2024

www.it-bastion.com

2024

КОНТРОЛЬ ПРИВИЛЕГИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ И КОНТРОЛЬ ОБМЕНА ИНФОРМАЦИЕЙ: КАК ИЗМЕНИЛСЯ РАМ СКДПУ НТ И ЧЕМ ПОЛЕЗЕН СИНОНИКС

АЛЕКСАНДРА ГОНЧАРОВА

АЙТИБАСТИОН

КОМПАНИЯ АЙТИ БАСТИОН

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

СКОПУ НТ СИНЭНИКС

СКДПУ НТ
ЗАКАЗЧИКИ

ОАК

НОРНИКЕЛЬ

ВЭБ РФ

МСП

РОССЕТИ ЛЕНЭНЕРГО

ОСК
ОБЪЕДИНЕННАЯ СУДОСТРОИТЕЛЬНАЯ КОРПОРАЦИЯ

РОСНЕФТЬ

РусГидро

ПРАВИТЕЛЬСТВО МОСКВЫ

Северсталь

МИНИСТЕРСТВО ТРАНСПОРТА РФ

РОСЭНЕРГОАТОМ
ЭЛЕКТРОЭНЕРГЕТИЧЕСКИЙ ДИВИЗИОН РОСАТОМА

Ростех

ГАЗПРОМ ЭНЕРГОХОЛДИНГ

ВОЕНТЕЛЕКОМ

СОГЛАСИЕ страхование

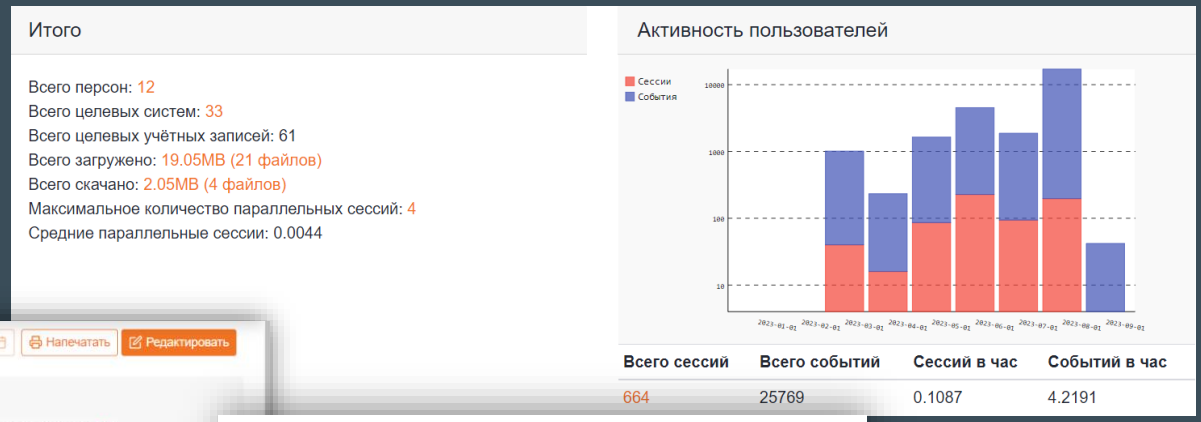
АЙТИБАСТИОН

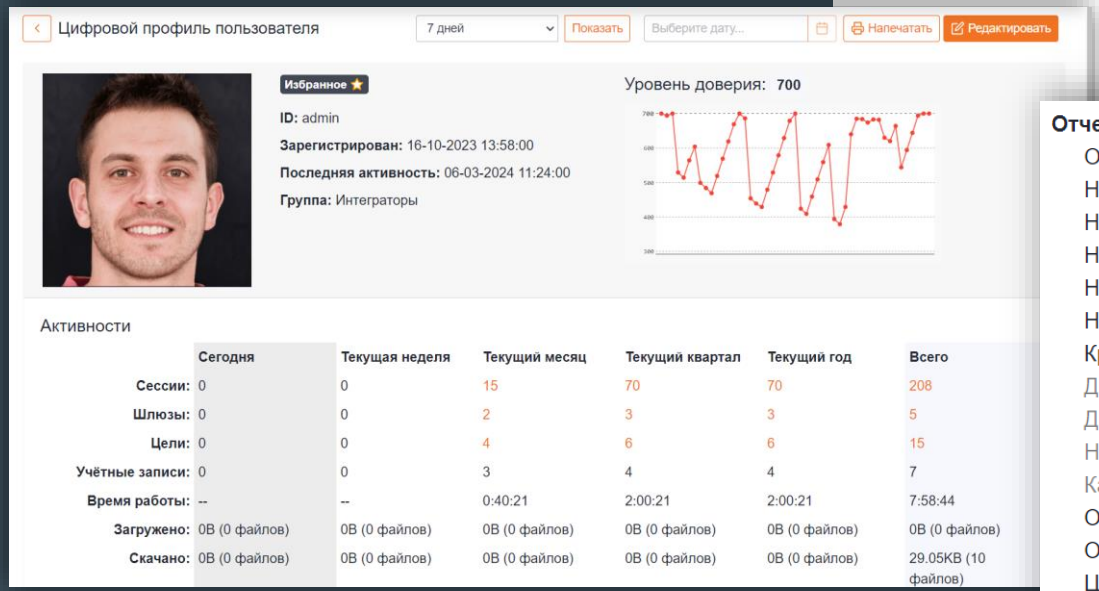
www.it-bastion.com

СКДПУ НТ
МОНИТОРИНГ И АНАЛИТИКА

АЙТИБАСТИОН

Единая точка мониторинга и аудита для нескольких площадок. Графическое представление событий в сессиях.





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

Обширная библиотека отчётов для ретроспективного анализа сессий и состояния инфраструктуры

Построение поведенческой модели пользователей и реакция на отклонение от типичного поведения в сессии

www.it-bastion.com

Сертификация

ФСТЭК России

Работа продукта на базе отечественной операционной системы Astra Linux SE

ASTRA LINUX®

Привлечение дистанционных специалистов

- Организация контролируемой работы подрядчиков
- Возможность обеспечения доступа в разные филиалы для решения задач
- Реализация доступов внутренних сотрудников в удалённые ЦОДы

СКДПУ НТ
ПОРТАЛ ДОСТУПА

АЙТИБАСТИОН

СКДПУ НТ
ШЛЮЗ ДОСТУПА
ХАБАРОВСК
10.0.56.789

СКДПУ НТ
ШЛЮЗ ДОСТУПА
САНКТ-ПЕТЕРБУРГ
172.15.98.765

СКДПУ НТ
ШЛЮЗ ДОСТУПА
НОРИЛЬСК
10.0.123.456

www.it-bastion.com

СКДПУ НТ
ПОРТАЛ ДОСТУПА

АЙТИБАСТИОН

Доступ в концепции «нулевого доверия»

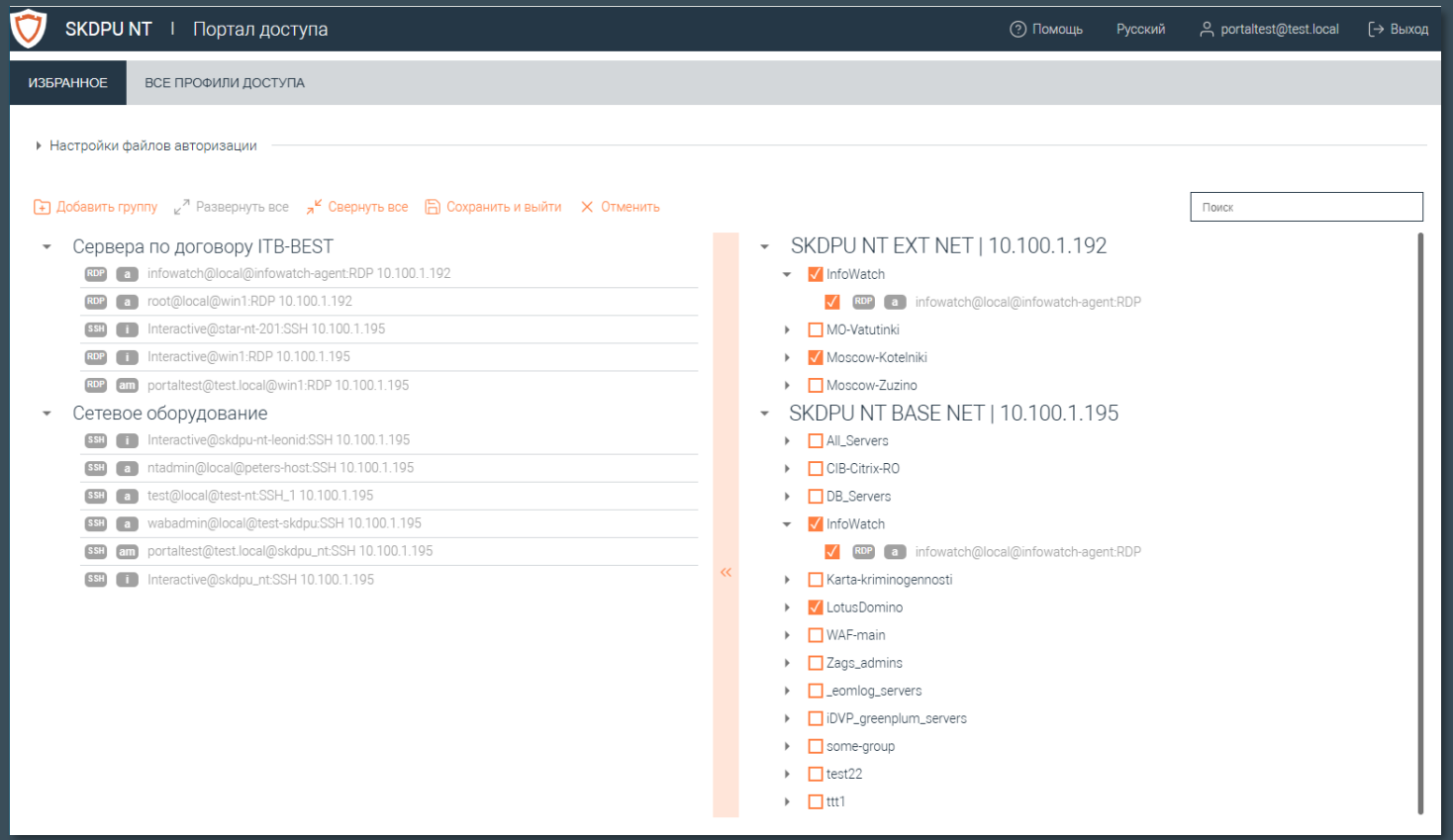
Система сохраняет концепцию «минимально необходимых прав» и не предоставляет доступы к инфраструктуре, если они не были выданы «в явном виде»

Группировка доступов

Система позволяет сформировать единый структурированный список для всех существующих объектов доступа

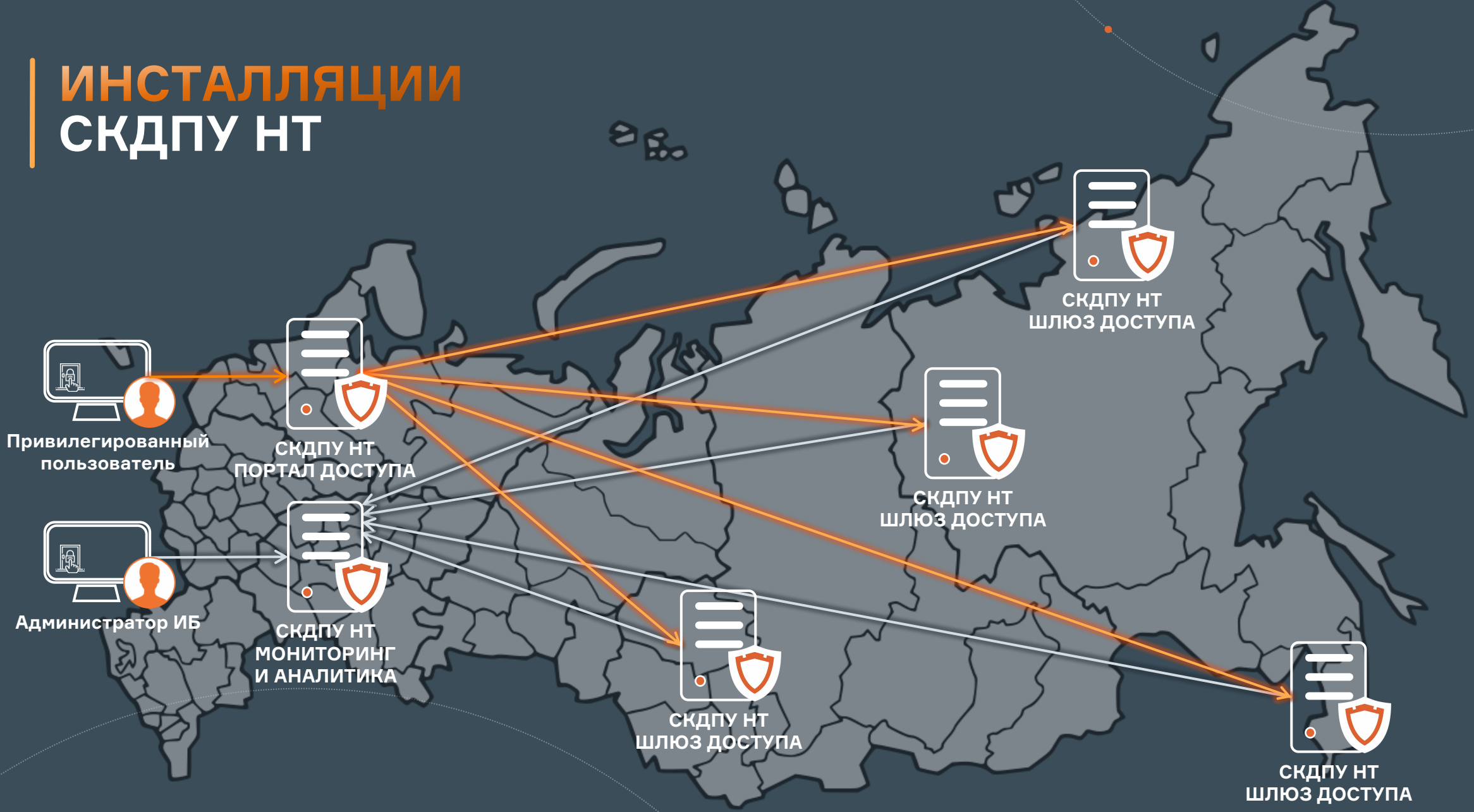
Поддержка встроенных клиентов доступа

Работа и доступ к целевым системам обеспечивается встроенными средствами рабочей станции пользователя. Установка дополнительного ПО для работы необязательна.



www.it-bastion.com

ИНСТАЛЛЯЦИИ
СКДПУ НТ

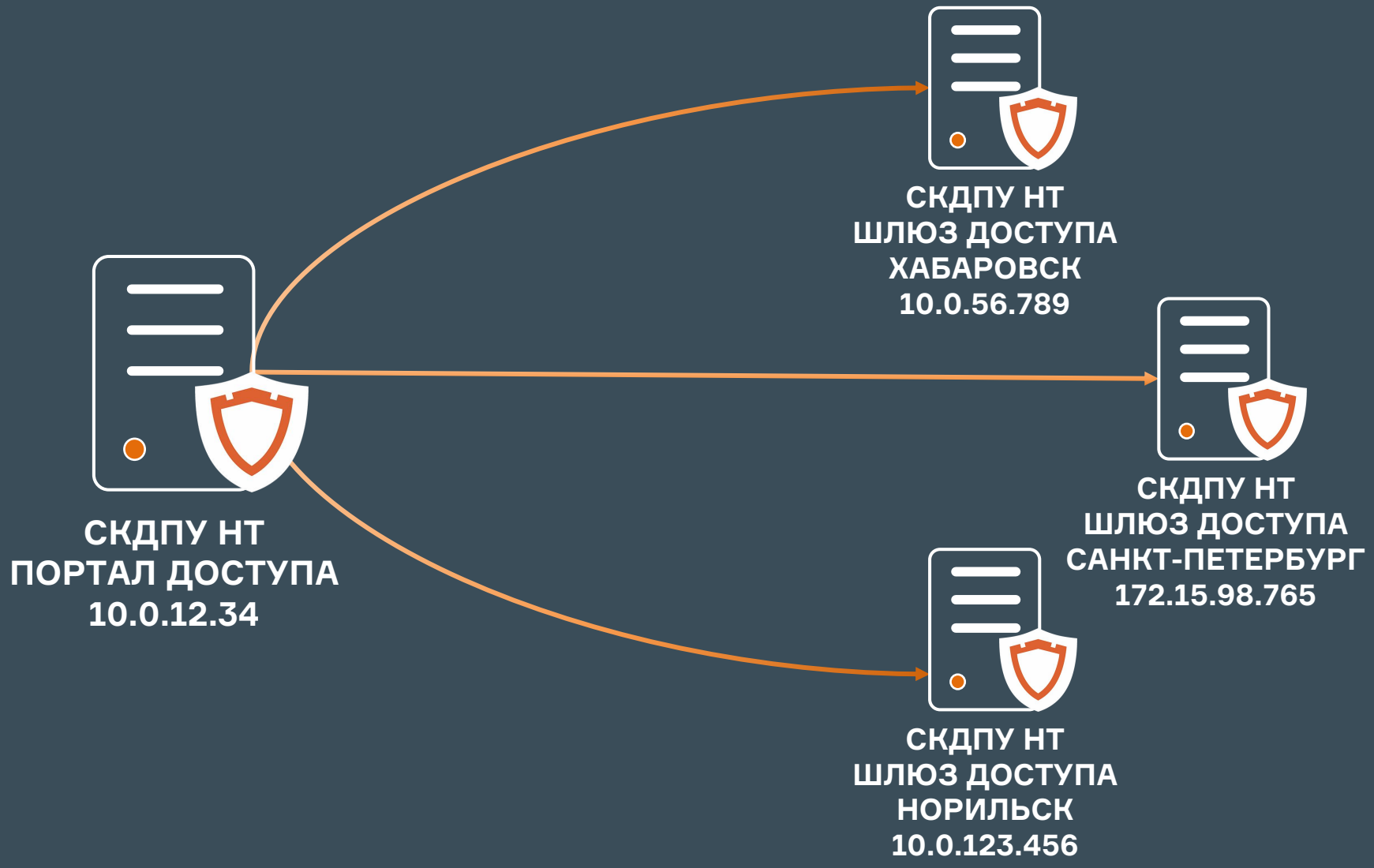


www.it-bastion.com

АЙТИБАСТИОН

СКДПУ НТ
ПОРТАЛ ДОСТУПА

АЙТИБАСТИОН



www.it-bastion.com

Повышение эффективности при работе с матрицей доступов

- Оптимизация управления доступами
- Минимизация ошибочных доступов
- Исключение назначения ролей, превышающих полномочия сотрудника

СКДПУ НТ
КАБИНЕТ ОПЕРАТОРА

Снижение нагрузки на Администратора ИБ

Сервис поможет упростить процесс предоставления и контроля привилегированного доступа, когда PAM-система используется сразу нескольким подразделениям и группам. При этом реализуется мультитенантность системы в рамках единой инфраструктуры.

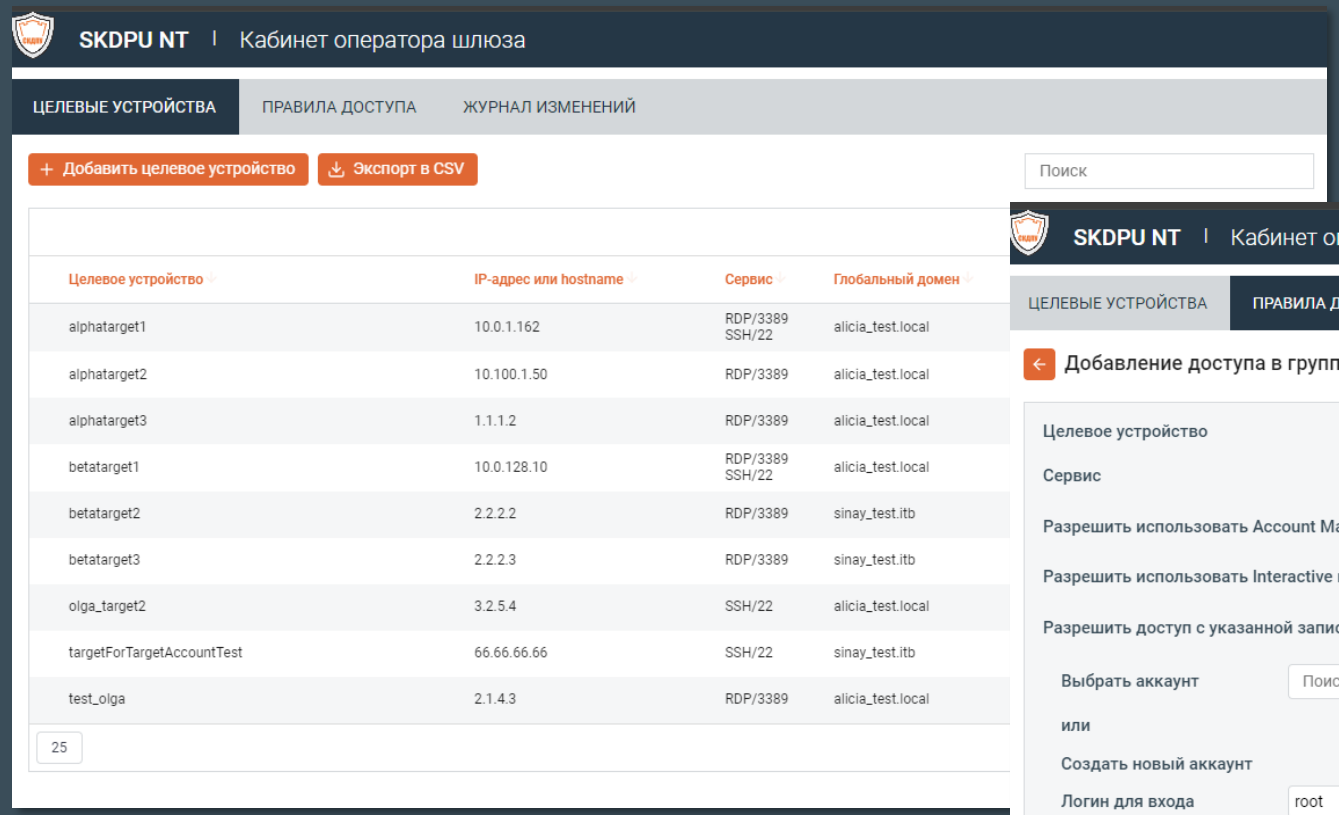
Сохранение минимально допустимых прав

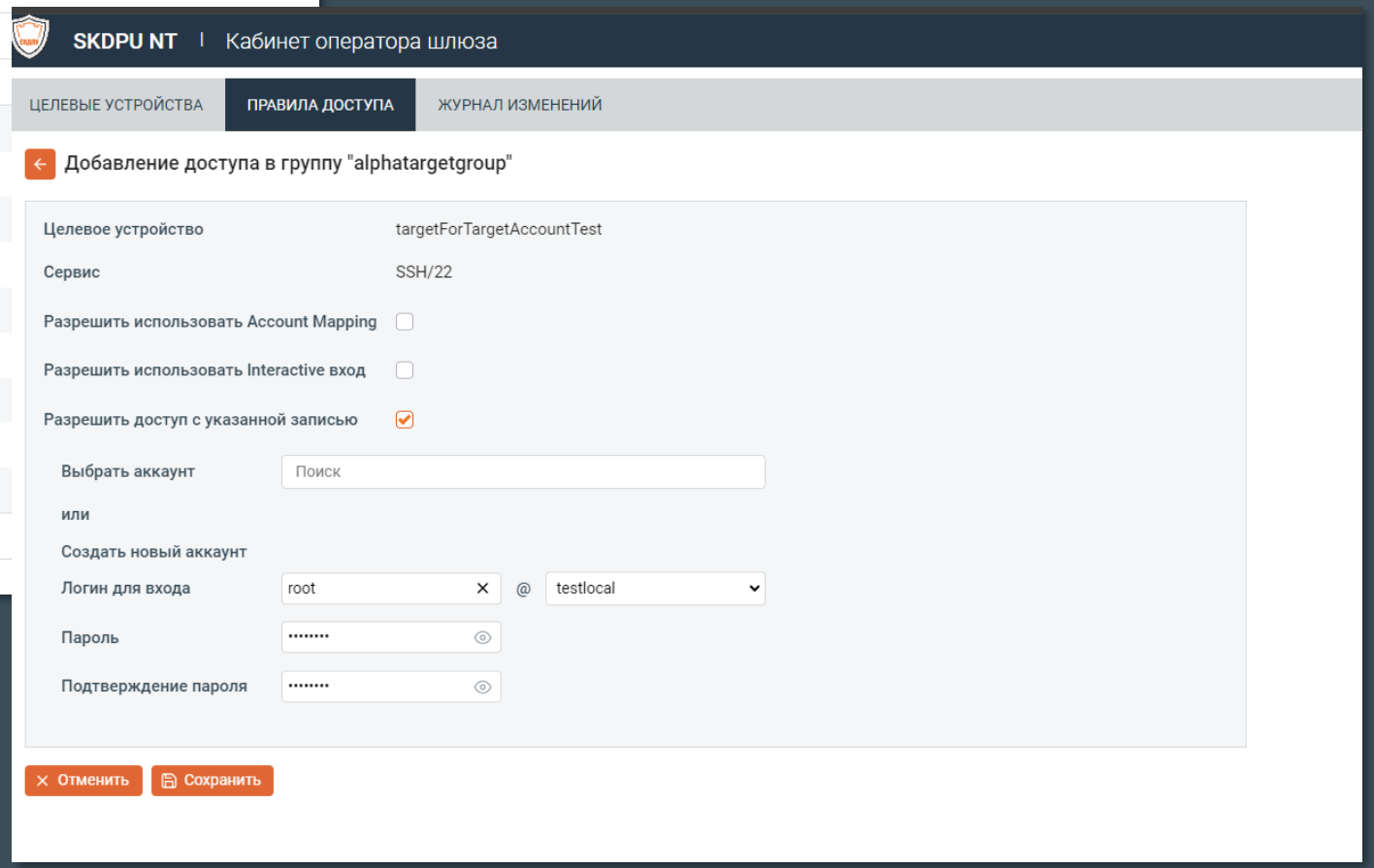
Операторам предоставляется минимально необходимые полномочия по организации доступа и за счет этого сокращается количест ошибок при передаче доступов пользователю

СКДПУ НТ
КАБИНЕТ ОПЕРАТОРА

АЙТИБАСТИОН

www.it-bastion.com





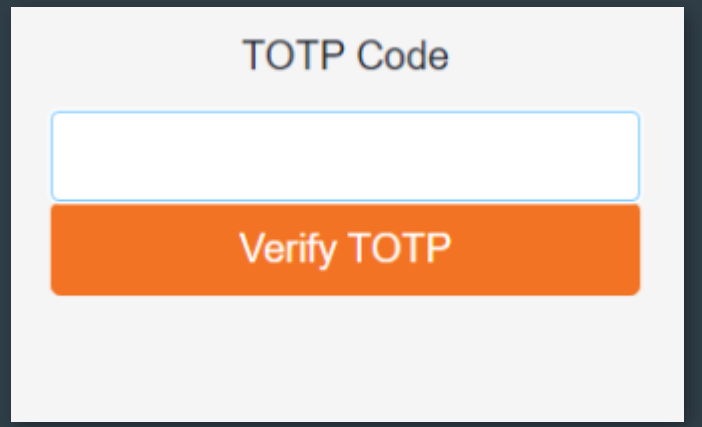
АРХИВ АУДИТА
В СКДПУ НТ КОМПЛЕКС

Централизованное хранилище записей сессий пользователей с разных Шлюзов, установленных в инфраструктуре

TOTP
В СКДПУ НТ КОМПЛЕКС

АЙТИБАСТИОН

2FA на базе TOTP



АЙТИБАСТИОН

СКДПУ НТ
ТЕХНОЛОГИЧЕСКИЕ ПАРТНЁРСТВА

ASTRA LINUX®

POSITIVE TECHNOLOGIES

kaspersky

INFOWATCH®

Пассворк

DATALINE

GIS
ГАЗИНФОРМ СЕРВИС

ROSA

CyberLympha®

РУТОКЕН

Аладдин

zVirt

alt linux

с•терра®

MULTIFACTOR

UserGate

Rusiem

КОД безопасности

РЕДОС

и другие партнеры

www.it-bastion.com

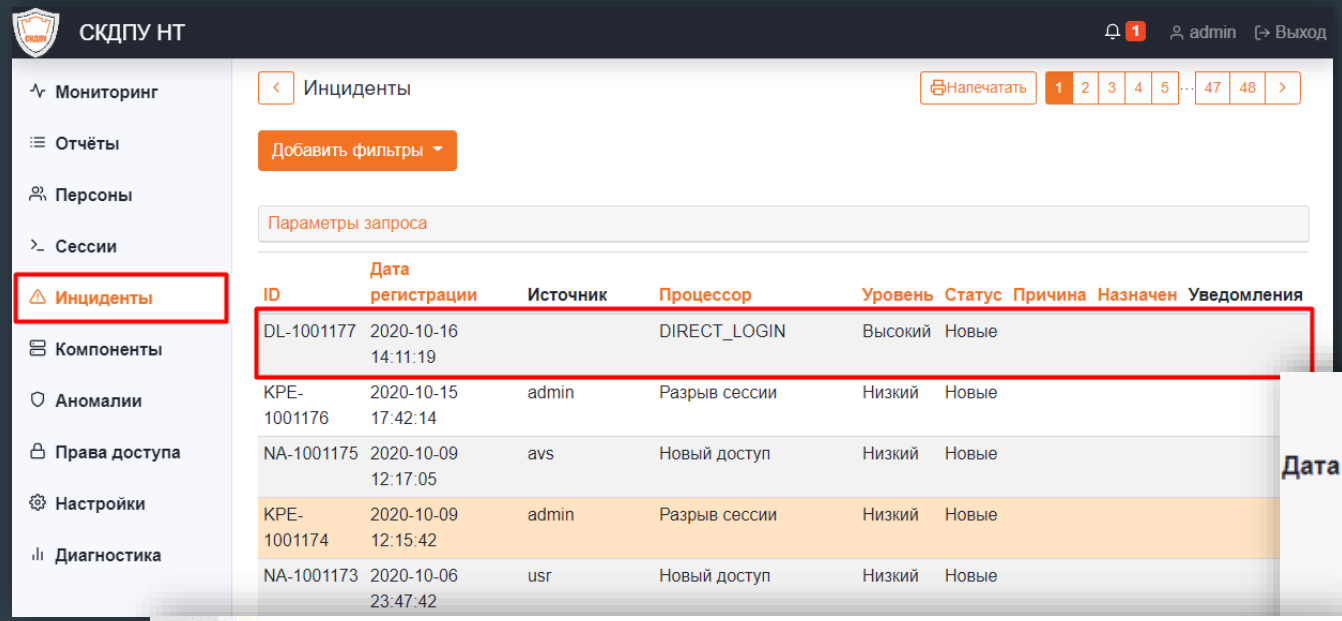
АЙТИБАСТИОН

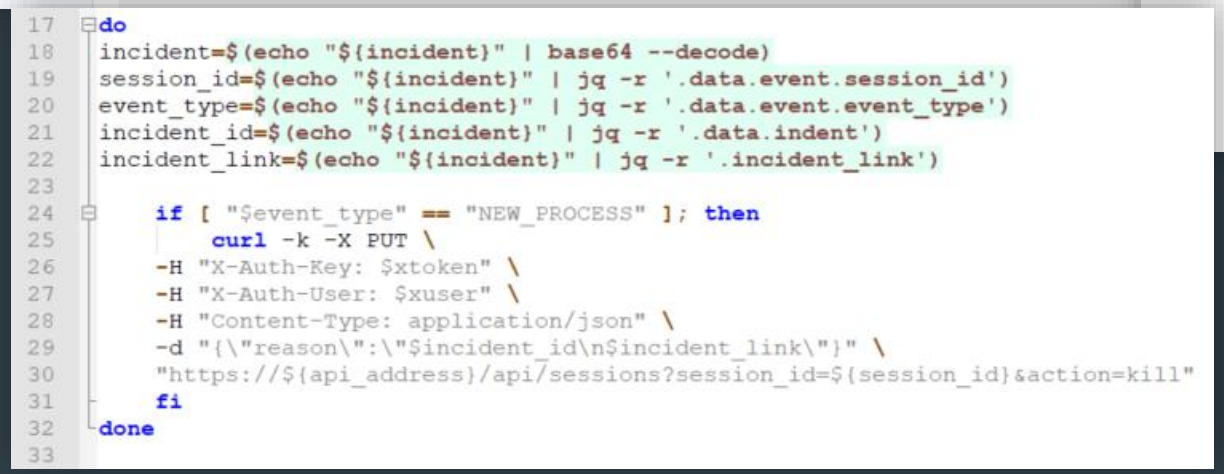
Исключение доступа в обход PAM

- Контроль всех подключений в инфраструктуре
- Выявление попыток нелегитимного доступа
- Обогащение смежных систем событиями

РЕАЛИЗАЦИЯ
В СКДПУ НТ КОМПЛЕКС

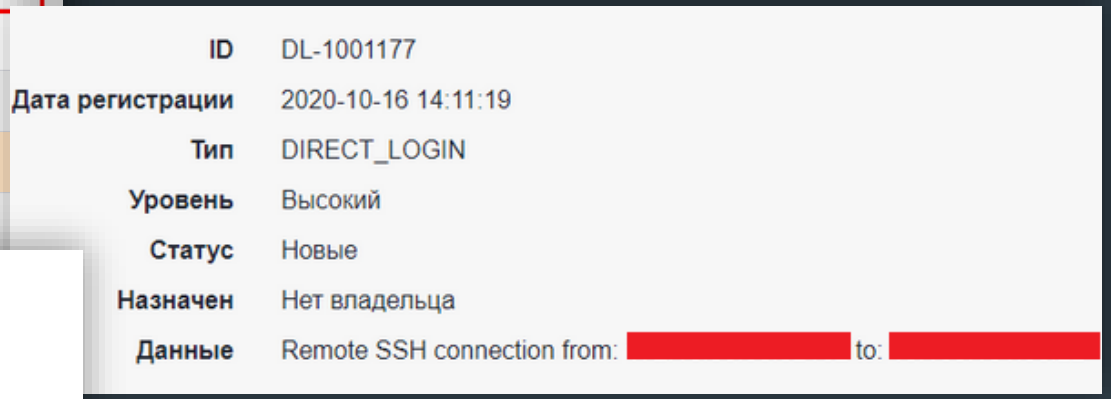
АЙТИБАСТИОН





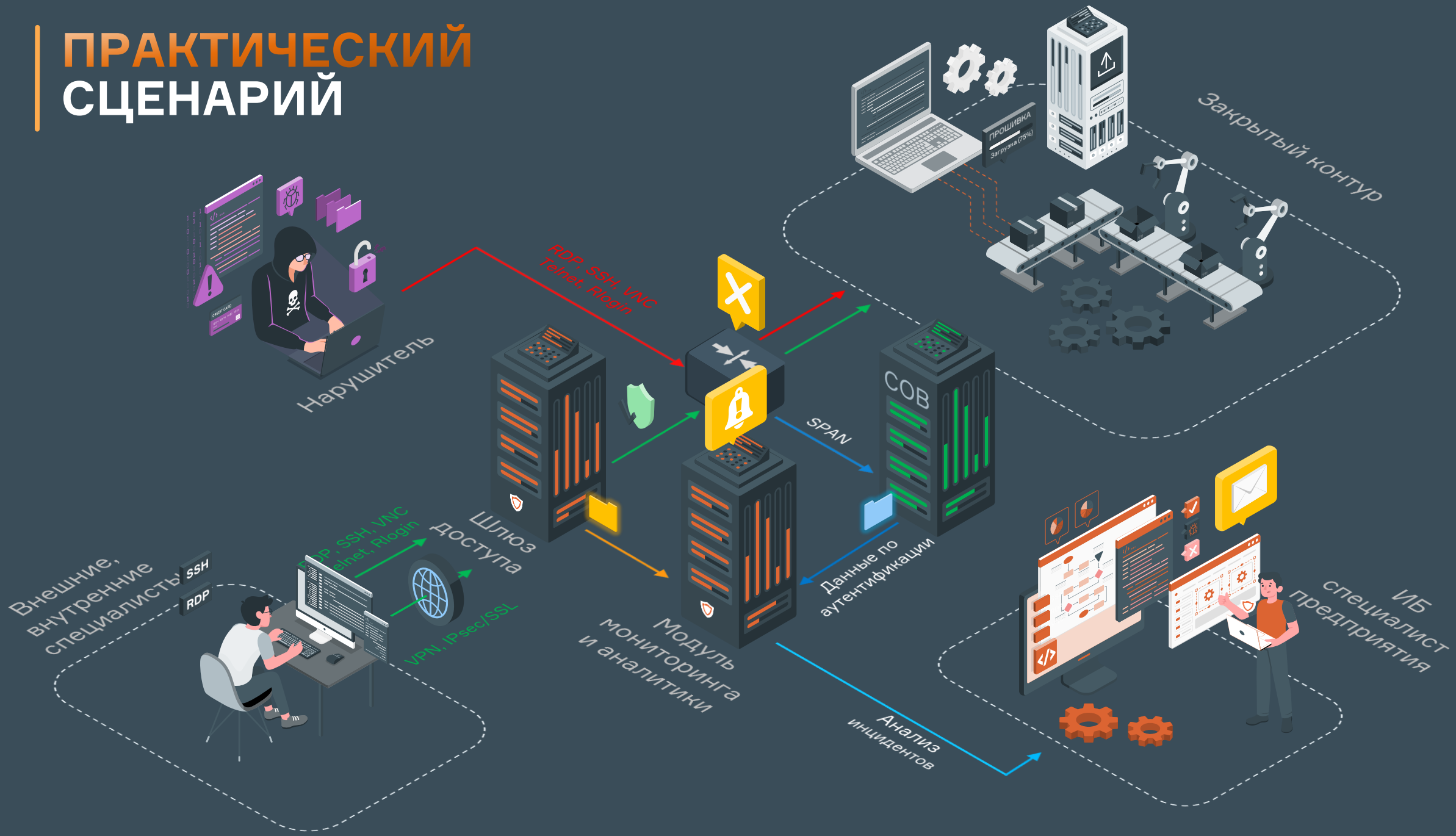
```
do
incident=$(echo "${incident}" | base64 --decode)
session_id=$(echo "${incident}" | jq -r '.data.event.session_id')
event_type=$(echo "${incident}" | jq -r '.data.event.event_type')
incident_id=$(echo "${incident}" | jq -r '.data.indent')
incident_link=$(echo "${incident}" | jq -r '.incident_link')

    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
```



www.it-bastion.com

ПРАКТИЧЕСКИЙ СЦЕНАРИЙ



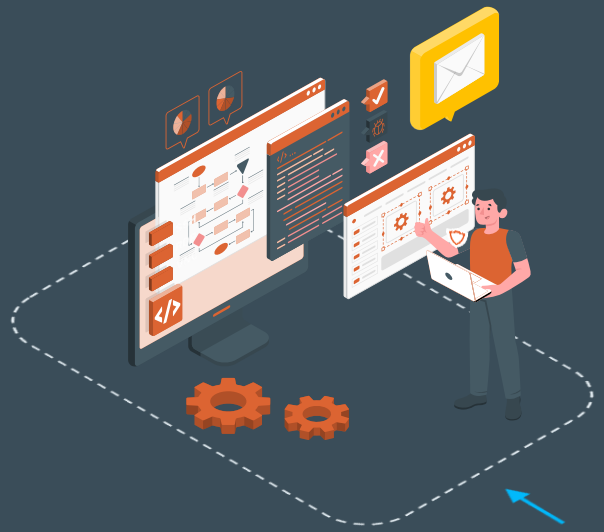
АЙТИБАСТИОН

ЗАДАЧИ
В ИЗОЛИРОВАННЫХ СИСТЕМАХ

www.it-bastion.com

АЙТИБАСТИОН

ЗАДАЧИ
В ИЗОЛИРОВАННЫХ СИСТЕМАХ

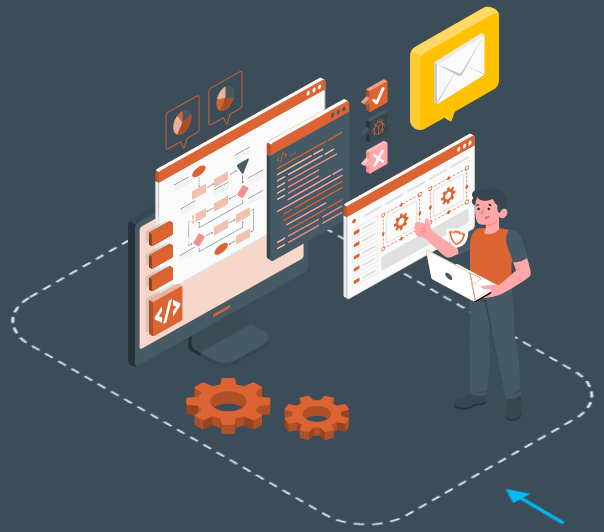


Внешние, внутренние специалисты

www.it-bastion.com

АЙТИБАСТИОН

ЗАДАЧИ
В ИЗОЛИРОВАННЫХ СИСТЕМАХ



Внешние, внутренние специалисты

VPN, IPsec/SSL

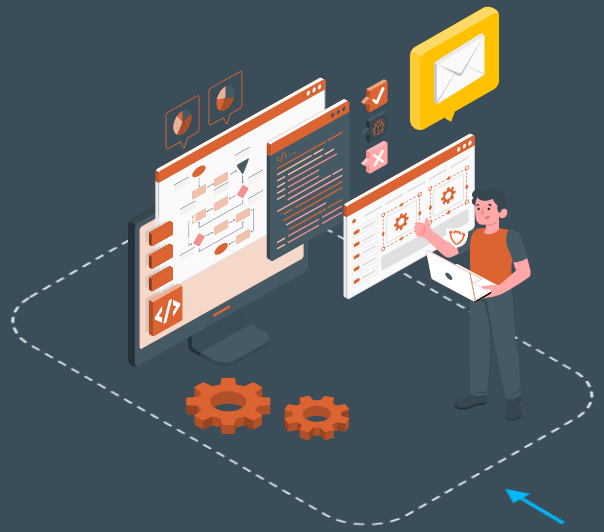
Передача в контур

Обновление
Настройка
Базы
Файлы
Иные данные

www.it-bastion.com

ЗАДАЧИ
В ИЗОЛИРОВАННЫХ СИСТЕМАХ

АЙТИБАСТИОН



Передача из контура

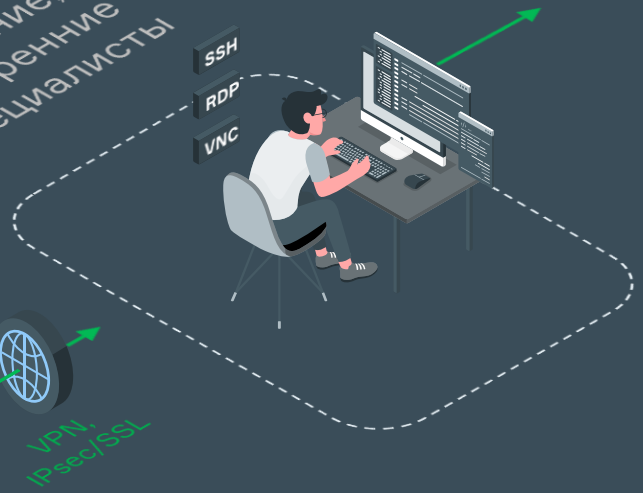
Телеметрия

Логи

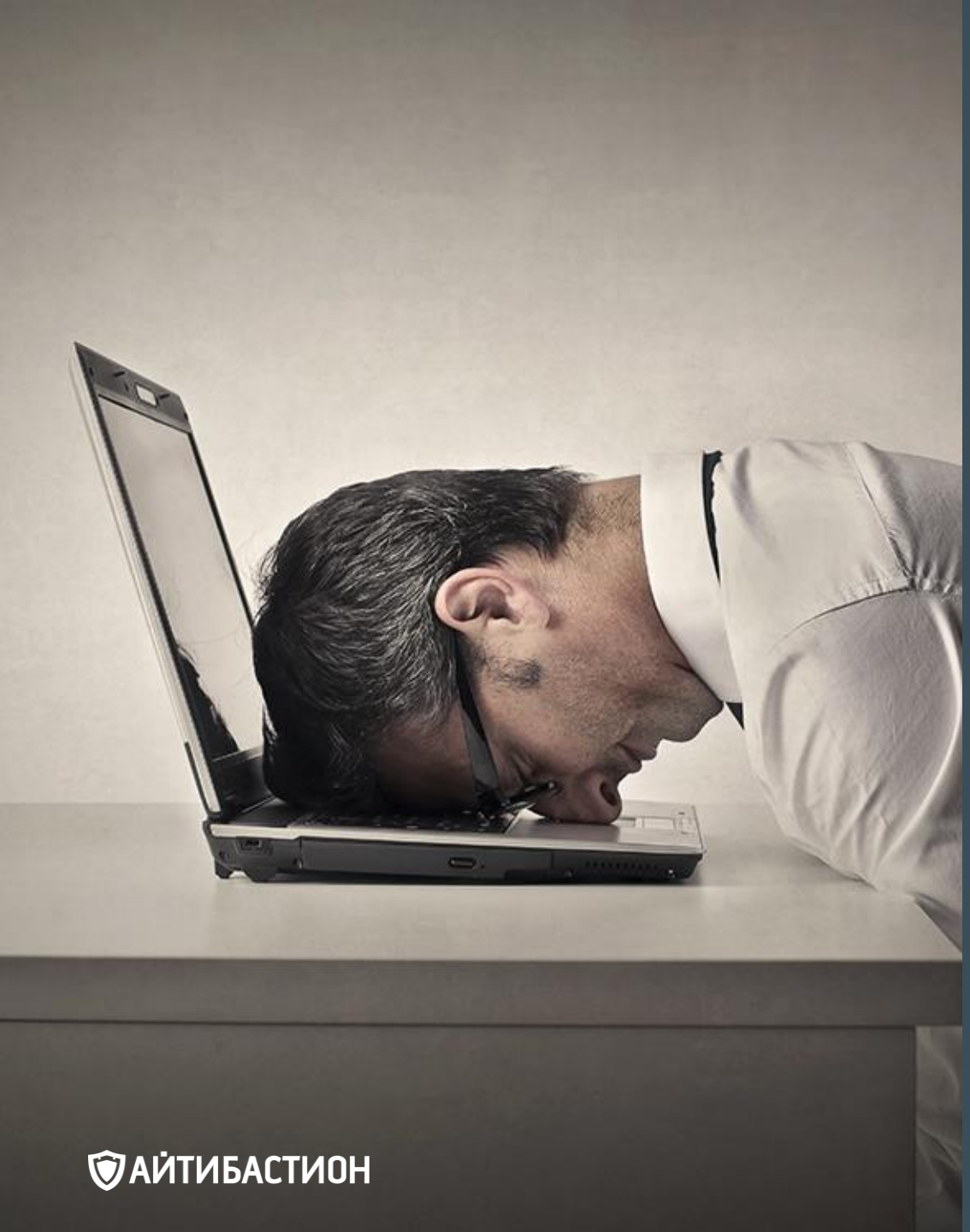
Базы

Иные данные

Внешние, внутренние специалисты



www.it-bastion.com



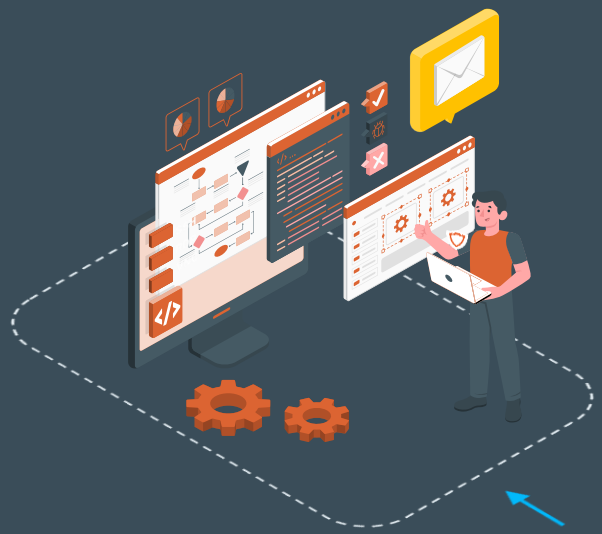
АЙТИБАСТИОН

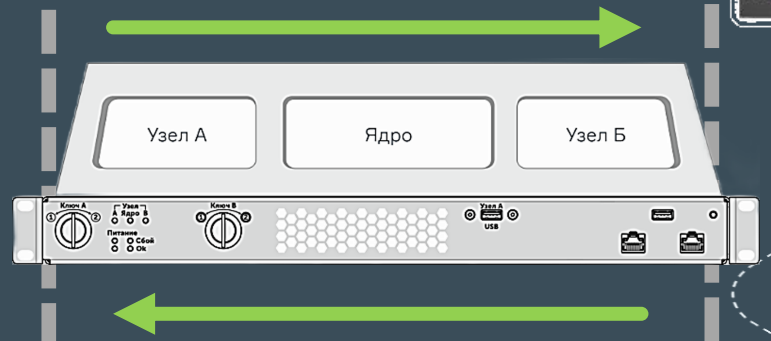
- ТРУДОЗАТРАТЫ
- ВРЕМЯ
- АКТУАЛЬНОСТЬ
- БЕЗОПАСНОСТЬ

www.it-bastion.com

АЙТИБАСТИОН

ЗАДАЧИ
В ИЗОЛИРОВАННЫХ СИСТЕМАХ





Внешние, внутренние специалисты

www.it-bastion.com

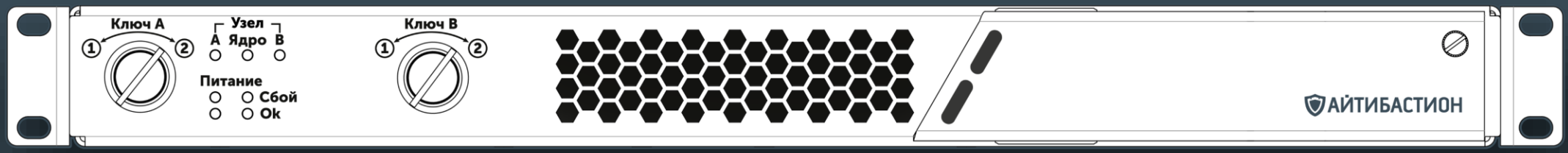
СИНОНИКС
ТЕХНИЧЕСКАЯ РЕАЛИЗАЦИЯ

АЙТИБАСТИОН

www.it-bastion.com

Система контроля информационного обмена

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



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 контрольных сумм, размера и маски файлов
- Внешняя валидация по ICAP (DLP, Sandbox, AV и др.)
- Автоматизация процесса доставки файлов

КОМБИНИРОВАННЫЙ РЕЖИМ

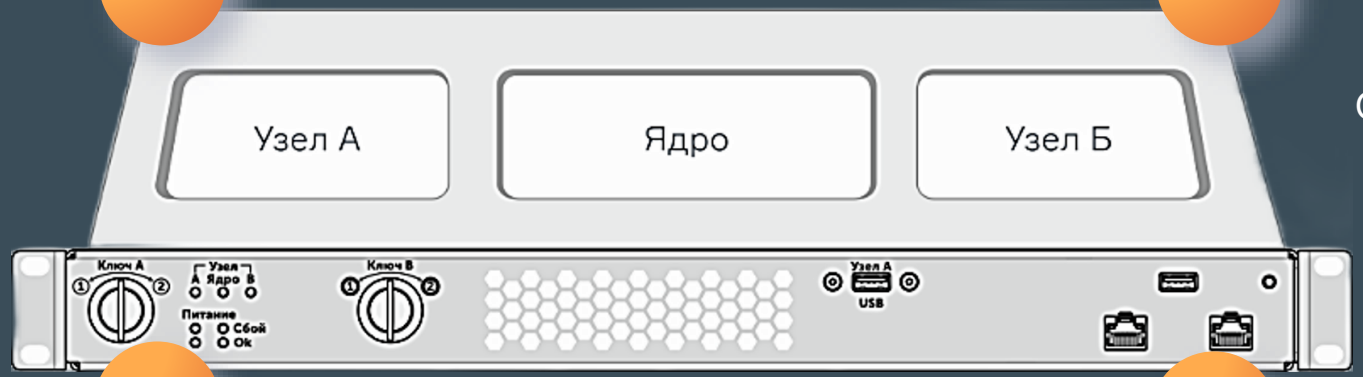
СИНОНИКС
ТЕХНИЧЕСКАЯ РЕАЛИЗАЦИЯ

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

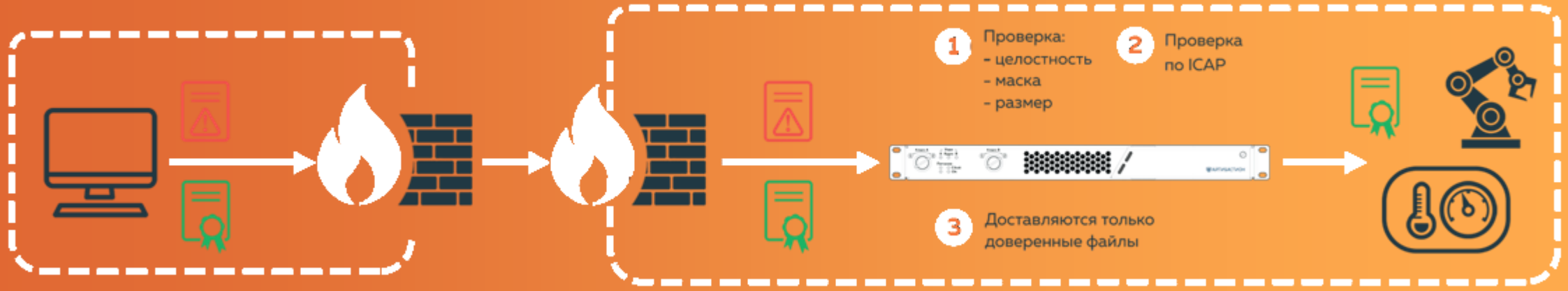
до 1 Гб/с
до 256 каналов

www.it-bastion.com

АЙТИБАСТИОН

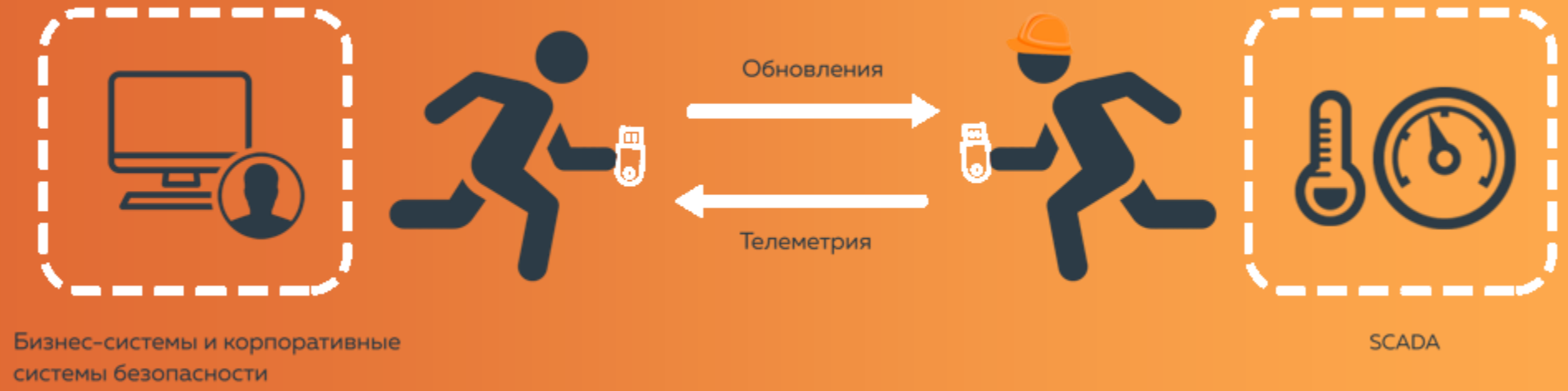
Обновление баз АВЗ в изолированных системах

Обновление баз АВЗ с использованием Синоникса



АЙТИБАСТИОН

Передача данных из изолированных систем



АЙТИБАСТИОН

Передача данных между системами при помощи Синоникса

Бизнес-системы и корпоративные системы безопасности

SCADA

СИНОНИКС
ТЕХНИЧЕСКАЯ РЕАЛИЗАЦИЯ

АЙТИБАСТИОН

Система А

192.168.xx.xx

Здесь правила задаю я

Приложения → Приложения → Приложения

TCP | UDP
IP
MAC
ETHERNET

✕ Блок передачи данных →

TCP | UDP
IP
MAC
ETHERNET

Система В

10.0.xx.xx

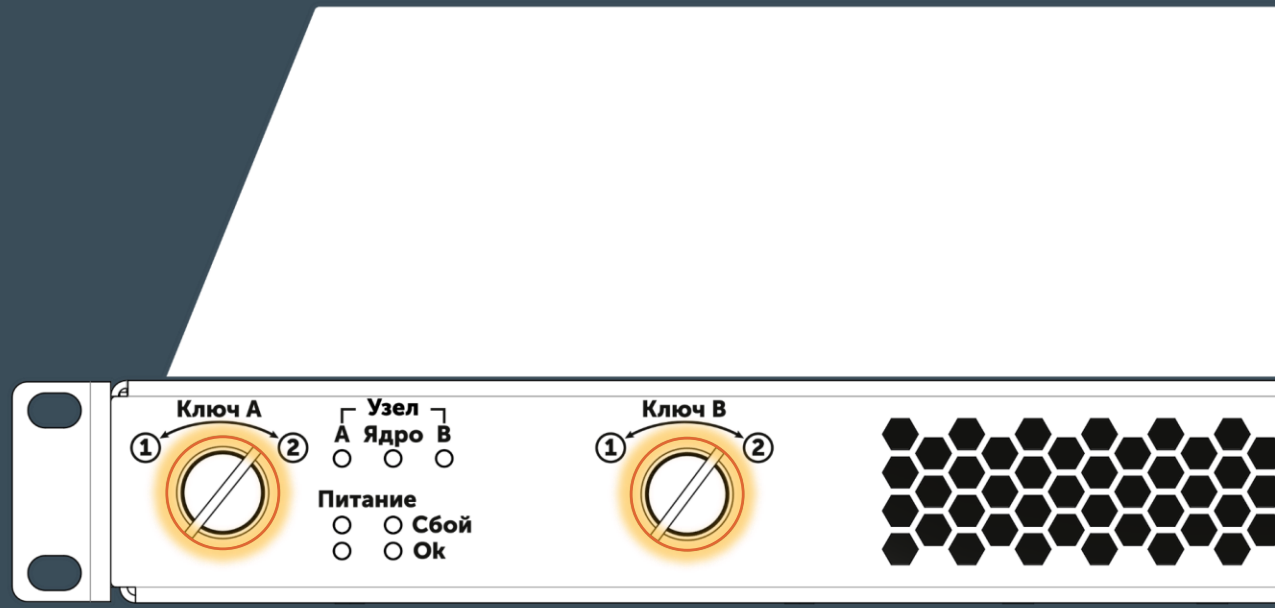
А здесь я

СИНОНИКС
ТЕХНИЧЕСКАЯ РЕАЛИЗАЦИЯ

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

СИНОНИКС
ТЕХНИЧЕСКАЯ РЕАЛИЗАЦИЯ

- 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

СИНОНИКС
ТЕХНОЛОГИЧЕСКИЕ ПАРТНЁРСТВА

Антивирусы

kaspersky

Dr.WEB

МЭ/NGFW

КОД безопасности

UserGate

сотерра

DLP

INFOWATCH

SOLAR

и другие решения

www.it-bastion.com

НАША ЭКСПЕРТИЗА

при решении ваших задач

Комплексный подход к ИБ позволяет АйТи Бастион решать множество задач в реальных инфраструктурах на практике.

Мы не только разрабатываем продукты, но и качественно используем компетенции и опыт, приобретённые в проектах разного масштаба.

Благодарю за внимание!

АЙТИБАСТИОН

Гончарова Александра
инженер-пресейл

a.goncharova@it-bastion.com

+7 499 495 45 40

it-bastion.com