АЙТИБАСТИОН


www.it-bastion.com

# КОМПАНИЯ
# АЙТИ БАСТИОН

2014

100+

## ОСНОВАНИЕ КОМПАНИИ

Более 9 лет на российском рынке информационной безопасности

www.it-bastion.com

# КОМПАНИЯ
# АЙТИ БАСТИОН

100+

180+

## ПАРТНЕРОВ-ИНТЕГРАТОРОВ

Интеграции с компаниями, позволяющие выполнить квалифицированную помощь в реализации защиты инфраструктуры

www.it-bastion.com

# КОМПАНИЯ
# АЙТИ БАСТИОН

180+

>50%

**ЗАКАЗЧИКОВ И ПРОЕКТОВ**

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

www.it-bastion.com

**КОМПАНИЯ**
**АЙТИ БАСТИОН**

# >50%

## РАМ-РЫНКА РФ

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

www.it-bastion.com

2023

# ЗАМЕТКИ ПО ПРОЕКТАМ

## ВНЕДРЕНИЕ PAM

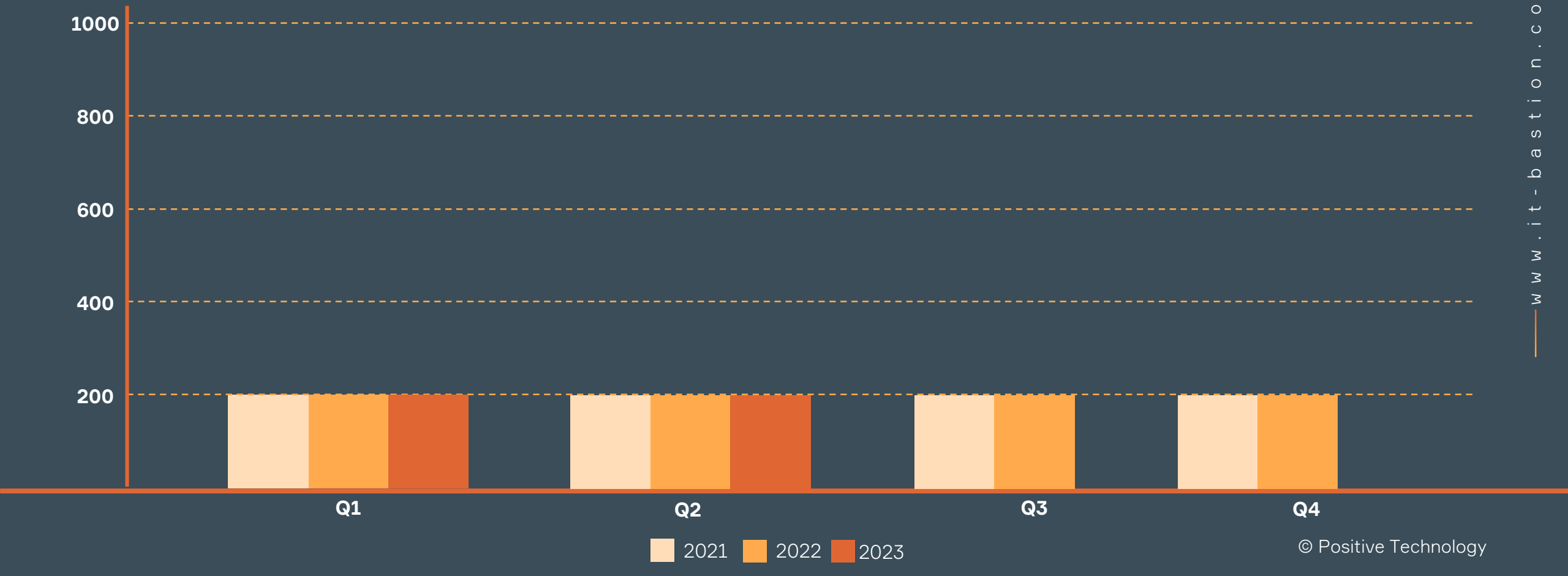
**ШИРИКАЛОВ АЛЕКСЕЙ**
Руководитель группы
Поддержки продаж

www.it-bastion.com

# НЕМНОГО СТАТИСТИКИ
## КОЛ-ВО ИНЦИДЕНТОВ

АЙТИБАСТИОН

- Кол-во инцидентов выросло на 20,8%
- Массовые утечки данных
- В 2023 году тенденция показывает еще большее число атак

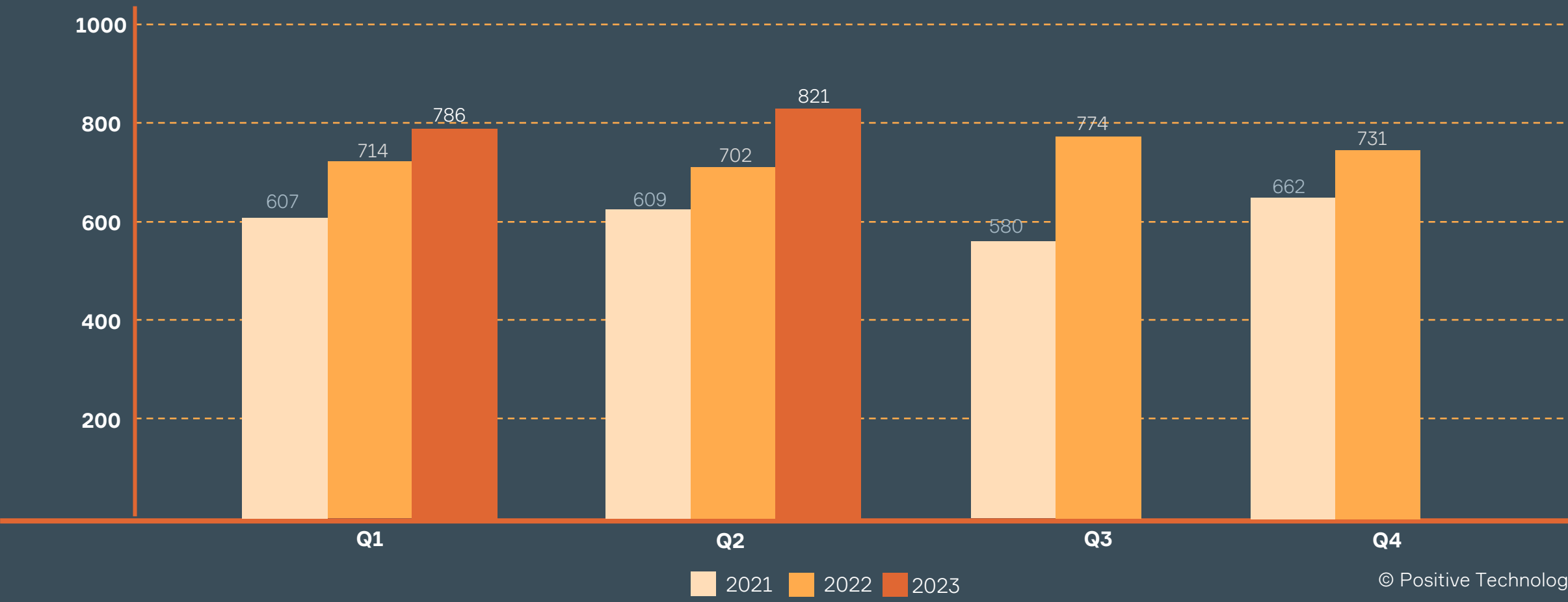



www.it-bastion.com

# НЕМНОГО СТАТИСТИКИ
## КОЛ-ВО ИНЦИДЕНТОВ

АЙТИБАСТИОН

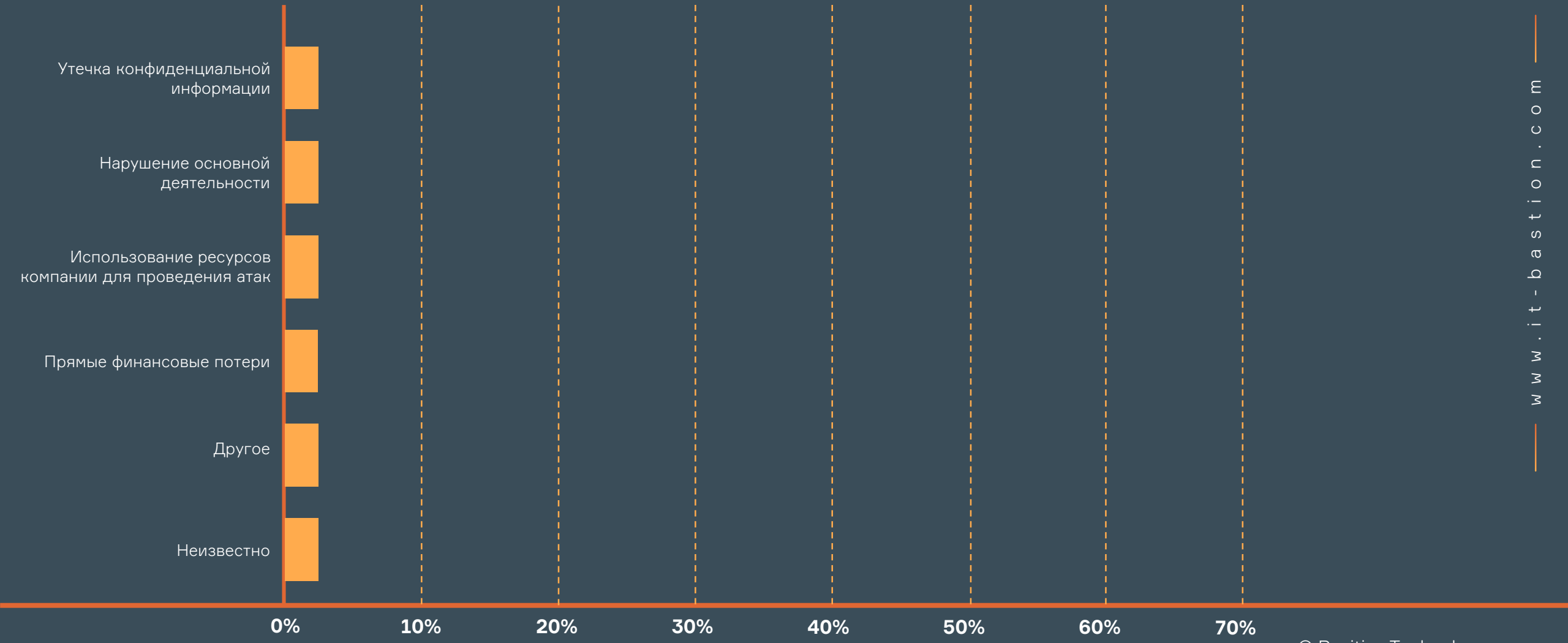
- Кол-во инцидентов выросло на 20,8%
- Массовые утечки данных
- В 2023 году тенденция показывает еще большее число атак




www.it-bastion.com

# НЕМНОГО СТАТИСТИКИ
## ПРОЦЕНТ УСПЕШНЫХ АТАК

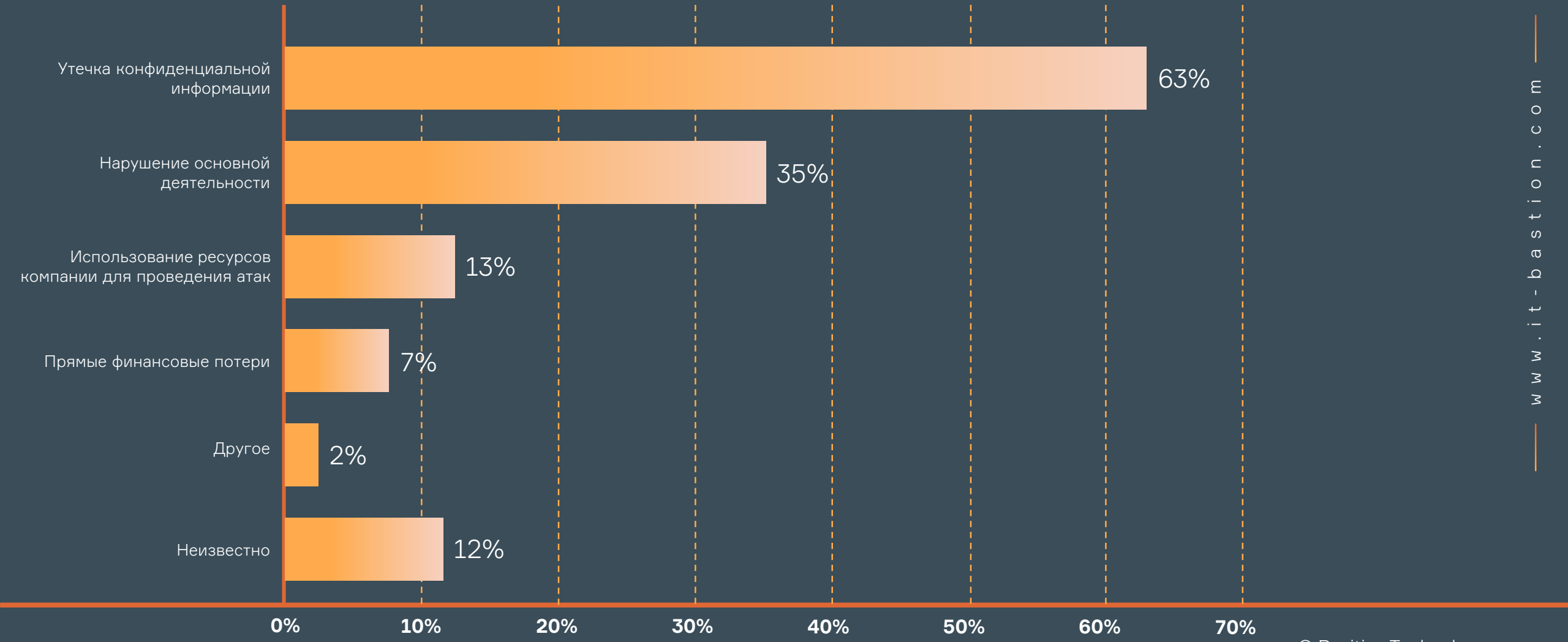
АЙТИБАСТИОН




www.it-bastion.com

# НЕМНОГО СТАТИСТИКИ
# ПРОЦЕНТ УСПЕШНЫХ АТАК

АЙТИБАСТИОН




www.it-bastion.com

# НЕМНОГО СТАТИСТИКИ
## ХАРАКТЕР АТАК

АЙТИБАСТИОН


### ЦЕЛЕНАПРАВЛЕННЫЕ АТАКИ

ПОДБОР ВЕКТОРА АТКИ НА КОНКРЕТНЫЕ ОРГАНИЗАЦИИ ДЛЯ ПОЛУЧЕНИЯ ДАННЫХ ИЛИ НАНЕСЕНИЯ УЩЕРБА ОРГАНИЗАЦИИ


### АТАКИ НАПРАВЛЕННЫХ НА ЧАСТНЫЕ ЛИЦА

ПОЛУЧЕНИЕ ДОСТУПА ЗА СЧЕТ АТАКИ НА ПОЛЬЗОВАТЕЛЯ, ИЗНАЧАЛЬНО ИМЕЮЩЕГО ДОСТУП К АТАКУЕМОЙ ИНФРАСТРУКТУРЕ


### АТАКИ SUPPLY CHAIN

РЕАЛИЗАЦИЯ АТАКИ ЧЕРЕЗ ПОДРЯДЧИКОВ, КОТОРЫЕ ЗАЧАСТУЮ ИМЕЮТ БОЛЕЕ СЛАБУЮ ЗАЩИТУ

www.it-bastion.com

# АСУ ТП


**Idaho National Lab**
**China Energy Engineering Corporation**
**Holding Slovenske elektrarne (HSE)**

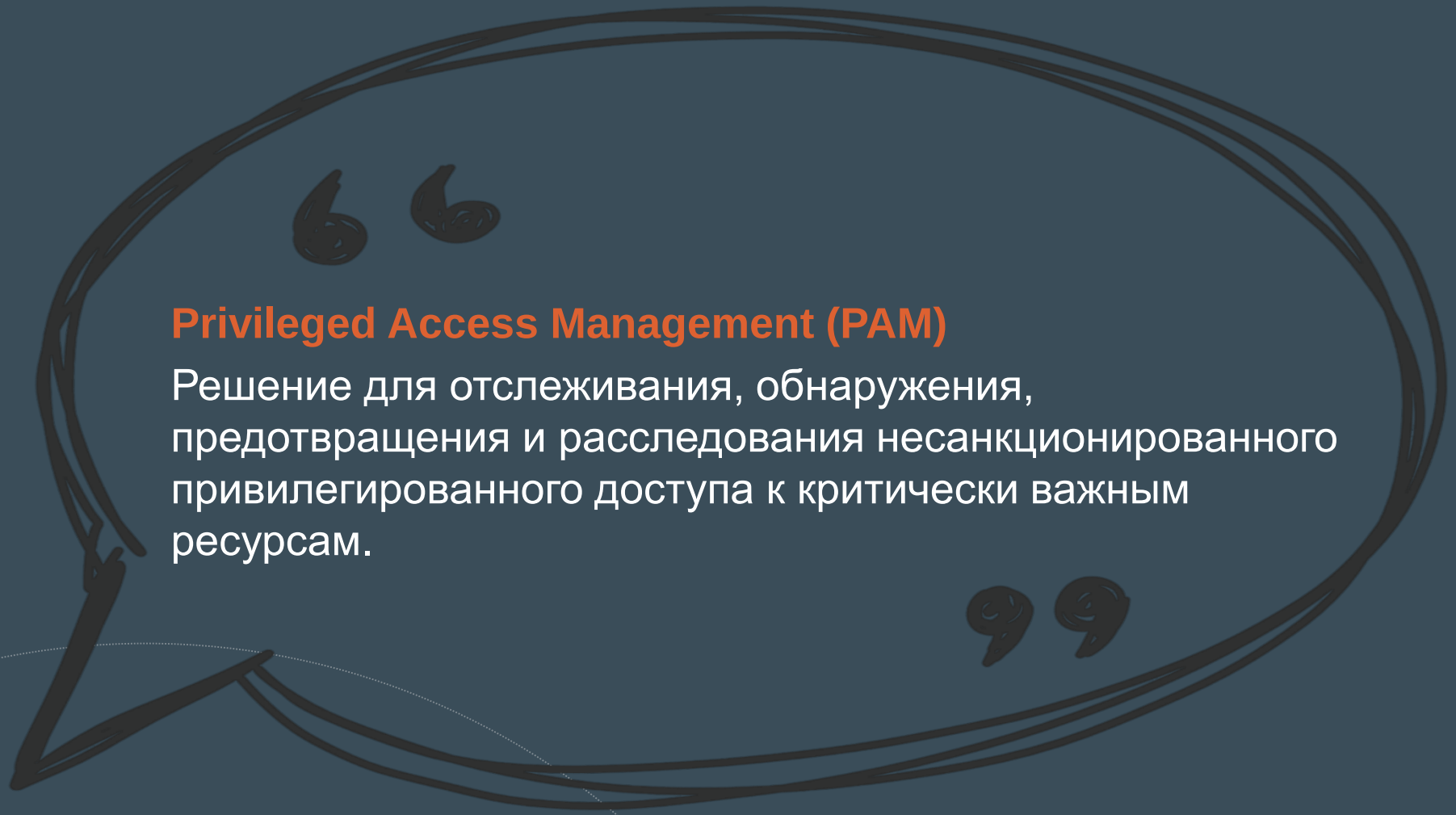
**Проприетарные** протоколы

www.it-bastion.com

АЙТИБАСТИОН

# Для кого открыт доступ?

# PAM



**Privileged Access Management (PAM)**

Решение для отслеживания, обнаружения, предотвращения и расследования несанкционированного привилегированного доступа к критически важным ресурсам.

# КОГО КОНТРОЛИРУЕМ?

- ПОДРЯДЧИКОВ
- СИСТЕМНЫХ АДМИНИСТРАТОРОВ
- ИНЖЕНЕРОВ ВЕНДОРА
- АУДИТОРОВ

www.it-bastion.com

АЙТИБАСТИОН

# НЮАНСЫ ПОСТРОЕНИЯ КОМПЛЕКСНОЙ ЗАЩИТЫ



- УЖЕ ЕСТЬ ОПРЕДЕЛЕННЫЙ ПАРК РЕШЕНИЙ
- НЕ ВСЕ РЕШЕНИЯ МОНОВЕНДОРНЫЕ
- ЗНАЧИТЕЛЬНЫЕ ИЗМЕНЕНИЯ ИНФРАСТРУКТУРЫ
- ИМПОРТОЗАМЕЩЕНИЕ
- ИНТЕГРАЦИИ
- ВЫБОР

АЙТИБАСТИОН

# СКДПУ НТ

## МА

- Центр анализа
- Мониторинг
- Уровень доверия
- Поведенческая модель
- Инцидент
- Отчетность
- Аномалии

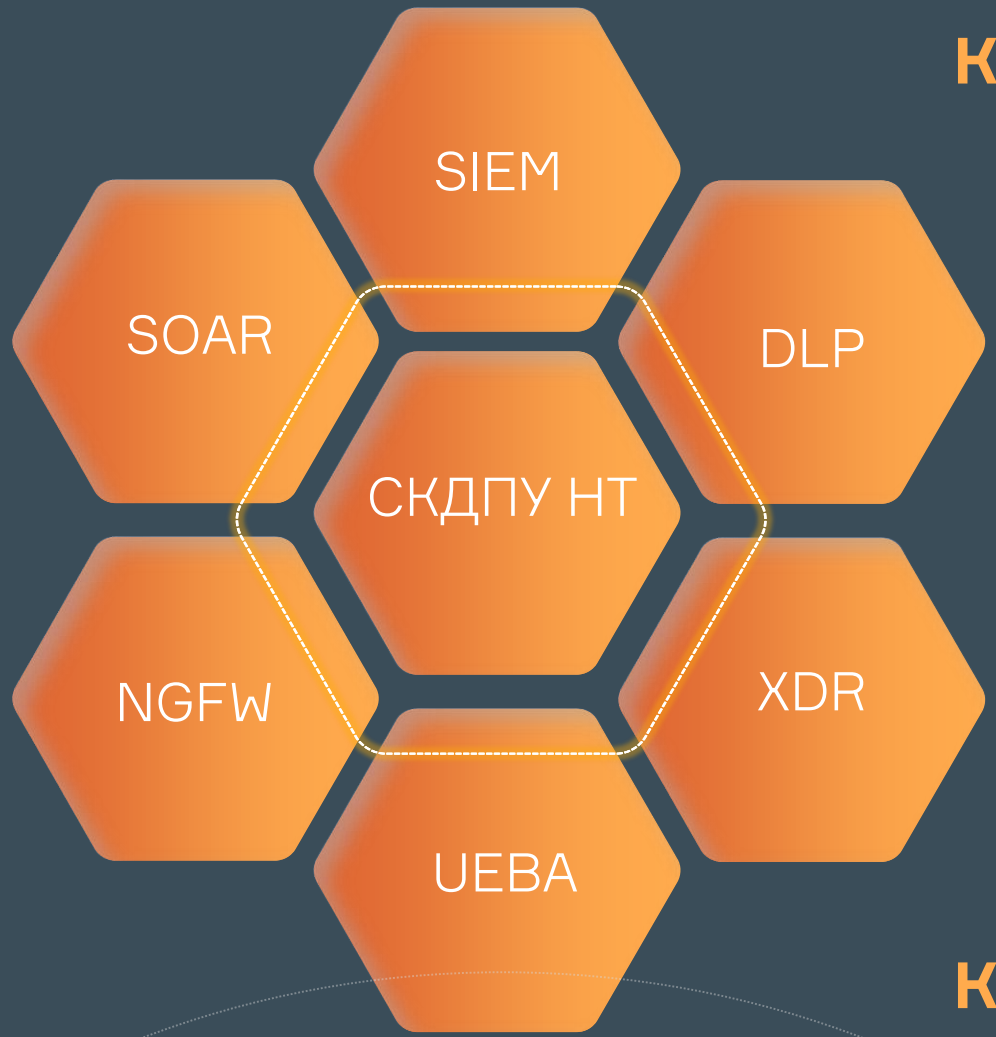
## ШД

- 2FA
- Профилирование
- Логирование
- Менеджер паролей
- Контроль доступа
- Паттерны
- Видеозапись
- Политики доступа

www.it-bastion.com

# СКДПУ НТ
# МУЛЬТИВЕНДОРНОСТЬ

АЙТИБАСТИОН




**Контроль и мониторинг доступа**

**Выявление инцидентов**

**Реагирование на инциденты**

**Кроссвендорная интеграция**

**Контроль доступа к информации**

www.it-bastion.com

# СКДПУ НТ
# ТЕХНОЛОГИЧЕСКИЕ ПАРТНЕРЫ

АЙТИБАСТИОН

ASTRA LINUX®

POSITIVE TECHNOLOGIES

kaspersky

INFOWATCH®

Пассворк

DATALINE

GIS
ГАЗИНФОРМ СЕРВИС

ROSA

CyberLympha®

РУТОКЕН

Аладдин

zVIRT

alt linux

сТерра®

MULTIFACTOR

UserGate

КОД безопасности

Rusiem

РЕДОС

и другие партнеры

www.it-bastion.com

# ПЛАТФОРМЕННОСТЬ

АЙТИБАСТИОН

# СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

АЙТИБАСТИОН

## 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.


## Сертификаты и реестр

Включен в реестр отечественного ПО, Сертификат ФСТЭК УД-4, Сертификат МО РФ НДВ-2

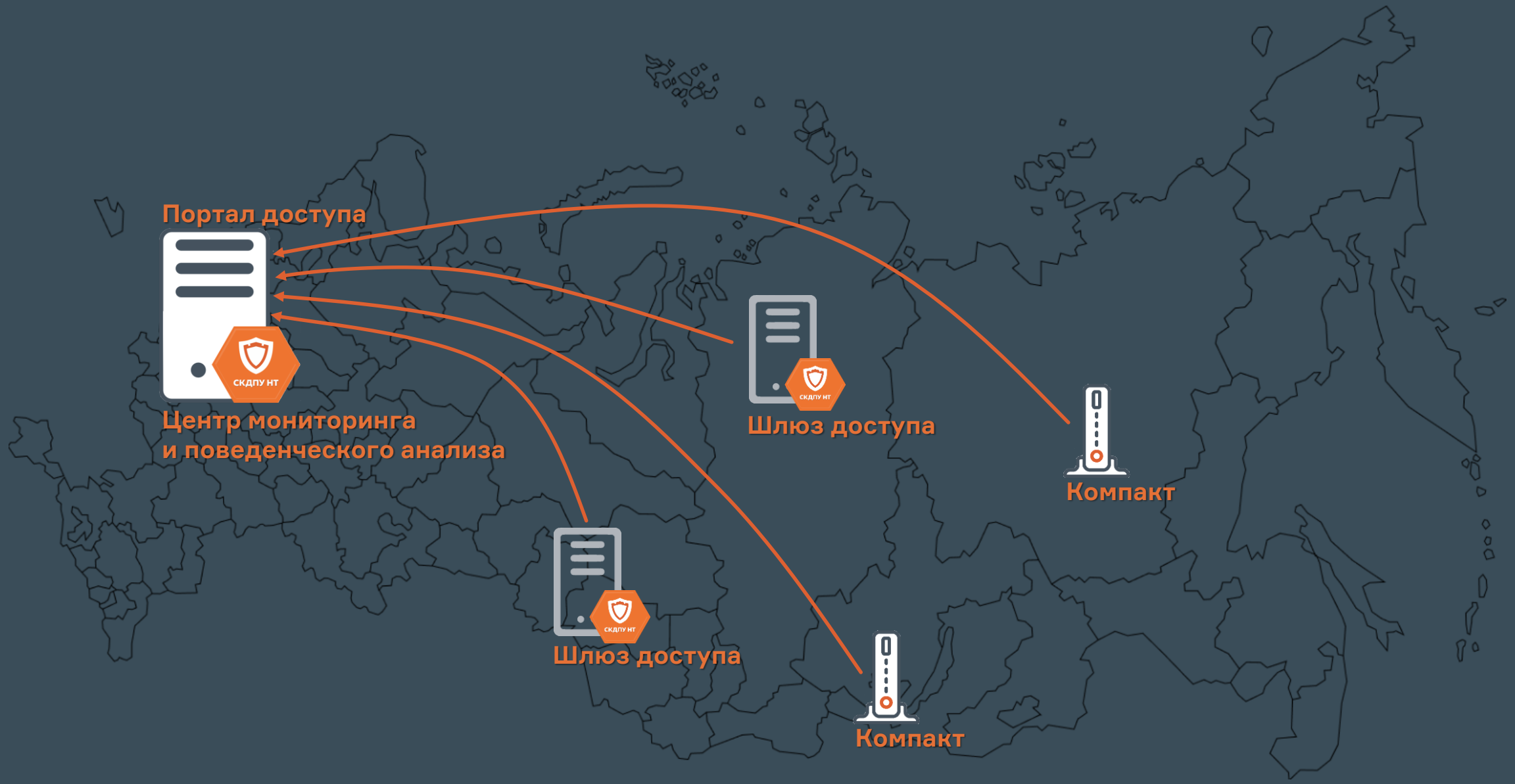
## Целевые и клиентские ОС

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.

www.it-bastion.com


Портал доступа
СКДПУ НТ
Центр мониторинга
и поведенческого анализа
СКДПУ НТ
Шлюз доступа
Компакт
СКДПУ НТ
Шлюз доступа
Компакт

# СКДПУ НТ КОМПАКТ

АЙТИБАСТИОН


- **Функциональность**: Решение обладает полным набором функций контроля действий привилегированных пользователей комплекса СКДПУ НТ.
- **Универсальность**: Система одинаково удобна в использовании как на геораспределенных площадках, так и в инфраструктуре небольших компаний. Размер и объем инфраструктуры для работы ИТ-специалиста значения не имеют.
- **Быстрое развертывание**: СКДПУ Компакт поставляется в виде программно-аппаратного комплекса, устанавливается **не в разрыв сетевого трафика и не требует агентов** на целевых системах. Уже готов к использованию.
- **Входит в состав комплекса**: **Возможность подключения к общему центру мониторинга и аналитики.**

АЙТИБАСТИОН

# КЕЙС 0

Нарушение работы предприятия

АЙТИБАСТИОН

# КЕЙС 1
# 2FA

Утечка информации в крупном промышленном предприятии

# КЕЙС №1
## 2FA

АЙТИБАСТИОН

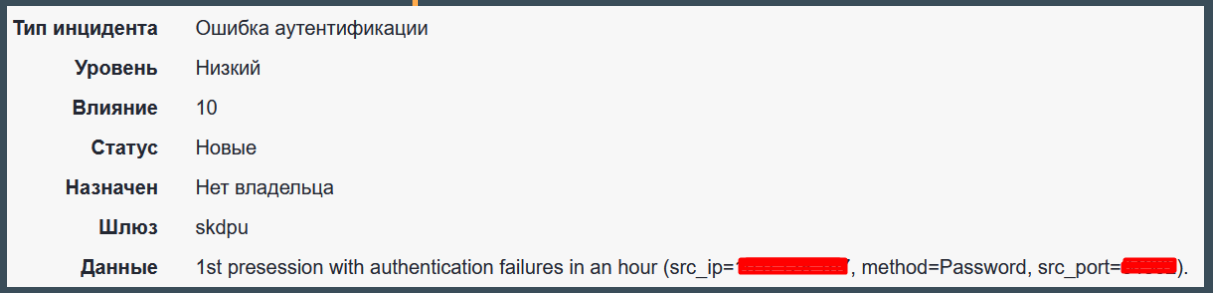
### 2FA СИСТЕМА В КОМПАНИИ
ВСЕ ПОЛЬЗОВАТЕЛИ ИСПОЛЬЗУЮТ МЕТОД ПОДТВЕРЖДЕНИЯ ВХОДА ЧЕРЕЗ PUSH-УВЕДОМЛЕНИЕ

### УДАЛЕННЫЙ ДОСТУП
ВОЗМОЖНОСТЬ ПОДКЛЮЧЕНИЯ В ИНФРАСТРУКТУРУ

### ДОМЕННЫЕ УЗ
ИСПОЛЬЗОВАНИЕ ДОМЕННЫХ УЗ ДЛЯ ДОСТУПА К БОЛЬШИНСТВУ ОБЪЕКТОВ

## ОШИБКИ АВТОРИЗАЦИИ

НЕСКОЛЬКО НЕУДАЧНЫХ ПОПЫТОК АВТОРИЗАЦИИ



| | |
|---|---|
| **Тип инцидента** | Ошибка аутентификации |
| **Уровень** | Низкий |
| **Влияние** | 10 |
| **Статус** | Новые |
| **Назначен** | Нет владельца |
| **Шлюз** | skdpu |
| **Данные** | 1st presession with authentication failures in an hour (src_ip=[redacted], method=Password, src_port=[redacted]). |

## НЕТИПИЧНОЕ МЕСТО

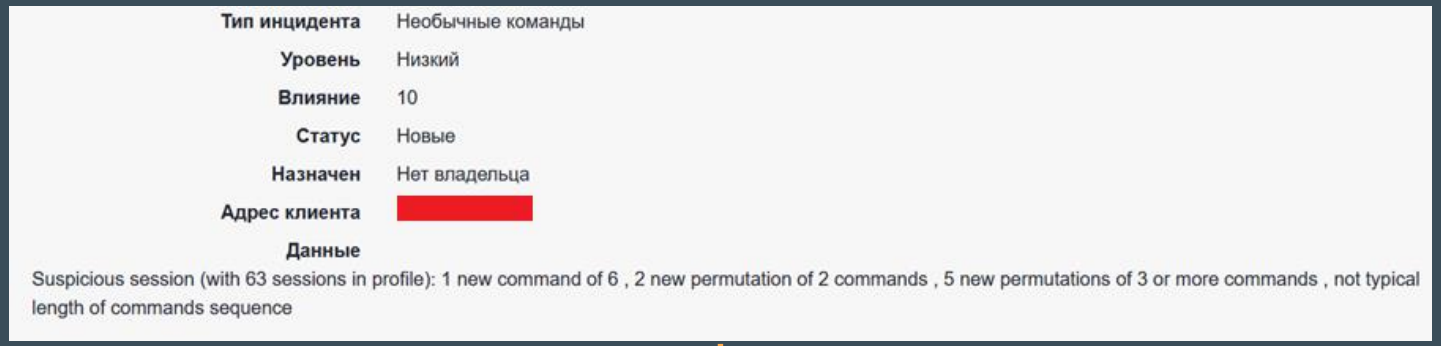
ИСПОЛЬЗОВАНИЕ ДЛЯ ПОДКЛЮЧЕНИЯ НЕСТАНДАРТНЫХ IP

## НЕТИПИЧНОЕ ВРЕМЯ

ПОЛЬЗОВАТЕЛЬ ПОДКЛЮЧАЕТСЯ В НЕ РАБОЧЕЕ ВРЕМЯ

## НЕТИПИЧНЫЙ ДОСТУП

ПОЛЬЗВОАТЕЛЬ ПЫТАЕТСЯ ПОДКЛЮЧИТЬСЯ К БОЛЬШОМУ КОЛИЧЕСТВУ УСТРОЙСТВ, НЕКТОРЫЕ ИЗ ПОДКЛЮЧЕНИ ТРЕБУЮТ ПОЛУЧЕНИЯ ДОПОЛНИТЕЛЬНОГО РАЗРЕШЕНИЯ

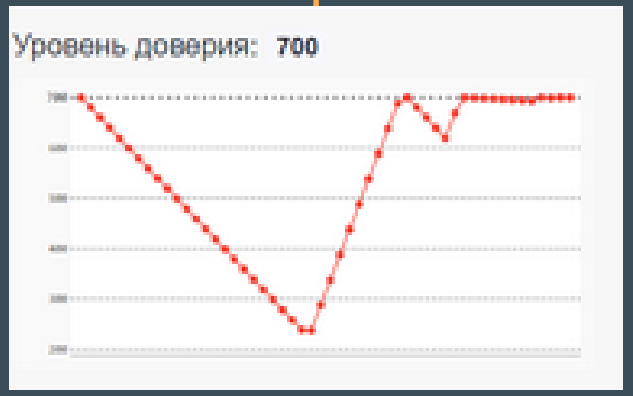



## ПОДОЗРИТЕЛЬНЫЕ КОМАНДЫ

ВЫПОЛНЕНИЕ ПОЛЬЗОВАТЕЛЕМ КОМАНД, КОТОРЫЕ ОТЛИЧАЮТСЯ ОТ ПРИВЫЧНЫХ

## ПАДЕНИЕ УРОВНЯ ДОВЕРИЯ

РЕЗКОЕ УМЕНЬШЕНИЕ УРОВНЯ ДОВЕРИЯ (УРОВЕНЬ – ДЕМОНСТРИРУЮЩИЙ КОРРЕКТНОСТЬ РАБОТЫ ПОЛЬЗОВАТЕЛЯ)




## БЛОКИРОВКА УЗ

ПРЕДОТВРАЩЕНИЕ ДОСТУПА В ИНФРАСТРУКТУРУ

# ИТОГ

НЕОБХОДИМО КОМПЛЕКСНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

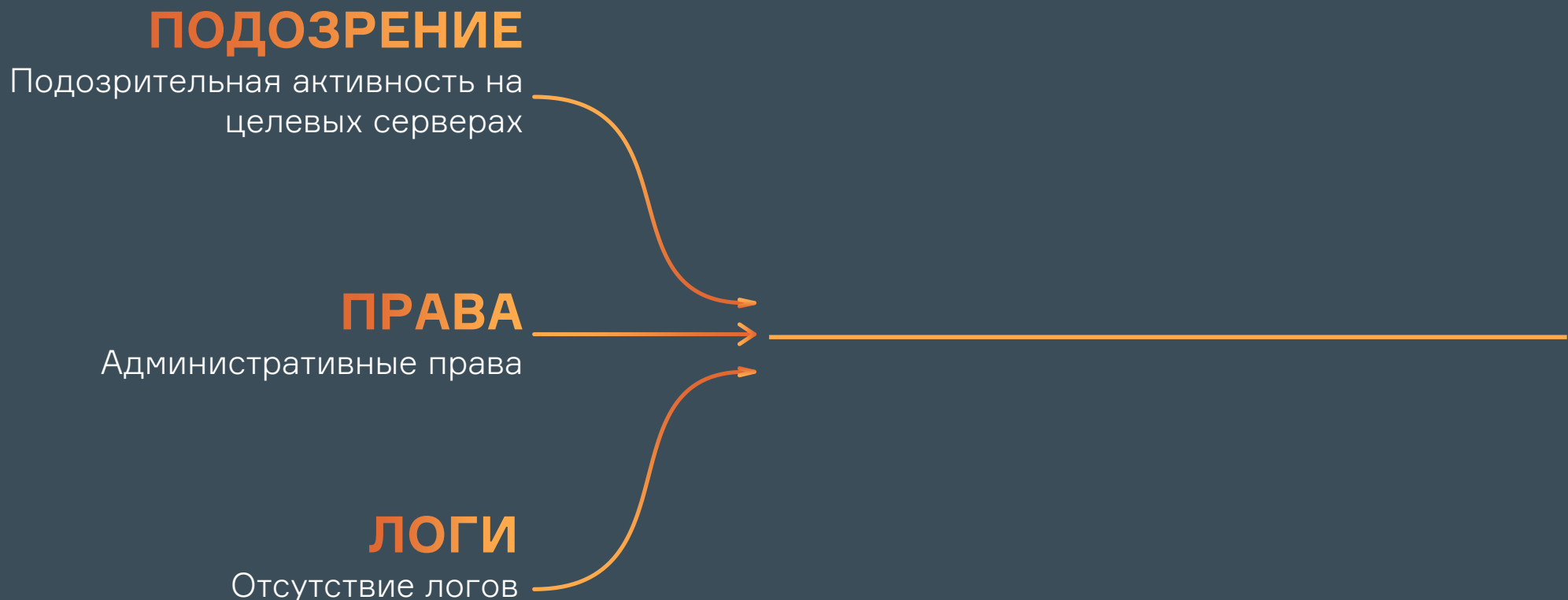
АЙТИБАСТИОН

# КЕЙС 2
# BACKDOOR

Определение и нейтрализация
несанкционированного доступа

# КЕЙС №2
# BACKDOOR

АЙТИБАСТИОН



# АНАЛИЗ СЕССИЙ

Поиск сессий с использованием команд создания новых пользователей

```
[root@rosaosch ~]# adduser test4
[root@rosaosch ~]# passwd test4
Изменяется пароль пользователя test4.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - основан на слове из словаря
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@rosaosch ~]# visudo



"/etc/sudoers.tmp" 120L, 4328C
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
```

| | | |
|---|---|---|
| 09-08-2023 17:10:25 | SESSION_ESTABLISHED_SUCCESSFULLY | |
| 09-08-2023 17:10:45 | KBD_INPUT | adduser testuser |
| 09-08-2023 17:10:52 | KBD_INPUT | passwd testuser |
| 09-08-2023 17:10:52 | KILL_PATTERN_DETECTED | **pattern:** passwd |

| | | |
|---|---|---|
| 09-08-2023 17:21:40 | SESSION_ESTABLISHED_SUCCESSFULLY | |
| 09-08-2023 17:21:52 | KBD_INPUT | adduser test4 |
| 09-08-2023 17:21:56 | KBD_INPUT | passwd test4 |
| 09-08-2023 17:22:07 | KBD_INPUT | visudo |

# ВЫЯВЛЕНИЕ НАРУШИТЕЛЕЙ

Фиксирование сессии с успешно отработанной командой

# АНАЛИЗ СЕССИЙ

Поиск сессий с использованием команд создания новых пользователей

| | | |
|---|---|---|
| 09-08-2023 17:10:25 | SESSION_ESTABLISHED_SUCCESSFULLY | |
| 09-08-2023 17:10:45 | KBD_INPUT | adduser testuser |
| 09-08-2023 17:10:52 | KBD_INPUT | passwd testuser |
| 09-08-2023 17:10:52 | KILL_PATTERN_DETECTED | **pattern:** passwd |

| | | |
|---|---|---|
| 09-08-2023 17:21:40 | SESSION_ESTABLISHED_SUCCESSFULLY | |
| 09-08-2023 17:21:52 | KBD_INPUT | adduser test4 |
| 09-08-2023 17:21:56 | KBD_INPUT | passwd test4 |
| 09-08-2023 17:22:07 | KBD_INPUT | visudo |

# АНАЛИЗ СЕССИЙ

Поиск сессий с использованием команд создания новых пользователей

```
[root@rosaosch ~]# adduser test4
[root@rosaosch ~]# passwd test4
Изменяется пароль пользователя test4.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - основан на слове из словаря
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@rosaosch ~]# visudo



"/etc/sudoers.tmp" 120L, 4328C
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
```

| | | |
|---|---|---|
| 09-08-2023 17:10:25 | SESSION_ESTABLISHED_SUCCESSFULLY | |
| 09-08-2023 17:10:45 | KBD_INPUT | adduser testuser |
| 09-08-2023 17:10:52 | KBD_INPUT | passwd testuser |
| 09-08-2023 17:10:52 | KILL_PATTERN_DETECTED | **pattern:** passwd |

| | | |
|---|---|---|
| 09-08-2023 17:21:40 | SESSION_ESTABLISHED_SUCCESSFULLY | |
| 09-08-2023 17:21:52 | KBD_INPUT | adduser test4 |
| 09-08-2023 17:21:56 | KBD_INPUT | passwd test4 |
| 09-08-2023 17:22:07 | KBD_INPUT | visudo |

# ВЫЯВЛЕНИЕ НАРУШИТЕЛЕЙ

Фиксирование сессии с успешно отработанной командой

```
[root@rosaosch ~]# adduser test4
[root@rosaosch ~]# passwd test4
Изменяется пароль пользователя test4.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - основан на слове из словаря
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@rosaosch ~]# visudo



"/etc/sudoers.tmp" 120L, 4328C
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
```

## ВЫЯВЛЕНИЕ НАРУШИТЕЛЕЙ

Фиксирование сессии с успешно отработанной командой

# АНАЛИЗ СЕССИЙ

Поиск сессий с использованием команд создания новых пользователей

```
[root@rosaosch ~]# adduser test4
[root@rosaosch ~]# passwd test4
Изменяется пароль пользователя test4.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - основан на слове из словаря
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@rosaosch ~]# visudo



"/etc/sudoers.tmp" 120L, 4328C
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
```

| | | |
|---|---|---|
| 09-08-2023 17:10:25 | SESSION_ESTABLISHED_SUCCESSFULLY | |
| 09-08-2023 17:10:45 | KBD_INPUT | adduser testuser |
| 09-08-2023 17:10:52 | KBD_INPUT | passwd testuser |
| 09-08-2023 17:10:52 | KILL_PATTERN_DETECTED | **pattern:** passwd |

| | | |
|---|---|---|
| 09-08-2023 17:21:40 | SESSION_ESTABLISHED_SUCCESSFULLY | |
| 09-08-2023 17:21:52 | KBD_INPUT | adduser test4 |
| 09-08-2023 17:21:56 | KBD_INPUT | passwd test4 |
| 09-08-2023 17:22:07 | KBD_INPUT | visudo |

# ВЫЯВЛЕНИЕ НАРУШИТЕЛЕЙ

Фиксирование сессии с успешно отработанной командой

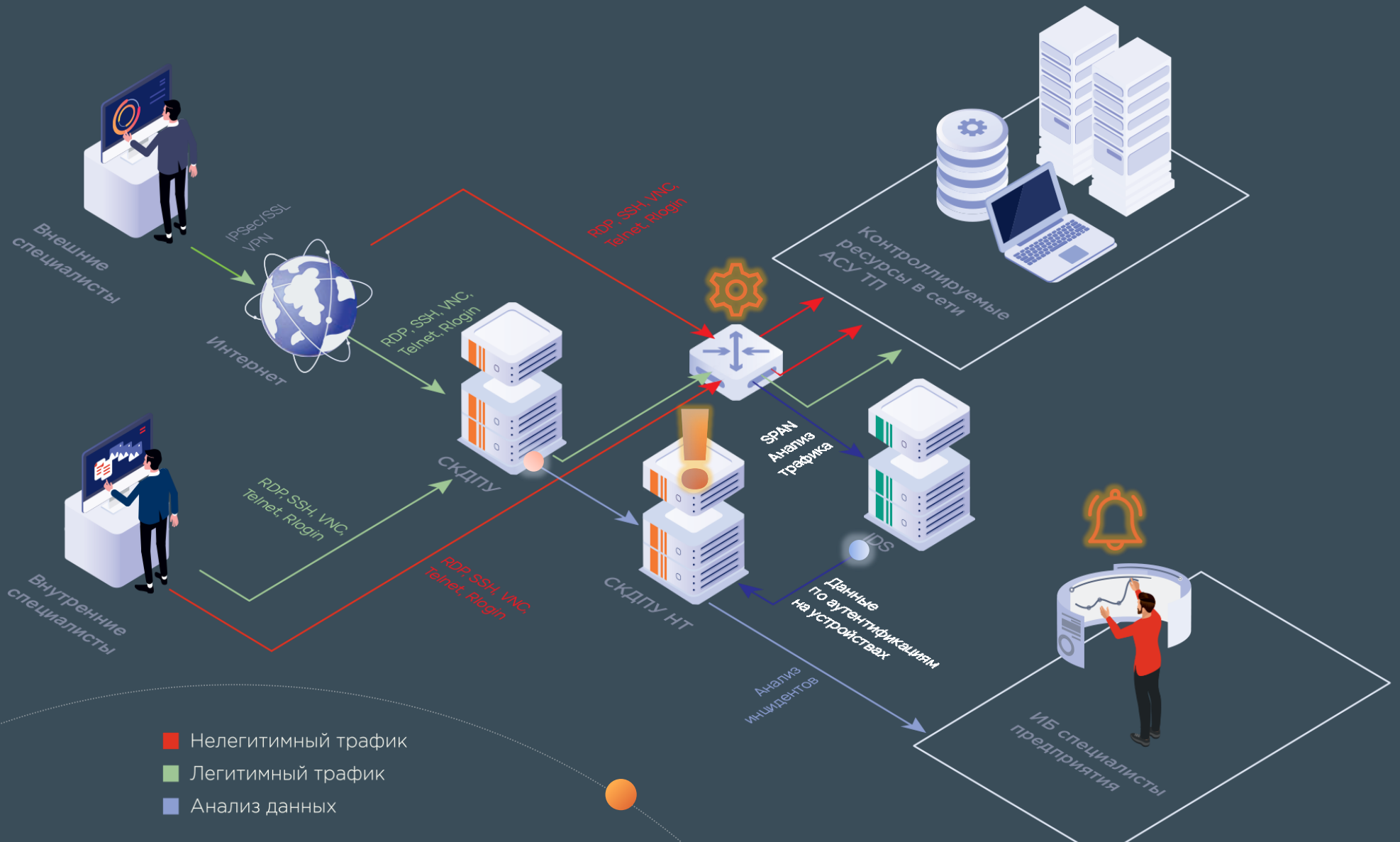
# ИТОГ

ЛЮБОЙ СЦЕНАРИЙ РЕАЛИЗУЕМ ПРИ НАЛИЧИИ ВОЗМОЖНОСТИ

# КАК НЕ ДОПУСТИТЬ ТАКОГО СЦЕНАРИЯ?

# КЕЙС №2
# BACKDOOR *(как не допустить)*

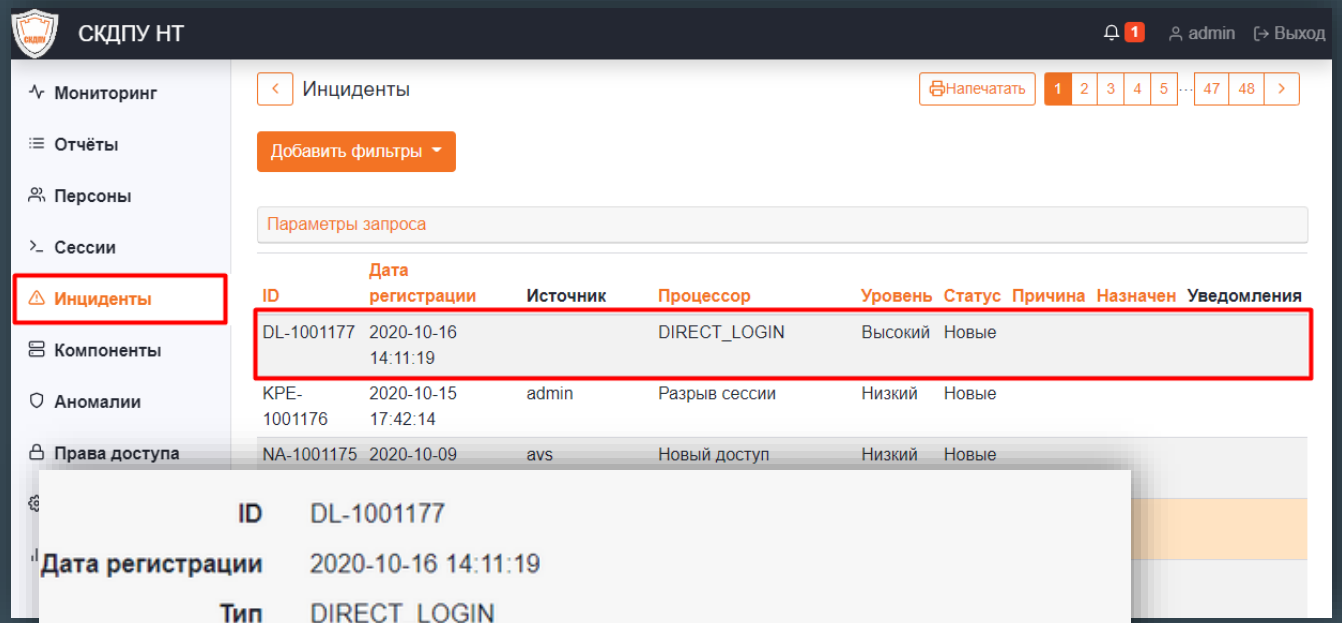
АЙТИБАСТИОН

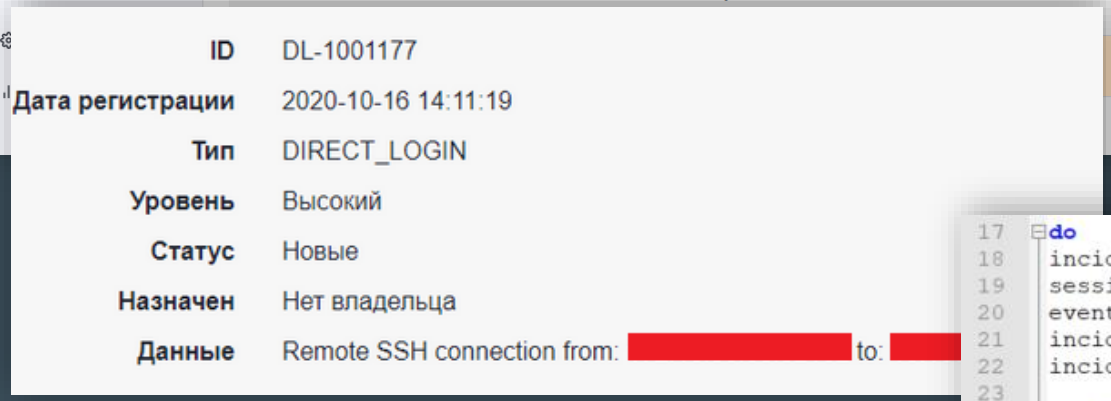



www.it-bastion.com

# КЕЙС №2
# BACKDOOR *(как не допустить)*

АЙТИБАСТИОН




```
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
```

## АВТОМАТИЗАЦИЯ

Возможность автоматизации реагирования на инциденты безопасности

www.it-bastion.com

АЙТИБАСТИОН

# КЕЙС 3
# ВРЕМЯ - ДЕНЬГИ

Как сохранить деньги при привлечении подрядчиков

# КЕЙС №3
# ВРЕМЯ ДЕНЬГИ

АЙТИБАСТИОН

## ДОП. СОГЛАШЕНИЕ

Заказчик запросил дополнительное соглашение, за дополнительную оплату из-за сложности проводимых работ

## РЕАЛЬНОЕ ВРЕМЯ

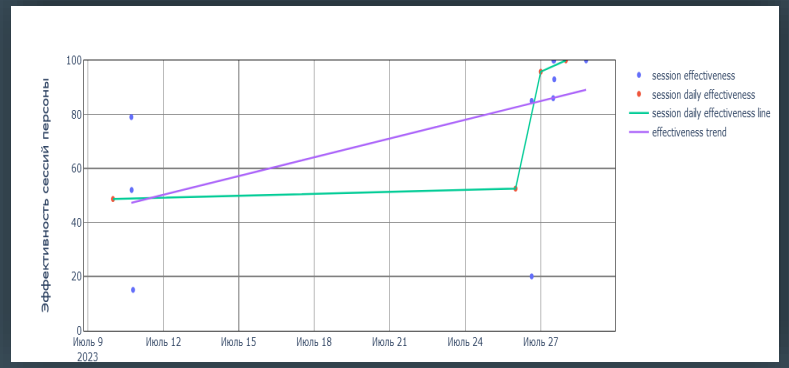
Какое реальное время работы подрядчика?

## ОБЪЕМ ВЫПОЛНЕННЫХ РАБОТ

Какой объем выполненных работ?

## ГРАФИК ЭФФЕКТИВНОСТИ

Позволил оценить общую эффективность работ на протяжении времени



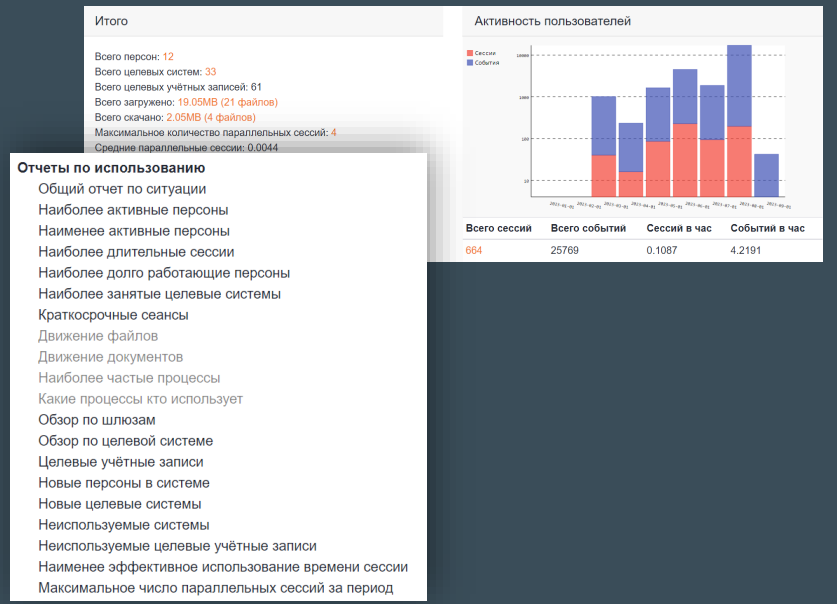

| | |
|---|---|
| **Тип инцидента** | Наименее эффективное использование времени сессии |
| **Уровень** | Низкий |
| **Влияние** | 10 |
| **Статус** | Новые |
| **Назначен** | Нет владельца |
| **Данные** | effectiveness decreased drastically: 41 % in 8 days |

## ИНЦИДЕНТЫ

Позволили своевременно зафиксировать простои в работе

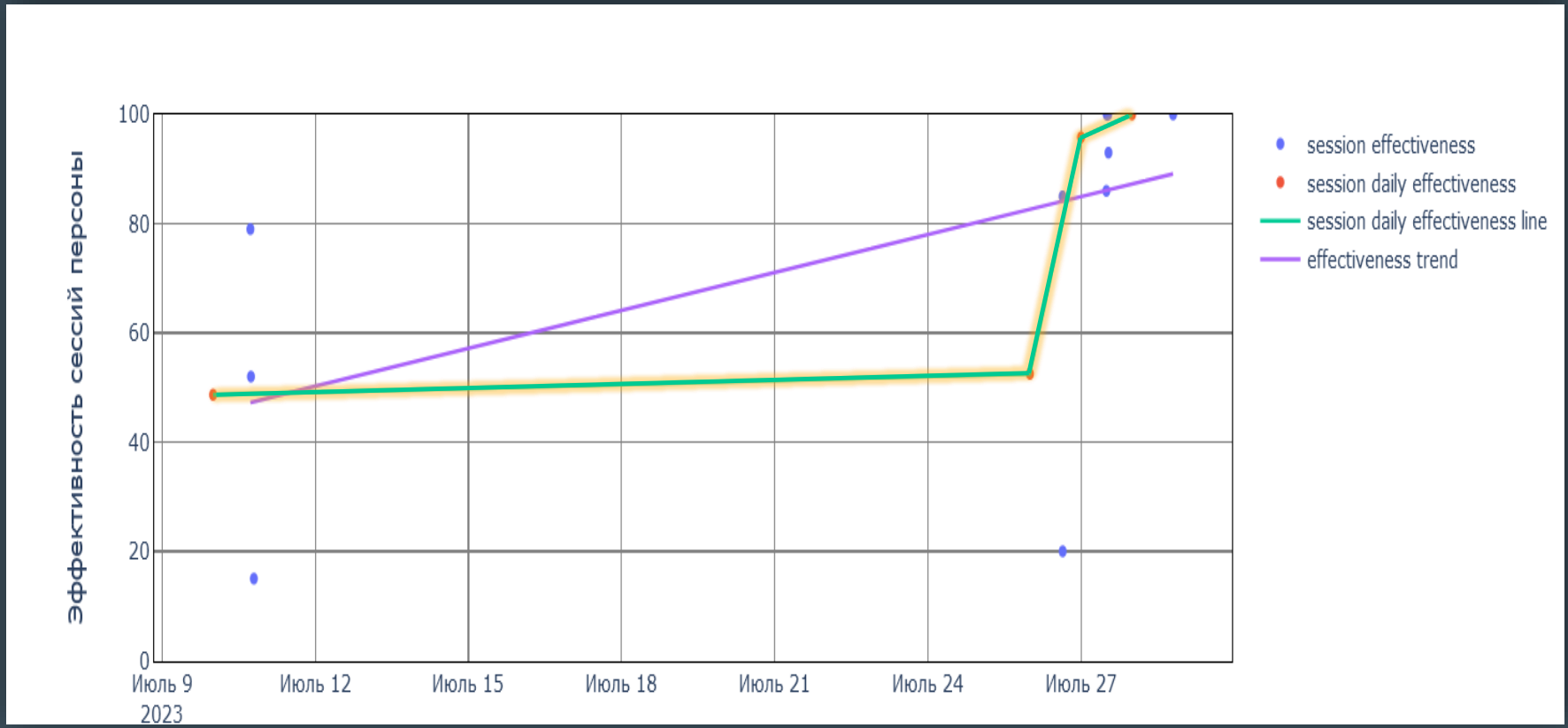
## ОТЧЕТЫ

Позволил оценить общую эффективность работ на протяжении времени



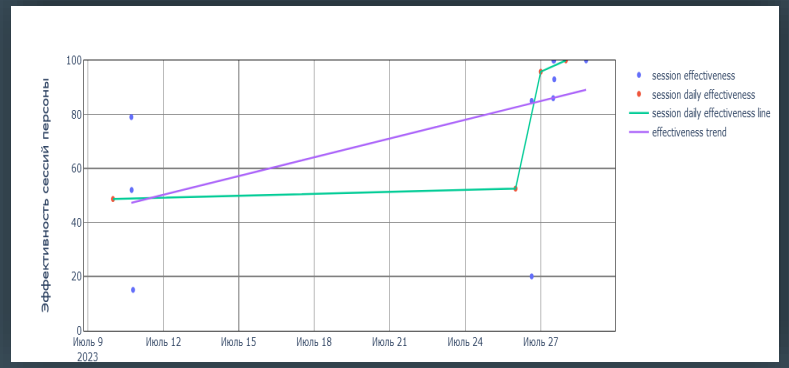
# ГРАФИК ЭФФЕКТИВНОСТИ

Позволил оценить общую эффективность работ на протяжении времени



## ГРАФИК ЭФФЕКТИВНОСТИ

Позволил оценить общую эффективность работ на протяжении времени



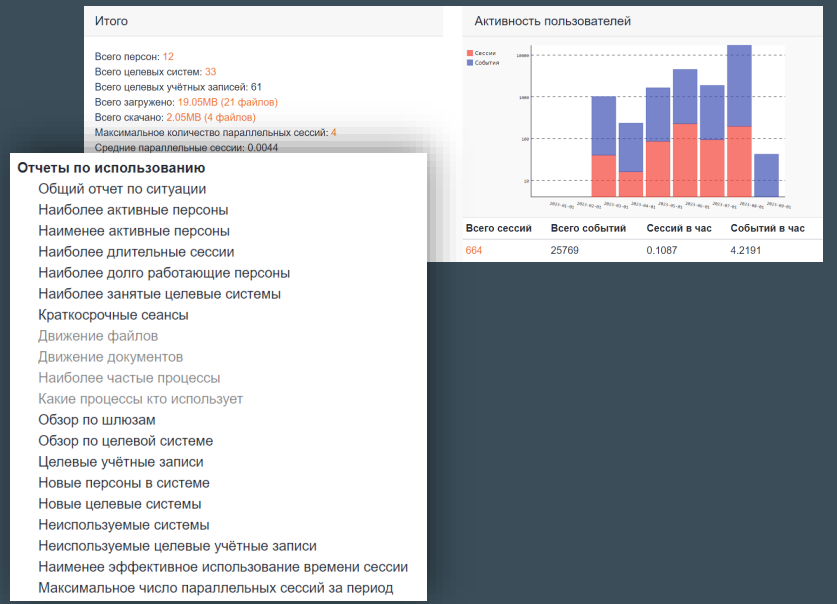

| | |
|---|---|
| **Тип инцидента** | Наименее эффективное использование времени сессии |
| **Уровень** | Низкий |
| **Влияние** | 10 |
| **Статус** | Новые |
| **Назначен** | Нет владельца |
| **Данные** | effectiveness decreased drastically: 41 % in 8 days |

## ИНЦИДЕНТЫ

Позволили своевременно зафиксировать простои в работе

## ОТЧЕТЫ

Позволил оценить общую эффективность работ на протяжении времени



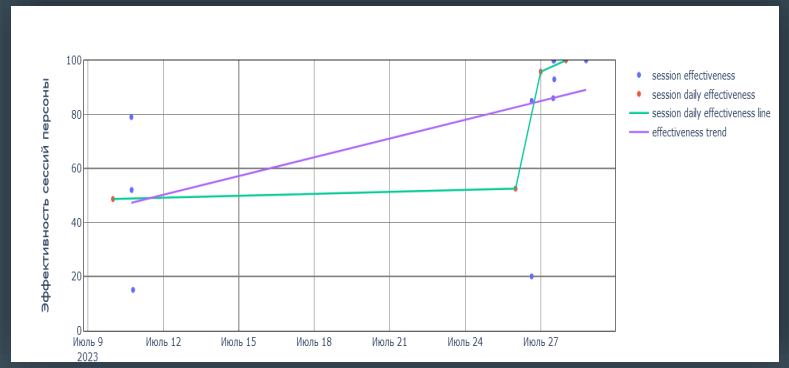
| | |
|---|---|
| **Тип инцидента** | Наименее эффективное использование времени сессии |
| **Уровень** | Низкий |
| **Влияние** | 10 |
| **Статус** | Новые |
| **Назначен** | Нет владельца |
| **Данные** | effectiveness decreased drastically: 41 % in 8 days |

## ИНЦИДЕНТЫ

Позволили своевременно зафиксировать простои в работе

## ГРАФИК ЭФФЕКТИВНОСТИ

Позволил оценить общую эффективность работ на протяжении времени



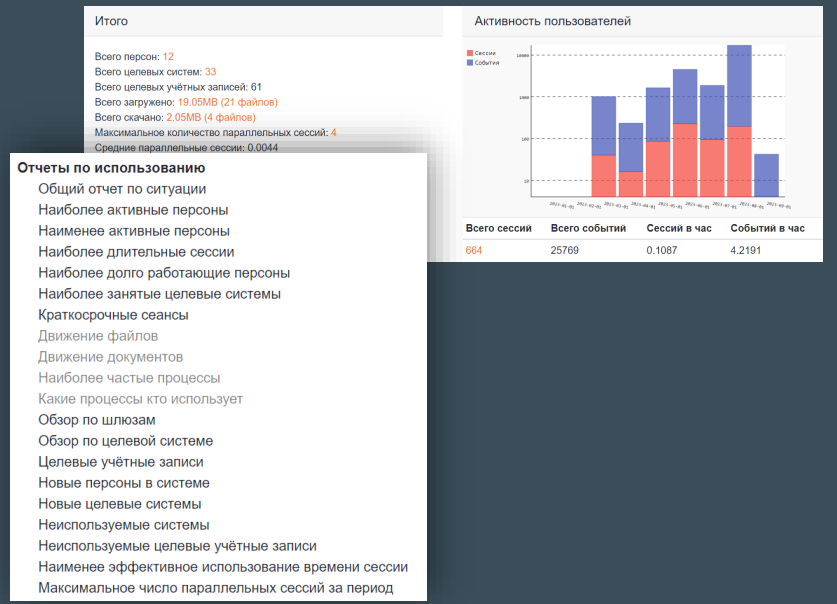

| | |
|---|---|
| **Тип инцидента** | Наименее эффективное использование времени сессии |
| **Уровень** | Низкий |
| **Влияние** | 10 |
| **Статус** | Новые |
| **Назначен** | Нет владельца |
| **Данные** | effectiveness decreased drastically: 41 % in 8 days |

## ИНЦИДЕНТЫ

Позволили своевременно зафиксировать простои в работе

## ОТЧЕТЫ

Позволил оценить общую эффективность работ на протяжении времени



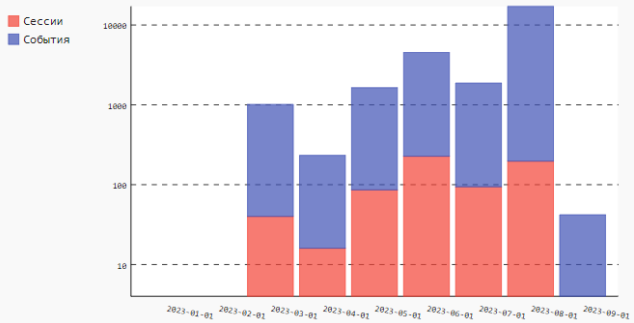
# ОТЧЕТЫ

Позволил оценить общую эффективность работ на протяжении времени

## Итого

Всего персон: 12
Всего целевых систем: 33
Всего целевых учётных записей: 61
Всего загружено: 19.05MB (21 файлов)
Всего скачано: 2.05MB (4 файлов)
Максимальное количество параллельных сессий: 4
Средние параллельные сессии: 0.0044

## Активность пользователей



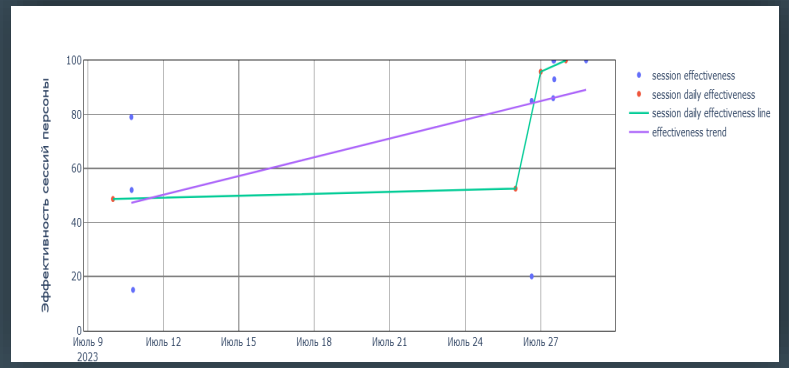

| Всего сессий | Всего событий | Сессий в час | Событий в час |
|---|---|---|---|
| 664 | 25769 | 0.1087 | 4.2191 |

**Отчеты по использованию**

- Общий отчет по ситуации
- Наиболее активные персоны
- Наименее активные персоны
- Наиболее длительные сессии
- Наиболее долго работающие персоны
- Наиболее занятые целевые системы
- Краткосрочные сеансы
- Движение файлов
- Движение документов
- Наиболее частые процессы
- Какие процессы кто использует
- Обзор по шлюзам
- Обзор по целевой системе
- Целевые учётные записи
- Новые персоны в системе
- Новые целевые системы
- Неиспользуемые системы
- Неиспользуемые целевые учётные записи
- Наименее эффективное использование времени сессии
- Максимальное число параллельных сессий за период

## ГРАФИК ЭФФЕКТИВНОСТИ

Позволил оценить общую эффективность работ на протяжении времени



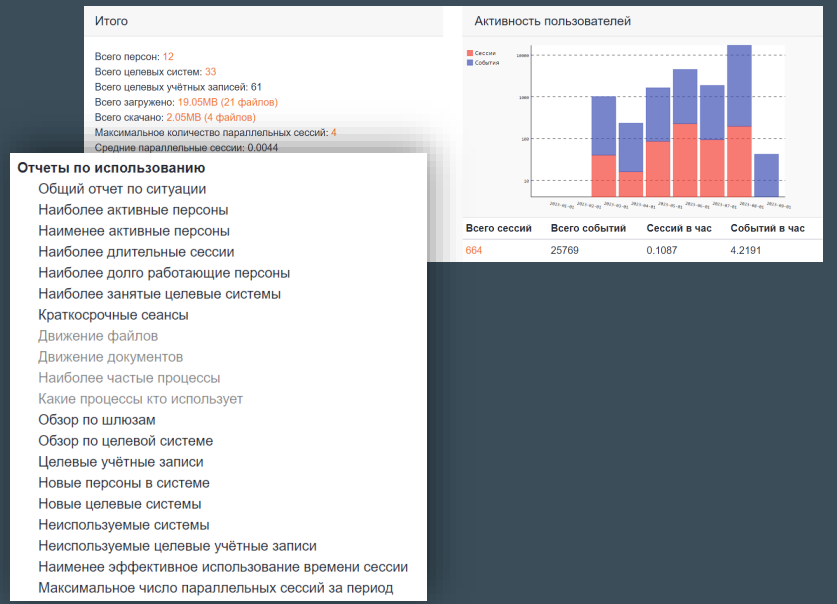

| | |
|---|---|
| **Тип инцидента** | Наименее эффективное использование времени сессии |
| **Уровень** | Низкий |
| **Влияние** | 10 |
| **Статус** | Новые |
| **Назначен** | Нет владельца |
| **Данные** | effectiveness decreased drastically: 41 % in 8 days |

## ИНЦИДЕНТЫ

Позволили своевременно зафиксировать простои в работе

## ОТЧЕТЫ

Позволил оценить общую эффективность работ на протяжении времени

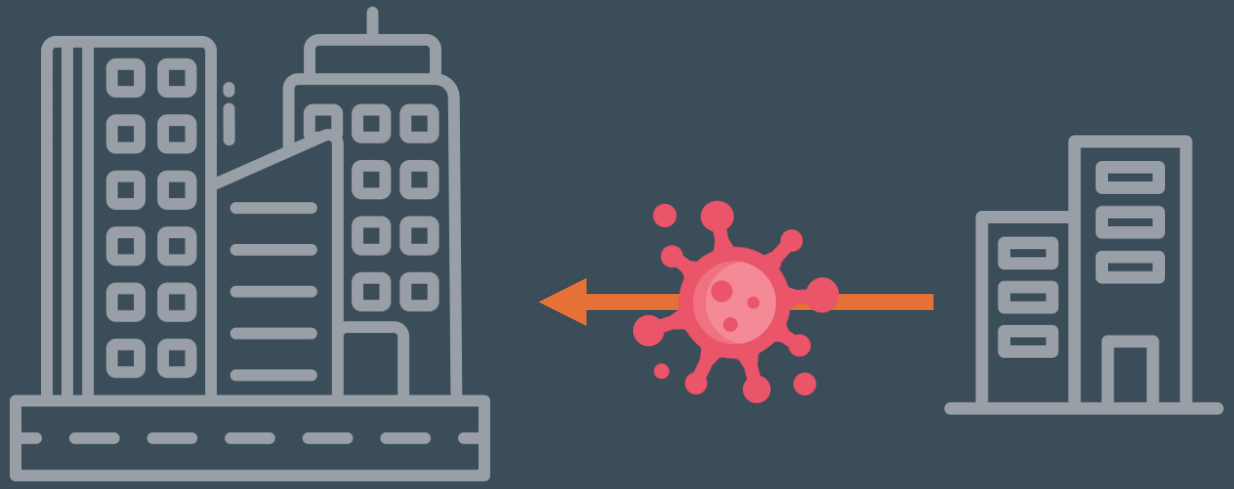


# ИТОГ

ЭКОНОМИЯ РЕСУРСОВ И ФИНАНСОВ

АЙТИБАСТИОН

# КЕЙС 4
# ЧУЖИЕ ОШИБКИ

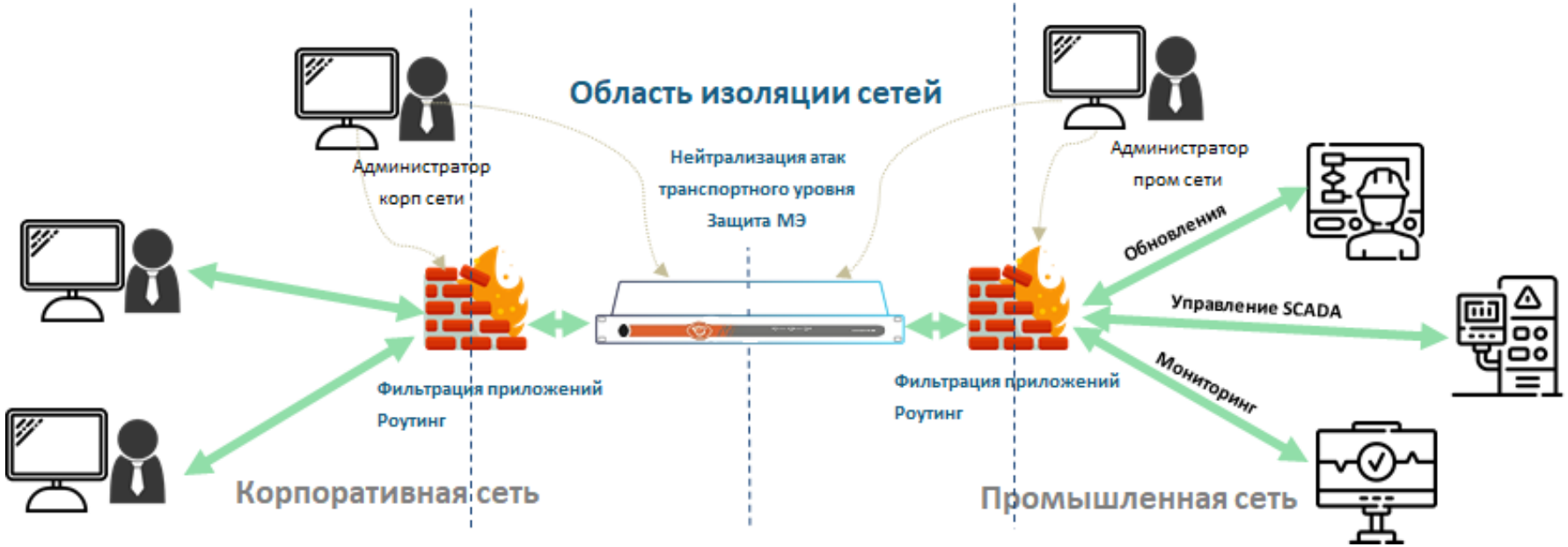


Предотвращение халатного отношения к информационной безопасности

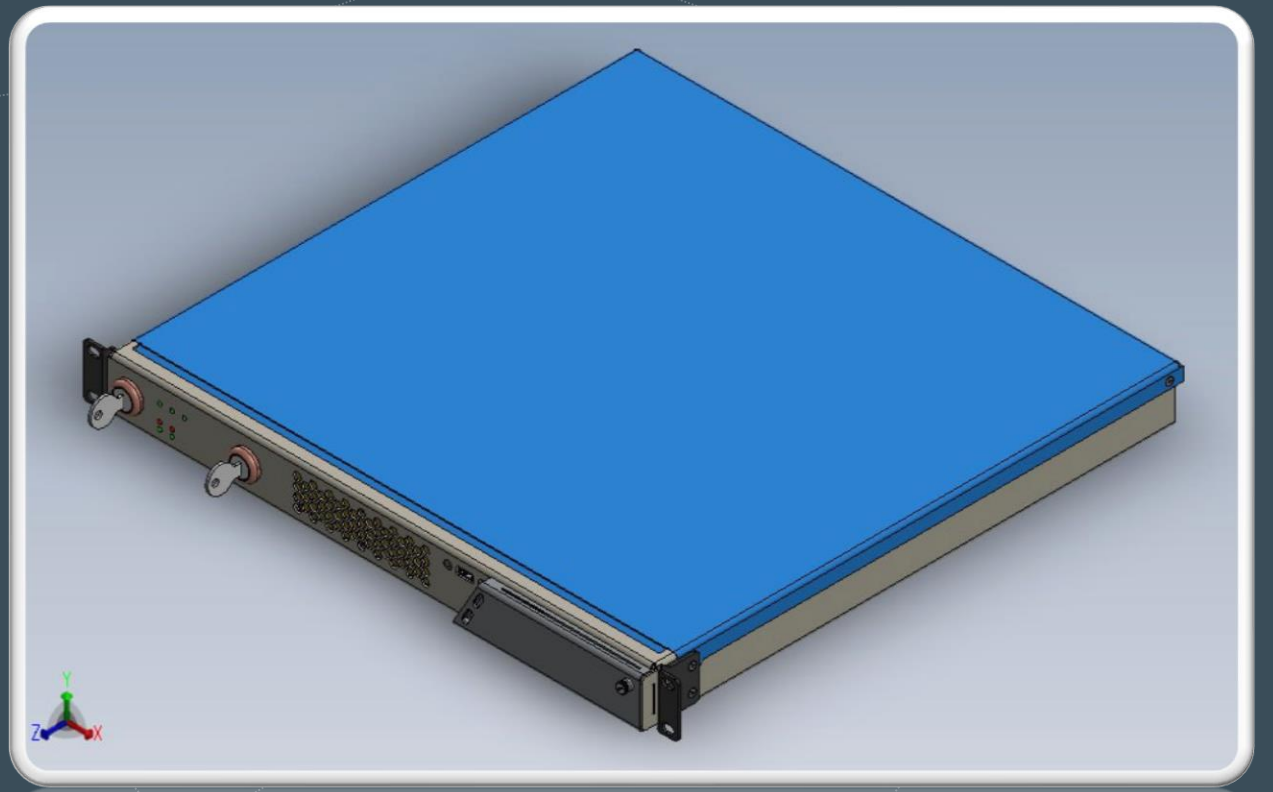
# Объединение изолированных сетей СКПДУ Синоним

АЙТИБАСТИОН

Обеспечение изоляции сетей с сохранением возможности непрерывного обмена данными. Защита МЭ на транспортном уровне, фильтрация и валидация передаваемых данных. Разделение зон ответственности между контурами инфраструктуры



# СИНОНИМ



## ПРОИЗВОДСТВО

На базе отечественного оборудования включенного в реестр Минпромторга

## ФОРМ-ФАКТОР

19’’ стойка – 1U

## КОНТРОЛЬ ЗАПУСКА

Дополнительная блокировка работы устройства двумя специальными «пусковыми» ключами

# КАК ЗАЩИТИТЬ ДОСТУП?

АЙТИБАСТИОН

- Контроль действий
- Ретроспективный анализ
- Реагирование на инциденты
- Однозначная идентификация
- Ролевая модель
- Поведенческий анализ
- Блокировка воздействия на инфраструктуру
- Представление детализированный данных
- Обмен данными между системами
- Автоматизация для исключения человеческого фактора и обеспечения экономии ресурсов
- И т.д.

АЙТИБАСТИОН

# Благодарю за внимание!


ШИРИКАЛОВ АЛЕКСЕЙ

a.shirikalov@it-bastion.com

+7 499 322 3667

it-bastion.com