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 УД-4

Реестр отечественного ПО

МО РФ РД НДВ-2

АЙТИБАСТИОН

Мониторинг действий и контроль инцидентов удаленного доступа.

Создание доверенных сред

Компания «АйТи БАСТИОН»

- Более 100 заказчиков и успешно реализованных проектов
- Проекты в корпоративных и АСУ ТП сегментах.
- Более 60 партнеров – интеграторов

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

ФСТЭК России УД-4

Реестр отечественного ПО

МО РФ РД НДВ-2

АЙТИБАСТИОН

Заказчики

ОАК

НОРНИКЕЛЬ

ВЭБ РФ

СМП БАНК

РОССЕТИ ЛЕНЭНЕРГО

ОСК
ОБЪЕДИНЕННАЯ СУДОСТРОИТЕЛЬНАЯ КОРПОРАЦИЯ

РОСНЕФТЬ

РусГидро

ПРАВИТЕЛЬСТВО МОСКВЫ

ВОЕНТЕЛЕКОМ

СОГЛАСИЕ
страхование

МИНИСТЕРСТВО ТРАНСПОРТА
РОССИЙСКОЙ ФЕДЕРАЦИИ

РОСЭНЕРГОАТОМ
РОСАТОМ

Ростех

ГАЗПРОМ
ЭНЕРГОХОЛДИНГ

Северсталь

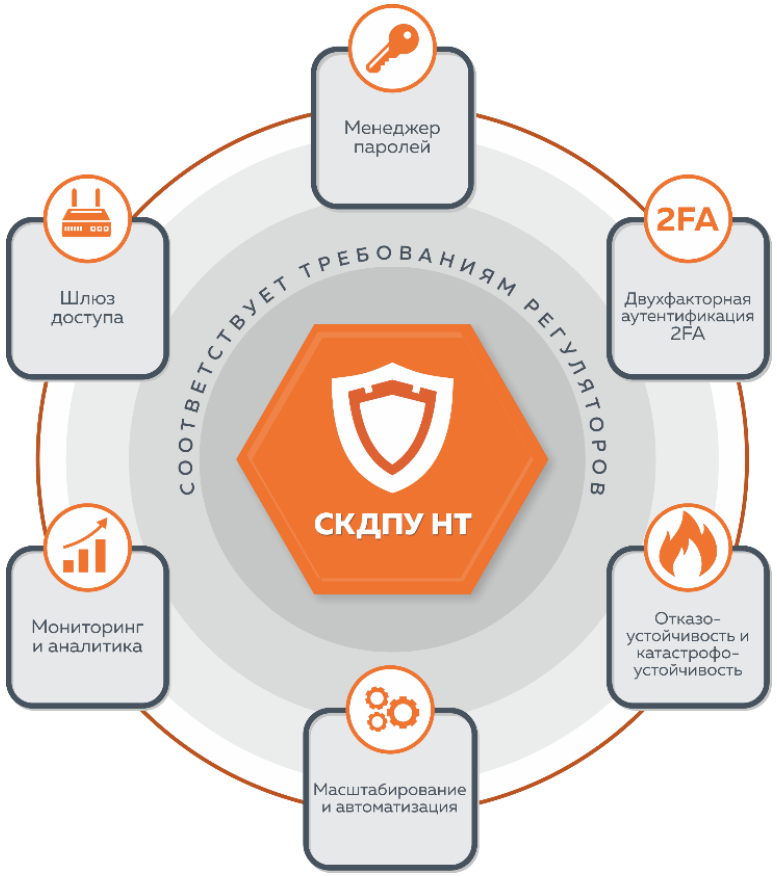
АЙТИБАСТИОН

Технологии и возможности

Соответствие требованиям
ФЗ-187 «О безопасности КИИ РФ», Приказы ФСТЭК России №239, №235, Приказы ФСТЭК России № 31, № 17, № 21

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**.



Сертификаты и реестр
Включен в реестр отечественного ПО, Сертификат ФСТЭК ОУД-4, Сертификат МО РФ НДВ-2

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**.

СКДПУ НТ. Базовые функции

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

БЕЗ УСТАНОВКИ АГЕНТОВ
Подключение к ЦУ без необходимости установки агентов, особенно важна при подключении к объектам КИИ.

РАБОТА ПО ЗАЯВКАМ И ПОДТВЕРЖДЕНИЯМ ДОСТУПА
Доступа по предварительным заявкам с согласованием на доступ, с возможностью интеграции с тикет-системами.

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.

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

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.

СКДПУ НТ. Базовые функции

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.

МАСШТАБИРУЕМОСТЬ
Легкая возможность наращивать мощности как вертикально, так и горизонтально, без привязки к территориальному расположению узлов.

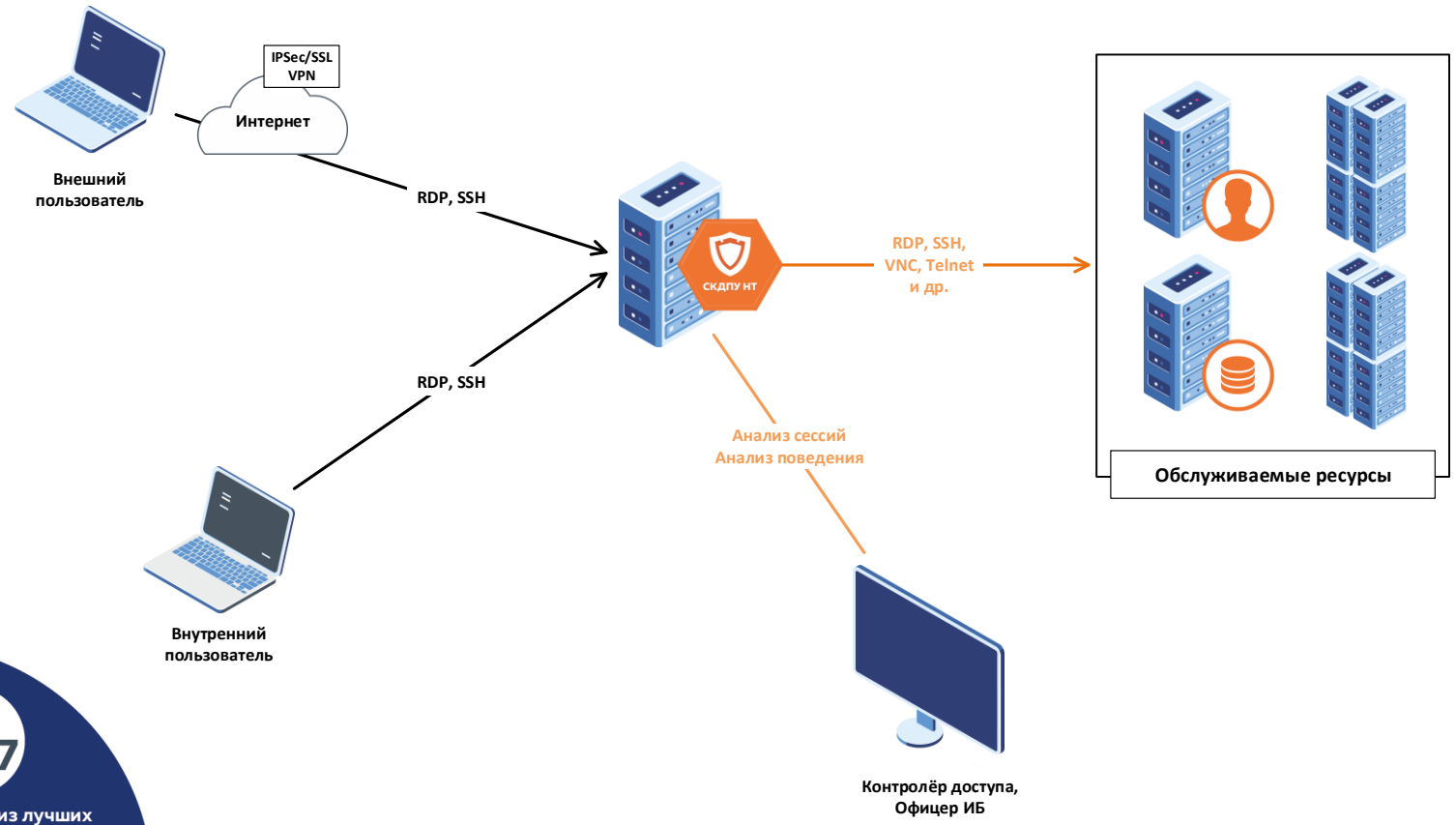
ОТЧЕТЫ И СТАТИСТИКА
Обработки информации и выдача её в виде понятных отчетах от оперативных до сводных, в т.ч. для руководителей.

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

ОТКАЗОУСТОЙЧИВОСТЬ, КАТАСТРОФОУСТОЙЧИВОСТЬ
Возможность построения действительно отказоустойчивых инсталляций, в т.ч. распределенных между городами и странами.

АЙТИБАСТИОН

Комплекс СКДПУ НТ



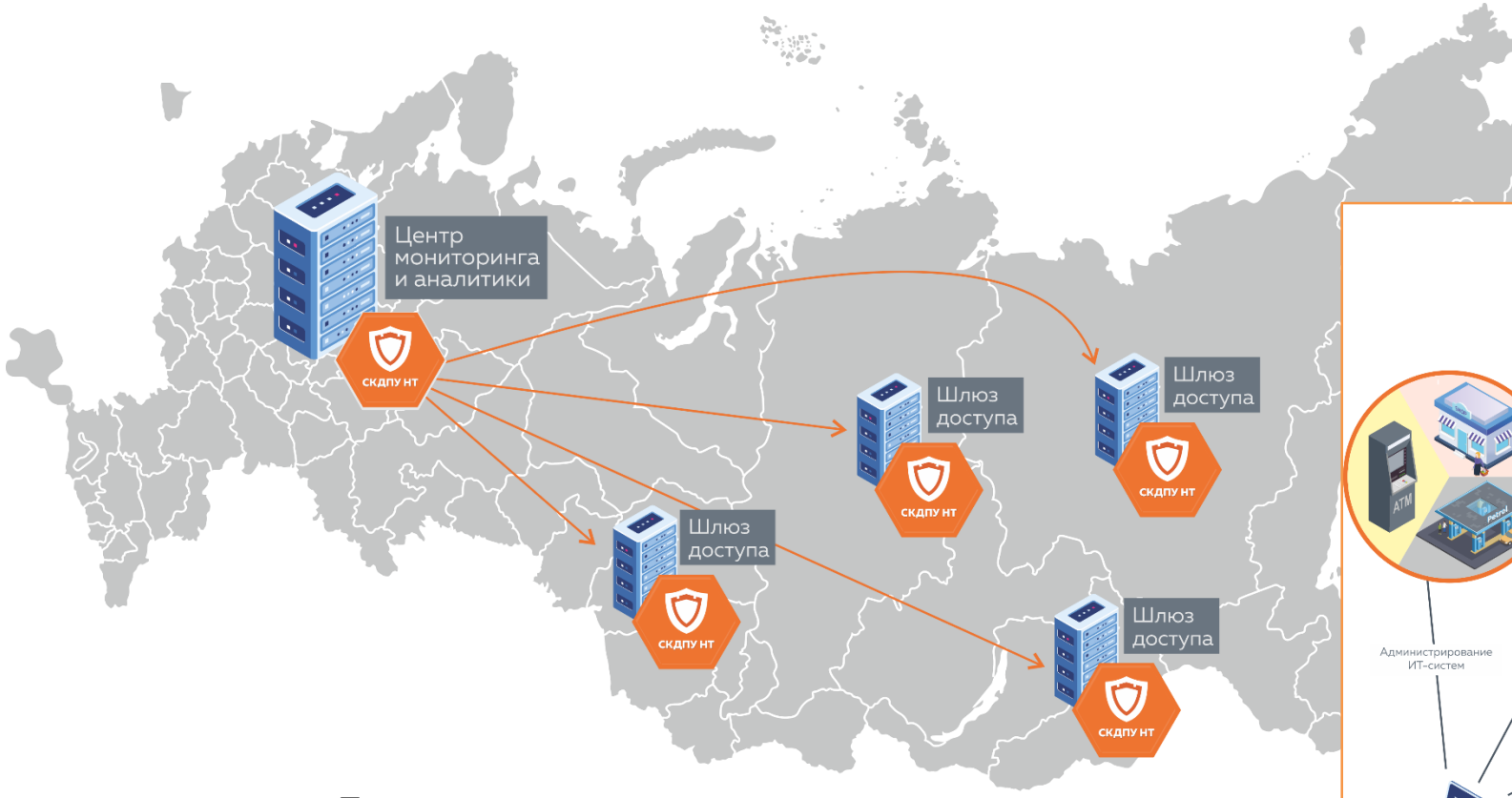
- **Контроль протоколов доступа** RDP, SSH, Telnet и других протоколов, включая RS-232
- **Сбор и анализ событий в сессиях** (видео сессии, запуск процессов, буфер обмена, клавиатурный ввод и др.)
- **Поведенческая аналитика** и статистика
- **Интеграция на уровне бизнес-процессов** с другими ИТ и ИБ 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

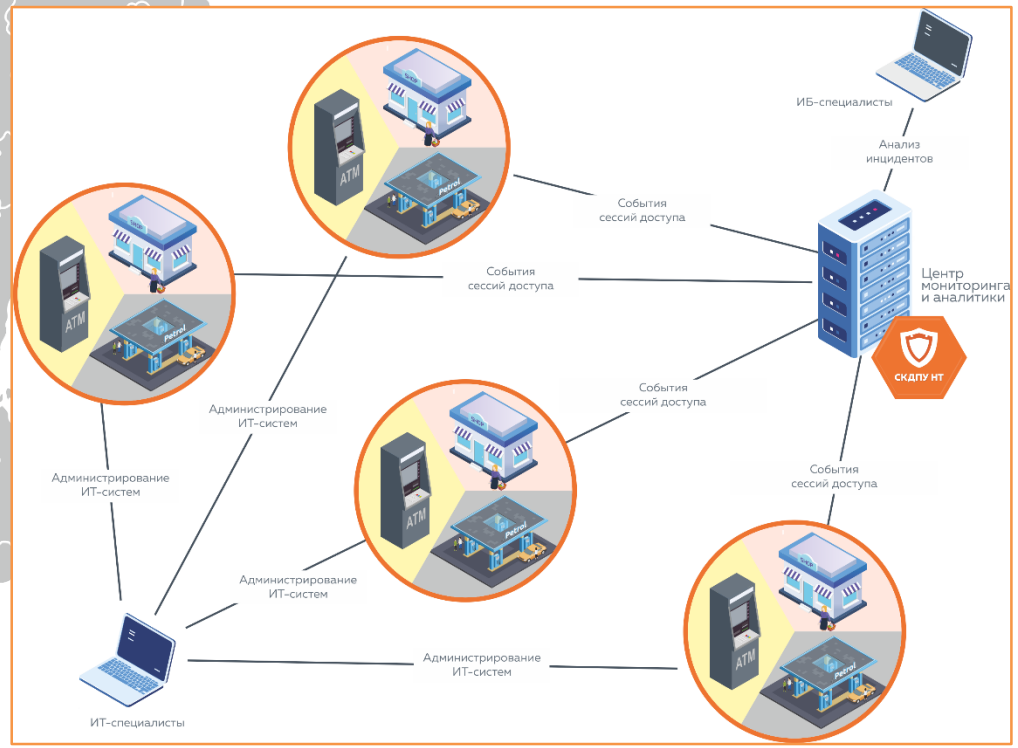
АЙТИБАСТИОН

От малого к большему



Гео-распределенные инсталляции

Компактные инсталляции



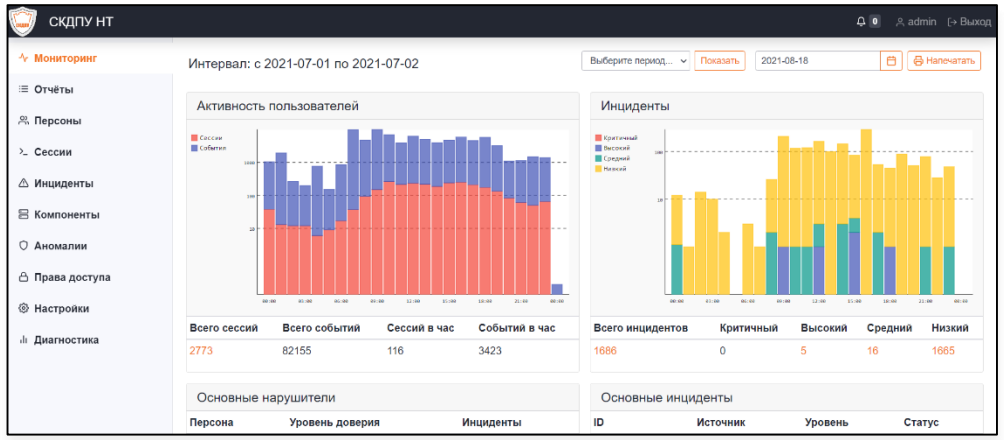
Контроль, доверие, мониторинг

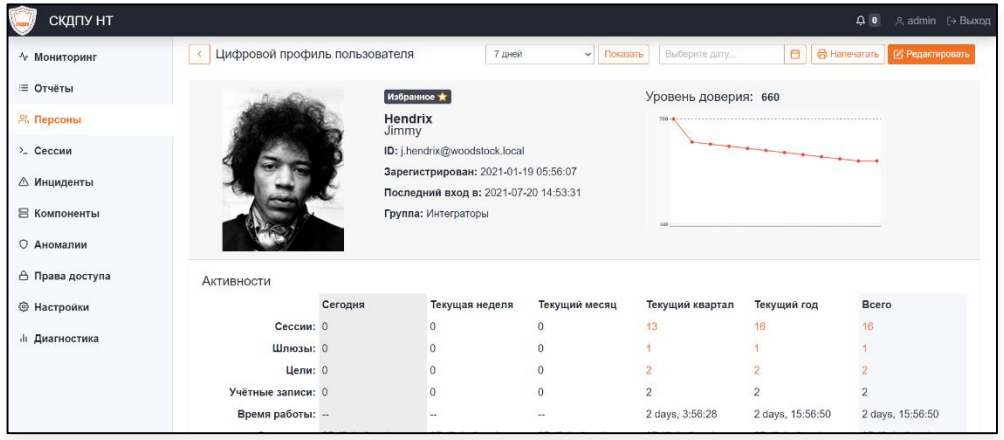
Контроль привилегированных пользователей
Реализация контролируемого доступа в корпоративных сегментах и объектах КИИ. Анализ всех действий в разрезе «пользователь-цель-действие», машинное обучение и математические модели.

Сегментирование доступов между контурами
Построение сети шлюзов доступа, с возможностью автоматизации переноса политик, разграничения доступа и контроль потоков данных между ними.

Единая дополняемая концепция работы
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.

Мониторинг действий специалистов





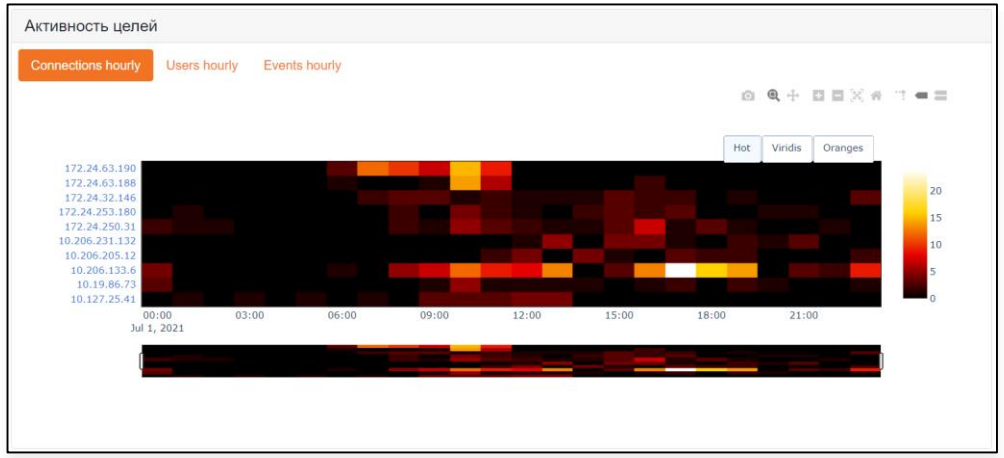
Единая панель мониторинга
Возможность быстрого просмотра активности и инцидентов по всем инсталляциям.

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.

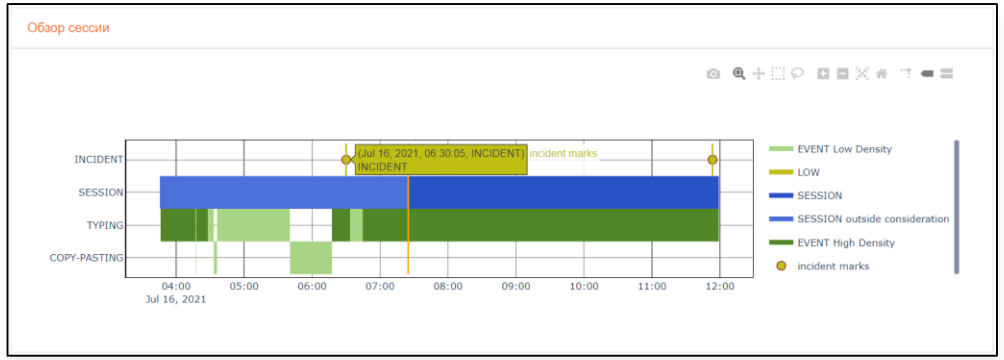
Экономия ресурсов
Сокращение времени на анализ потенциальных инцидентов.

Мониторинг действий специалистов



«Тепловая карта» активности

Выделение наиболее активных зон.
Оценка нагруженности инсталляций и конкретных целей.



Карта событий

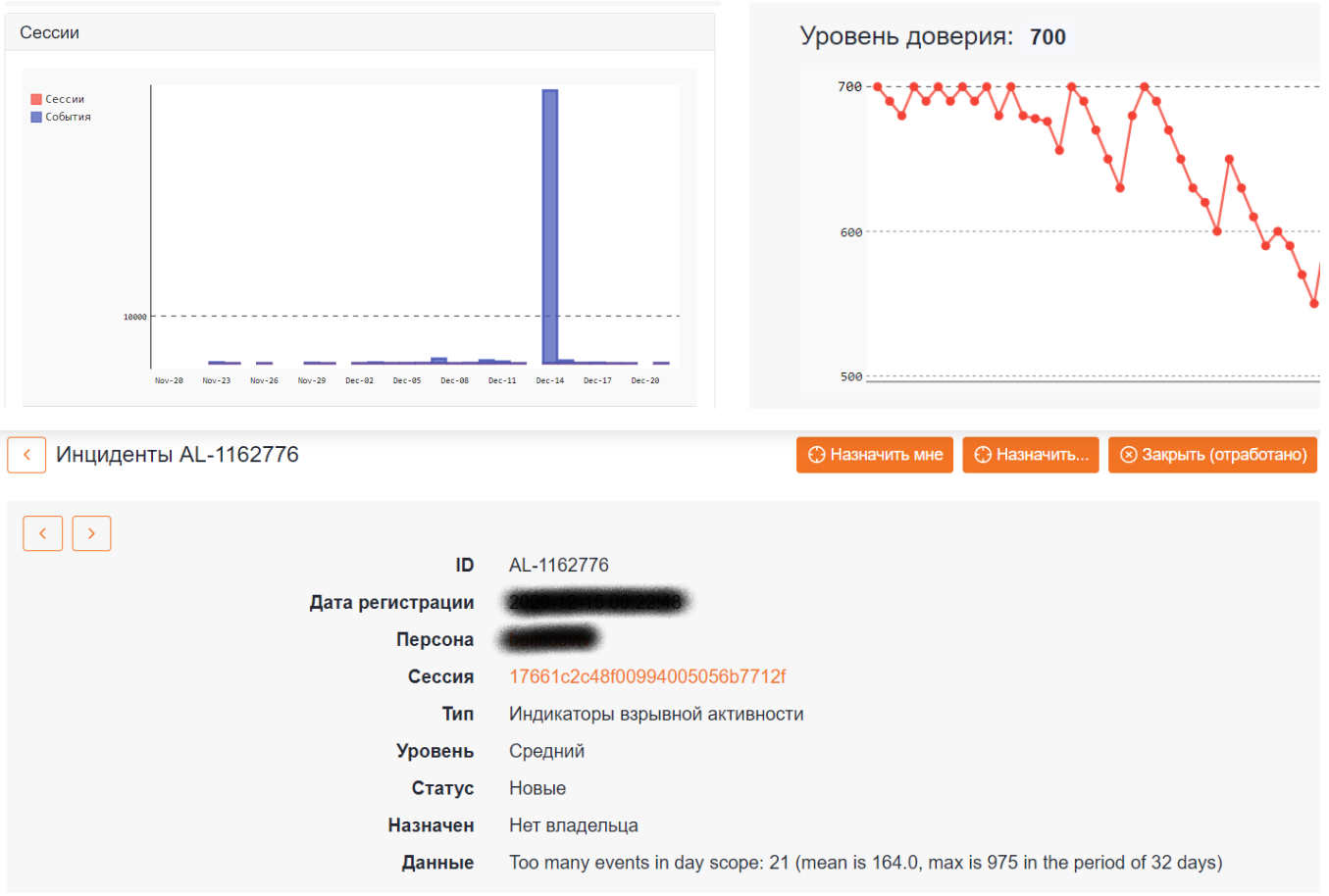
Быстрый обзор «больших» сессий по типам событий и поиск инцидентов.

Из жизни наших заказчиков

- «Забытые доступы»;
- «Изменение привычек» или анализ системы под скомпрометированной УЗ;
- «Взрывная активность пользователя»;
- «Резервный туннель, а вдруг пригодится»;
- Нарушение регламента доступа.

«Взрывная активность пользователя»

- Копирование данных с ИС;
- Исследование ИС «посторонними»;
- «что-то пошло не так».



АЙТИБАСТИОН

«Резервный туннель, а вдруг пригодится»

Дата регистрации	[redacted]
Персона	[redacted]
Сессия	177169a0150b4450005056b7712f
Тип	Туннели и прыжки
Уровень	Средний
Статус	Новые
Назначен	Нет владельца
Данные	Open Direct TCPIP Channel www.google.com:443

Подробности:

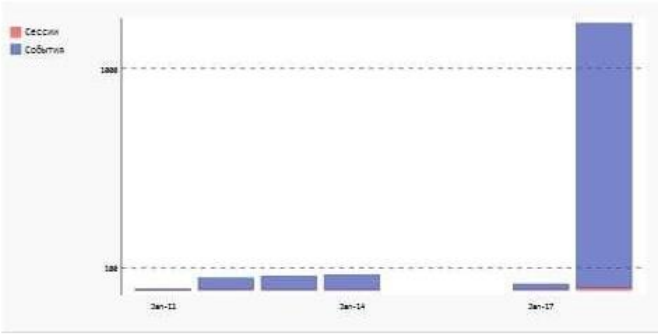
Дата и время записи	Тип события	Данные	
[redacted]	CHANNEL_EVENT	**data:**	Open Direct TCPIP Channel
		channel_id:	C0086
		dst:	www.google.com
		src_port:	53942
		dst_port:	443
		src:	127.0.0.1

Цель [redacted] 7 дней

Избранное

Устройство:	[redacted]
IP-адрес цели:	[redacted]
Компонент:	SSH
Время последнего использования:	[redacted]

Сессии



АЙТИБАСТИОН

Построение единых доверенных инфраструктур

MULTIFACTOR

KASPERSKY lab

- KICS
- KOS - тонкий клиент
- KUMA SIEM

INFOWATCH®

- ARMA IF*
- DLP Traffic Monitor

Rusiem

ASTRA LINUX®

CyberLympha®

POSITIVE TECHNOLOGIES

- PT ISIM
- PT MaxPatrol SIEM

РЕДОС

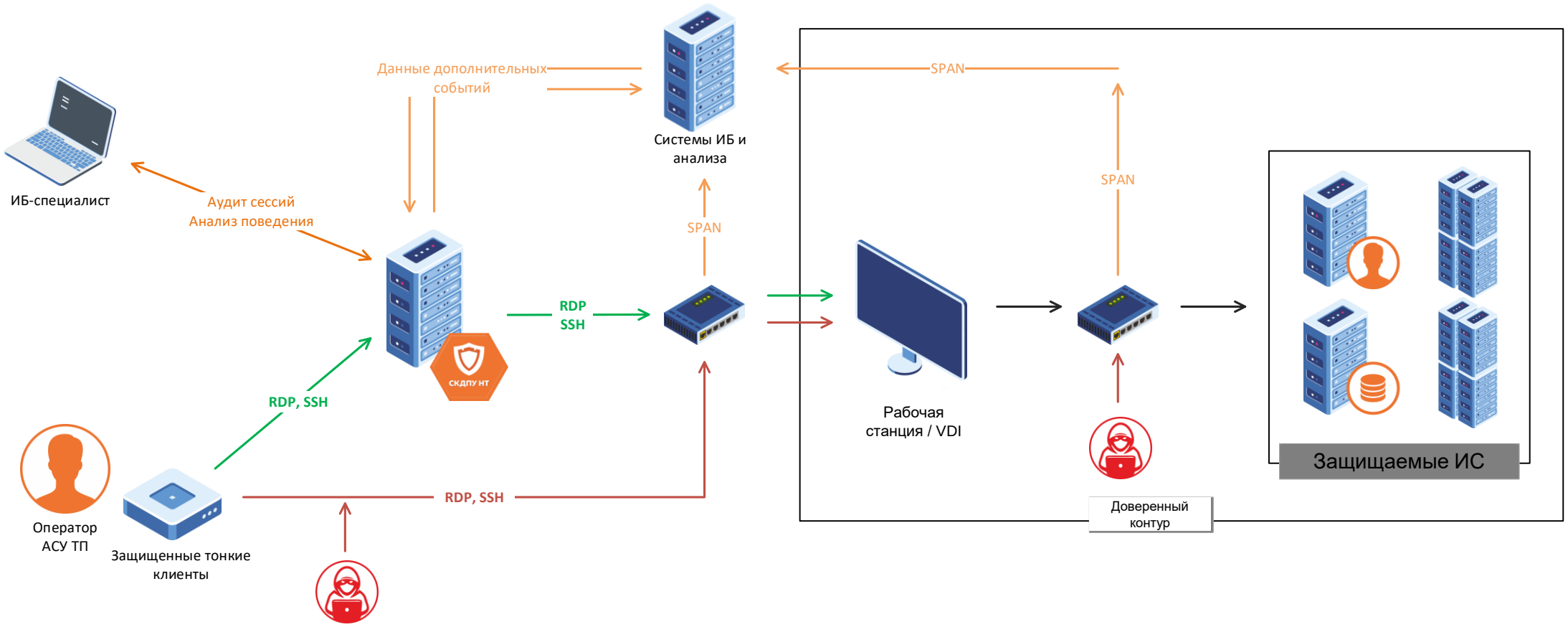
РУТОКЕН

и другие партнеры и интеграции…скоро!

** -- в процессе*

АЙТИБАСТИОН

Комплексная защита сегмента



АЙТИБАСТИОН

СКДПУ НТ
Настоящее и будущее мониторинга удаленного доступа

- Безопасный и контролируемый доступ в инфраструктуру
- Мониторинг и идентификация инцидентов ИБ
- Двунаправленное наполнение профилей и событий от внешних систем
- Распределенные шлюзы доступа и сегментированные контуры
- Единый центр сбора и аналитики данных
- Централизованное хранилище событий и инцидентов
- Централизованное управление и развертывание*

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 УД-4

Реестр отечественного ПО

МО РФ РД НДВ-2

АЙТИБАСТИОН

Спасибо за внимание!

Константин Родин
Руководитель технического центра

k.rodin@it-bastion.com