АйТи БАСТИОН

ПАК
контроль подрядчиков
данные
РАМ
отказоустойчивость
Цифровой профиль пользователя
контроль
СКДПУ НТ
односторонняя передача
КИИ
контроль удаленной работы
SSO
удаленный доступ
уровень доверия
API
аналитика
детектор аномалий
отчеты
Синоним
SIEM
ICAP
безопасная передача данных
контроль данных
DLP
масштабирование
AstraLinux
поведенческий анализ
АСУ ТП
контроль администраторов
однонаправленный шлюз

ФСТЭК России ОУД-4

Реестр отечественного ПО

МО РФ РД НДВ-2

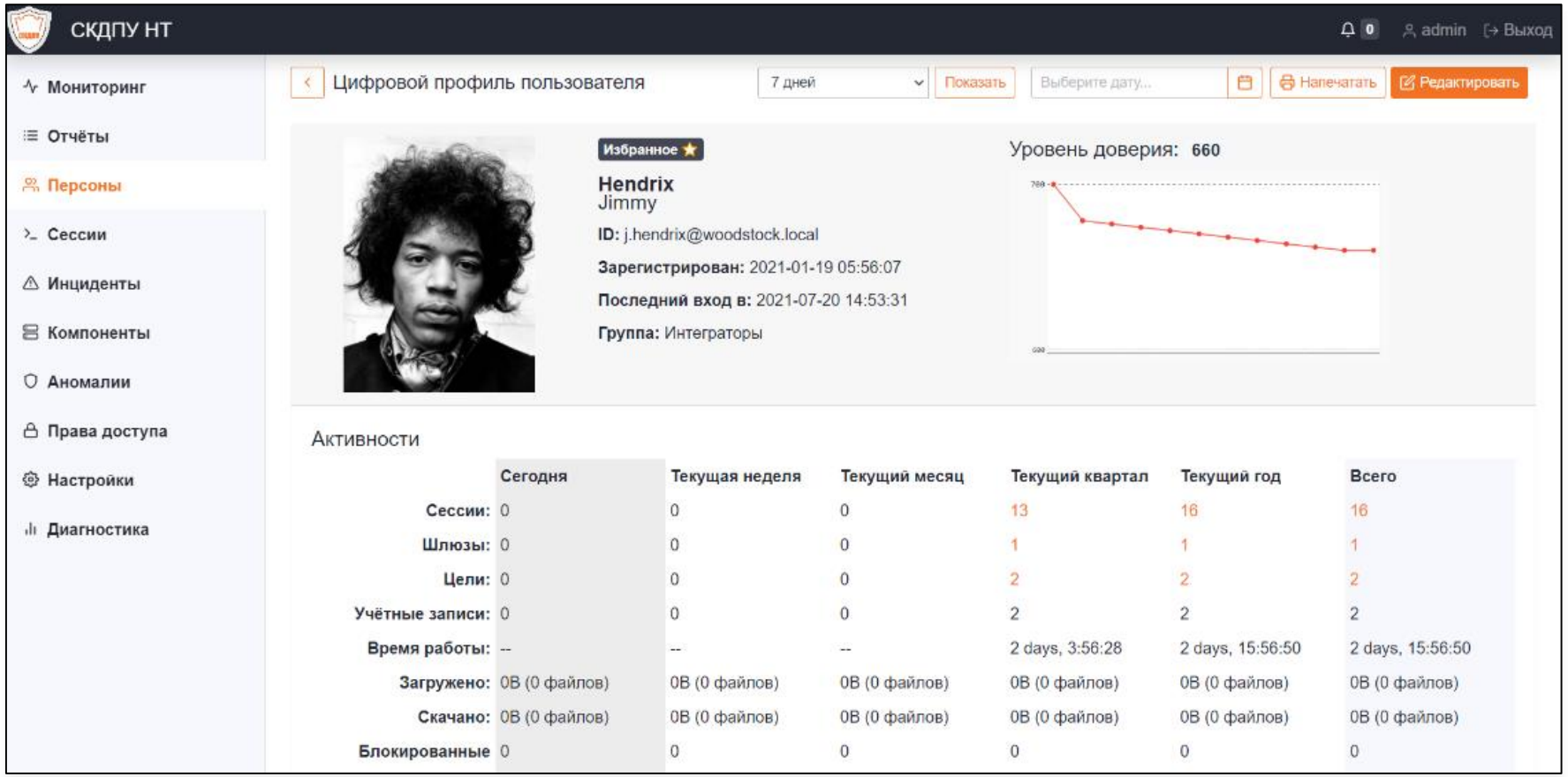
АЙТИБАСТИОН

Работа с привилегированными пользователями

Построение контролируемого доступа и мониторинг действий

АЙТИБАСТИОН

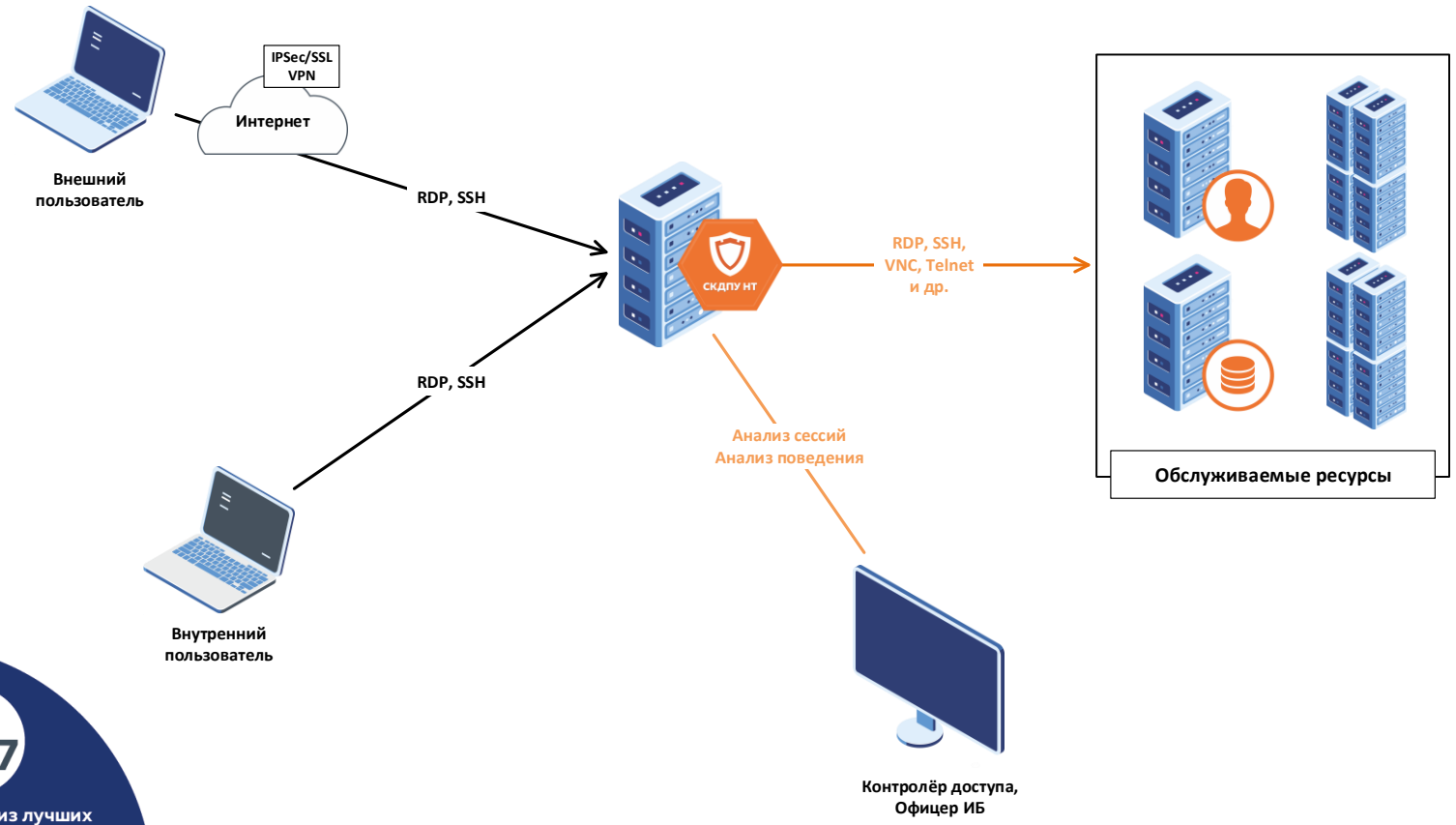
Важнее всего – человек...



	Сегодня	Текущая неделя	Текущий месяц	Текущий квартал	Текущий год	Всего
Сессии:	0	0	0	13	16	16
Шлюзы:	0	0	0	1	1	1
Цели:	0	0	0	2	2	2
Учётные записи:	0	0	0	2	2	2
Время работы:	--	--	--	2 days, 3:56:28	2 days, 15:56:50	2 days, 15:56:50
Загружено:	0B (0 файлов)	0B (0 файлов)	0B (0 файлов)	0B (0 файлов)	0B (0 файлов)	0B (0 файлов)
Скачано:	0B (0 файлов)	0B (0 файлов)	0B (0 файлов)	0B (0 файлов)	0B (0 файлов)	0B (0 файлов)
Блокированные	0	0	0	0	0	0

…и то, насколько мы ему доверяем!

Комплекс СКДПУ НТ



- **Контроль протоколов доступа** RDP, SSH, Telnet и других протоколов, включая RS-232
- **Сбор и анализ событий в сессиях** (видео сессии, запуск процессов, буфер обмена, клавиатурный ввод и др.)
- **Поведенческая аналитика** и статистика
- **Интеграция на уровне бизнес-процессов** с другими ИТ и ИБ решениями
- **Смена паролей УЗ** и сокрытие их при доступе к системам
- **Без агентов. Без единой точки отказа**

24/7

Одна из лучших техподдержек на рынке, по мнению наших заказчиков

СКДПУ НТ и доверие к человеку

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.

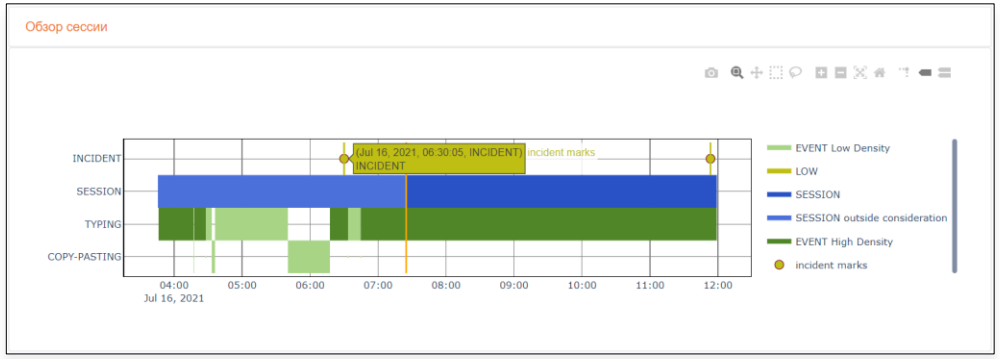
ОТЧЕТЫ И СТАТИСТИКА
Обработка информации и выдача её в виде понятных отчетов – от оперативных до сводных, в т.ч. для руководителей.

КОНТРОЛЬ НА СТОРОНЕ ИС
Блокировка туннелей, доступа вне разрешенных диапазонов, запрет на запуск процессов и т.д.

Актуальные кейсы: мониторинг действий специалистов

«Тепловая карта» активности

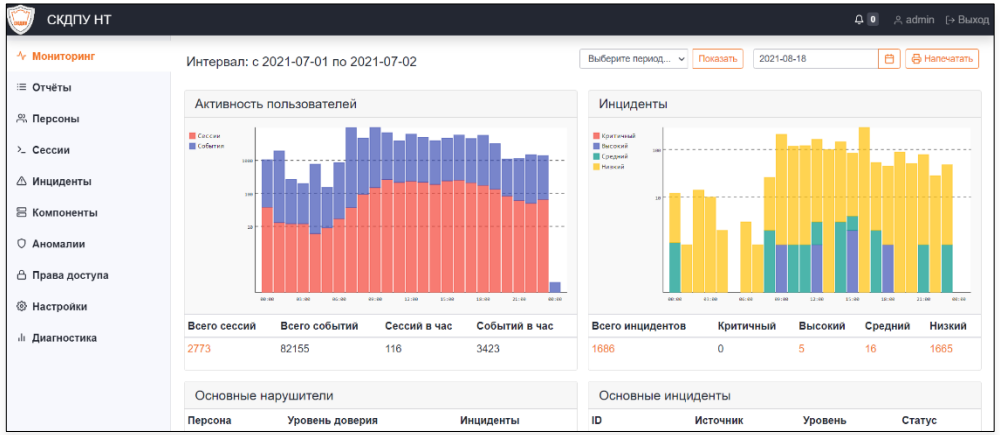
Выделение наиболее активных зон. Оценка нагруженности инсталляций и конкретных целей

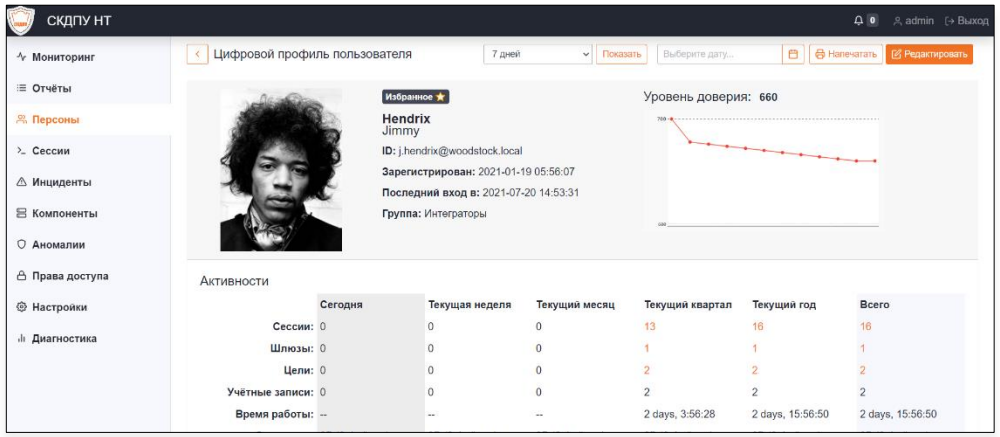


Карта событий

Быстрый обзор «больших» сессий по типам событий и поиск инцидентов

Мониторинг действий специалистов





Единая панель мониторинга
Возможность быстрого просмотра активности и инцидентов по всем инсталляциям.

Профилирование пользователей
Анализ действий пользователей, накопление данных для анализа и автоматическое построение уровня доверия к пользователю на основе модели поведения.

Скорость анализа
Предварительная обработка «сырых» событий доступа

Экономия ресурсов
Сокращение времени на анализ потенциальных инцидентов

Человек и доверие к СКДПУ НТ

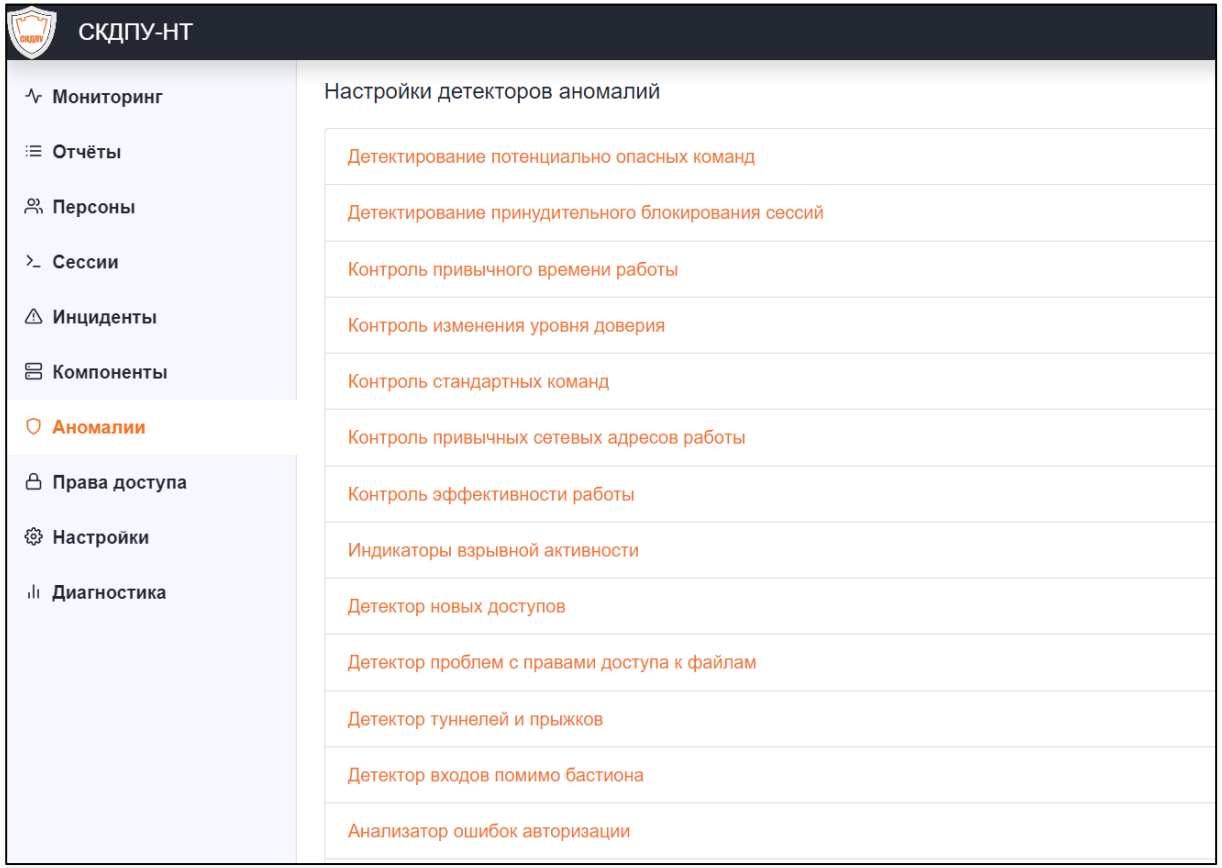
ЕДИНАЯ ТОЧКА ДОСТУПА
Единая точка доступа в инфраструктуру (SSO). Гибкая ролевая модель доступов с возможностью интеграции в существующую инфраструктуру (LDAP, AD, Radius).

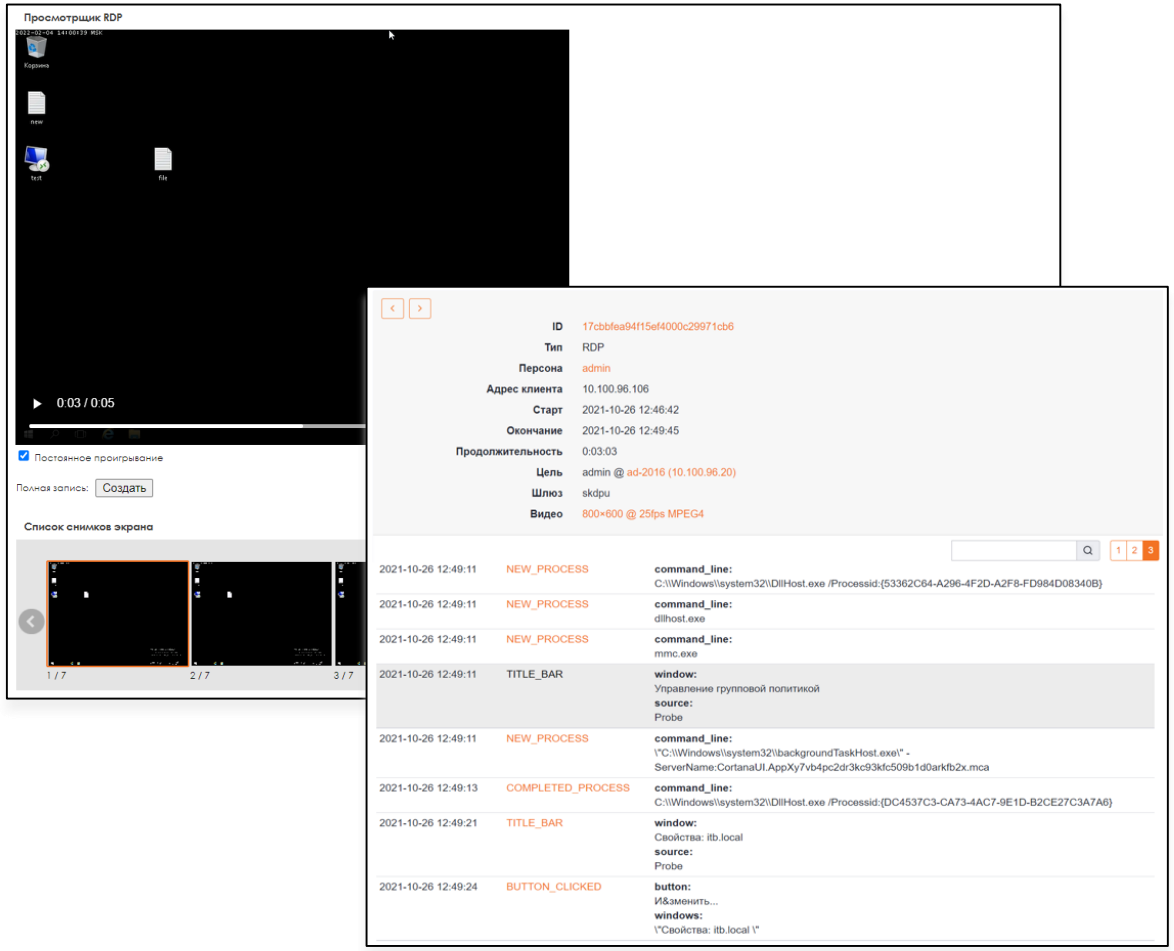
ЗАПИСЬ СОБЫТИЙ ДОСТУПА
Полная запись видео и мета-данных сессий с созданием долгосрочного архива. Клавиатурный ввод, буфер обмена, передача файлов, OCR, элементы интерфейсов, процессы, команды и т.д.

РАБОТА С ПОДТВЕРЖДЕНИЕМ ДОСТУПА
Доступ по предварительным заявкам с согласованием на доступ, с возможностью интеграции с тикет-системами.

ПРОСМОТР И ПРЕРЫВАНИЕ СЕССИЙ
Возможность просмотра открытой сессии в режиме реального времени, а так же её прерывания в ручном режиме или по обнаружению подозрительных действий или команд.

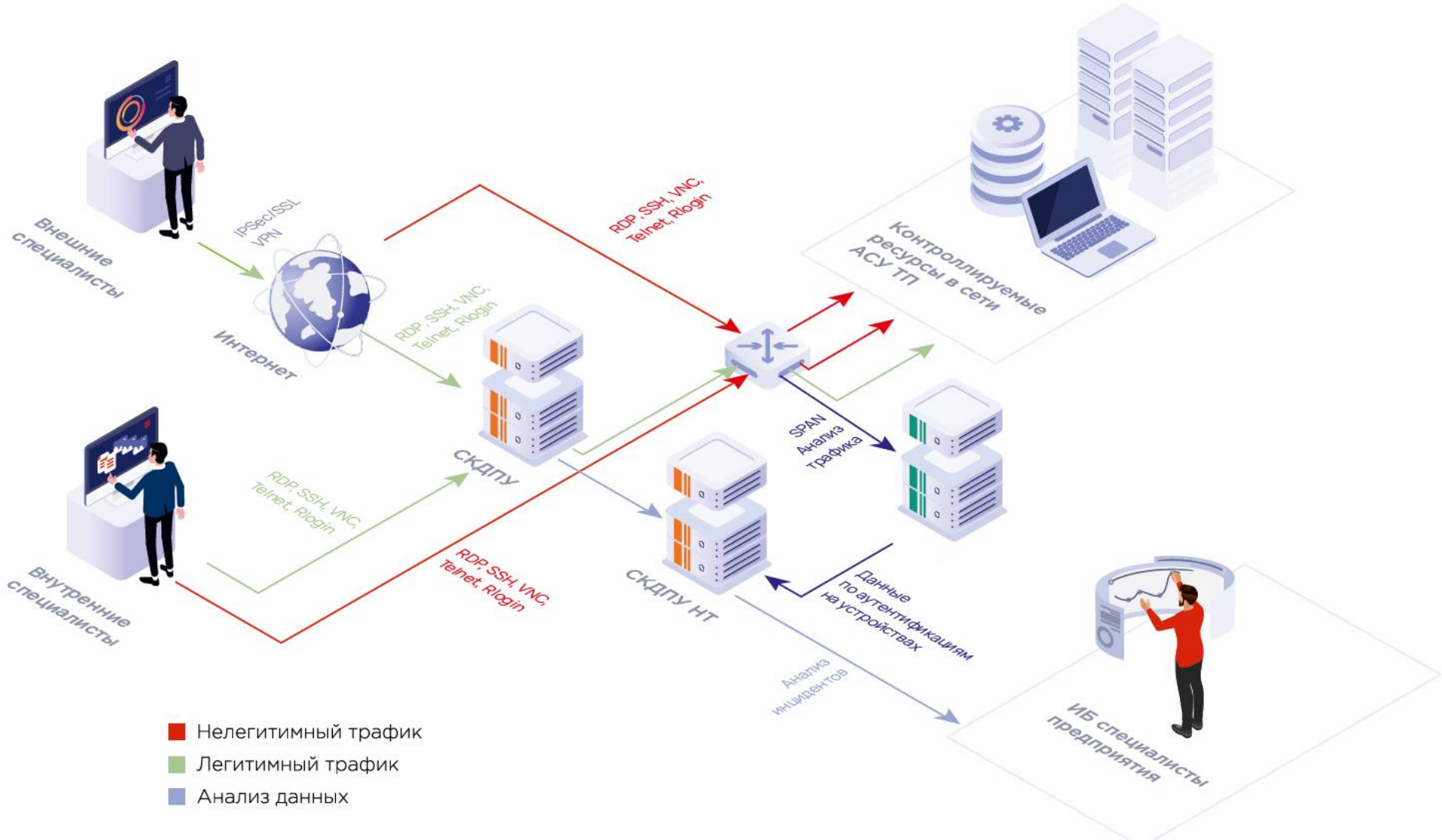
Актуальные кейсы: защита своей «невиновности»





АЙТИБАСТИОН

Про технологию работы СКДПУ НТ в одной картинке



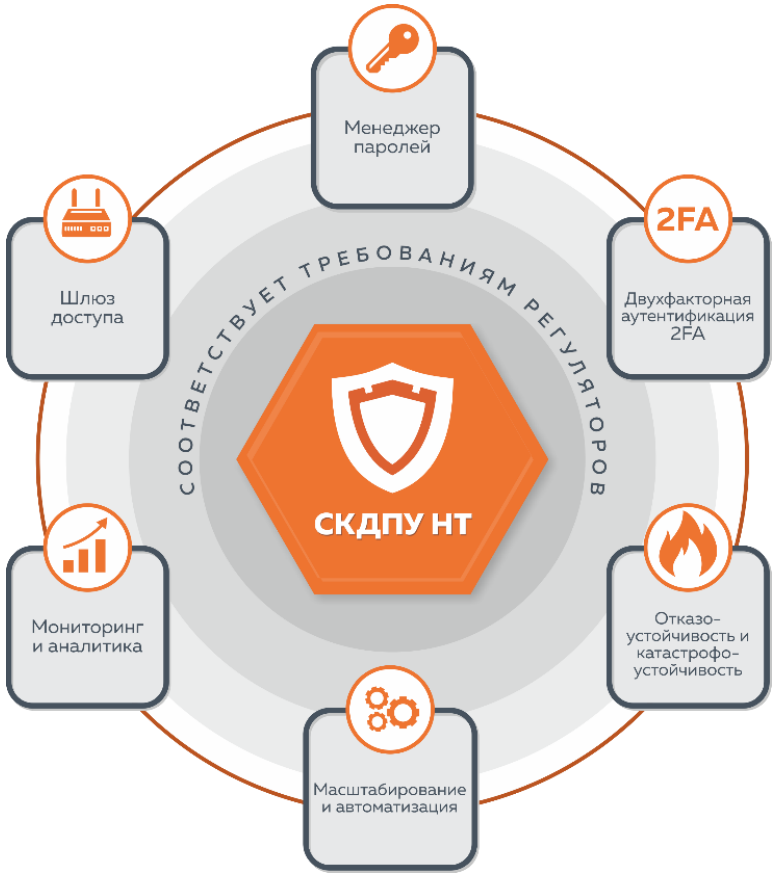
АЙТИБАСТИОН

СКДПУ НТ. Про технологии и возможности

Масштабируемость
Возможность наращивать мощности как вертикально, так и горизонтально, без привязки к территориальному расположению узлов.

Базовая ОС
Комплекс работает под управление ОС AstraLinux SE, внесенной в реестр отечественного ПО и имеет сертификаты ФСТЭК, ФСБ и МО.

Варианты поставки
Комплекс может быть реализован как в **виртуальной среде**, так и в виде **ПАК**.



ASTRA LINUX®

Отказоустойчивость, катастрофоустойчивость
Возможность построения действительно отказоустойчивых инсталляций, в т.ч. распределенных между городами и странами.

Целевые и клиентские ОС
Поддерживается работа с различными ОС как для клиентских, так и для целевых систем – **AstraLinux**, **РЕД ОС**, Windows и др.

Техническая поддержка
осуществляется сотрудниками компании и специалистами партнера, в т.ч. **в режиме 24/7**.

Суммарный эффект применения

- **Контроль доступа** к информационной инфраструктуре в реальном времени
- **Создание доказательной базы** для ретроспективного аудита и анализа сбоев или инцидентов ИБ
- Контроль соблюдения корпоративной **политики ИБ**
- **Контроль действий подрядчиков**, потенциально влекущих за собой утечку информации и различные атаки
- **Защита собственных специалистов** от неправомерных претензий в случае инцидентов ИБ или аварий
- **Контроль за исполнением условий SLA** подрядчиками
- Соблюдение **требований регуляторов**
- **Ведение отчётности**: быстрый доступ к аналитике, отчётам и потенциальным инцидентам

АЙТИБАСТИОН

Соответствие требованиям регуляторов

- ГОСТ Р 57580.1—2017
- GDPR и ФЗ 152
- Приказы ФСТЭК России № 31, № 17, № 21
- Приказ ФСТЭК России №239, №235
- ФЗ-187 «О безопасности КИИ РФ»:
  - Предотвращение неправомерного доступа к информации;
  - Недопущение воздействия на технические средства обработки информации;
  - Восстановление функционирования значимого объекта КИИ.
- 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.

ФСТЭК России ОУД-4

Реестр отечественного ПО

МО РФ РД НДВ-2

АЙТИБАСТИОН

Технологические партнеры

MULTIFACTOR

Rusiem

- PT ISIM
- PT MaxPatrol SIEM

KASPERSKY lab

- KICS
- KOS - тонкий клиент
- KUMA SIEM

ASTRA LINUX®

РЕДОС

INFOWATCH®

- ARMA IF*
- DLP Traffic Monitor

CyberLympha®

РУТОКЕН

и другие партнеры и интеграции…скоро!

** -- в процессе*

Компания «АйТи БАСТИОН»

- Российская компания;
- Более 100 заказчиков и успешно реализованных проектов;
- Более 60 партнеров – интеграторов;

- Разработчик:
  - **СКДПУ НТ** – Системы контроля действий поставщиков ИТ-услуг.
  - **Синоним** – Безопасный шлюз передачи данных между сетями.

Заказчики

ОАК

НОРНИКЕЛЬ

ВЭБ РФ

ГАЗПРОМ ЭНЕРГОХОЛДИНГ

ОСК
ОБЪЕДИНЕННАЯ СУДОСТРОИТЕЛЬНАЯ КОРПОРАЦИЯ

РОСНЕФТЬ

РусГидро

ПРАВИТЕЛЬСТВО МОСКВЫ

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

РОСЭНЕРГОАТОМ
РОСАТОМ

ВОЕНТЕЛЕКОМ

Ростех

Северсталь

АЙТИБАСТИОН

Спасибо за внимание!

Константин Родин
Руководитель технического центра

k.rodin@it-bastion.com