АЙТИБАСТИОН

# РАМ-ПЛАТФОРМА СКДПУ НТ: ПОРТАЛ ДОСТУПА И АВТОМАТИЗИРОВАННОЕ ПРЕДОСТАВЛЕНИЕ ДОСТУПА К ВИРТУАЛЬНЫМ РЕСУРСАМ ПОЛЬЗОВАТЕЛЕЙ

www.it-bastion.com

# ЭКСПЕРТИЗА И ОПЫТ
# АЙТИ БАСТИОН

АЙТИБАСТИОН

## PAM-система
## СКДПУ НТ

Многолетний опыт эксплуатации и внедрения решений по контролю доступа в банковской сфере с учетом требований доступности, функциональности и автоматизации процессов.

**200+**
Проектов по контролю доступа, в т.ч. в финансовой сфере

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

**50%**
Отечественного рынка PAM-систем

**130+**
Сотрудников компании

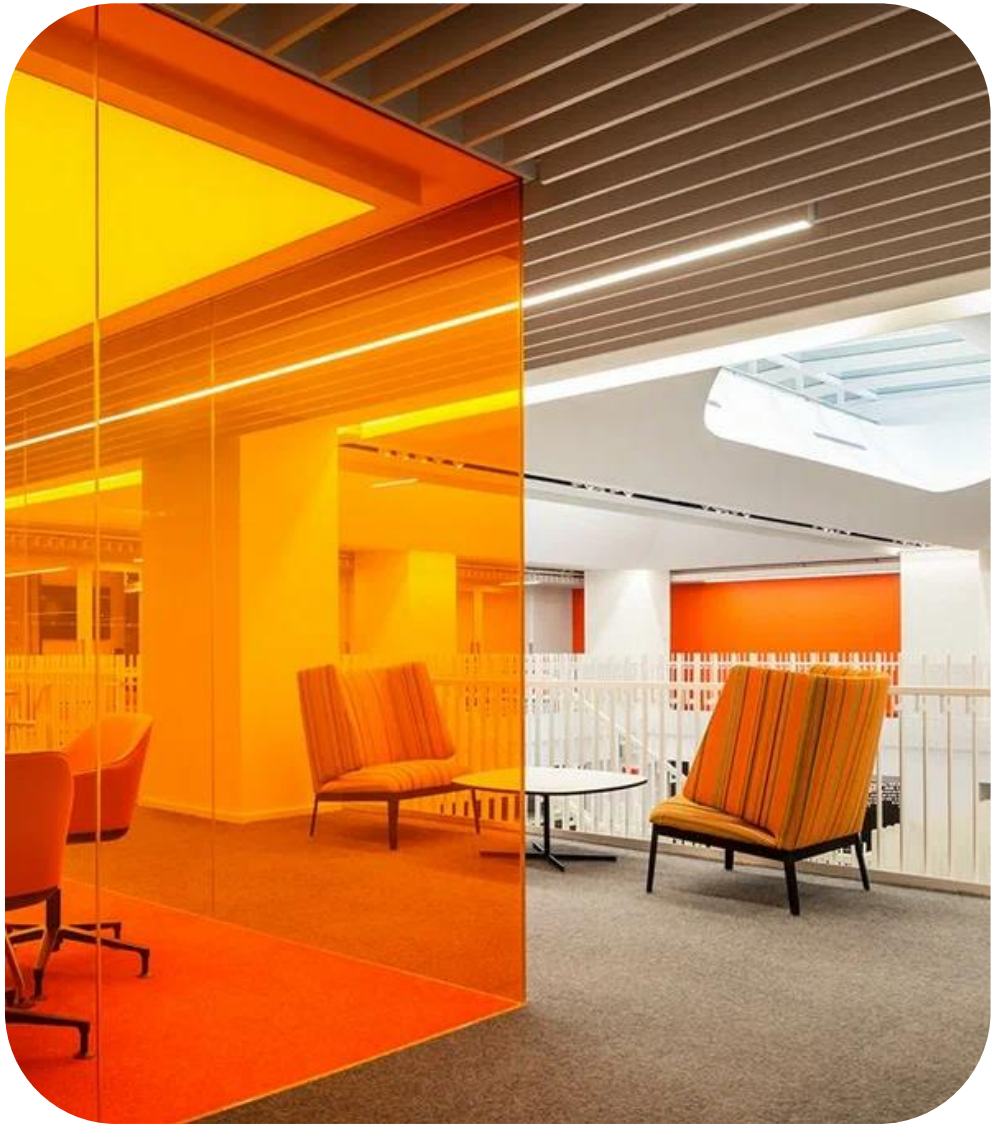
www.it-bastion.com

# ЦЕЛЬ ПРОЕКТА

**Реализация единого автоматизированного механизма предоставления доступа** к пользовательским ресурсам в виртуальной среде финансовой организации **в концепции «Единого окна»** с функциями дополнительного контроля действий пользователей.

В рамках автоматизации должны быть задействованы:

- Система отечественной виртуализации.
- Система контроля действий пользователей PAM.



# ПРЕДПОСЫЛКИ К ВОЗНИКНОВЕНИЮ ПОТРЕБНОСТИ К СОЗДАНИЮ РЕШЕНИЯ

АЙТИБАСТИОН

01

**Уход с рынка РФ компаний и решений**, обеспечивающих привычные механизмы предоставления доступа к ресурсам для пользователей, **в т.ч. VMWare, Citrix и др**. **Импортозамещение средств виртуализации** и доступа пользователей к собственным ресурсам, **в т.ч. VDI.**

02

**Обеспечение требований безопасности** в части предоставления доступа к ресурсам финансовых организаций, **формирование данных для расследований потенциальных инцидентов**, а также **соответствие требованиям регуляторов**.

03

Реализация системы **автоматизированного предоставления доступа** пользователей, в т.ч. **в режиме единого окна** запроса и получения доступа к ресурсам через систему контроля действий пользователей.

# КЛЮЧЕВЫЕ ПОКАЗАТЕЛИ И ТРЕБОВАНИЯ К РЕАЛИЗУЕМОМУ ПРОЕКТУ

АЙТИБАСТИОН

## Виртуальные ресурсы

Инфраструктура рабочих столов и других ресурсов расположена в виртуальной среде финансовой организации

## Контроль доступа

Действия сотрудников в сессии должны быть зафиксированы в видео и текстовом формате, средствами PAM

## Удобство администрирования

Решение должно быть максимально автоматизировано и не требовать дополнительных ресурсов для предоставления доступа

## Безопасность удаленного доступа

Удаленный доступ должен быть контролируемым, с возможностью детального анализа событий и идентификации отклонений поведения

## Удобство эксплуатации

Решение должно быть приближено к стандартному сценарию использования удаленного доступа пользователями

# ВЫБРАННЫЙ ВАРИАНТ РЕШЕНИЯ ЗАДАЧИ

АЙТИБАСТИОН

## ВАРИАНТ 1

**Ручное добавление** ресурсов и управление ими в системе виртуализации и PAM-системе.

**Достоинства:**
- Гранулярное разграничение доступа к ресурсам
- Полный контроль и гибкость конфигурации
- Расширенный набор данных для анализа

**Недостатки:**
- Трудоемкость настройки и эксплуатации
- Низкая скорость внесения изменений
- Требуются дополнительные человеческие ресурсы

## ВАРИАНТ 2

**Автоматизация добавления** ресурсов и управление ими **в системе виртуализации**. Открытие доступа пользователям через **PAM-систему на все ресурсы и IP-адреса** системы виртуализации.

**Достоинства:**
- Простота настройки и эксплуатации
- Высокая скорость внесения изменений
- Расширенный набор данных для анализа

**Недостатки:**
- Отсутствие гранулярного разграничения доступа к ресурсам
- Требуются дополнительные человеческие ресурсы
- Ограниченный контроль и гибкость конфигурации

## ВАРИАНТ 3

**Автоматизация добавления ресурсов** и управление ими в системе виртуализации, а также автоматическое добавление ресурсов в PAM-систему **в режиме гранулярного доступа «пользователь-целевая система»**

**Достоинства:**
- Гранулярный доступ к ресурсам
- Полный контроль и гибкость конфигурации
- Расширенный набор данных для анализа
- Простота настройки и эксплуатации
- Высокая скорость внесения изменений
- Расширенный набор данных для анализа

**Недостатки:**
- Требуется создание системы автоматизации процесса добавления и синхронизации

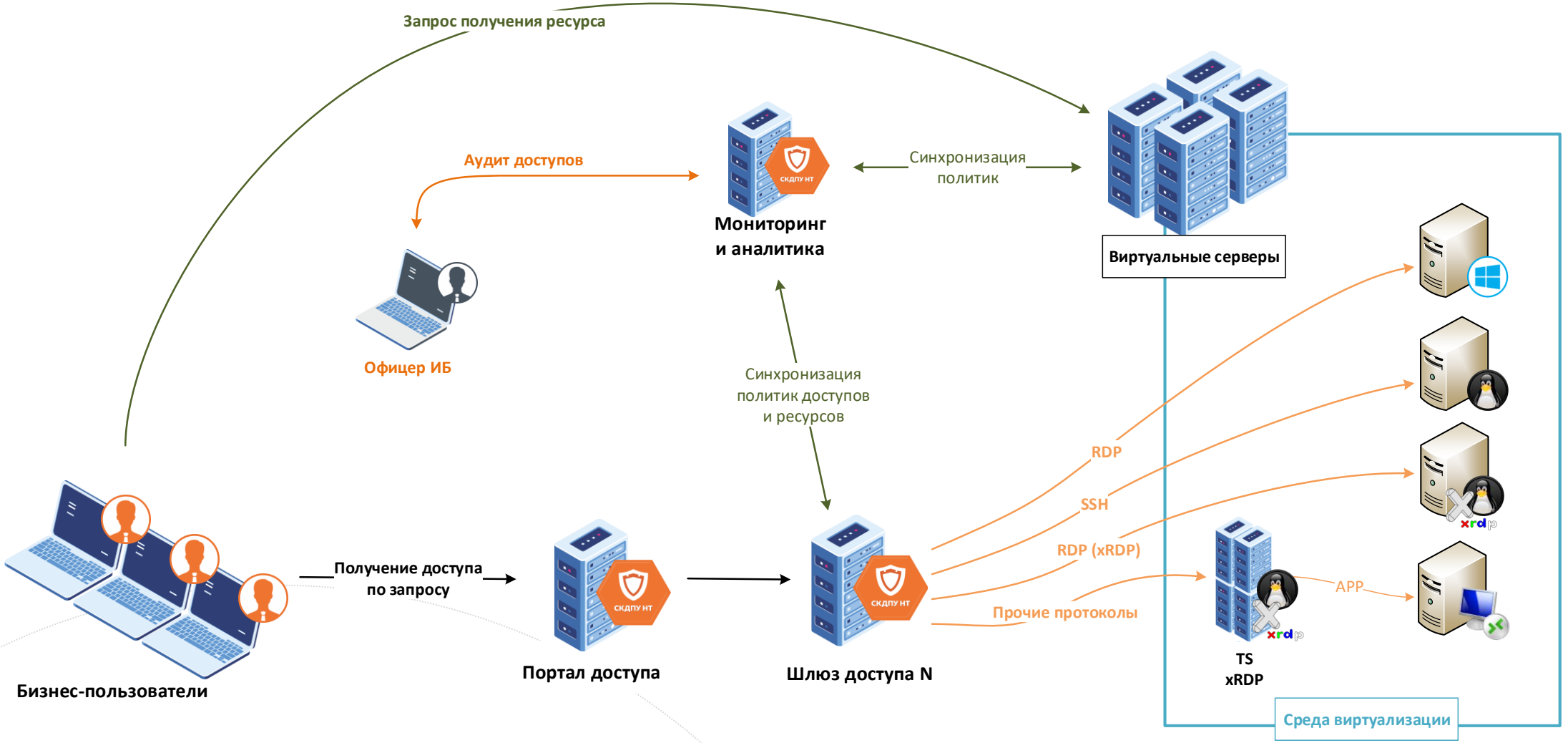
АЙТИБАСТИОН

**Пользователь запрашивает создание** или удаление ресурса **в едином интерфейсе** системы виртуализации в рамках своей учетной записи

Информация о **создаваемых или удаляемых ресурсах синхронизируется** с сервером СКДПУ НТ Шлюз доступа

**Ресурсы пользователя автомагически становятся доступны** пользователю, запросившему доступ в рамках **единого интерфейса Портала доступа**

# СХЕМА РЕАЛИЗОВАННОГО ВАРИАНТА 3



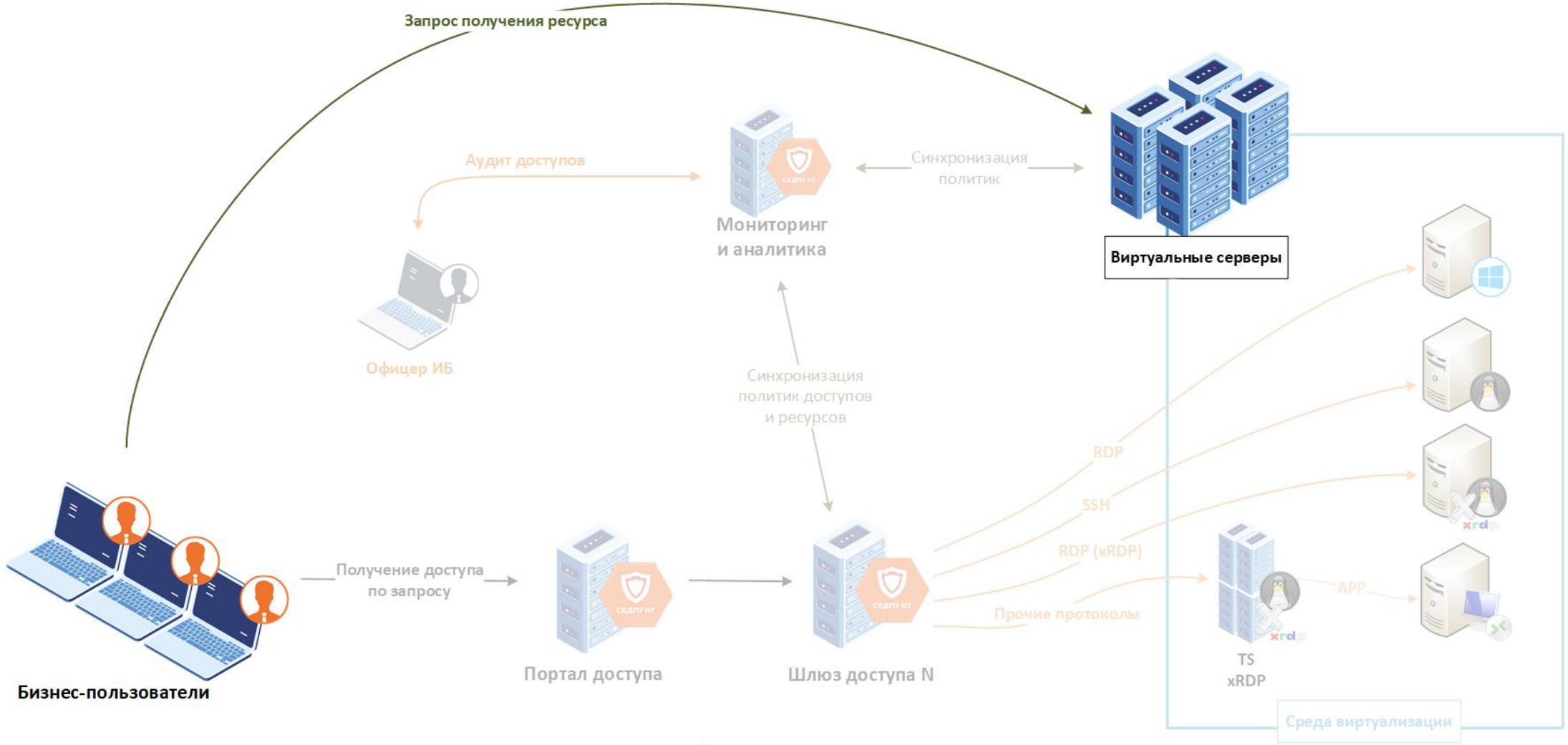
# Единый интерфейс **запроса доступа**

Пользователь запрашивает создание или удаление ресурса в едином интерфейсе системы виртуализации в рамках своей учетной записи и своих полномочий.

Запрос ресурса производится через интерфейс доступной системы виртуализации с последующей привязкой его к конкретному пользователю.

# СХЕМА РЕАЛИЗОВАННОГО ВАРИАНТА 3

АЙТИБАСТИОН



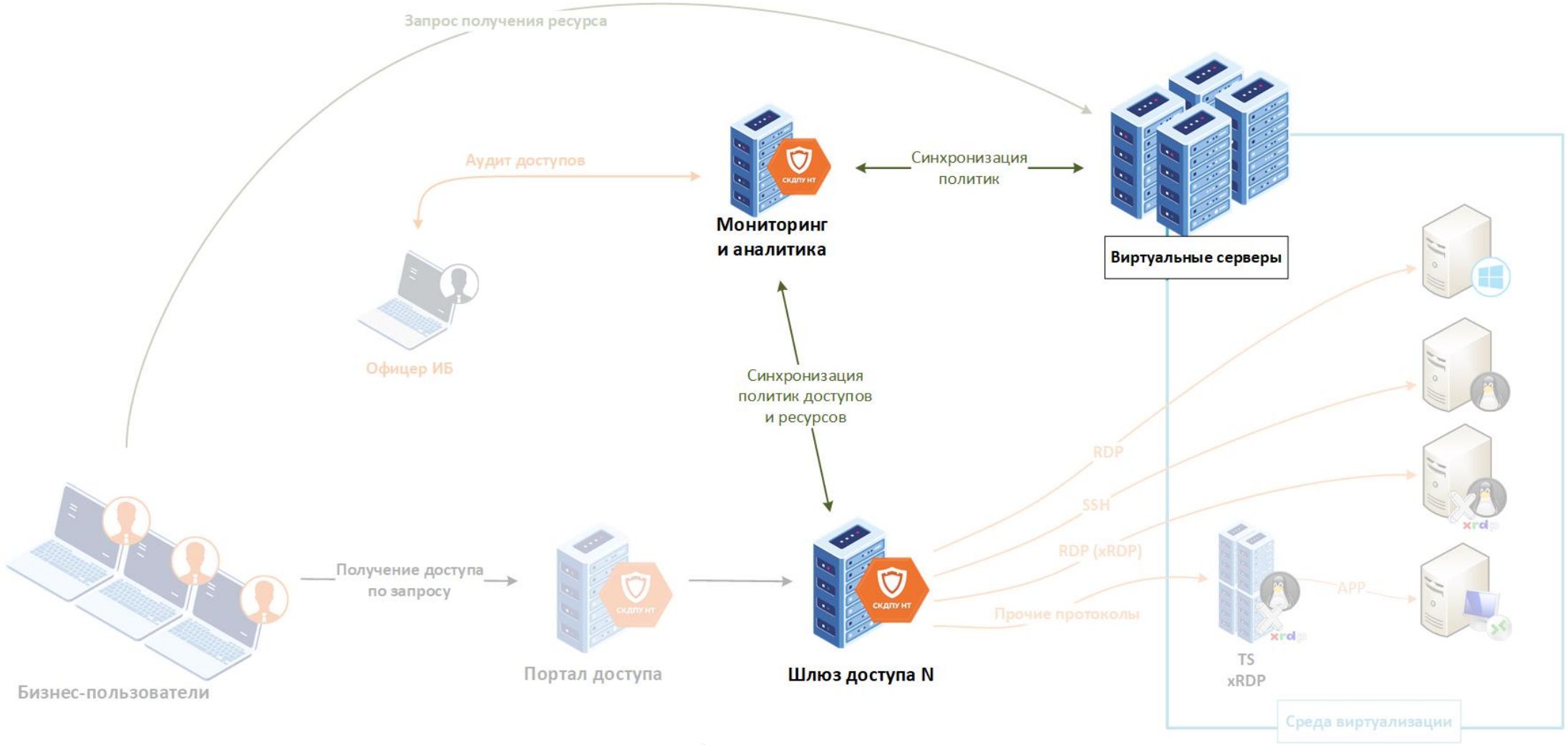
## Синхронизация
# политик доступа

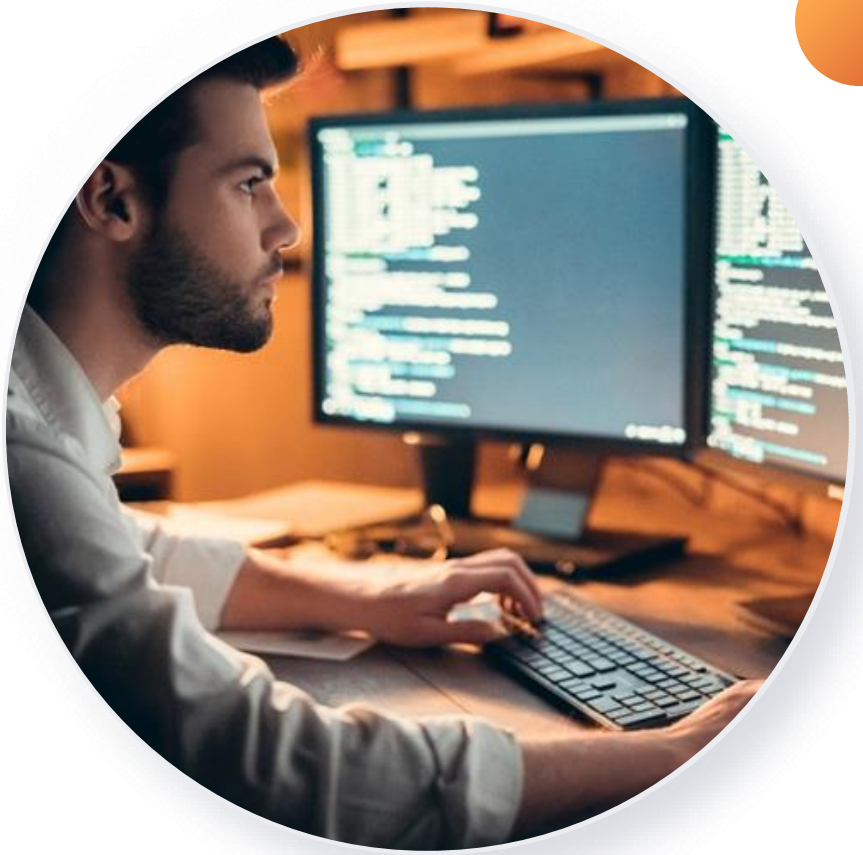
Информация о создаваемых или удаляемых ресурсах автомагически синхронизируется с сервером СКДПУ НТ Шлюз доступа средствами внутренней системы автоматизации политик доступа.

Система обеспечивает функции:

- Чтение актуальных доступных пользователям ресурсов в системе виртуализации.
- Создание пользователей и их групп в PAM-системе.
- Создание ресурсов пользователей в PAM-системе.
- Создание учетных записей для доступа к ресурсам в PAM-системе.

# СХЕМА РЕАЛИЗОВАННОГО ВАРИАНТА 3





# Единый портал доступа к ресурсам

Предоставление доступа к ресурсам пользователя через единый веб-интерфейс Портала доступа.
Все ресурсы, доступные пользователю, предоставляются в виде структурированного списка с возможностью сортировки и группировки.
Портал доступа объединяет доступы пользователя даже в распределенных инфраструктурах Шлюзов доступа.

# БРОКЕР СОЕДИНЕНИЙ К РЕСУРСАМ СКДПУ НТ

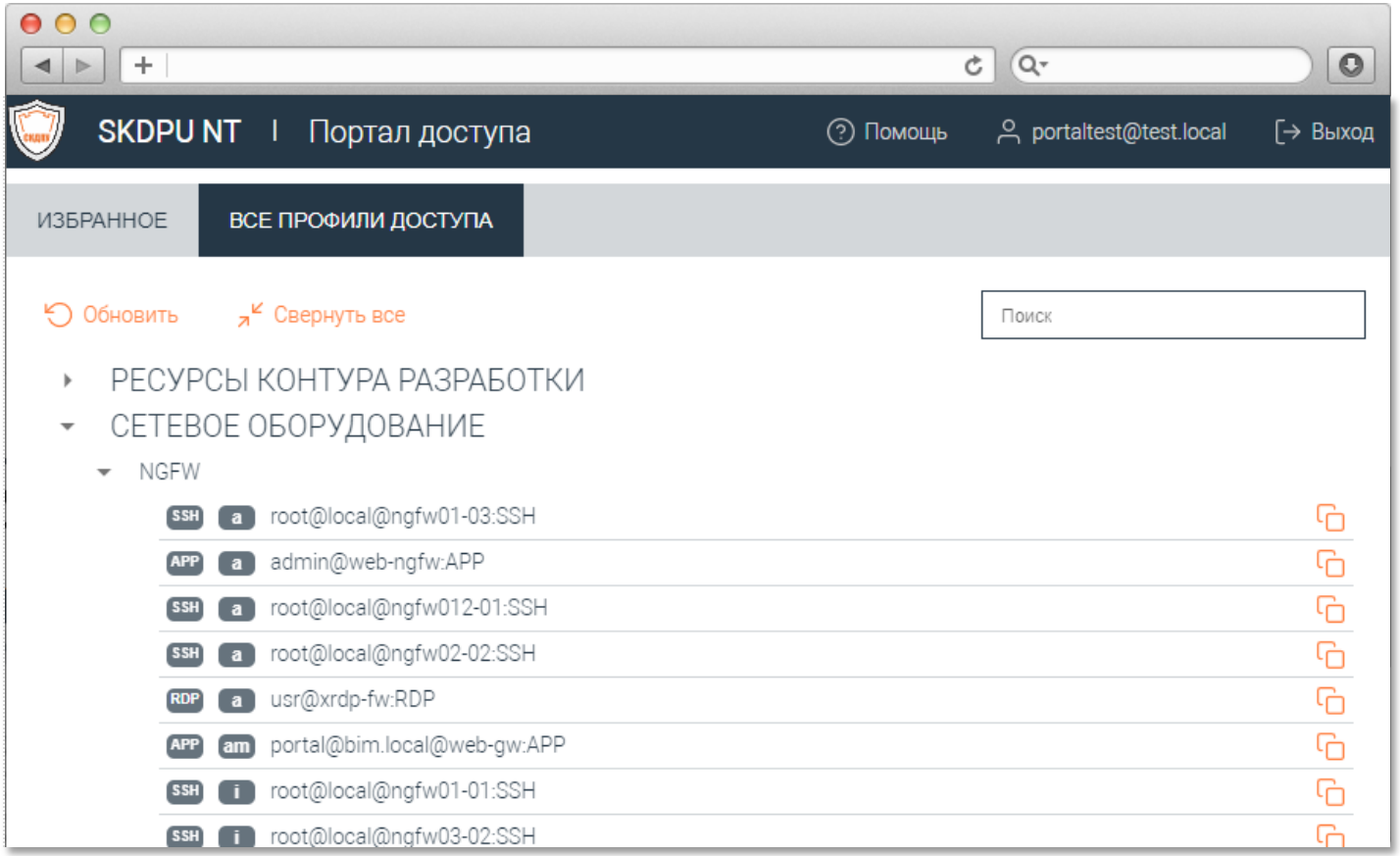
АЙТИБАСТИОН

## Единый доступ

**Единая точка доступа** к инфраструктуре шлюзов доступа и запрашиваемым ресурсам в рамках виртуальной инфраструктуры

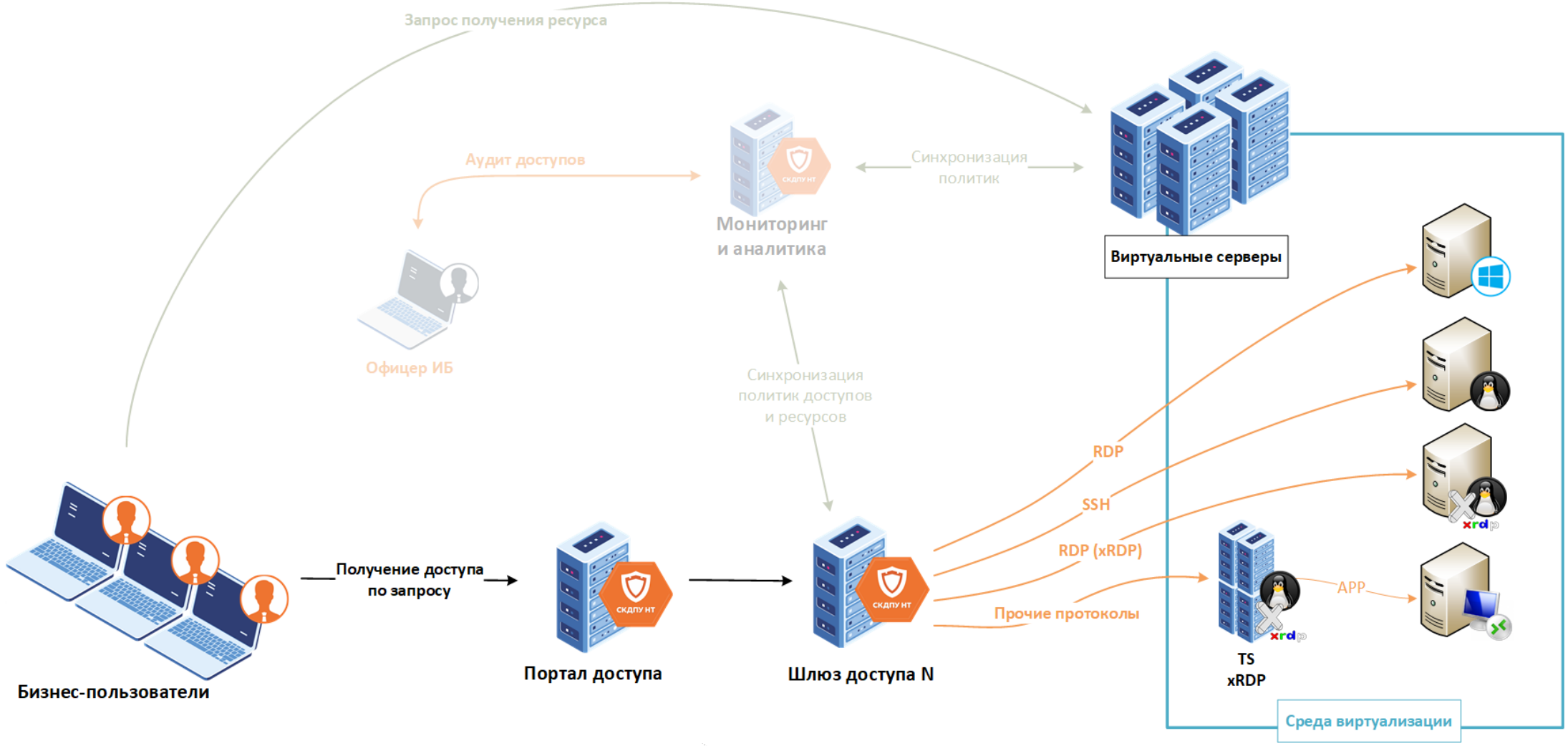
## Единое отображение

Настраиваемая группировка доступов ко всем доступным ресурсам



# СХЕМА РЕАЛИЗОВАННОГО ВАРИАНТА 3

АЙТИБАСТИОН



# СУММАРНЫЙ ЭФФЕКТ
# АВТОМАТИЗАЦИИ И КОНТРОЛЯ ДОСТУПА

АЙТИБАСТИОН

**Пользователи получают оперативный доступ к ресурсам без дополнительных действий** со стороны смежных отделов и в рамках единой системы подтверждения доступа

**Снижается общая стоимость владения виртуальной инфраструктурой с дополнительными средствами контроля доступа** за счет автоматизированного процесса работы систем

**Соблюдаются требуемые регламенты работы служб ИТ и ИБ** в части эффективности, скорости и безопасности работы, **а так же требованиям по импортозамещению ПО**

# УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМ ДОСТУПОМ
## ПЛАТФОРМА СКДПУ НТ

АЙТИБАСТИОН

### 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 метаданных 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

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

# УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМ ДОСТУПОМ
# ПЛАТФОРМА СКДПУ НТ

АЙТИБАСТИОН

## КОНТРОЛЬ ПРИЛОЖЕНИЙ И УЗ В НИХ

Подключение к конечным приложениям без предоставления полного доступа с сокрытием УЗ от приложений

## ПРОСМОТР И ПРЕРЫВАНИЕ СЕССИЙ

Возможность не только контролировать сессию по её результату, но и видеть все действия в режиме реального времени. А в случае необходимости - блокировать сессию пользователя, предотвращая потенциальную угрозу

## РАБОТА ПО ЗАЯВКАМ С ВОЗМОЖНОСТЬЮ ПОДТВЕРЖДЕНИЯ ДОСТУПА

Возможность предоставления доступа по запросу как в момент подключения, так и заранее. Согласование доступа возможно с добавлением одного и более подтверждающих лиц

## КОНТРОЛЬ НА СТОРОНЕ ИС

Блокировка туннелей, доступа вне разрешенных диапазонов, запрет на запуск процессов и т.д.

# УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМ ДОСТУПОМ
# ПЛАТФОРМА СКДПУ НТ

АЙТИБАСТИОН

## ПРОФИЛИРОВАНИЕ И 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 её выдача в виде понятных отчетов от оперативных до сводных, в т.ч. для руководителей.

## ОТКАЗОУСТОЙЧИВОСТЬ И МАСШТАБИРОВНИЕ

Возможность построения действительно отказоустойчивых инсталляций, в т.ч. распределенных между городами и странами. Легкая возможность наращивать мощности как вертикально, так и горизонтально без привязки к территориальному расположению узлов.

АЙТИБАСТИОН

# Спасибо за внимание!

info@it-bastion.com

+7 (499) 322-366-7

it-bastion.com