АЙТИБАСТИОН

# ПЛАТФОРМА СКДПУ НТ
# КОМПЛЕКСНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ЗАЩИЩЕННОСТИ ПРИВИЛЕГИРОВАННОГО ДОСТУПА

www.it-bastion.com

# ЭКСПЕРТИЗА И ОПЫТ «АЙТИ БАСТИОН»

АЙТИБАСТИОН

## PAM-платформа СКДПУ НТ

Многолетний опыт эксплуатации и внедрения решений по контролю доступа в различных сферах с учетом требований доступности, функциональности и автоматизации процессов

**300+**
Проектов по контролю доступа и анализу действий пользователей

**10 лет**
Разработки, поддержки и внедрения PAM-систем

**>70%**
Отечественного рынка PAM-систем

**170+**
Сотрудников компании

www.it-bastion.com

# ЧТО МЫ ЗНАЕМ О ПРИВИЛЕГИРОВАННЫХ УЧЕТКАХ?

АЙТИБАСТИОН

**Привилегированные**
учетные записи

- Нужны для доступа к критически важным целевым системам
- Есть в каждой организации
- Сложно контролировать организационно и технически
- Основная цель атак злоумышленников

www.it-bastion.com

# ВИДЫ ПРИВИЛЕГИРОВАННЫХ УЧЕТНЫХ ЗАПИСЕЙ

АЙТИБАСТИОН

# ПРОБЛЕМЫ ПРИВИЛЕГИРОВАННОГО ДОСТУПА

АЙТИБАСТИОН

- Отсутствие контроля и мониторинга использования привилегий
- Несоответствие требованиям и стандартам безопасности
- Атаки на цепочку поставок
- Внедрение ВПО
- Сложность управления большим числом УЗ
- Злоупотребление привилегиями
- Фишинг и социальная инженерия
- Нелояльные сотрудники
- Несанкционированный доступ
- Эксплуатация уязвимостей

# ВОЗМОЖНЫЕ ПОСЛЕДСТВИЯ

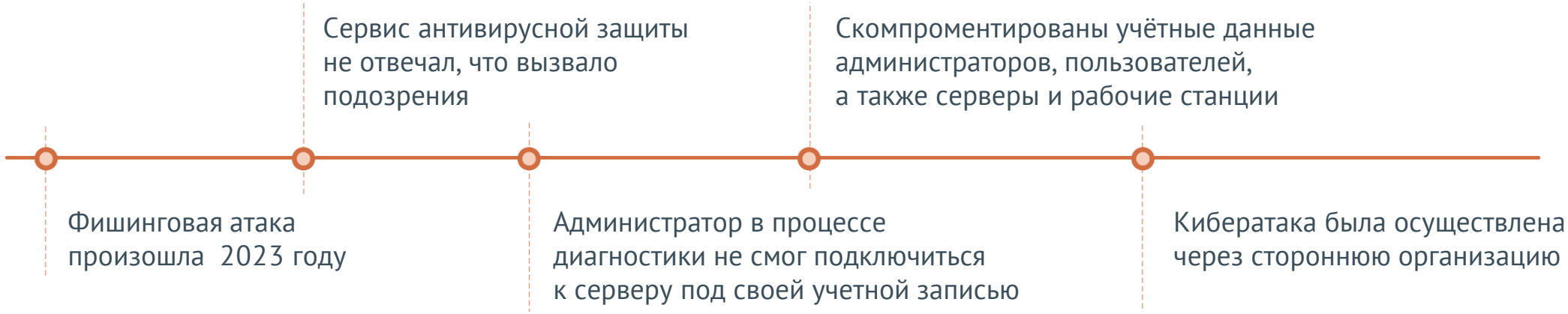
АЙТИБАСТИОН

# ПРИМЕР ИЗ РЕАЛЬНОЙ ЖИЗНИ

АЙТИБАСТИОН

## Кибератака на инфраструктуру интегратора Platformix

### Ход атаки




Реальной утечки данных не произошло, однако было потеряно рабочее время сотрудников (2 недели), также Platformix заплатила за привлечение сторонней организации для проведения профессионального ИБ-анализа

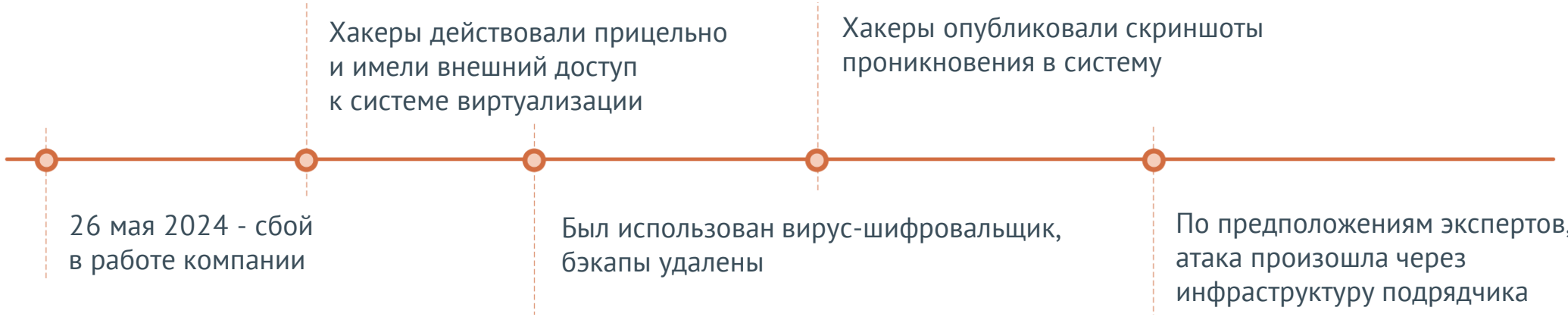
# ПРИМЕР ИЗ РЕАЛЬНОЙ ЖИЗНИ

АЙТИБАСТИОН

## Взлом курьерской компании СДЭК

Организаторы – международная хакерская группа Head Mare

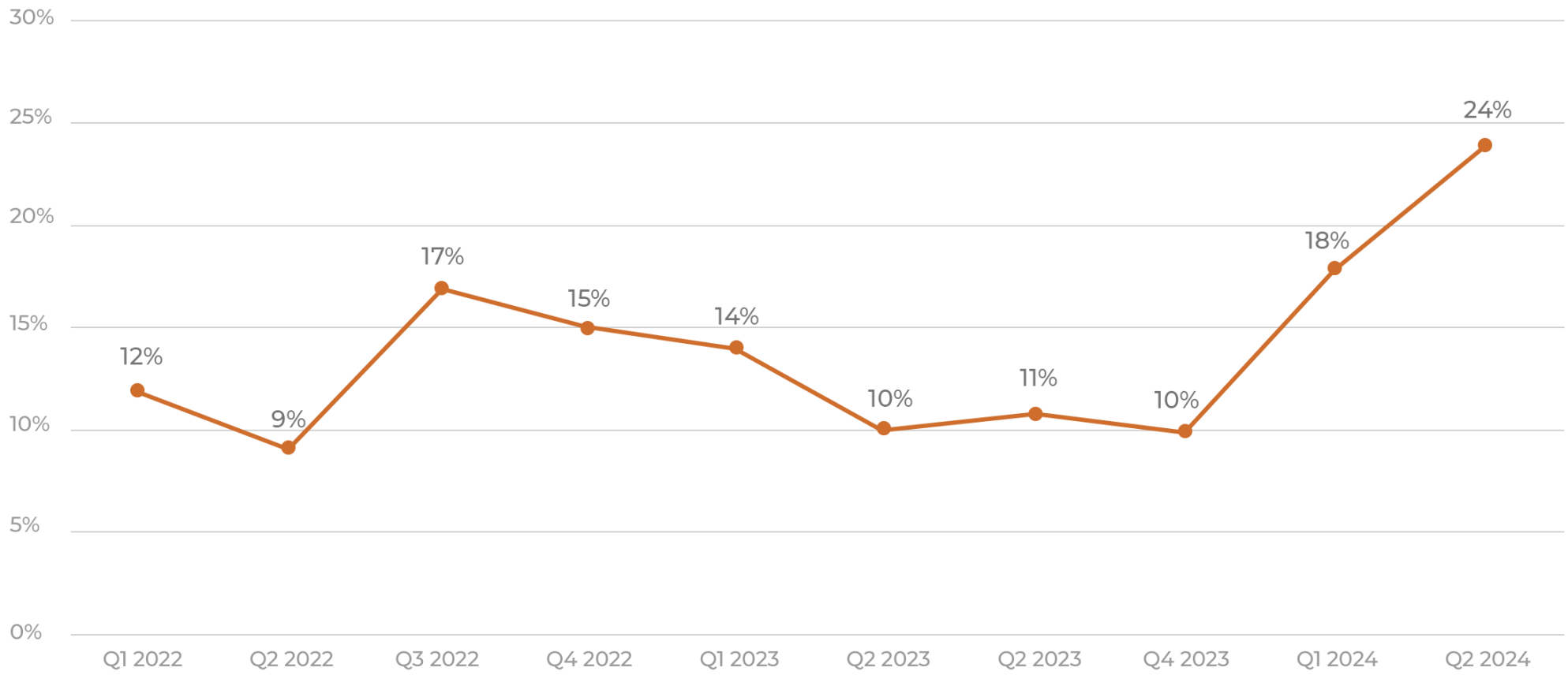
### Ход атаки




- СДЭК не работала 3 дня
- Пострадали десятки тысяч клиентов, в том числе крупные маркетплейсы
- Задержались доставки 1,75 – 3 миллионов заказов

# РОСТ ЧИСЛА УТЕЧЕК УЧЕТНЫХ ДАННЫХ
## ПОЧЕМУ ЭТО ПРОИСХОДИТ?

АЙТИБАСТИОН




Динамика утечек учетных данных у организаций (2022 год – первое полугодие 2024 года). Источник: PT

# СТАНДАРТНЫХ МЕТОДОВ ЗАЩИТЫ НЕДОСТАТОЧНО?
## ЧТО ДЕЛАТЬ?

АЙТИБАСТИОН

# СКДПУ НТ

Платформа обеспечения защищенности привилегированного доступа

Минцифры России

МИНИСТЕРСТВО ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФСТЭК России

# СОСТАВ ПЛАТФОРМЫ СКДПУ НТ

АЙТИБАСТИОН

## Шлюз доступа

Контроль сессий,
запись событий доступа,
менеджер паролей,
двухфакторная
аутентификация

## Портал доступа

Единая точка доступа
к инфраструктуре шлюзов.
Удобная структурированная и
настраиваемая группировка доступов

## Кабинет оператора

Оптимизация управления целевыми
устройствами
и правилами доступа.
Разделение зон ответственности

## Мониторинг и аналитика

Мониторинг, отчетность
и статистика.
Поведенческий анализ
и детектирование аномалий.
Выявление инцидентов и реагирование
на них

## Архив аудита

Централизованное хранение
и просмотр событий доступа.
Оптимизация хранения сессий на
Шлюзах доступа

## Агрегатор доступов

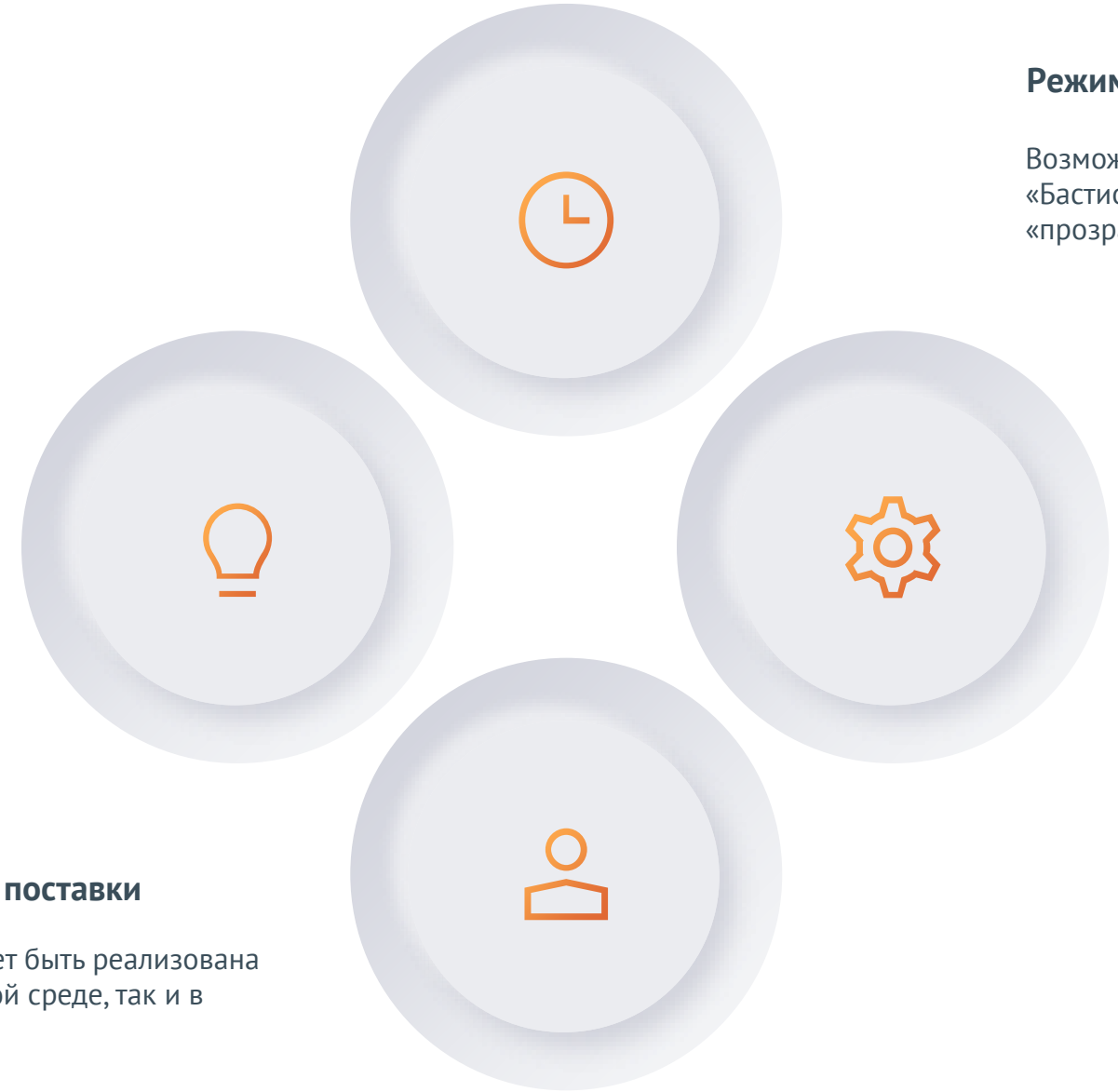
Автоматизированный перенос данных
авторизаций и политик доступа к
ресурсам из сторонних систем в
структуру Шлюза доступа

# ОСОБЕННОСТИ ПЛАТФОРМЫ
## СКДПУ НТ

АЙТИБАСТИОН

### Режимы работы

Возможна работа в режиме «Бастион» (прокси) или в «прозрачном» режиме



### Операционные системы

Платформа базируется на ОС AstraLinux SE. Поддерживается работа с AstraLinux, РЕД ОС, Альт, Windows и другими ОС

### Интеграционные возможности

Способность к интеграциям с продуктами других классов (SIEM,DLP,NGFW, IDS,VDI и др.)

### Варианты поставки

Платформа может быть реализована как в виртуальной среде, так и в виде ПАК

# ПРОБЛЕМНЫЕ ВОПРОСЫ
## МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

АУД.4 Регистрация событий безопасности

УПД.6 Ограничение неуспешных попыток доступа в информационную систему

УКФ.1 Идентификация объектов управления конфигурацией

УПД.1 Управление учетными записями пользователей

Идентификация и аутентификация

ИНЦ.2 Информирование о компьютерных инцидентах

ОДТ.1 Использование отказоустойчивых технических средств

ИАФ

Управление доступом

УПД

ИНЦ.1 Выявление компьютерных инцидентов

АУД.7 Мониторинг безопасности

АУД

ИПО

АУД.8 Реагирование на сбои при регистрации событий безопасности

ИАФ.1 Идентификация и аутентификация пользователей и инициируемых ими процессов

Защита информационной системы и ее компонентов

УПД.7 Предупреждение пользователя при его доступе к информационным ресурсам

Реагирование на компьютерные инциденты

ИАФ.5 Идентификация и аутентификация внешних пользователей

УПД.10 Блокирование сеанса доступа пользователя при неактивности

УПД.5 Назначение минимально необходимых прав и привилегий

АУД.9 Анализ действий отдельных пользователей

ИНЦ.6 Хранение и защита информации о компьютерных инцидентах

Аудит безопасности

ИНЦ.3 Анализ компьютерных инцидентов

ИАФ.2 Идентификация и аутентификация устройств

УПД.13 Реализация защищенного удаленного доступа

УПД.2 Реализация модели управления доступом

УКФ

Управление конфигурацией

ОДТ

ЗИС

ИНЦ

Обеспечение доступности

ЗИС.30 Использование устройств терминального доступа

ОДТ.2 Резервирование средств и систем

Информирование и обучение персонала

ОДТ.7 Кластеризация информационной системы

УПД.9 Ограничение числа параллельных сеансов доступа

ИАФ.3 Управление идентификаторами

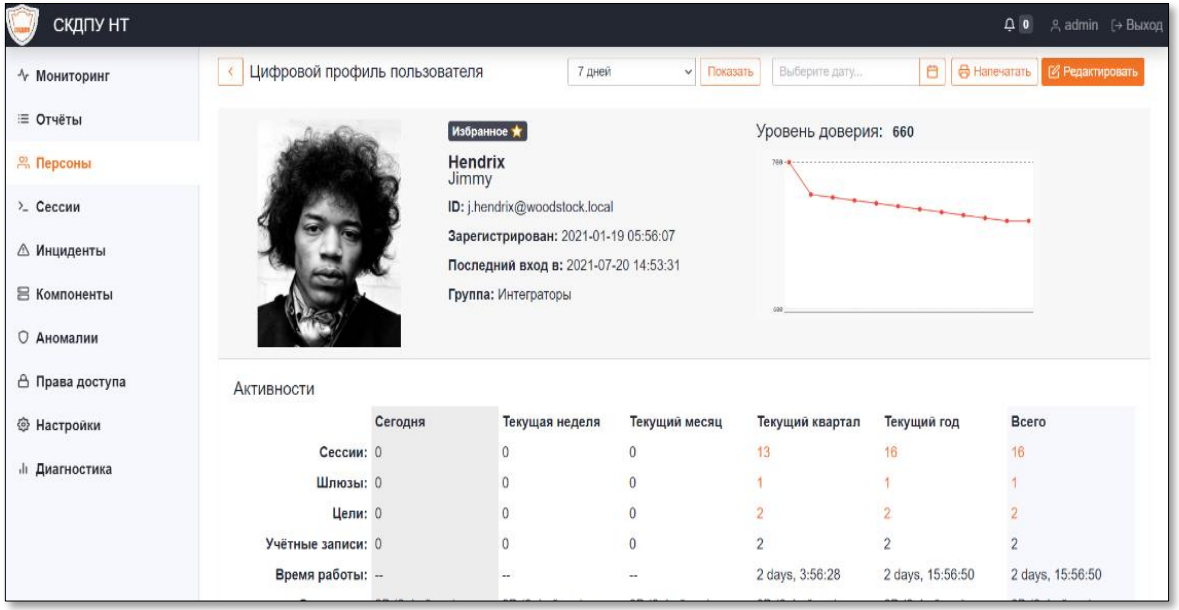
ИПО.2 Обучение персонала правилам безопасной работы

ОДТ.6 Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях

УПД.4 Разделение полномочий (ролей) пользователей

# ОСНОВНЫЕ ВОЗМОЖНОСТИ СИСТЕМЫ
## МОНИТОРИНГ И АНАЛИТИКА


- Цифровой профиль
- Поведенческая модель
- Уровень доверия пользователя

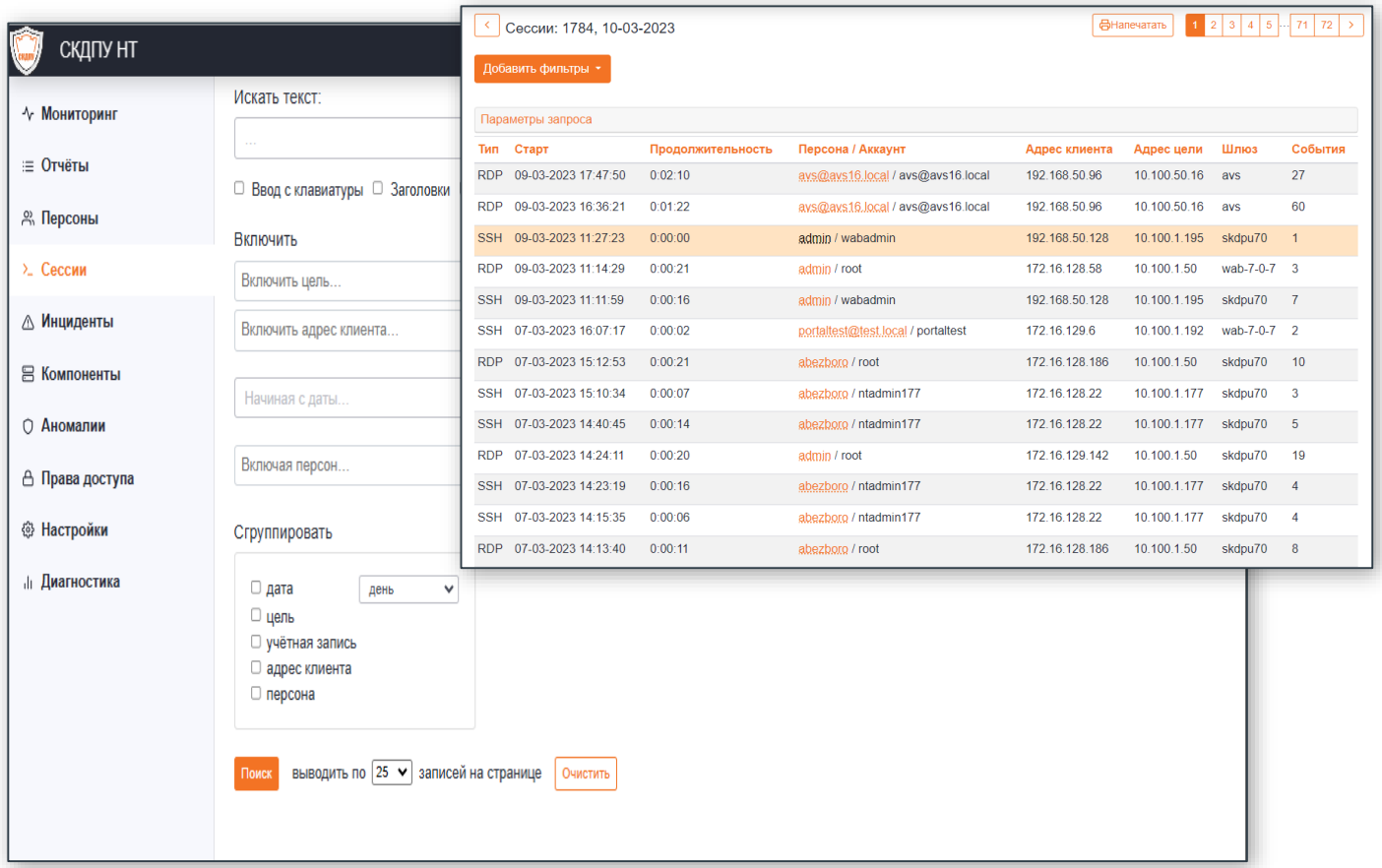


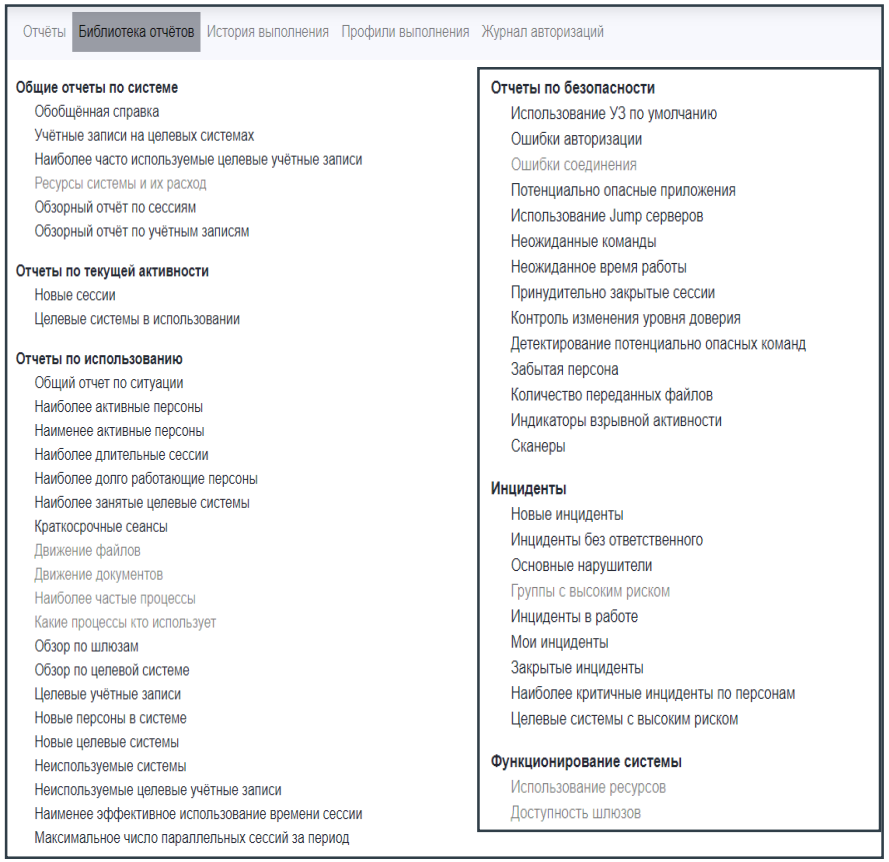

**Мониторинг и централизованный поиск** по всем доступным параметрам

# ОСНОВНЫЕ ВОЗМОЖНОСТИ СИСТЕМЫ
## МОНИТОРИНГ И АНАЛИТИКА

АЙТИБАСТИОН

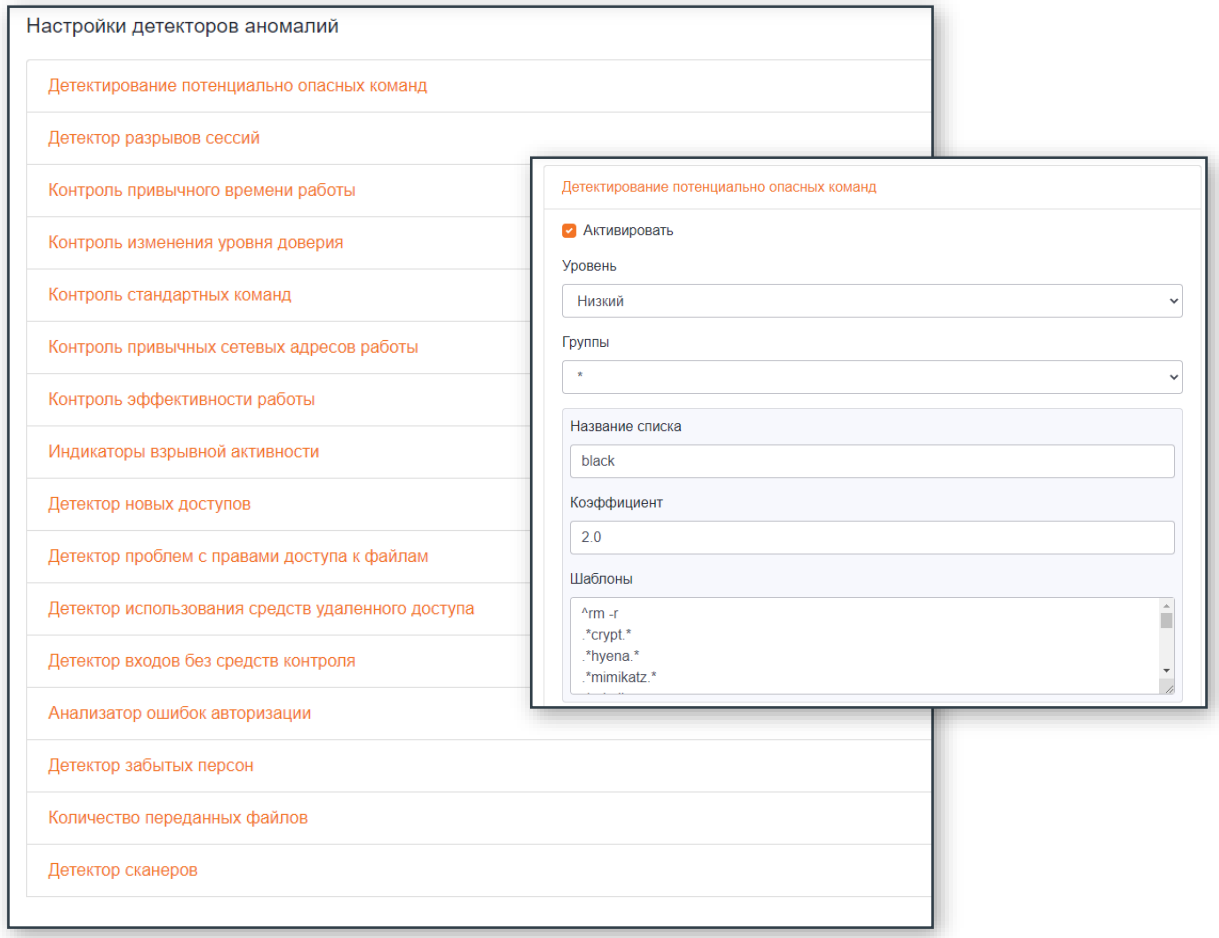
**Предоставление расширенной статистики** по всем действиям и подключениям пользователей, возможность формировать сводные отчеты по различным сценариям



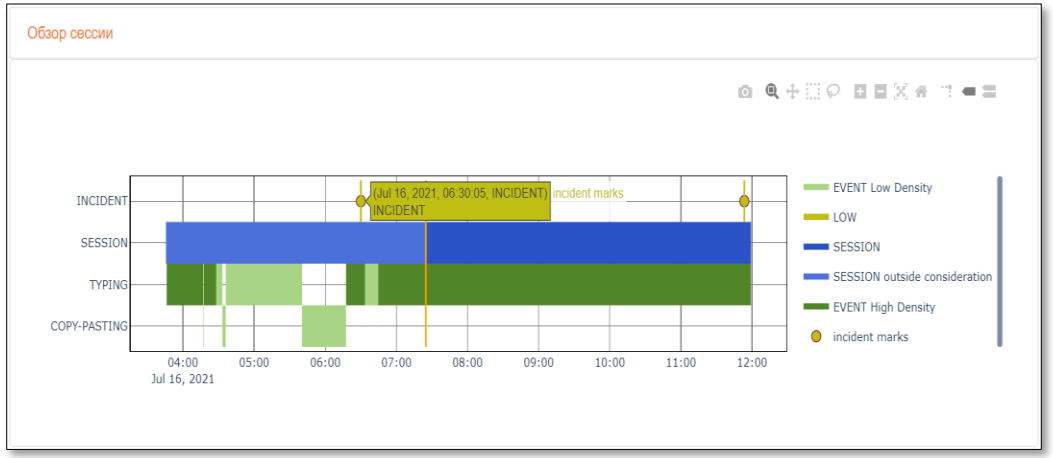



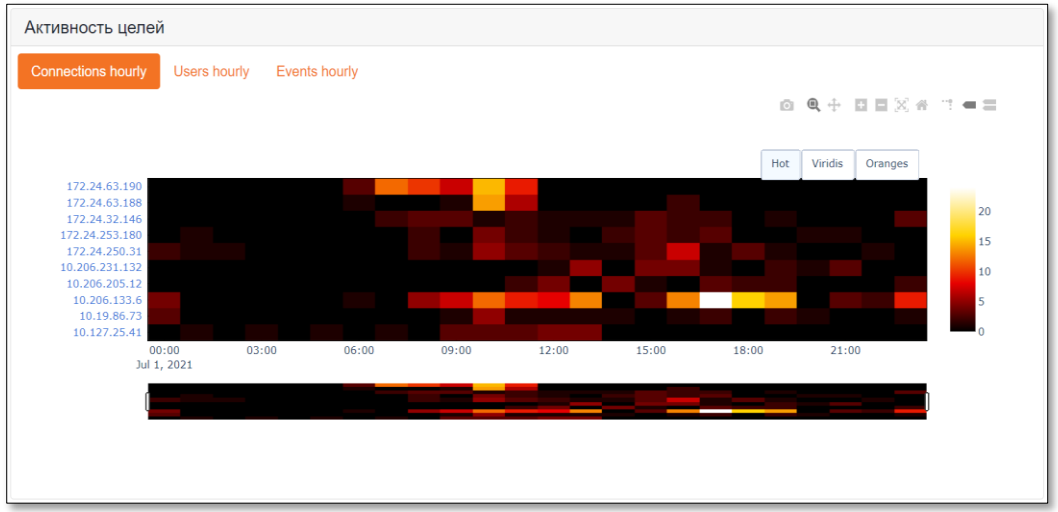
# ОСНОВНЫЕ ВОЗМОЖНОСТИ СИСТЕМЫ
# МОНИТОРИНГ И АНАЛИТИКА

АЙТИБАСТИОН




## Карта событий и тепловая карта активности



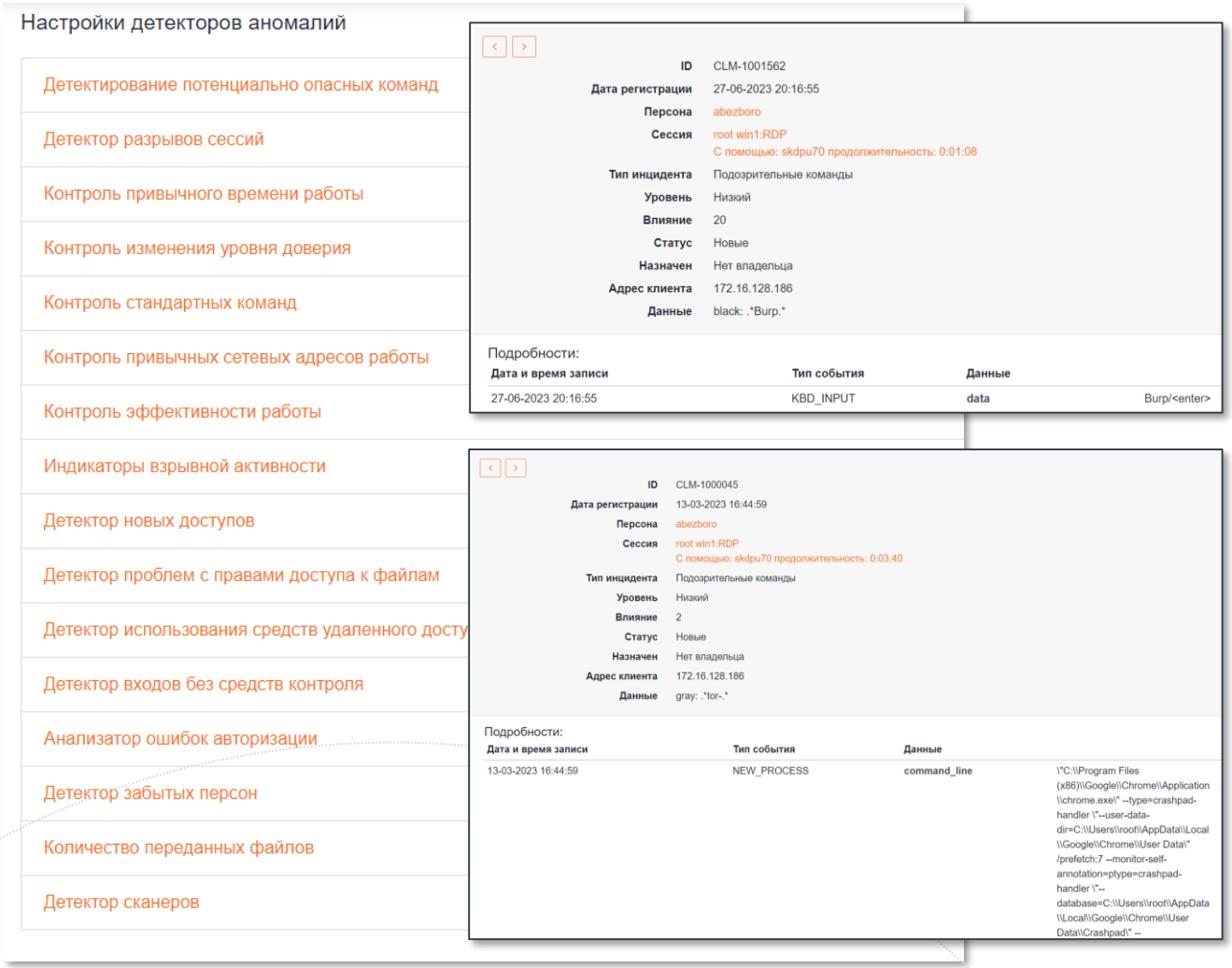




**Детектирование** аномального поведения пользователей и **фиксация** инцидентов безопасности

www.it-bastion.com

# ОСНОВНЫЕ ВОЗМОЖНОСТИ СИСТЕМЫ
## МОНИТОРИНГ И АНАЛИТИКА

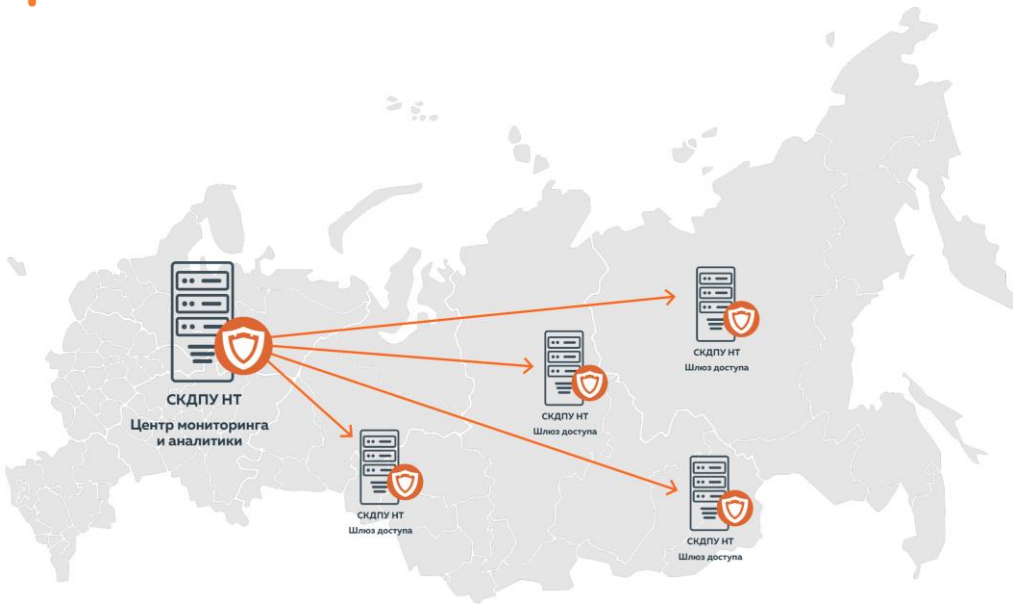
АЙТИБАСТИОН




- Индивидуальные **модели реагирования**
- Подключение **функций реагирования на инциденты** и интеграция в единую систему реагирования
- Взаимодействие с **SOAR/IRP**

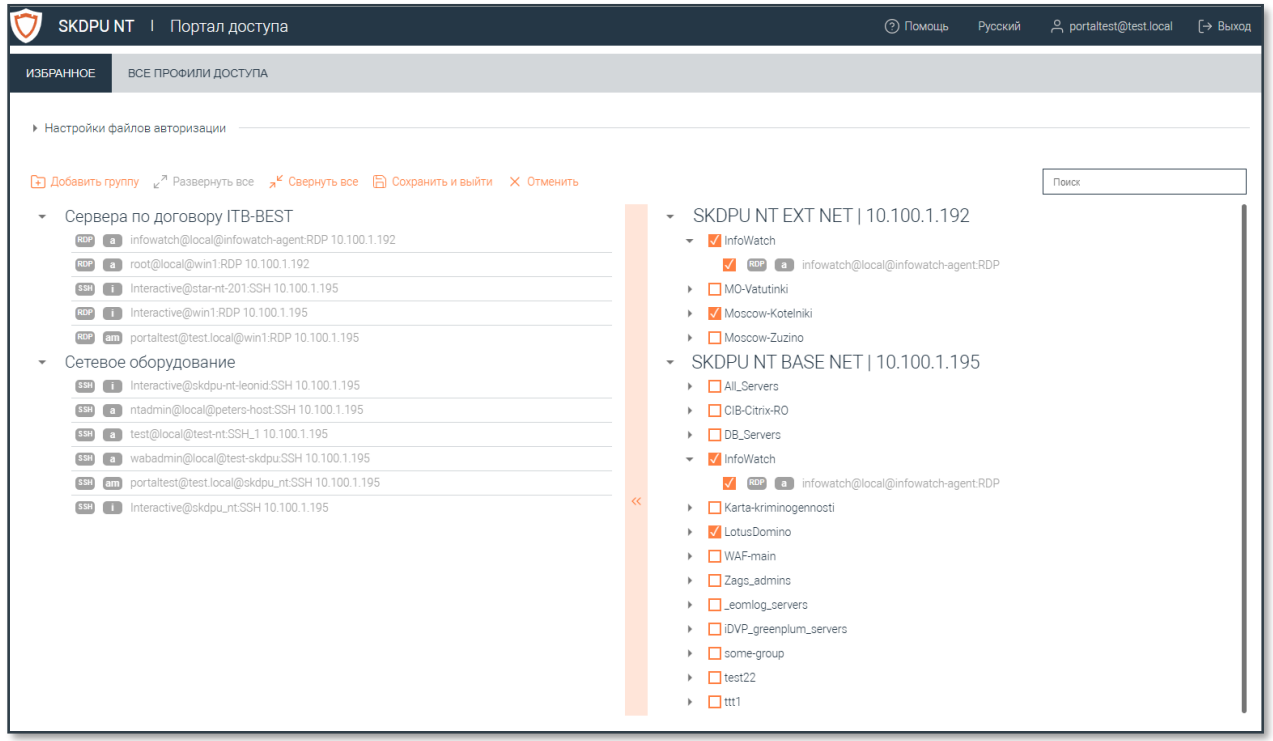
```
do
incident=$(echo "${incident}" | base64 --decode)
session_id=$(echo "${incident}" | jq -r '.data.event.session_id')
event_type=$(echo "${incident}" | jq -r '.data.event.event_type')
incident_id=$(echo "${incident}" | jq -r '.data.indent')
incident_link=$(echo "${incident}" | jq -r '.incident_link')

    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
```

# ОСНОВНЫЕ ВОЗМОЖНОСТИ ПЛАТФОРМЫ
## ПОРТАЛ ДОСТУПА

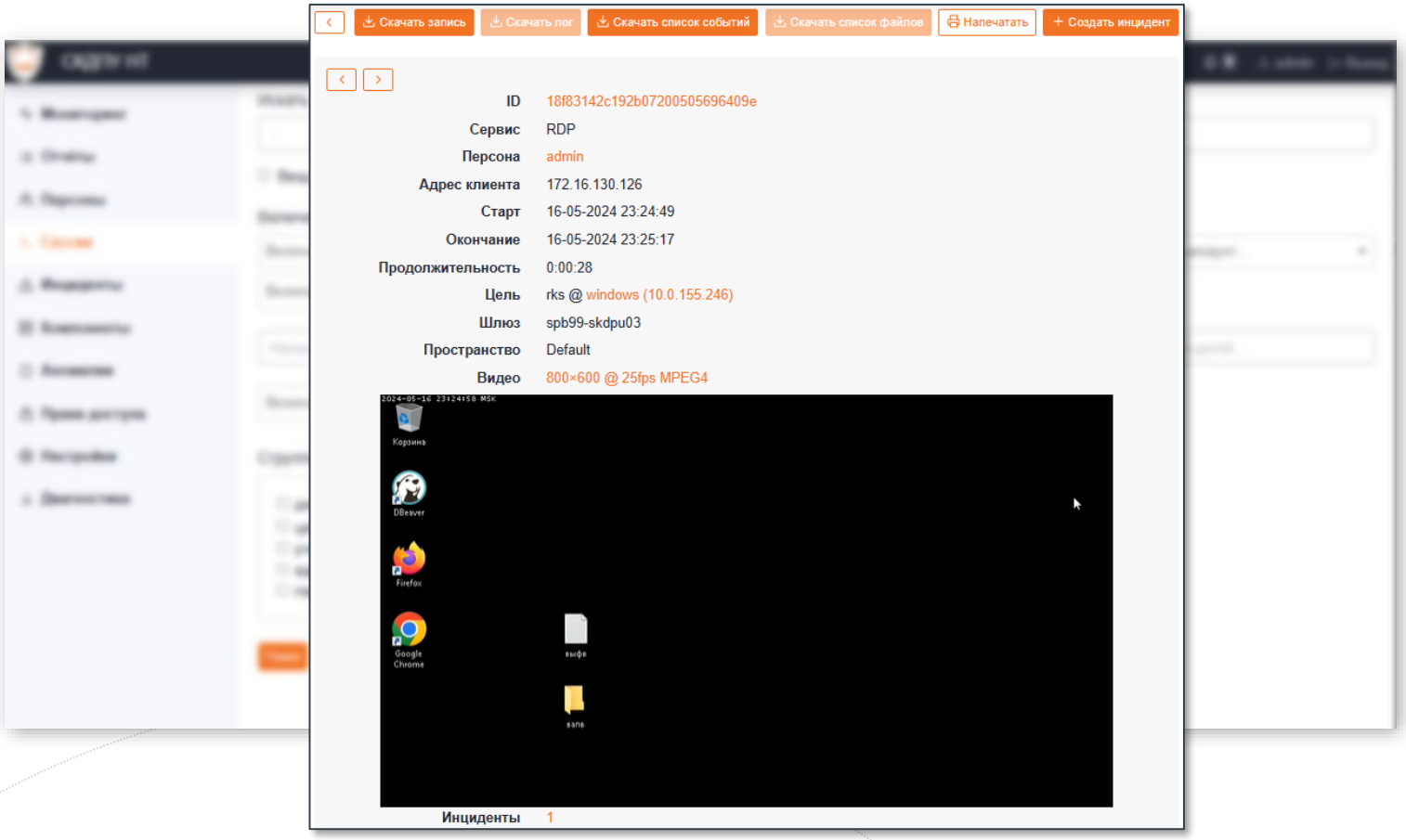



- **Единая точка доступа** к инфраструктуре шлюзов доступа
- Доступ в концепции **«нулевого доверия»**
- Доступ к **приложениям и ресурсам VDI**
- Настраиваемая **группировка доступов**

**Быстрый и удобный доступ к ресурсам СКДПУ НТ**
для всех типов пользователей и при любых размерах ИТ-инфраструктуры



# ОСНОВНЫЕ ВОЗМОЖНОСТИ ПЛАТФОРМЫ
## АРХИВ АУДИТА



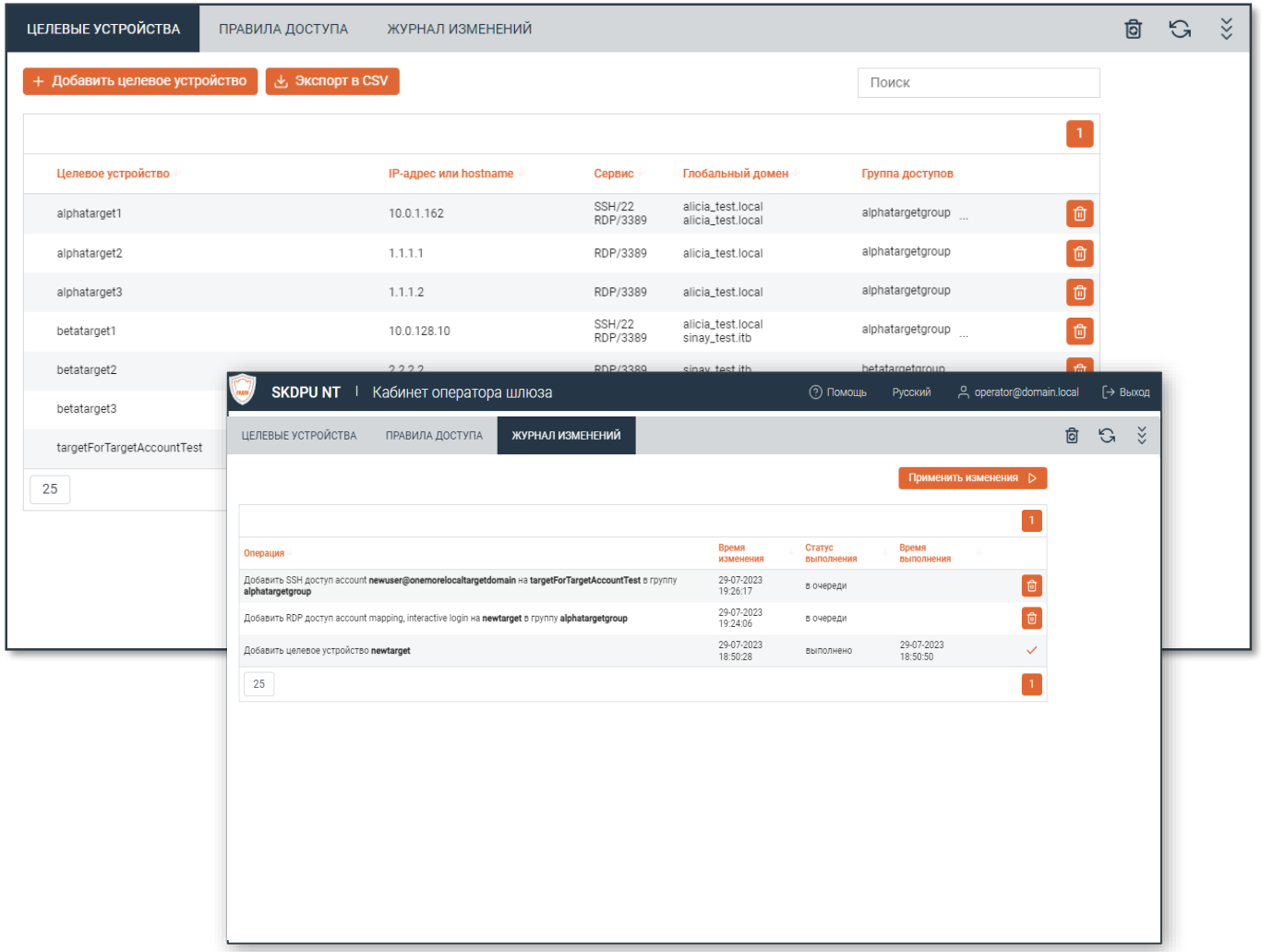

**Централизованный архив данных и событий по сессиям**

- **Автоматическое освобождение** занятого места на шлюзах
- **Выгрузка** записей сессий в видеоформате для подтверждения расследований
- **Ротация и восстановление** данных аудита

# ОСНОВНЫЕ ВОЗМОЖНОСТИ ПЛАТФОРМЫ
## КАБИНЕТ ОПЕРАТОРА

АЙТИБАСТИОН

- **Оптимизация** управления доступами
- **Разделение** зон ответственности
- **Делегирование** части полномочий
- **Минимизация** ошибочных доступов
- **Контроль** критичных изменений



# ОСНОВНЫЕ ВОЗМОЖНОСТИ ПЛАТФОРМЫ
## ШЛЮЗ ДОСТУПА

АЙТИБАСТИОН

Контроль приложений и УЗ в них

Единая точка доступа

Просмотр и прерывание сессий

Запись событий доступа

Работа по заявкам с возможностью подтверждения доступа

Управление паролями

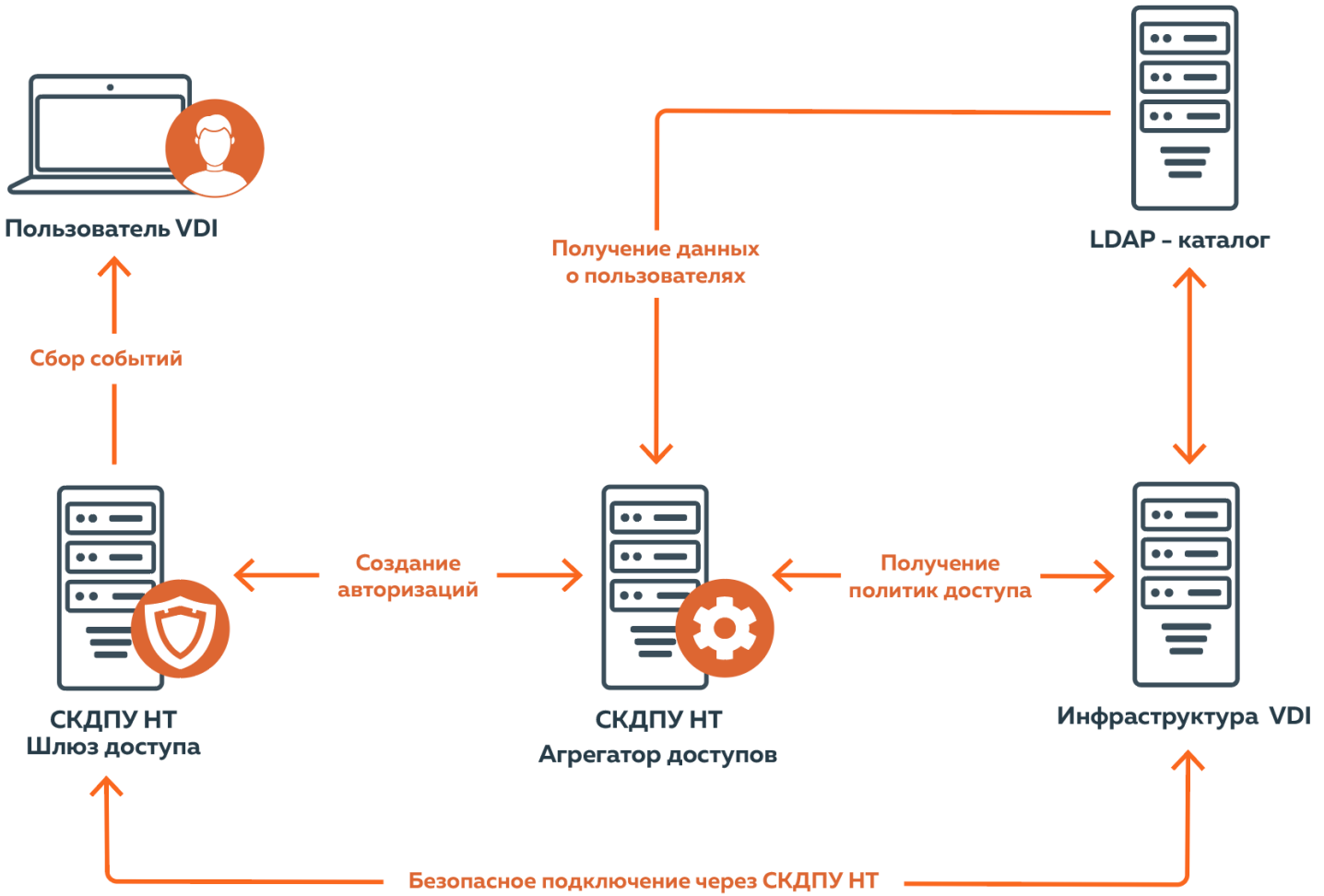
Контроль на стороне ИС

Без установки агентов

# ОСНОВНЫЕ ВОЗМОЖНОСТИ ПЛАТФОРМЫ
## АГРЕГАТОР ДОСТУПОВ

АЙТИБАСТИОН

**Автоматическое предоставление доступа к пользовательским ресурсам** в виртуальной среде с функциями расширенного контроля и мониторинга действий пользователей



# ВОЗМОЖНОСТИ
# МЕЖВЕНДОРНЫХ ИНТЕГРАЦИЙ

АЙТИБАСТИОН


www.it-bastion.com

# Спасибо за внимание!

АЙТИБАСТИОН

Дмитрий Симак
Менеджер продукта СКДПУ НТ

d.simak@it-bastion.com

+7 910 949 32 75

it-bastion.com