# АЙТИБАСТИОН

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

info@it-bastion.com it-bastion.com +7 499 322 3667

# Отечественная PAM-платформа СКДПУ НТ

## От задачи контроля к экосистеме анализа и реагирования

АЙТИБАСТИОН

# Компания «АйТи Бастион»

**2014**

## Основание компании

Более 9 лет на российском рынке информационной безопасности

**100+**

## Сотрудников

Команда разработчиков, инженеров, менеджеров, маркетинга и пиара, ориентированная на продукт и решение реальных задач

**180+**

## Заказчиков и проектов

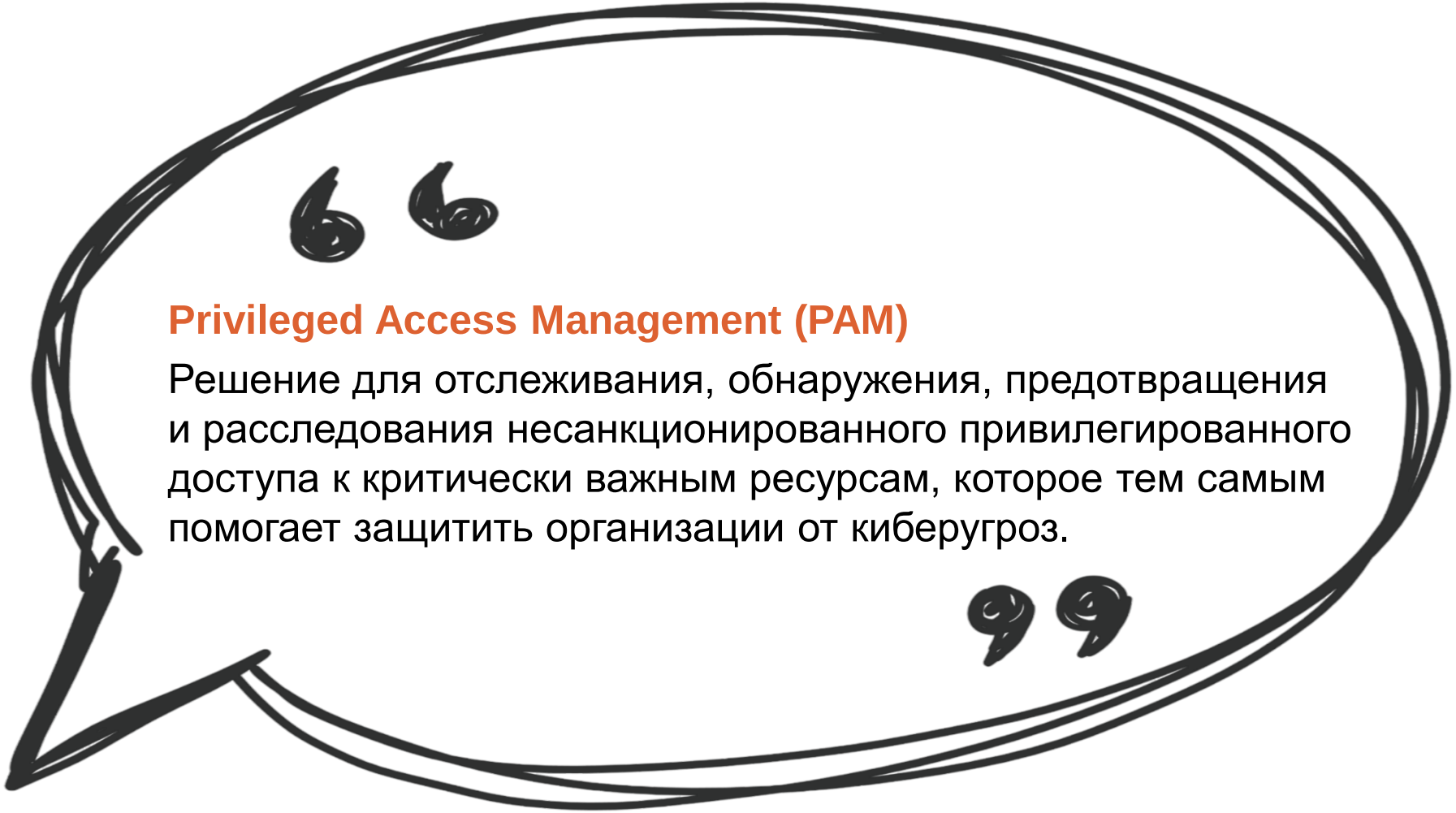
Присутствие во всех отраслях от нефтяных компаний до футбольных клубов, от небольших офисов до геораспределенных площадок

**> 50%**

## PAM-рынка РФ

**Комплекс СКДПУ НТ** решение, проверенное «в боях» и доказавшее свою эффективность, надежность и качество

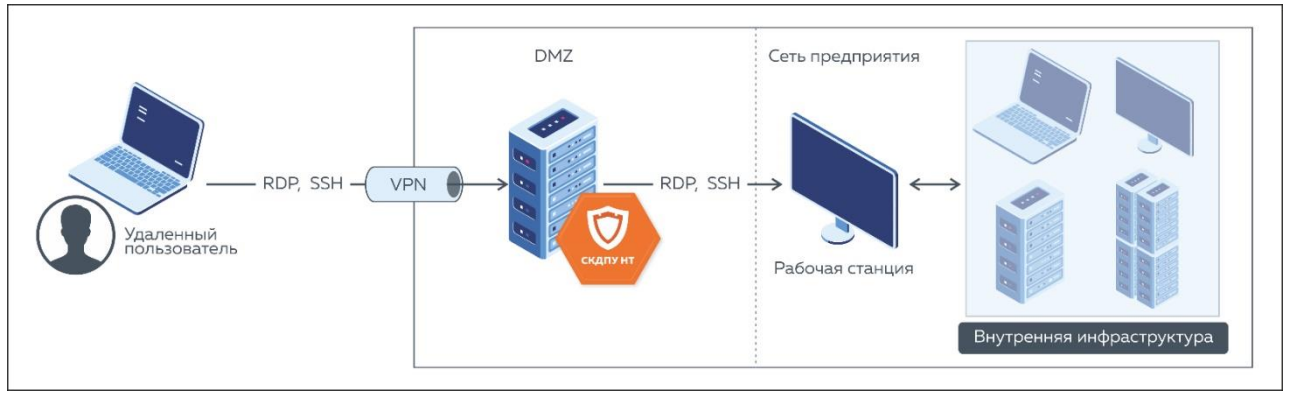
# Что такое PAM для большинства?



**Privileged Access Management (PAM)**

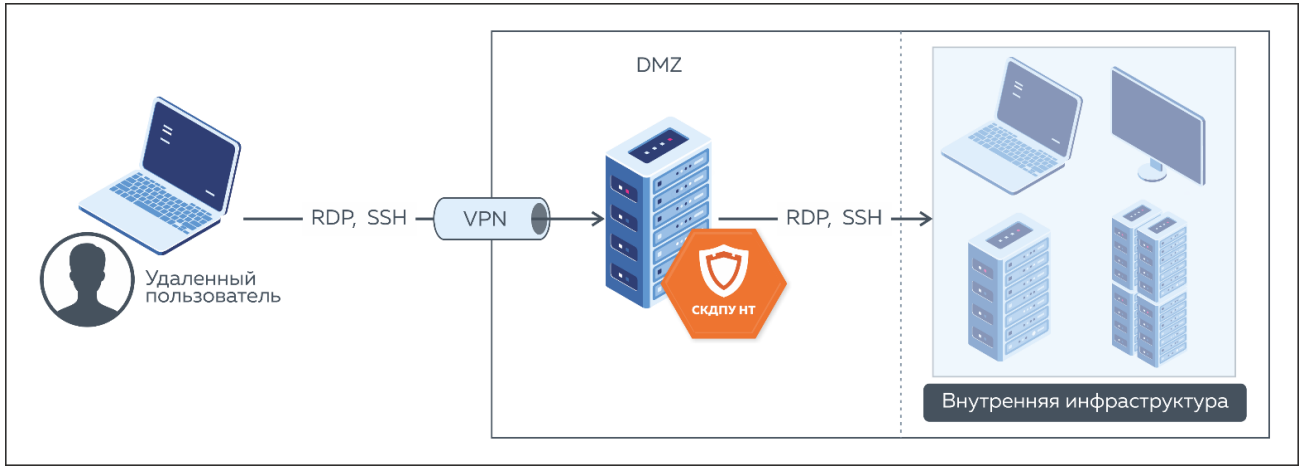
Решение для отслеживания, обнаружения, предотвращения и расследования несанкционированного привилегированного доступа к критически важным ресурсам, которое тем самым помогает защитить организации от киберугроз.

# Чем помогает PAM-система




- ✓ Привилегии и права на «минимум»
- ✓ Идентификация удаленных устройств
- ✓ Только для «своих» сотрудников
- ✓ Свой домен для удаленных АРМ
- ✓ Двухфакторная аутентификация
- ✓ VPN
- ✓ Запрет постороннего ПО

- ✓ Антивирусная защита
- ✓ Блокировка сеансов при неактивности
- ✓ Реагирование на инциденты
- ✓ Сегментация прав доступа
- ✓ Обновление паролей



АЙТИБАСТИОН

# Наше видение PAM-систем

- Технологии
- Люди
- Процессы

# Все атаки начинались с утечки учетной записи

## Colonial Pipeline

- Атака остановила работу всех трубопроводов системы на пять дней 88 % АЗС в Вашингтоне были без бензина
- Из-за нехватки авиакеросина авиакомпания American Airlines была вынуждена временно изменить некоторые рейсы
- Розничные цены на бензин в США при этом достигли десятилетнего максимума
- В части Северной Каролины, в связи с нехваткой топлива 71 % АЗС были закрыты

**Руководство Colonial Pipeline заплатило выкуп в 75 биткоинов (4,5 млн долл. на момент выплаты)**

## Венесуэльская ГЭС

Атака была направлена на автоматическую систему контроля ГЭС "Гури". Гидроэлектростанция производит 80% электроэнергии, потребляемой в стране. Почти вся страна осталась без электроснабжения до возобновления работы.

## Creos Luxembourg S.A

Крупный центральноевропейский оператор электросетей и газопроводов, поставляющий энергию в пять стран ЕС.

Украдено 180 тыс. файлов общим объёмом 150 ГБ, - контракты, соглашения, паспорта, счета и электронную переписку.

Выполнен переход на аварийное обслуживание.

## ENI

**ENI** – Итальянская топливная компания

Представитель ENI заявил, что в последние дни внутренние системы защиты обнаружили несанкционированный доступ и быстро пресекли атаку, поэтому последствия были незначительными.

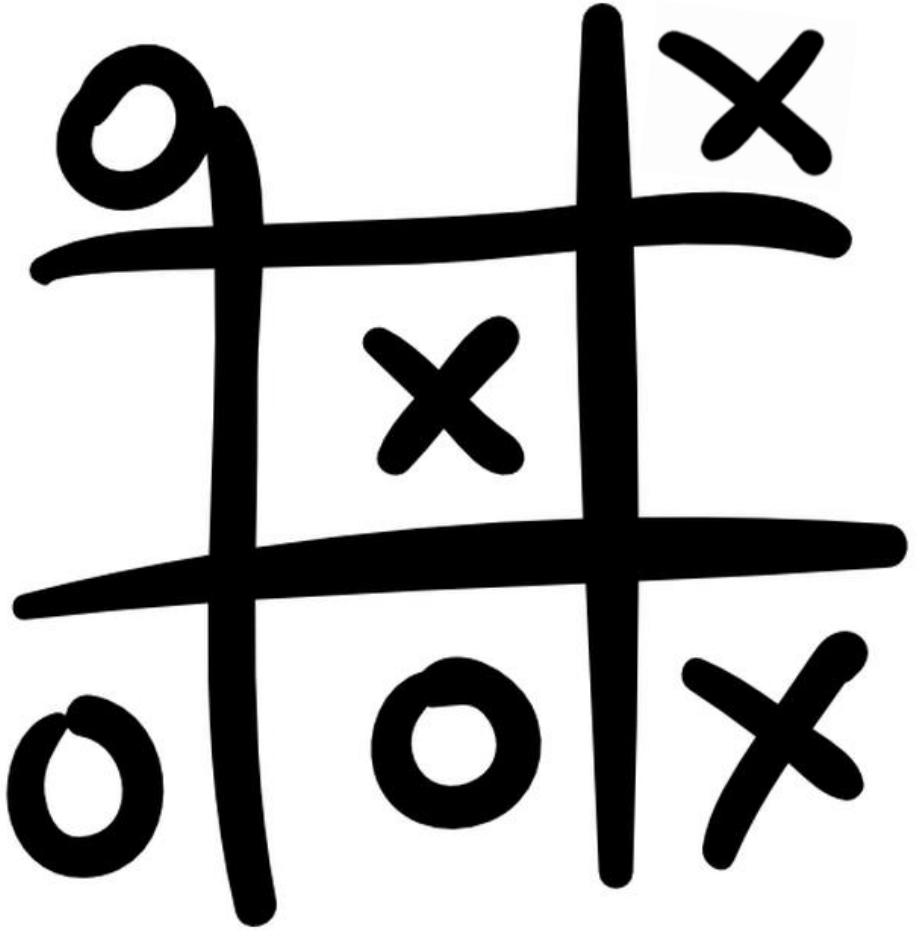
Однако заявляется об утечке конфиденциальной информации и частичным сбоям в работе инфраструктуры.

АЙТИБАСТИОН

# Про угрозы привилегированного доступа

- Человеческий фактор
- Shadow IT и «обидчивые люди»
- Несоответствие требованиям
- Репутационные риски

- Поставщики услуг
- Цепочки поставок
- Геополитика и санкции



# 65% атак – целевые атаки

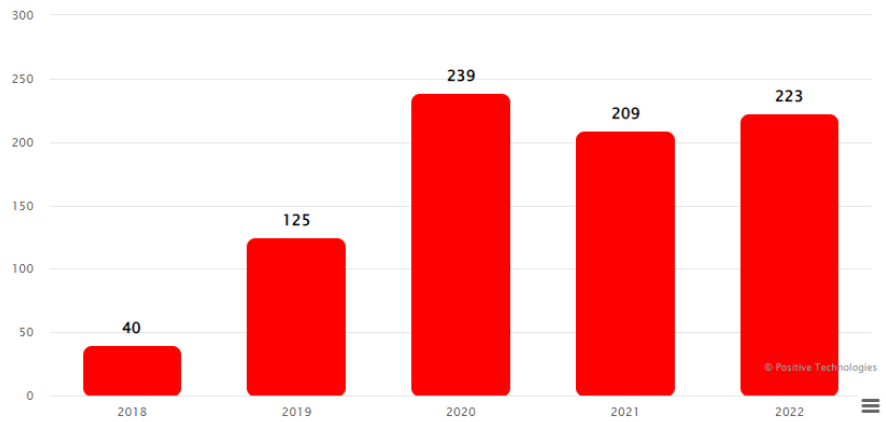



*Рисунок 2. Динамика инцидентов (количество по годам)*

Инциденты


*Рисунок 16. Последствия атак на промышленные организации (доля атак)*

Последствия

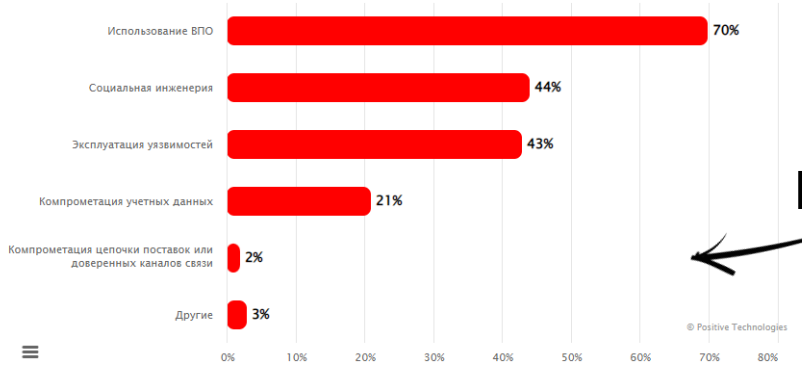



*Рисунок 5. Методы атак на промышленные организации (доля атак)*

Методы

- 75% объявлений в дарквебе про «доступ»
- 45% последствий – нарушение деятельности
- 8% прямы финансовые потери

https://www.ptsecurity.com/ru-ru/research/analytics/industrial-cybersecurity-threatscape-2022/

# СКДПУ НТ – это PAM-платформа

**Контроль и активный мониторинг**
Фиксация видео и метаданных сессий, реагирование и сегментация

**Скорость анализа**
Предварительная обработка «сырых» событий доступа, UEBA, расширенные инструменты поиска аномалий

**Экосистемный подход**
Объединение компетенций сторонних вендоров

**Экономия ресурсов**
Сокращение времени на анализ потенциальных инцидентов

# Базовые возможности 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 сессий: клавиатурный ввод, буфер обмена, передача файлов, OCR, элементы интерфейсов, процессы, команды и др.

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

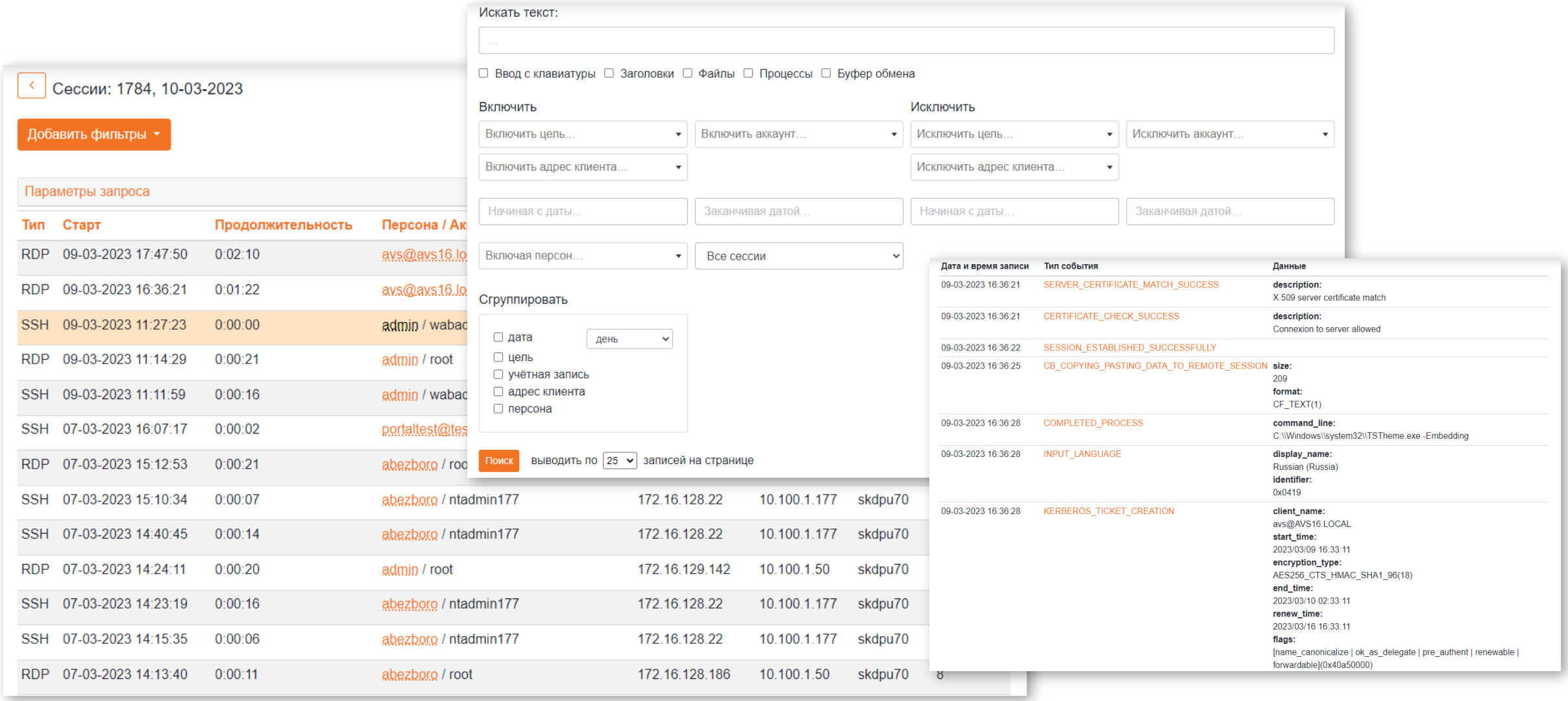
### REST API И АВТОМАТИЗАЦИЯ
Интеграции с внешними системами для создания и управления доступом

### ПОЛНЫЙ ЦИКЛ УПРАВЛЕНИЯ ПАРОЛЯМИ
От предоставления доступа к гранулярной смене паролей для пользователей и выдачи паролей из сейфа, в т.ч. и для автоматизированных систем

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

АЙТИБАСТИОН

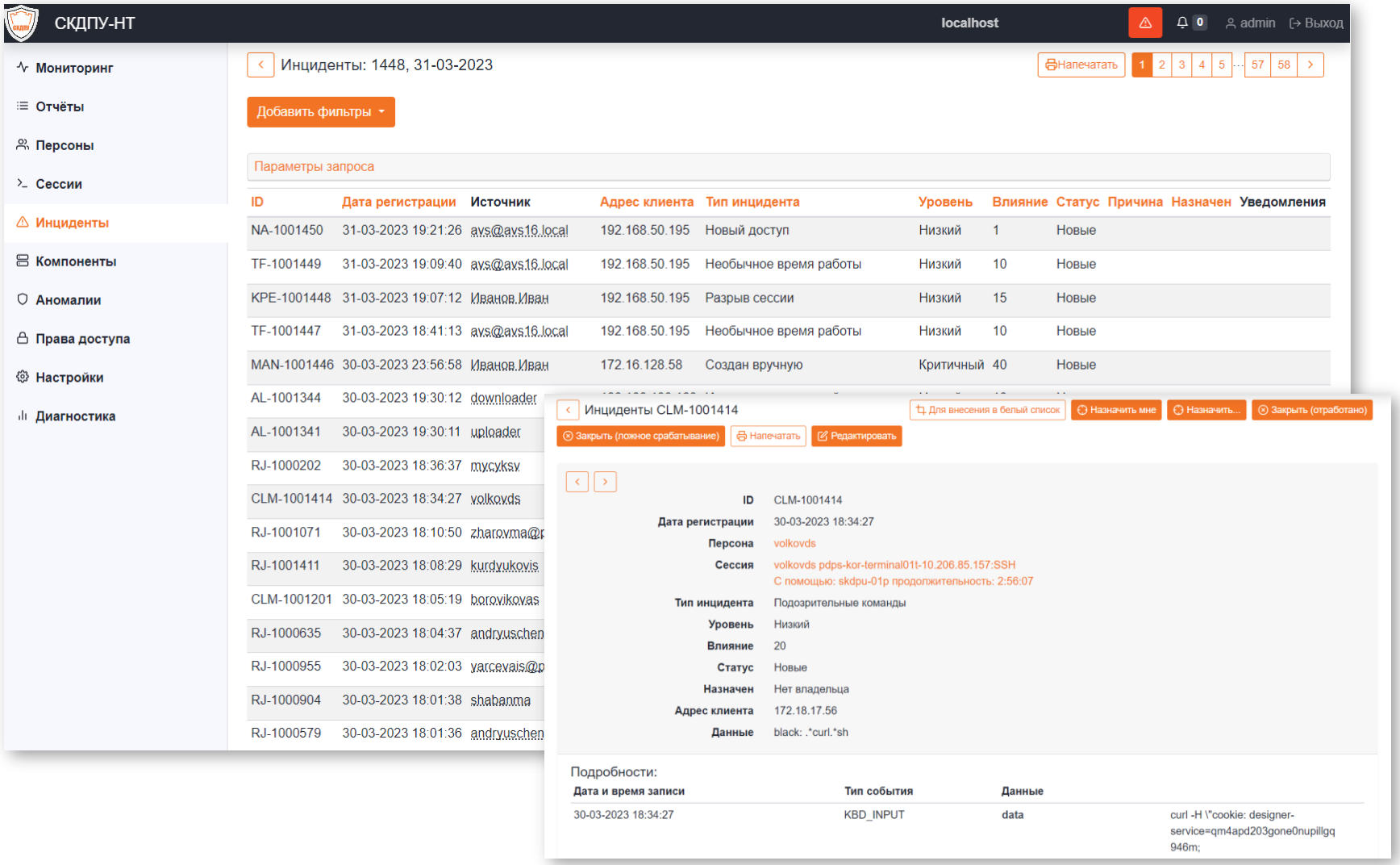
# Централизованный архив данных по сессиям




| Тип | Старт | Продолжительность | Персона / Ак | | | | |
|---|---|---|---|---|---|---|---|
| RDP | 09-03-2023 17:47:50 | 0:02:10 | avs@avs16.lo | | | | |
| RDP | 09-03-2023 16:36:21 | 0:01:22 | avs@avs16.lo | | | | |
| SSH | 09-03-2023 11:27:23 | 0:00:00 | admin / wabac | | | | |
| RDP | 09-03-2023 11:14:29 | 0:00:21 | admin / root | | | | |
| SSH | 09-03-2023 11:11:59 | 0:00:16 | admin / wabac | | | | |
| SSH | 07-03-2023 16:07:17 | 0:00:02 | portaltest@tes | | | | |
| RDP | 07-03-2023 15:12:53 | 0:00:21 | abezboro / roo | | | | |
| SSH | 07-03-2023 15:10:34 | 0:00:07 | abezboro / ntadmin177 | 172.16.128.22 | 10.100.1.177 | skdpu70 | |
| SSH | 07-03-2023 14:40:45 | 0:00:14 | abezboro / ntadmin177 | 172.16.128.22 | 10.100.1.177 | skdpu70 | |
| RDP | 07-03-2023 14:24:11 | 0:00:20 | admin / root | 172.16.129.142 | 10.100.1.50 | skdpu70 | |
| SSH | 07-03-2023 14:23:19 | 0:00:16 | abezboro / ntadmin177 | 172.16.128.22 | 10.100.1.177 | skdpu70 | |
| SSH | 07-03-2023 14:15:35 | 0:00:06 | abezboro / ntadmin177 | 172.16.128.22 | 10.100.1.177 | skdpu70 | |
| RDP | 07-03-2023 14:13:40 | 0:00:11 | abezboro / root | 172.16.128.186 | 10.100.1.50 | skdpu70 | 8 |

АЙТИБАСТИОН

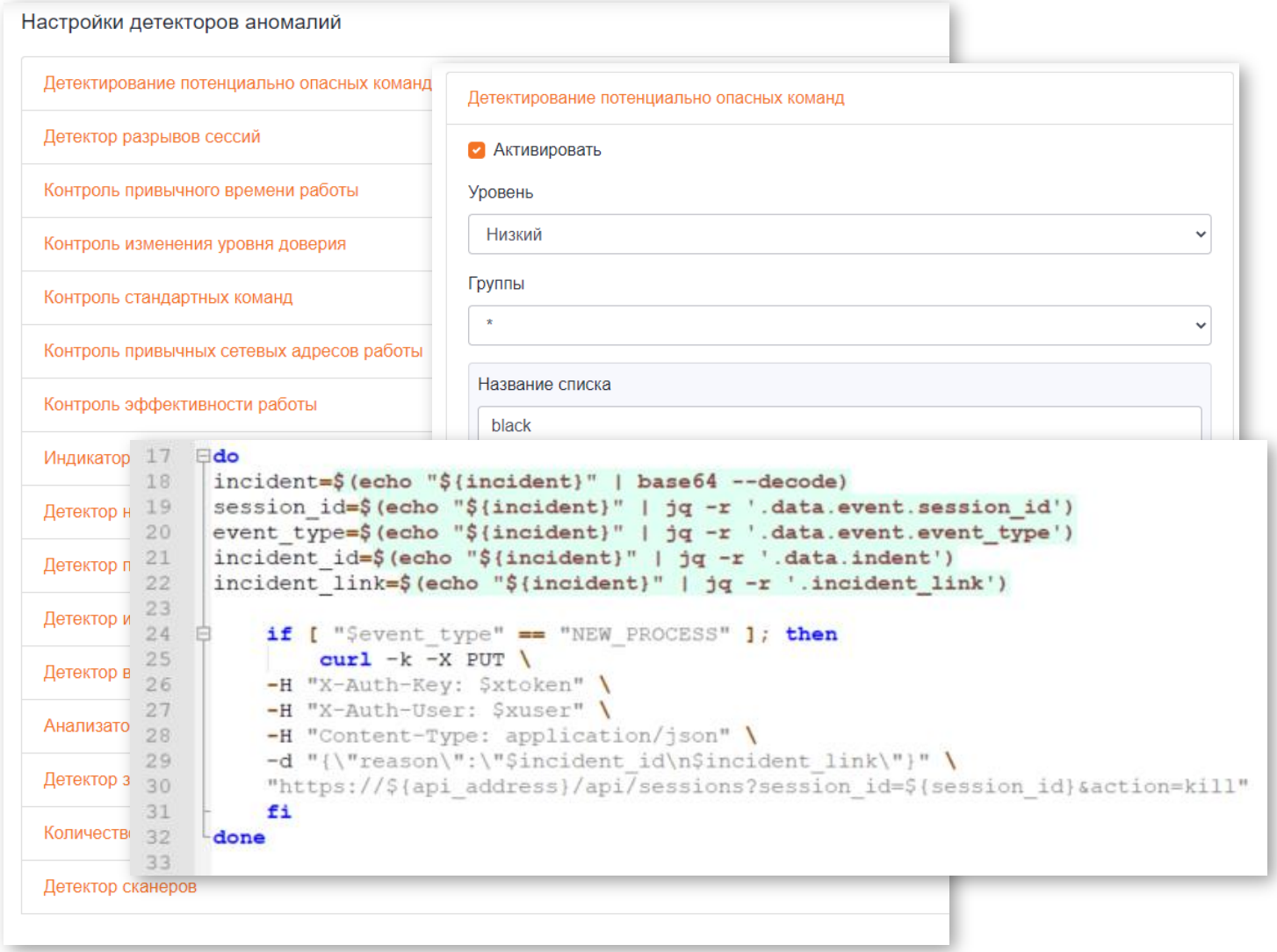
# Управляемая база данных инцидентов




- Обучаемая модель детектора аномалий
- Белые списки инцидентов
- Рабочий процесс обработки инцидентов

АЙТИБАСТИОН

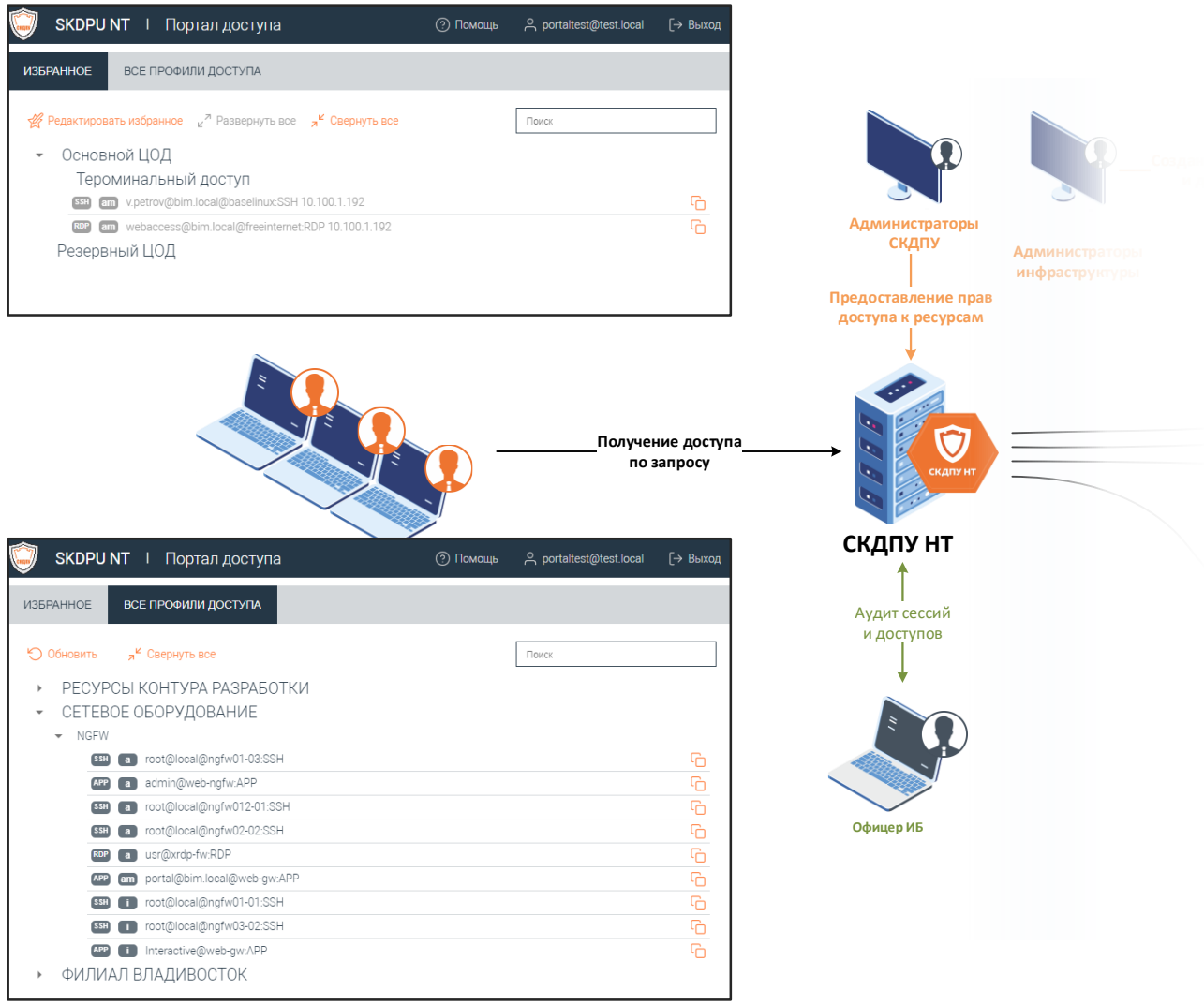
# Детектирование аномального поведения и реагирование




- **Детектирование аномалий** на основе статистических и математических моделей
- Подключение функций **реагирования на инциденты** и интеграция в единую систему реагирования
- Индивидуальные модели реагирования
- Взаимодействие с **SOAR/IRP**

# Портал доступа. Брокер доступов к ресурсам

- **Единая точка доступа** к инфраструктуре шлюзов доступа
- Поддержка встроенных клиентов доступа без необходимости их установки
- Доступ в концепции **«нулевого доверия»**
- Доступ к приложениям и ресурсам VDI
- Настраиваемая **группировка доступов**



# Новые задачи – новые возможности

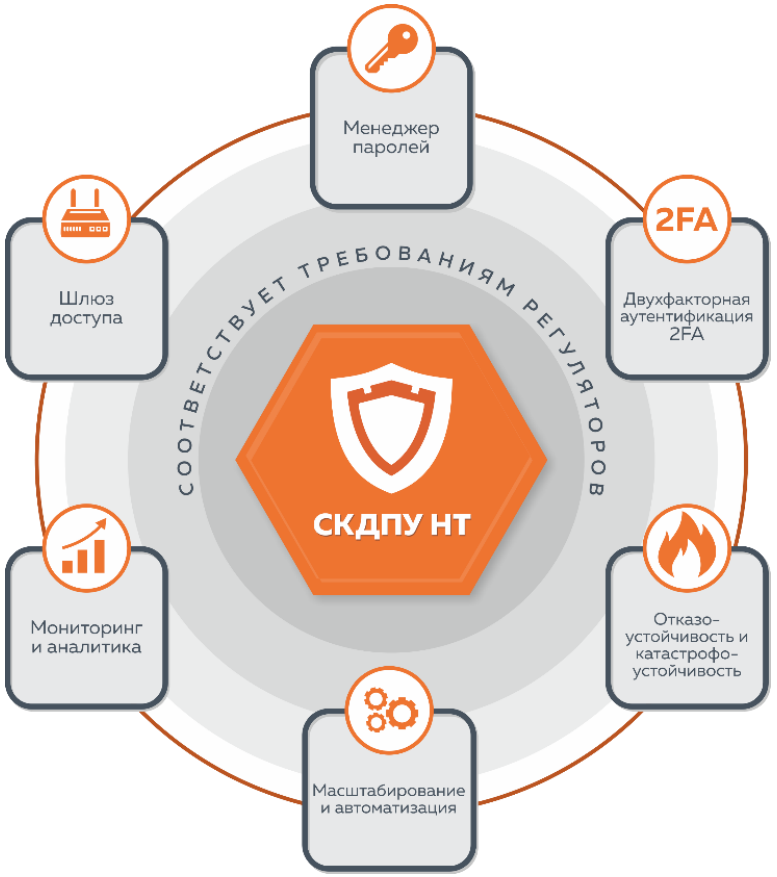
- ✓ Организация независимых точек доступа к ресурсам виртуализации и VDI
- ✓ «Терминальный интернет» для сотрудников
- ✓ Поддержка отечественных ОС и каталогов FreeIPA, ALD Pro и других LDAP
- ✓ Сократить до +-5
- ✓ Ограничения в рамках протоколов: файловый обмен, буфер обмена и т.д.
- ✓ Публикация ресурсов на Шлюзе доступа
- ✓ Фиксация действий и событий, в т.ч. видео
- ✓ Интеграция с системой глубокой аналитики СКДПУ НТ Мониторинг и аналитика

# СКДПУ НТ – это про управление доступом

**Соответствие требованиям**
ФЗ-187 «О безопасности КИИ РФ», Приказы ФСТЭК России №239, №235, Приказы ФСТЭК России № 31, № 17, № 21, Указ Президента РФ от 01.05.2022 №250

**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®

**Сертификаты и реестр**
Включен в реестр отечественного ПО,
Сертификат **ФСТЭК УД-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, Альт**, Windows и др.
Поддержка **FreeIPA**, **ALD Pro** и других **LDAP**

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

АЙТИБАСТИОН

# От большого к малому


## СКДПУ НТ КОМПАКТ

**Программно-аппаратный комплекс, предназначенный для контроля действий собственных администраторов и внешних технических специалистов**

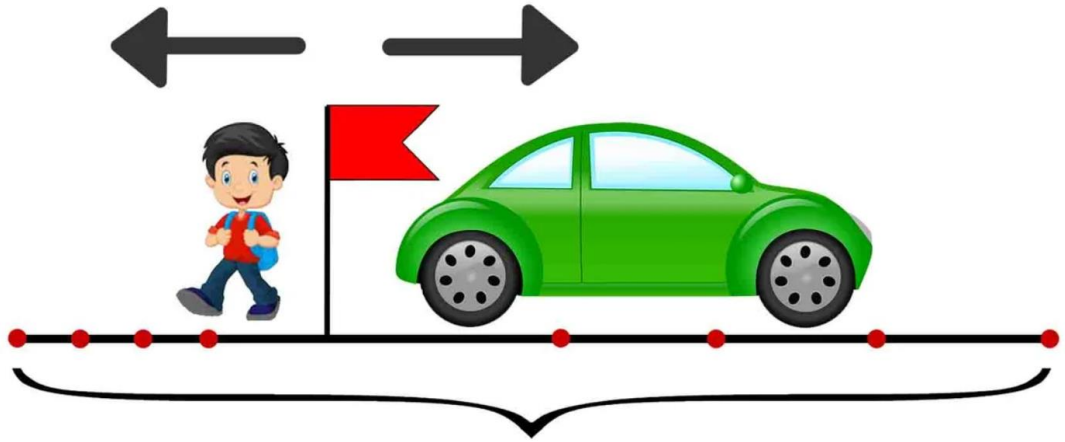
**СКДПУ НТ Компакт** - компактный ПАК, обладающий функциональностью шлюза доступа:

- рассчитан на контроль до 10 одновременных сессий
- удобен в использовании в георасределенной инфраструктуре и небольших компаниях
- доступен по цене

# «Из контура А в контур Б подключался...»

**Дано:**

1. N – собственные сотрудники
2. N+1 – аутсорсеров
3. Наличие данных высокой критичности
4. Распределенная инфраструктура



**Проблема:**

1. Непрозрачность действий при обработке данных
2. Подключение сторонних организаций
3. Подключение к внутренней сети с личных устройств

# Решение от заказчика

**Решение:**

1. СКДПУ НТ в качестве единой точки доступа
   - «извне» и «внутри»
   - с личных и корпоративных устройств
   - к критичным системам

2. «Нулевое доверие» с ограничением привилегий

3. Фиксация событий:
   - запуска и остановки процессов
   - буфера обмена
   - команд, окон и др. событий

4. Фиксация активности и аномального поведения, в т.ч. вредоносного ПО

# Единый контур ИБ с технологическими партнерами

**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.

- ✓ Система обнаружения вторжений
- ✓ Средства виртуализации и облачные сервисы
- ✓ Многофакторная аутентификация
- ✓ Отечественные ОС
- ✓ IRP/SOAR*
- ✓ SIEM-системы
- ✓ Безопасные рабочие места. Тонкие клиенты и т.п.
- ✓ Криптошлюзы и VPN-туннели
- ✓ Token и Smart Card
- ✓ DLP*

АЙТИБАСТИОН

# Технологии и партнеры




















и другие партнеры и интеграции...

АЙТИБАСТИОН

# PAM-платформа СКДПУ НТ

Интеграция и обогащение событиями

Единое управление конфигурацией

Реагирование и расследование

«Точно в срок» (Just –in-time)

Поведенческая аналитика (UEBA)

## Контроль доступа

Анализ инфраструктуры и поиск УЗ

**Нулевое доверие**

Сценарный доступ

Управление паролями

**Автоматизация и оркестрация**

АЙТИБАСТИОН

# Спасибо за внимание!

**Константин Родин**
Руководитель направления
по развитию продуктов

k.rodin@it-bastion.com