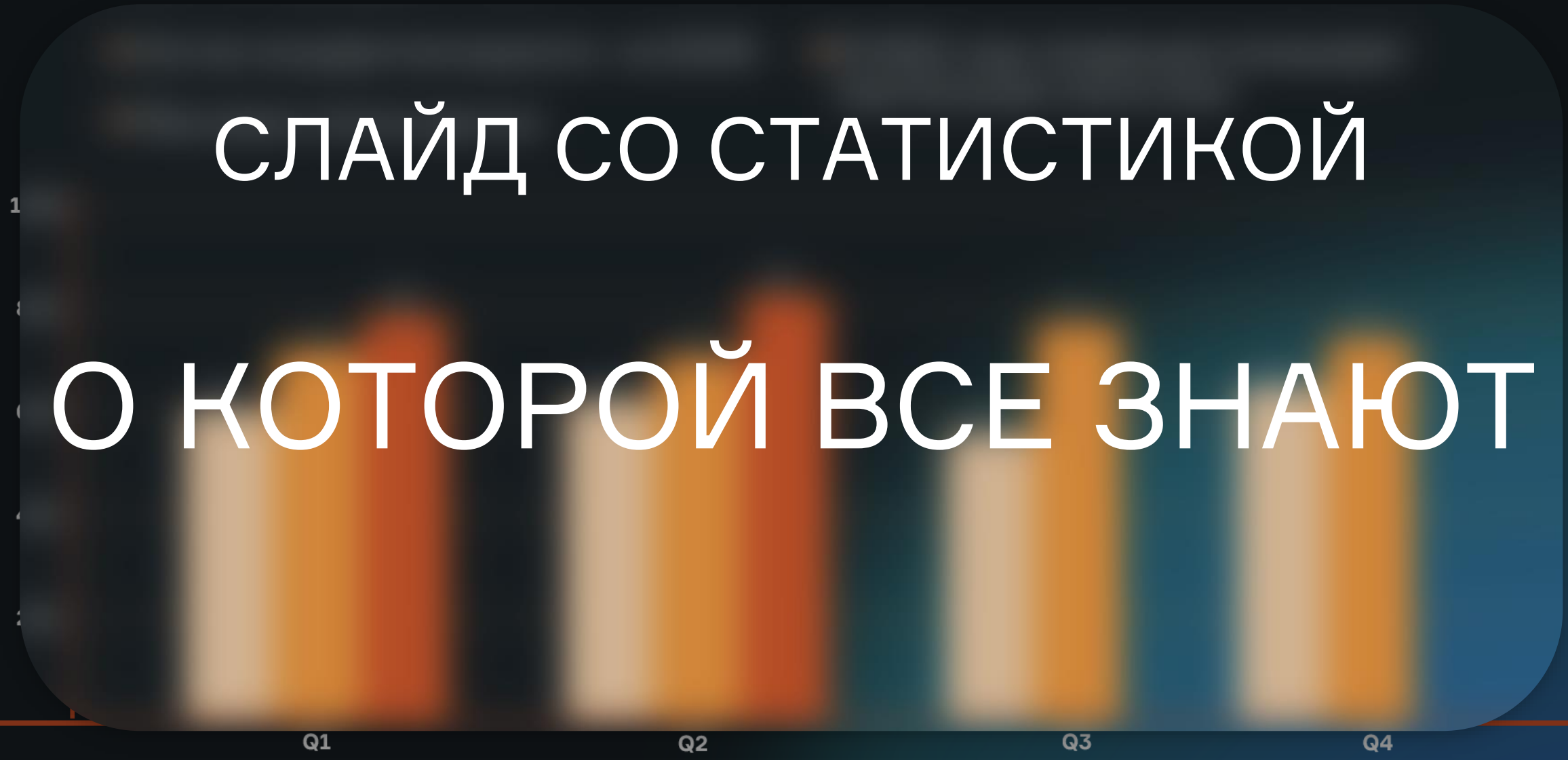


ПРАВИТЕЛЬСТВО
МОСКВЫ

МИНИСТЕРСТВО
ТРАНСПОРТА РФ

НЕМНОГО СТАТИСТИКИ
КОЛ-ВО ИНЦИДЕНТОВ

АЙТИБАСТИОН



СЛАЙД СО СТАТИСТИКОЙ

О КОТОРОЙ ВСЕ ЗНАЮТ

www.it-bastion.com

АЙТИБАСТИОН

КОНТРОЛЬ ПОДРЯДЧИКОВ=?

Взлом 1 подрядчика - страдают ~ 10 заказчиков

Не хотят брать на себя ответственность

Отсутствует нормативная база

Отказ от взаимодействия с регуляторами

АЙТИБАСТИОН

КОНТРОЛЬ ПОДРЯДЧИКОВ = PAM

ЧТО ТАКОЕ PAM?

АЙТИБАСТИОН

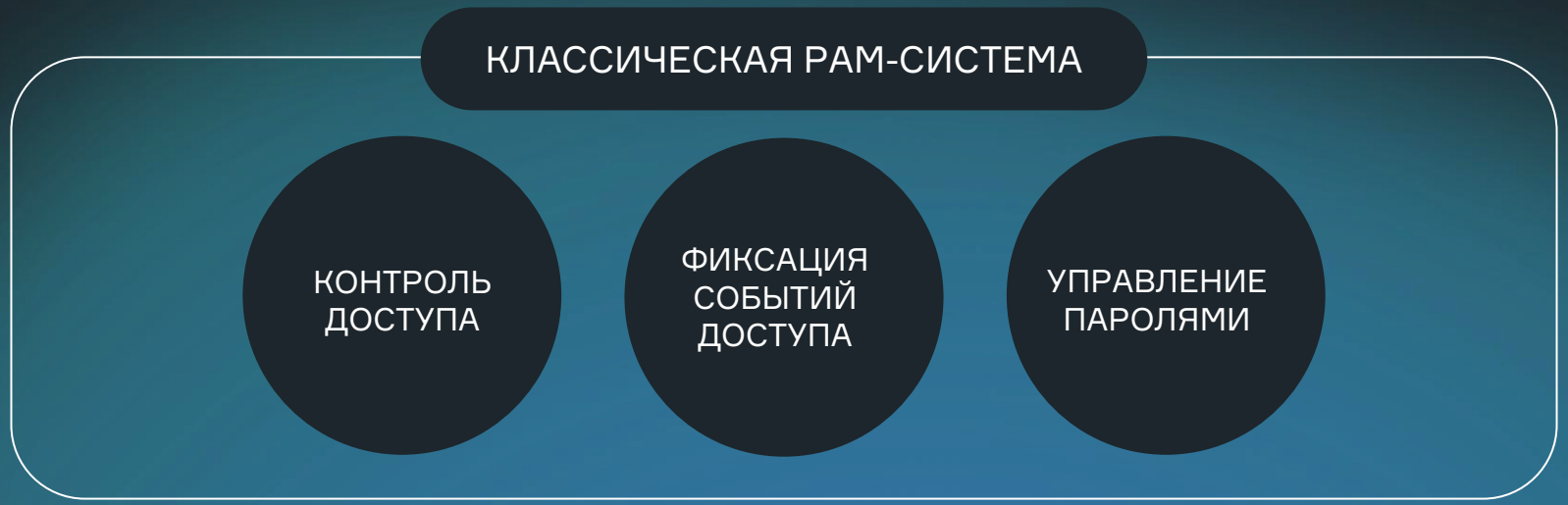
Privileged Access Management (PAM) – Решение для отслеживания, обнаружения, предотвращения и расследования несанкционированного привилегированного доступа к критически важным ресурсам, которое тем самым помогает защитить организации от киберугроз

АЙТИБАСТИОН

ЧТО ТАКОЕ РАМ К КОТОРОМУ МЫ ПРИВЫКЛИ?

ПРОСТО PAM:

АЙТИБАСТИОН



АЙТИБАСТИОН

ЧТО ТАКОЕ PAM В 2024?

PAM В 2024, ЭТО:

АЙТИБАСТИОН

- РАСШИРЕННЫЙ КОНТРОЛЬ ДОСТУПА
- НЕПРЕРЫВНЫЙ МОНИТОРИНГ
- 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

PAM В 2024
МНОГО БУКВ

АЙТИБАСТИОН

Следование концепции Zero trust

Создание и ведение профилирования пользователей

Анализ всех действий в разрезе «пользователь — цель — действие», машинное обучение и математические модели

Возможности реагирования на инциденты в рамках системы

Поддержка REST API

Для загрузки и выгрузки данных, для управления

Следование концепции Just-in-time

Предобработка, анализ и детектирование аномального поведения пользователей

На основе профилирования и событий

Обработка информации и её выдача в виде понятных отчётов

От оперативных до сводных, в том числе для руководителей

Возможности интеграции с другими решениями

АЙТИБАСТИОН

СКОПУ НТ

ПЛАТФОРМА СКДПУ НТ

АЙТИБАСТИОН

СКДПУ НТ Шлюз доступа

СКДПУ НТ Мониторинг и аналитика

СКДПУ НТ Портал доступа

СКДПУ НТ Аудит-архив *

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

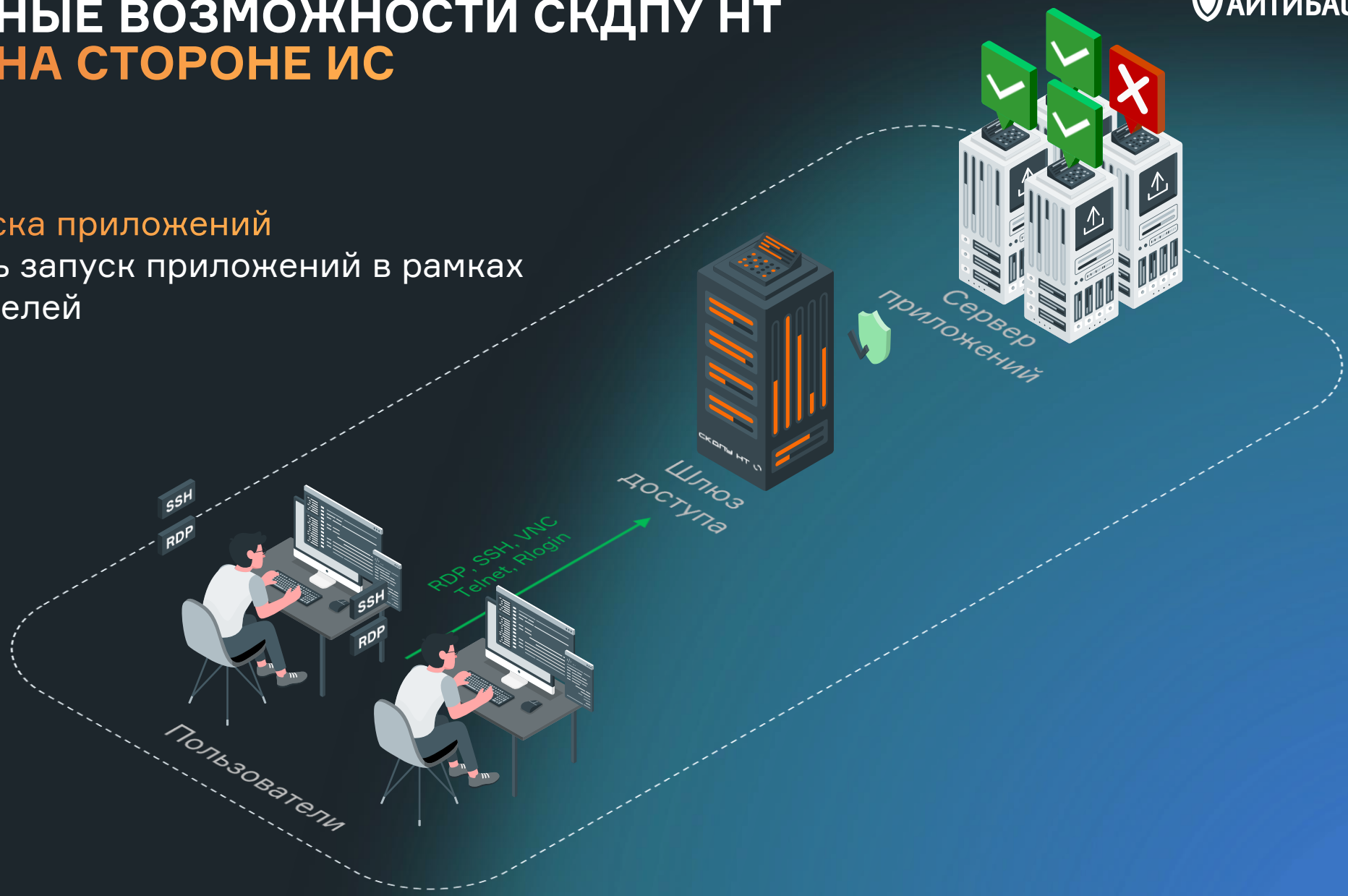
Подключение к ЦУ без необходимости установки агентов, что особенно важно при подключении к объектам КИИ

РАСШИРЕННЫЕ ВОЗМОЖНОСТИ СКДПУ НТ
КОНТРОЛЬ НА СТОРОНЕ ИС

АЙТИБАСТИОН

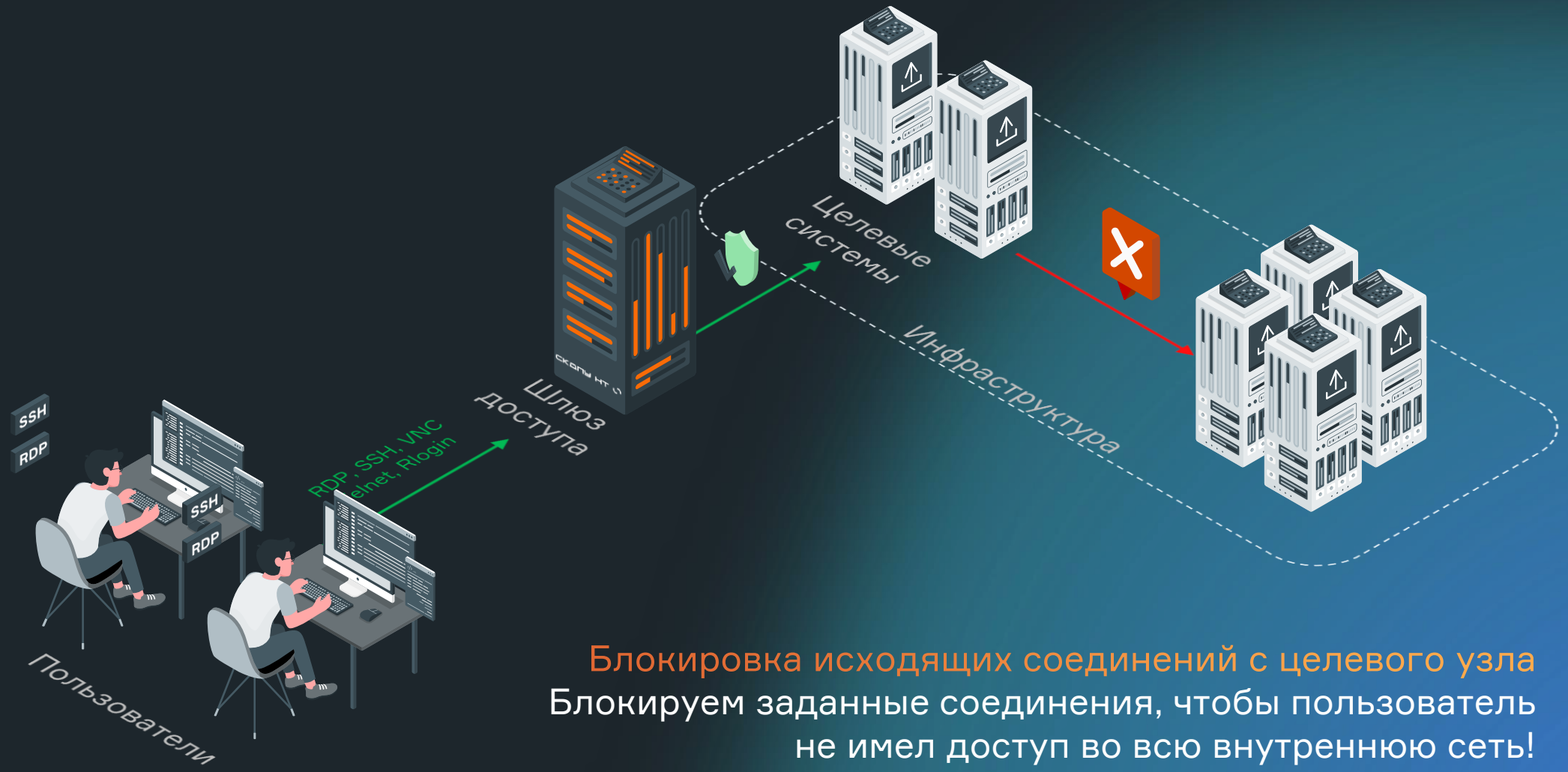
Блокировка запуска приложений

Можем запрещать запуск приложений в рамках сессий пользователей



РАСШИРЕННЫЕ ВОЗМОЖНОСТИ СКДПУ НТ
КОНТРОЛЬ НА СТОРОНЕ ИС

АЙТИБАСТИОН



Блокировка исходящих соединений с целевого узла

Блокируем заданные соединения, чтобы пользователь не имел доступ во всю внутреннюю сеть!

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.

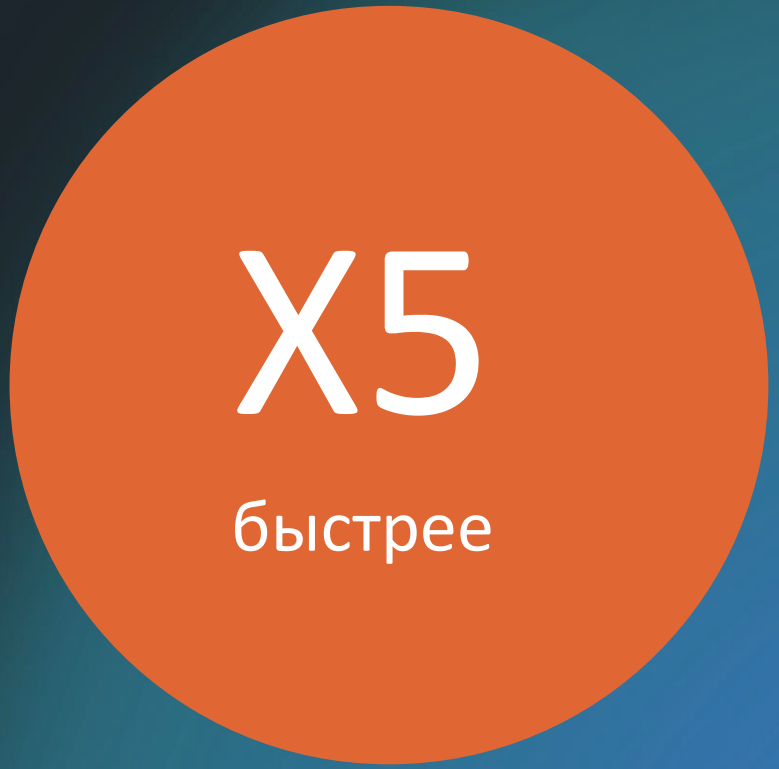
ОТКАЗОУСТОЙЧИВОСТЬ И МАСШТАБИРОВАНИЕ

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.

НАША СТАТИСТИКА
СКОРОСТИ РАССЛЕДОВАНИЯ

АЙТИБАСТИОН

СТАНДАРТНЫМИ МЕТОДАМИ



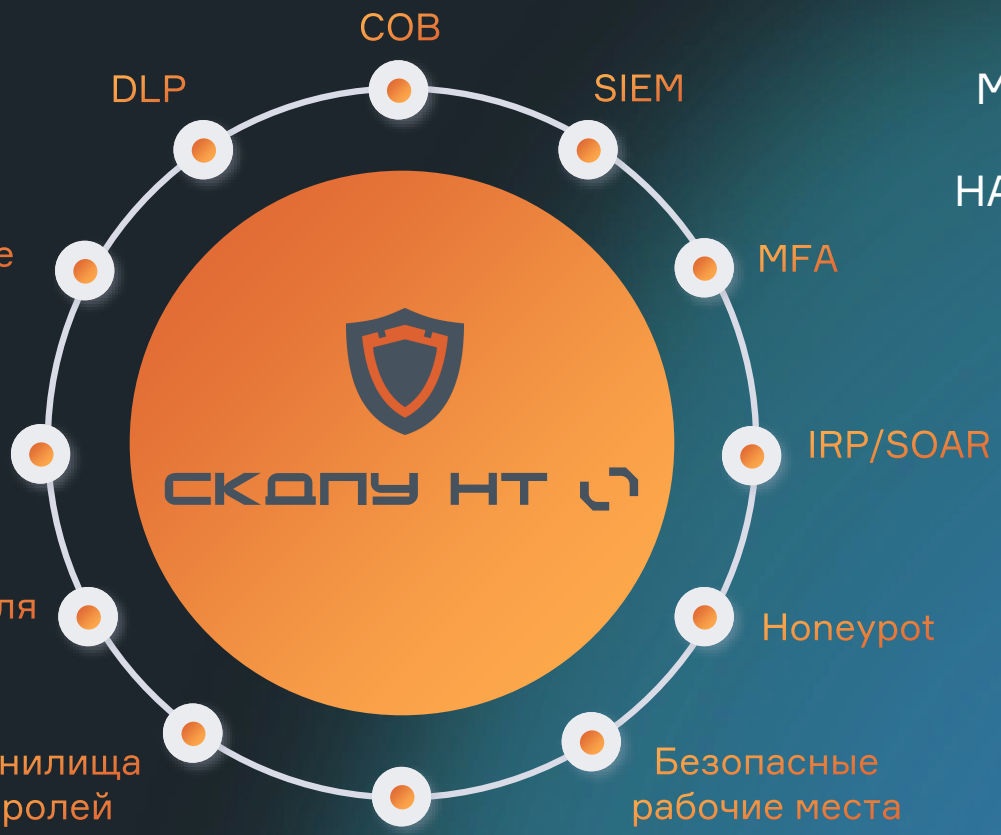
С АНАЛИТИКОЙ СКДПУ НТ

ПЛАТФОРМА СКДПУ.НТ
ИНТЕГРАЦИИ

АЙТИБАСТИОН

ВЗАИМОДЕЙСТВИЕ ПРОДУКТОВ РАЗЛИЧНЫХ КЛАССОВ

МУЛЬТИВЕНДОРНАЯ ЭКОСИСТЕМА НАДЕЖНЫХ РЕШЕНИЙ



РАСШИРЕНИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ

МАКСИМАЛЬНОЕ СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ИБ/ИТ

СКДПУ НТ
ТЕХНОЛОГИЧЕСКИЕ ПАРТНЕРЫ

АЙТИБАСТИОН

ASTRA LINUX®

POSITIVE TECHNOLOGIES

kaspersky

INFOWATCH®

Пассворк

Rusiem

GIS
ГАЗИНФОРМ СЕРВИС

ROSA

CyberLympha®

РУТОКЕН

Аладдин

zVIRT

alt linux

сотерра®

MULTIFACTOR

UserGate

КОД безопасности

РЕДОС

и другие партнеры

АЙТИБАСТИОН

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

АЙТИБАСТИОН

Включен в реестр отечественного ПО

Сертификат ФСТЭК УД-4

Сертификат МО РФ НДВ-2

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-182
«О безопасности КИИ РФ»

GDPR и ФЗ 152

ГОСТ Р 57580.1—2017

BACKDOOR

КЕЙС
BACKDOOR

АНАЛИЗ СЕССИЙ

Поиск сессий с использованием команд создания новых пользователей

```
[root@rosaosch ~]# adduser test4
[root@rosaosch ~]# passwd test4
Изменяется пароль пользователя test4.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - основан на слове из словаря
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@rosaosch ~]# visudo



"/etc/sudoers.tmp" 120L, 4328C
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
```

09-08-2023 17:10:25	SESSION_ESTABLISHED_SUCCESSFULLY	
09-08-2023 17:10:45	KBD_INPUT	adduser testuser
09-08-2023 17:10:52	KBD_INPUT	passwd testuser
09-08-2023 17:10:52	KILL_PATTERN_DETECTED	**pattern:** passwd
09-08-2023 17:21:40	SESSION_ESTABLISHED_SUCCESSFULLY	
09-08-2023 17:21:52	KBD_INPUT	adduser test4
09-08-2023 17:21:56	KBD_INPUT	passwd test4
09-08-2023 17:22:07	KBD_INPUT	visudo

ВЫЯВЛЕНИЕ НАРУШИТЕЛЕЙ

Фиксирование сессии с успешно отработанной командой

АНАЛИЗ СЕССИЙ

Поиск сессий с использованием команд создания новых пользователей

09-08-2023 17:10:25	SESSION_ESTABLISHED_SUCCESSFULLY	
09-08-2023 17:10:45	KBD_INPUT	adduser testuser
09-08-2023 17:10:52	KBD_INPUT	passwd testuser
09-08-2023 17:10:52	KILL_PATTERN_DETECTED	**pattern:** passwd

09-08-2023 17:21:40	SESSION_ESTABLISHED_SUCCESSFULLY	
09-08-2023 17:21:52	KBD_INPUT	adduser test4
09-08-2023 17:21:56	KBD_INPUT	passwd test4
09-08-2023 17:22:07	KBD_INPUT	visudo

АНАЛИЗ СЕССИЙ

Поиск сессий с использованием команд создания новых пользователей

```
[root@rosaosch ~]# adduser test4
[root@rosaosch ~]# passwd test4
Изменяется пароль пользователя test4.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - основан на слове из словаря
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@rosaosch ~]# visudo



"/etc/sudoers.tmp" 120L, 4328C
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
```

09-08-2023 17:10:25	SESSION_ESTABLISHED_SUCCESSFULLY	
09-08-2023 17:10:45	KBD_INPUT	adduser testuser
09-08-2023 17:10:52	KBD_INPUT	passwd testuser
09-08-2023 17:10:52	KILL_PATTERN_DETECTED	**pattern:** passwd
09-08-2023 17:21:40	SESSION_ESTABLISHED_SUCCESSFULLY	
09-08-2023 17:21:52	KBD_INPUT	adduser test4
09-08-2023 17:21:56	KBD_INPUT	passwd test4
09-08-2023 17:22:07	KBD_INPUT	visudo

ВЫЯВЛЕНИЕ НАРУШИТЕЛЕЙ

Фиксирование сессии с успешно отработанной командой

```
[root@rosaosch ~]# adduser test4
[root@rosaosch ~]# passwd test4
Изменяется пароль пользователя test4.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - основан на слове из словаря
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@rosaosch ~]# visudo



"/etc/sudoers.tmp" 120L, 4328C
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
```

ВЫЯВЛЕНИЕ НАРУШИТЕЛЕЙ

Фиксирование сессии с успешно отработанной командой

АНАЛИЗ СЕССИЙ

Поиск сессий с использованием команд создания новых пользователей

```
[root@rosaosch ~]# adduser test4
[root@rosaosch ~]# passwd test4
Изменяется пароль пользователя test4.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - основан на слове из словаря
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@rosaosch ~]# visudo



"/etc/sudoers.tmp" 120L, 4328C
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
```

09-08-2023 17:10:25	SESSION_ESTABLISHED_SUCCESSFULLY	
09-08-2023 17:10:45	KBD_INPUT	adduser testuser
09-08-2023 17:10:52	KBD_INPUT	passwd testuser
09-08-2023 17:10:52	KILL_PATTERN_DETECTED	**pattern:** passwd
09-08-2023 17:21:40	SESSION_ESTABLISHED_SUCCESSFULLY	
09-08-2023 17:21:52	KBD_INPUT	adduser test4
09-08-2023 17:21:56	KBD_INPUT	passwd test4
09-08-2023 17:22:07	KBD_INPUT	visudo

ВЫЯВЛЕНИЕ НАРУШИТЕЛЕЙ

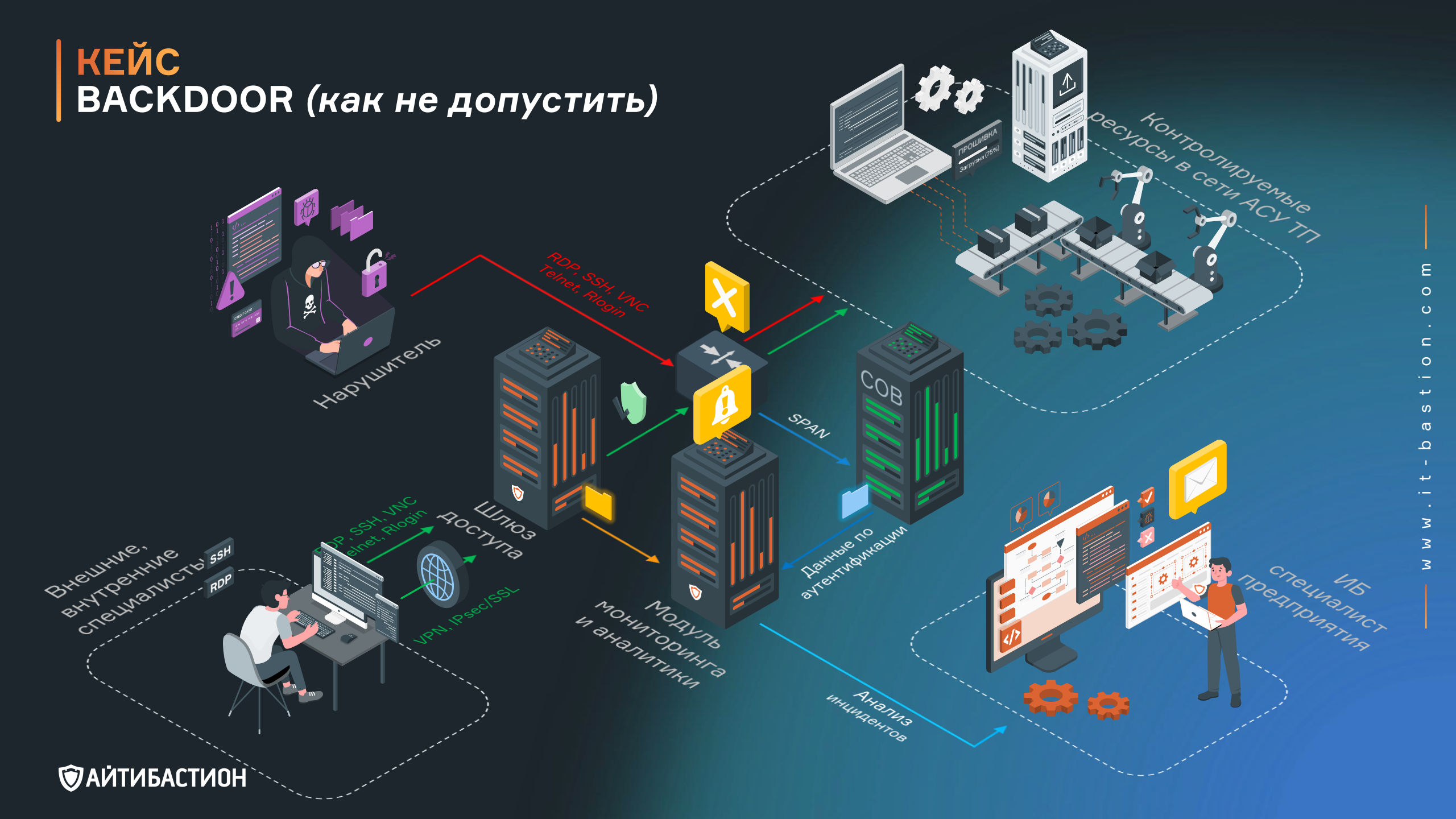
Фиксирование сессии с успешно отработанной командой

ОБНАРУЖЕНИЕ

Обнаружение нарушителя
и применение
административных мер

КАК НЕ ДОПУСТИТЬ ТАКОГО СЦЕНАРИЯ?

КЕЙС
BACKDOOR (*как не допустить*)

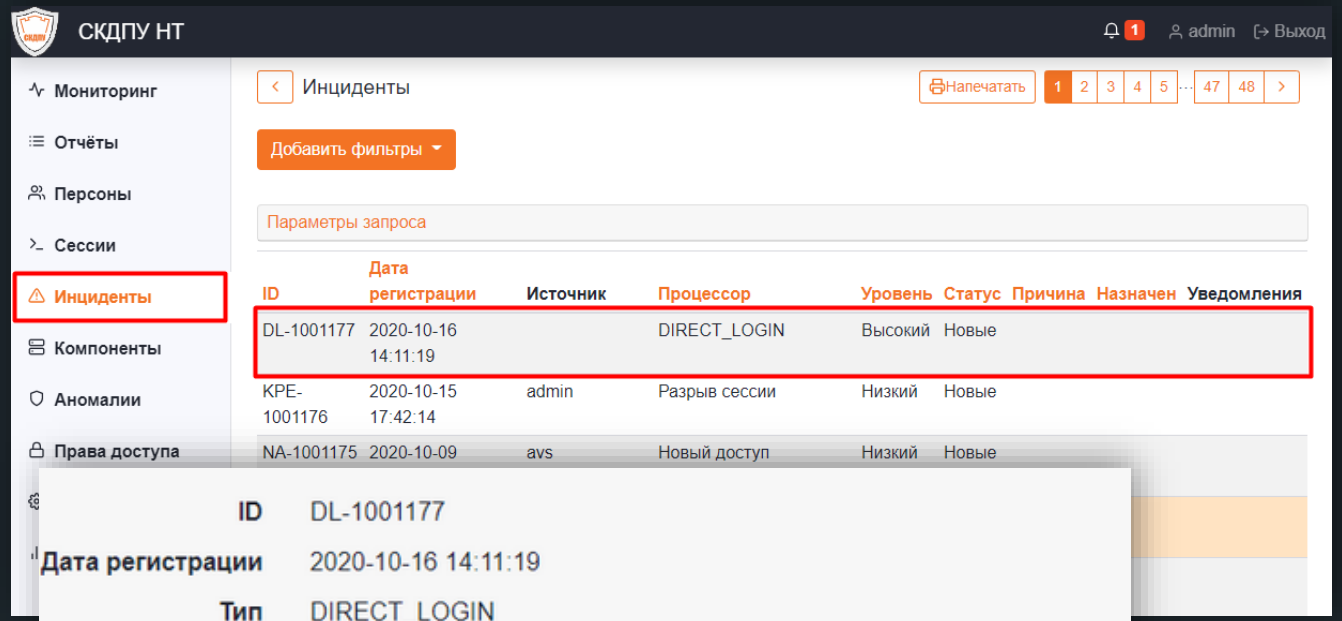


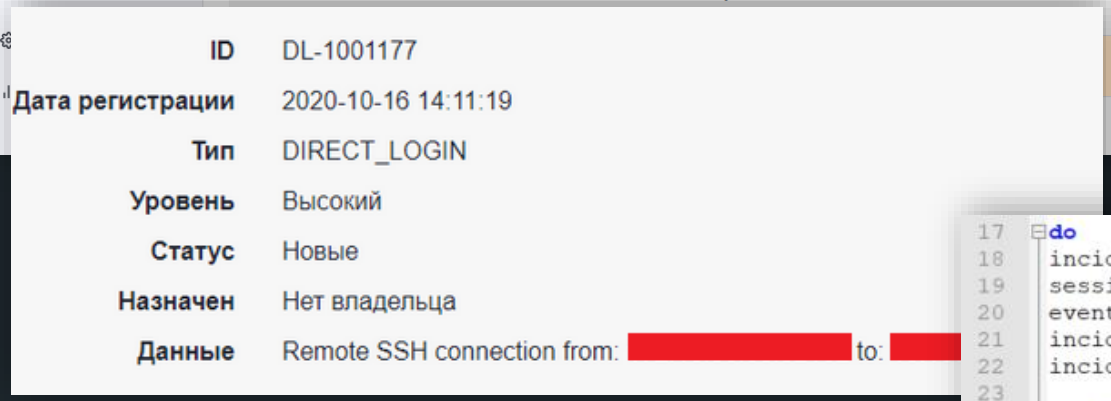
АЙТИБАСТИОН

www.it-bastion.com

КЕЙС
BACKDOOR *(как не допустить)*

АЙТИБАСТИОН






```
do
incident=$(echo "${incident}" | base64 --decode)
session_id=$(echo "${incident}" | jq -r '.data.event.session_id')
event_type=$(echo "${incident}" | jq -r '.data.event.event_type')
incident_id=$(echo "${incident}" | jq -r '.data.indent')
incident_link=$(echo "${incident}" | jq -r '.incident_link')

    if [ "$event_type" == "NEW_PROCESS" ]; then
        curl -k -X PUT \
    -H "X-Auth-Key: $xtoken" \
    -H "X-Auth-User: $xuser" \
    -H "Content-Type: application/json" \
    -d "{\"reason\":\"$incident_id\n$incident_link\"}" \
    "https://${api_address}/api/sessions?session_id=${session_id}&action=kill"
    fi
done
```

АВТОМАТИЗАЦИЯ

Возможность автоматизации реагирования на инциденты безопасности

www.it-bastion.com

АЙТИБАСТИОН

РЕАЛЬНЫЕ ДЕНЬГИ

КЕЙС
РЕАЛЬНЫЕ ДЕНЬГИ

ДОП. СОГЛАШЕНИЕ

Подрядчик запросил дополнительное соглашение, за дополнительную оплату из-за сложности проводимых работ

РЕАЛЬНОЕ ВРЕМЯ

Какое реальное время работы подрядчика?

ОБЪЕМ ВЫПОЛНЕННЫХ РАБОТ

Какой объем выполненных работ?

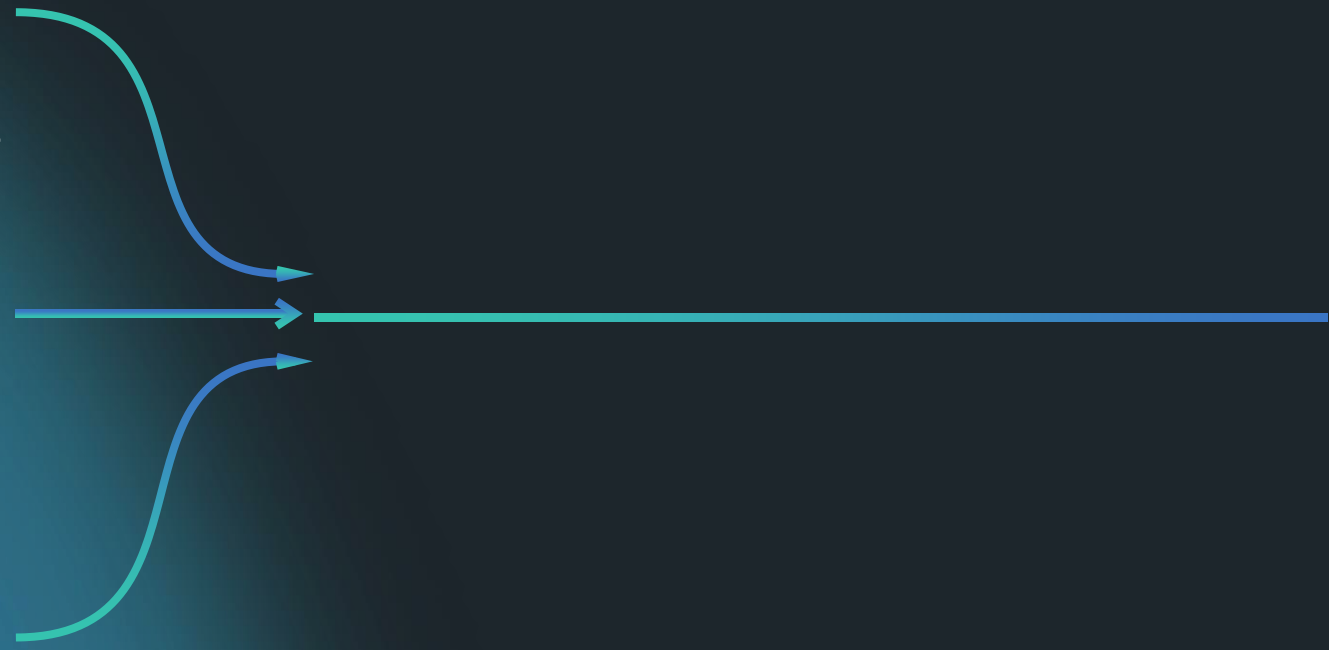
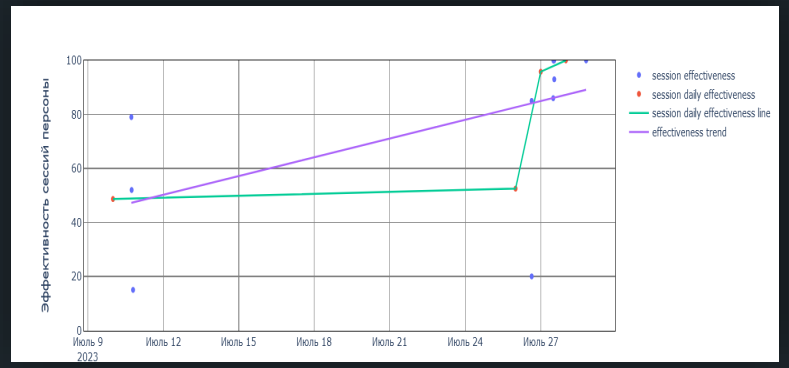


ГРАФИК ЭФФЕКТИВНОСТИ

Позволил оценить общую эффективность работ на протяжении времени



Тип инцидента	Наименее эффективное использование времени сессии
Уровень	Низкий
Влияние	10
Статус	Новые
Назначен	Нет владельца
Данные	effectiveness decreased drastically: 41 % in 8 days

ИНЦИДЕНТЫ

Позволили своевременно зафиксировать простои в работе

ОТЧЕТЫ

Позволил оценить общую эффективность работ на протяжении времени

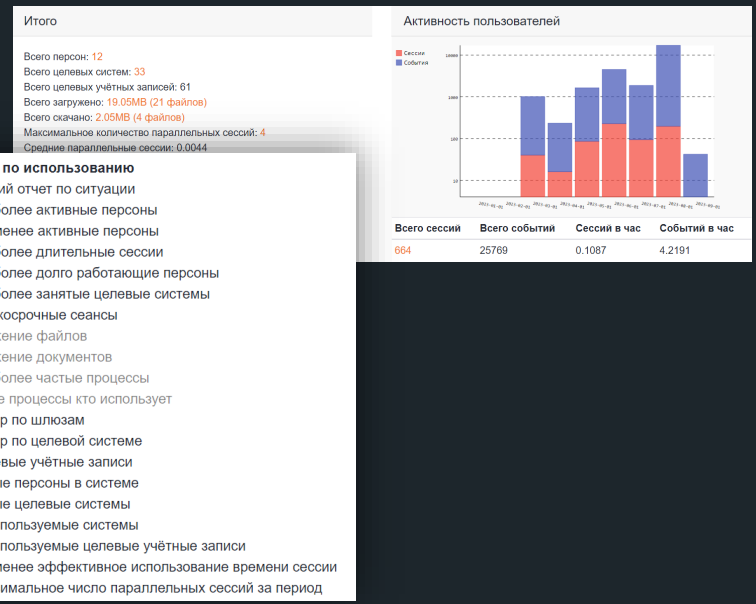


ГРАФИК ЭФФЕКТИВНОСТИ

Позволил оценить общую эффективность работ на протяжении времени

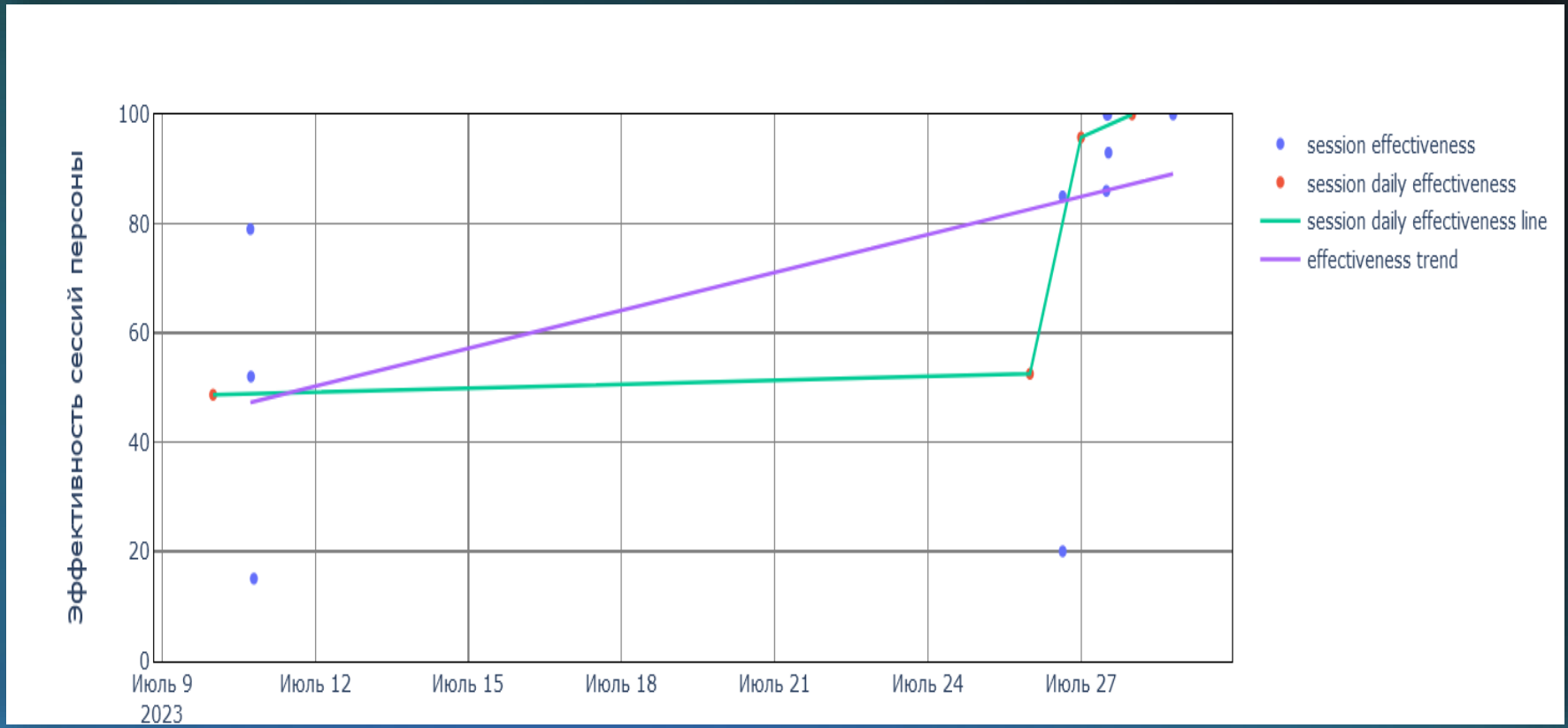
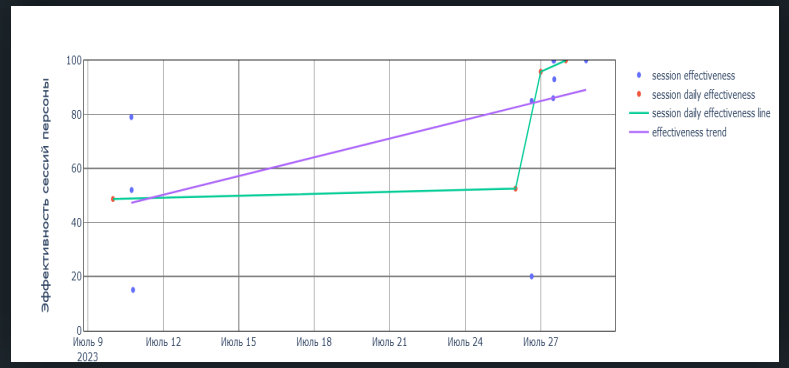


ГРАФИК ЭФФЕКТИВНОСТИ

Позволил оценить общую эффективность работ на протяжении времени



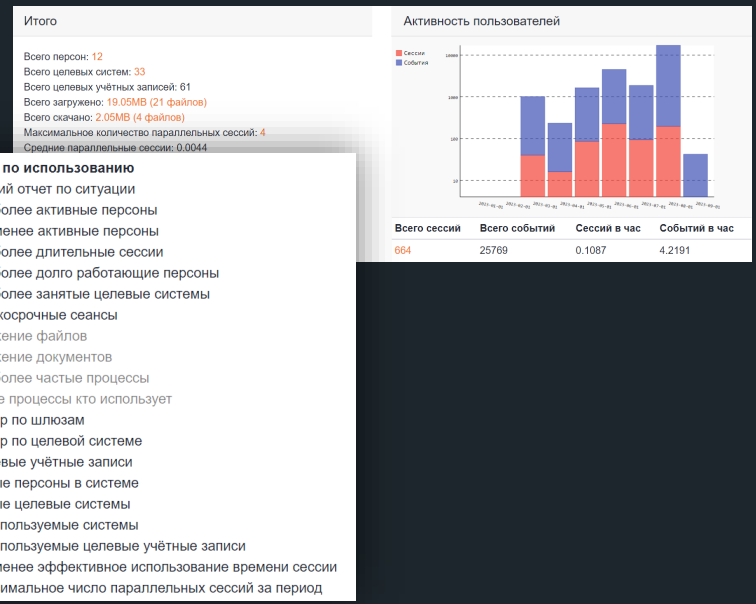
Тип инцидента	Наименее эффективное использование времени сессии
Уровень	Низкий
Влияние	10
Статус	Новые
Назначен	Нет владельца
Данные	effectiveness decreased drastically: 41 % in 8 days

ИНЦИДЕНТЫ

Позволили своевременно зафиксировать простои в работе

ОТЧЕТЫ

Позволил оценить общую эффективность работ на протяжении времени



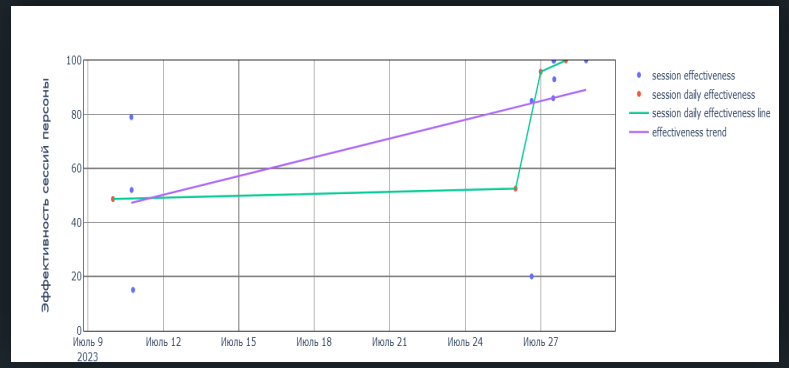
Тип инцидента	Наименее эффективное использование времени сессии
Уровень	Низкий
Влияние	10
Статус	Новые
Назначен	Нет владельца
Данные	effectiveness decreased drastically: 41 % in 8 days

ИНЦИДЕНТЫ

Позволили своевременно зафиксировать простои в работе

ГРАФИК ЭФФЕКТИВНОСТИ

Позволил оценить общую эффективность работ на протяжении времени



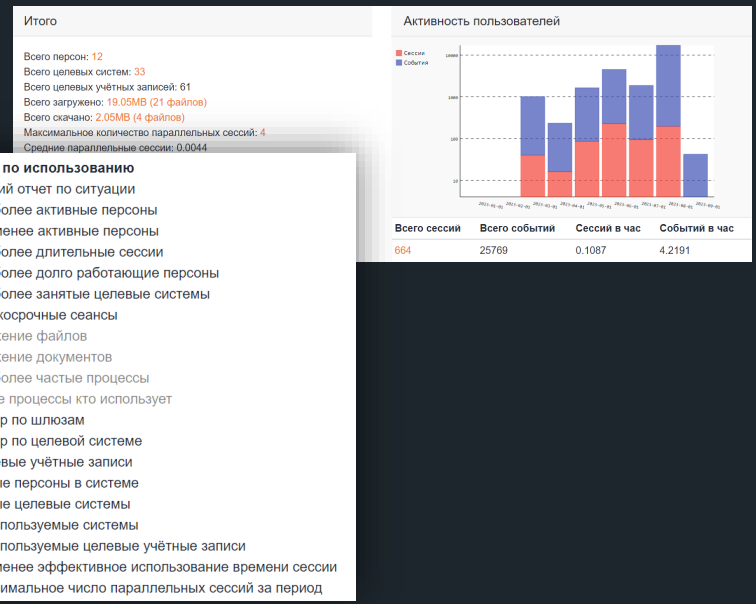
Тип инцидента	Наименее эффективное использование времени сессии
Уровень	Низкий
Влияние	10
Статус	Новые
Назначен	Нет владельца
Данные	effectiveness decreased drastically: 41 % in 8 days

ИНЦИДЕНТЫ

Позволили своевременно зафиксировать простои в работе

ОТЧЕТЫ

Позволил оценить общую эффективность работ на протяжении времени



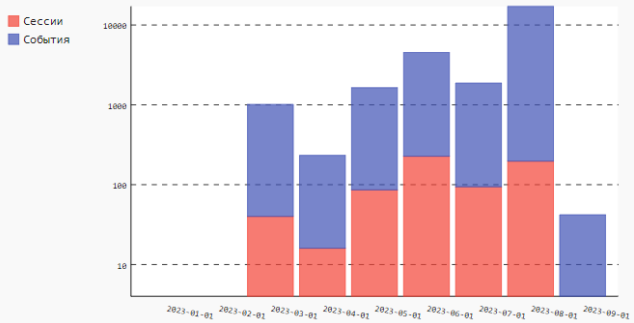
ОТЧЕТЫ

Позволил оценить общую эффективность работ на протяжении времени

Итого

Всего персон: 12
Всего целевых систем: 33
Всего целевых учётных записей: 61
Всего загружено: 19.05MB (21 файлов)
Всего скачано: 2.05MB (4 файлов)
Максимальное количество параллельных сессий: 4
Средние параллельные сессии: 0.0044

Активность пользователей



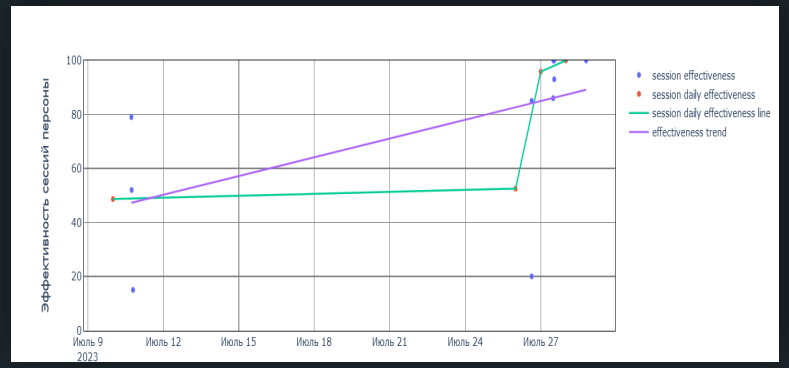
Всего сессий	Всего событий	Сессий в час	Событий в час
664	25769	0.1087	4.2191

Отчеты по использованию

- Общий отчет по ситуации
- Наиболее активные персоны
- Наименее активные персоны
- Наиболее длительные сессии
- Наиболее долго работающие персоны
- Наиболее занятые целевые системы
- Краткосрочные сеансы
- Движение файлов
- Движение документов
- Наиболее частые процессы
- Какие процессы кто использует
- Обзор по шлюзам
- Обзор по целевой системе
- Целевые учётные записи
- Новые персоны в системе
- Новые целевые системы
- Неиспользуемые системы
- Неиспользуемые целевые учётные записи
- Наименее эффективное использование времени сессии
- Максимальное число параллельных сессий за период

ГРАФИК ЭФФЕКТИВНОСТИ

Позволил оценить общую эффективность работ на протяжении времени



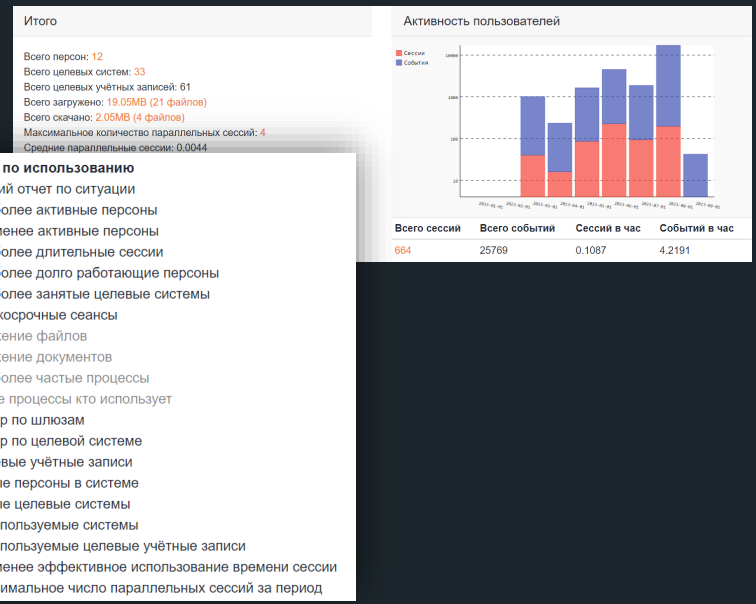
Тип инцидента	Наименее эффективное использование времени сессии
Уровень	Низкий
Влияние	10
Статус	Новые
Назначен	Нет владельца
Данные	effectiveness decreased drastically: 41 % in 8 days

ИНЦИДЕНТЫ

Позволили своевременно зафиксировать простои в работе

ОТЧЕТЫ

Позволил оценить общую эффективность работ на протяжении времени



АЙТИБАСТИОН

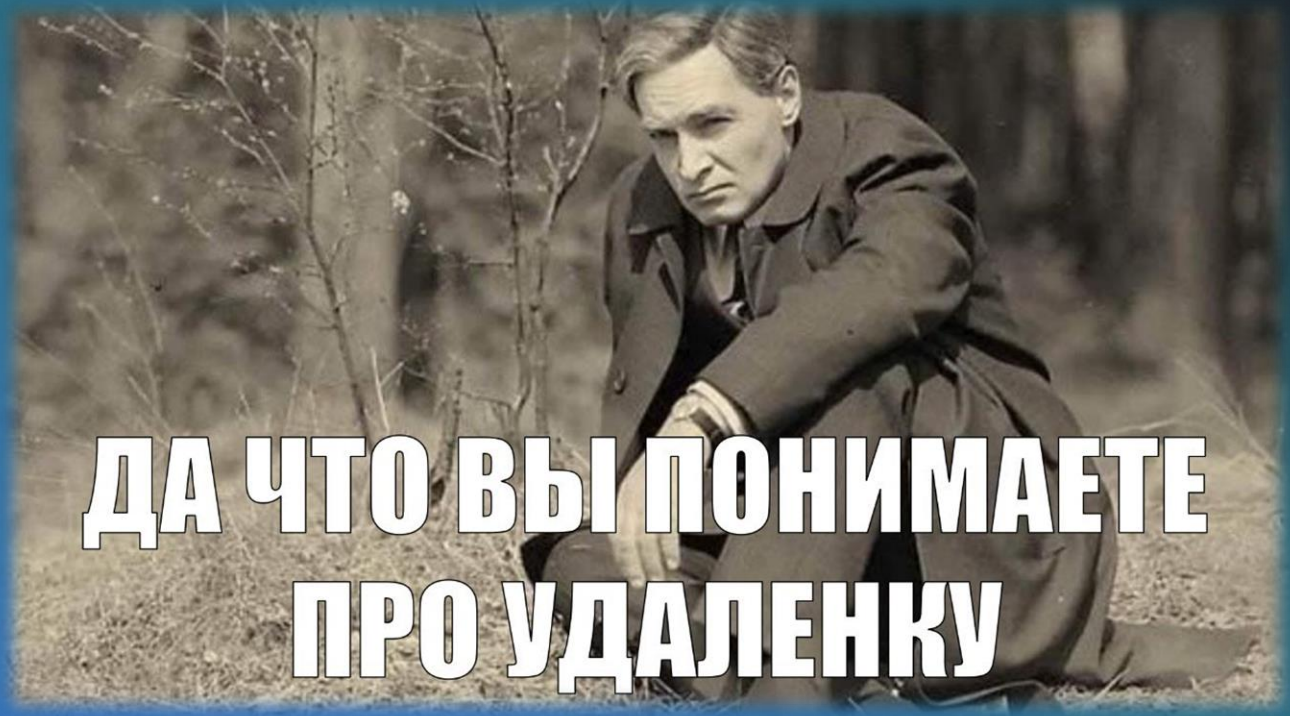
ВЫГОДА

Сохранение финансов при заключении договоров

www.it-bastion.com

АЙТИБАСТИОН

А ЧТО ДЕЛАТЬ, ЕСЛИ ВСЁ ЗАПРЕЩЕНО?



АЙТИБАСТИОН

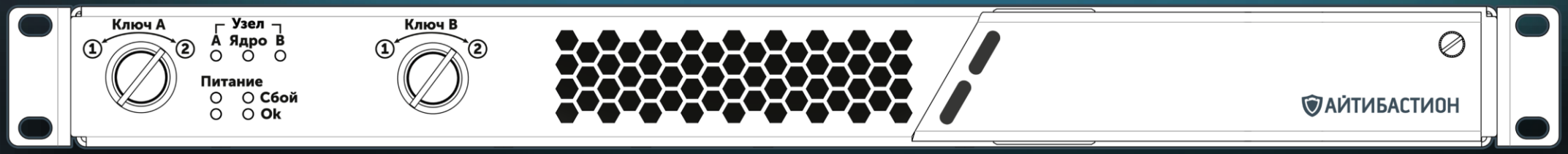
СИНЭНИКС

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

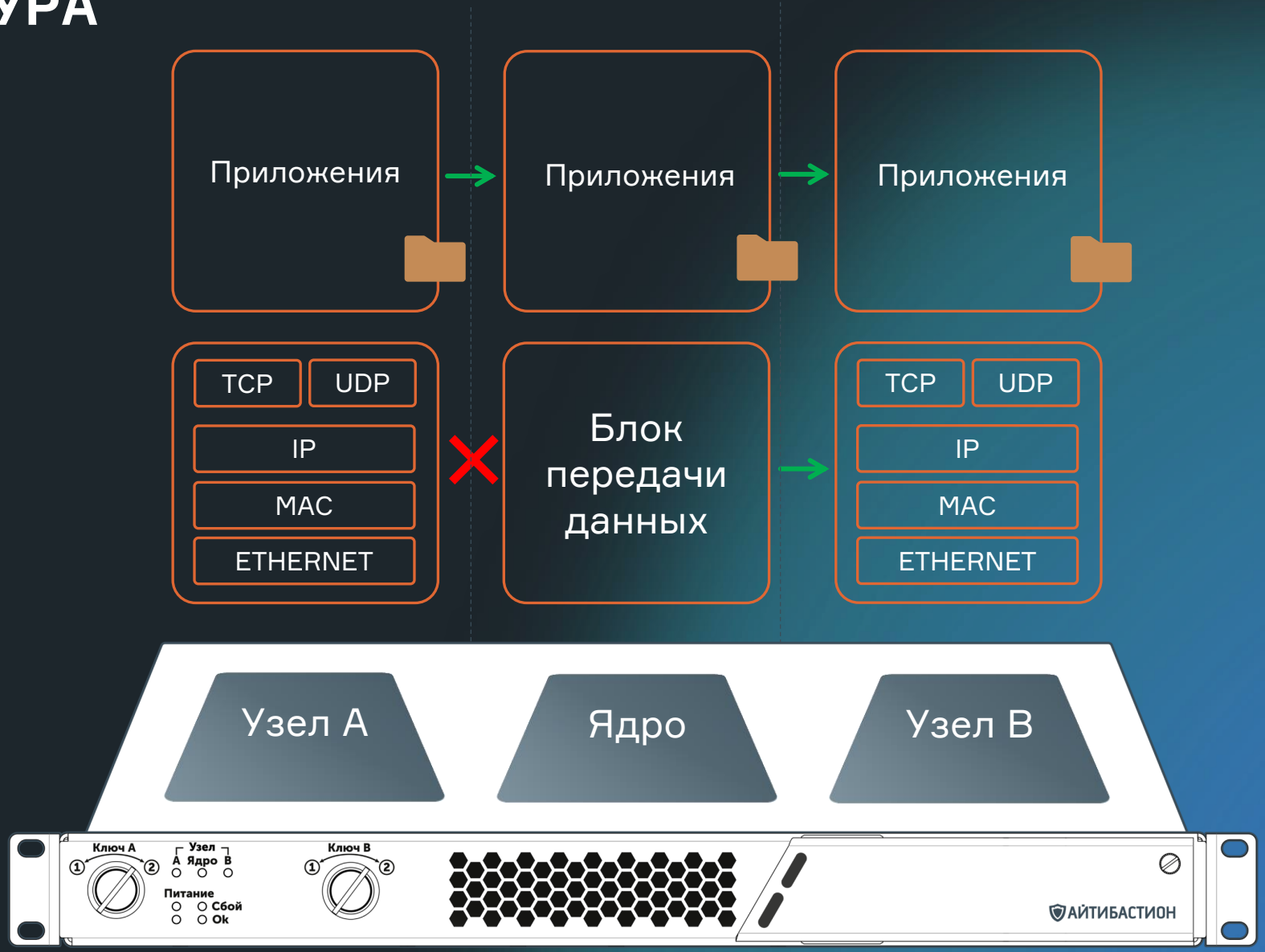
- TCP, UDP, в т.ч. Однонаправленная
- Независимые политики для двух контуров
- Скорость до 1 Гб/с
- Соединение «точка-точка»
- Поддержка работы с МЭ, NGFW и другим сетевым оборудованием

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
АРХИТЕКТУРА

АЙТИБАСТИОН

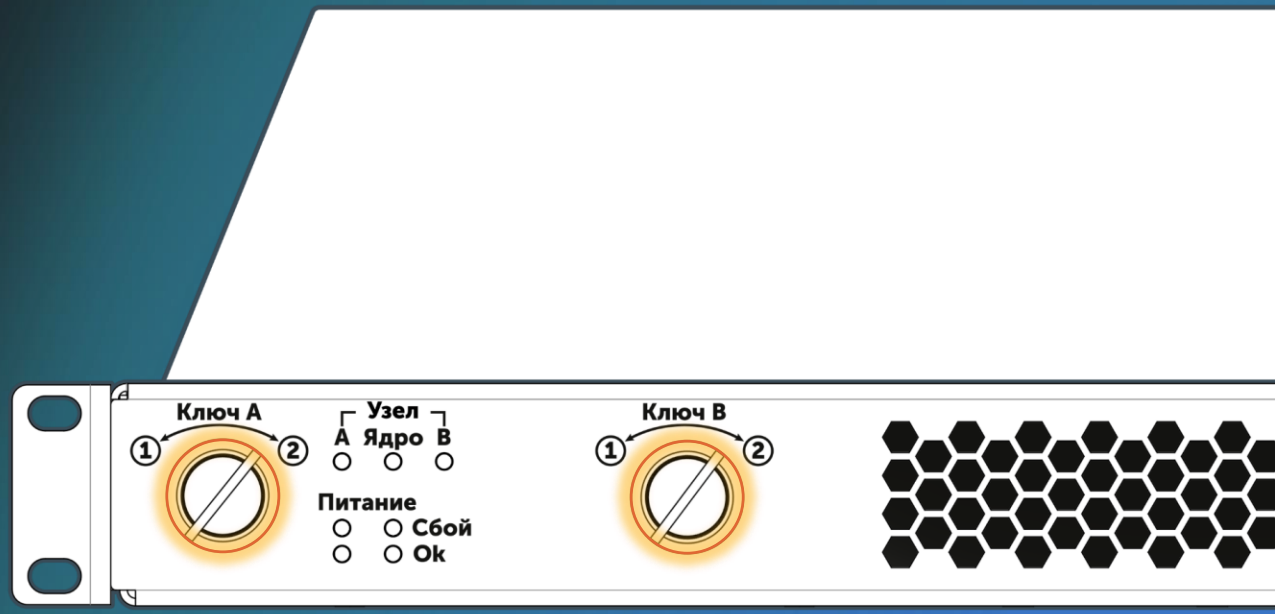


СИНОНИКС
АРХИТЕКТУРА

АЙТИБАСТИОН

ДОПОЛНИТЕЛЬНЫЙ ФИЗИЧЕСКИЙ КОНТРОЛЬ

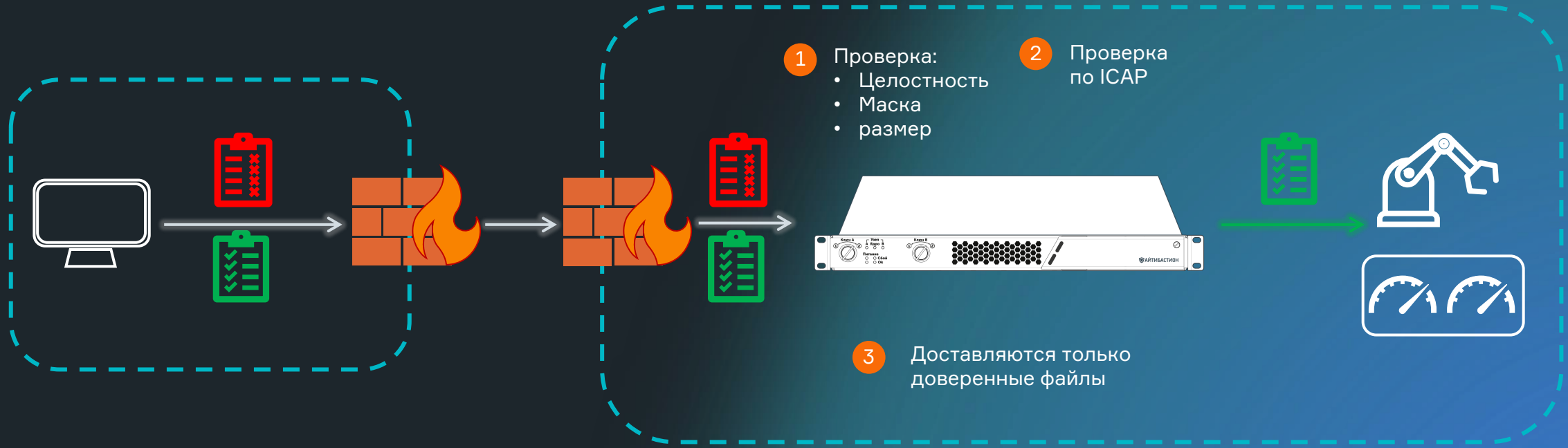
Дополнительный контроль обеспечивается с помощью физических пусковых ключей, разделяемых между сотрудниками, каждый из которых ответственен за свою сеть. Ключи разрешают или блокируют передачу данных через Синоникс путем полного отключения питания Ядра. При повороте одного из них, центральная плата отключается.



СИНЕНИКС
СЦЕНАРИЙ

АЙТИБАСТИОН

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



АЙТИБАСТИОН

Спасибо за внимание!

Александр Карпов

a.karpov@it-bastion.com

+7 499 322 3667

it-bastion.com