



# Новый приказ ФСТЭК России № 117. Что изменилось?

Спикеры:

- **Михаил Шипицын** – Технический директор, КСБ-СОФТ
- **Александра Гончарова** – Инженер поддержки продаж/пресейл, АйТи Бастион

Модератор:

- **Дмитрий Чирков** – руководитель регионального направления, КСБ-СОФТ

## «Айти Бастион»



Телеграм-канал  
компании

# 11 лет

на российском рынке  
информационной безопасности

# 250+

заказчиков и проектов. Присутствие  
во всех отраслях от нефтяных компаний  
до футбольных клубов, от небольших офисов  
до геораспределенных площадок

# > 50%

РАМ-рынка в РФ и присутствие  
на рынке в СНГ



Обменивайтесь сообщениями во вкладке «Чат»



Запись вебинара направим Всем участникам на указанный при регистрации e-mail



Задавайте вопросы во вкладке «Вопросы»



Telegram-канал «Мнение интегратора»

## Темы для обсуждения

- новые требования и новые организации, попадающие под действие приказа;
- что делать с системами, аттестованными по-старому (17 приказу)?
- какие СЗИ теперь обязательны?
- мониторинг ИБ - необходимость;
- просто новые меры или новый подход, разберемся...



Наградим авторов 3 лучших вопросов фирменным мерчем!

# «КСБ-СОФТ»

- Лицензиат ФСТЭК России
- Лицензиат ФСБ России



Телеграм-канал  
«Мнение интегратора»

Системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий

**80+**

регионов внедрения

**4000+**

реализованных проектов

[Портфолио](#) КСБ-СОФТ

# Новые ИС, попадающие под действие 117 приказа ФСТЭК России:

- ИС государственных органов
- ИС государственных унитарных предприятий
- ИС государственных учреждений
- Муниципальные информационные системы

а также:

- ИС подрядчиков (разработчиков и интеграторов)
- ИС организаций, взаимодействующих с вышеперечисленными ИС

**Расширение сферы действия регулятора**

не одними ГИСами живем...

## Аттестованные системы?

Действующие аттестаты ГИС будут действительны после 1 марта 2026 года, пока не потребуются контроль

**3 фактора, требующие переаттестации ГИС:**

**1**

**Угрозы**

**2**

**Проектное решение**

**3**

**Класс защиты**

Напоминаем: оператор = заказчик, заключивший контракт

## Классические свойства ИБ:

- Конфиденциальность
- Целостность
- Доступность

Не только информационная безопасность

Требования распространяются также на последствия от нарушения функционирования самой инфраструктуры ИС вследствие реализации угроз ИБ!

## Больше документов по ИБ

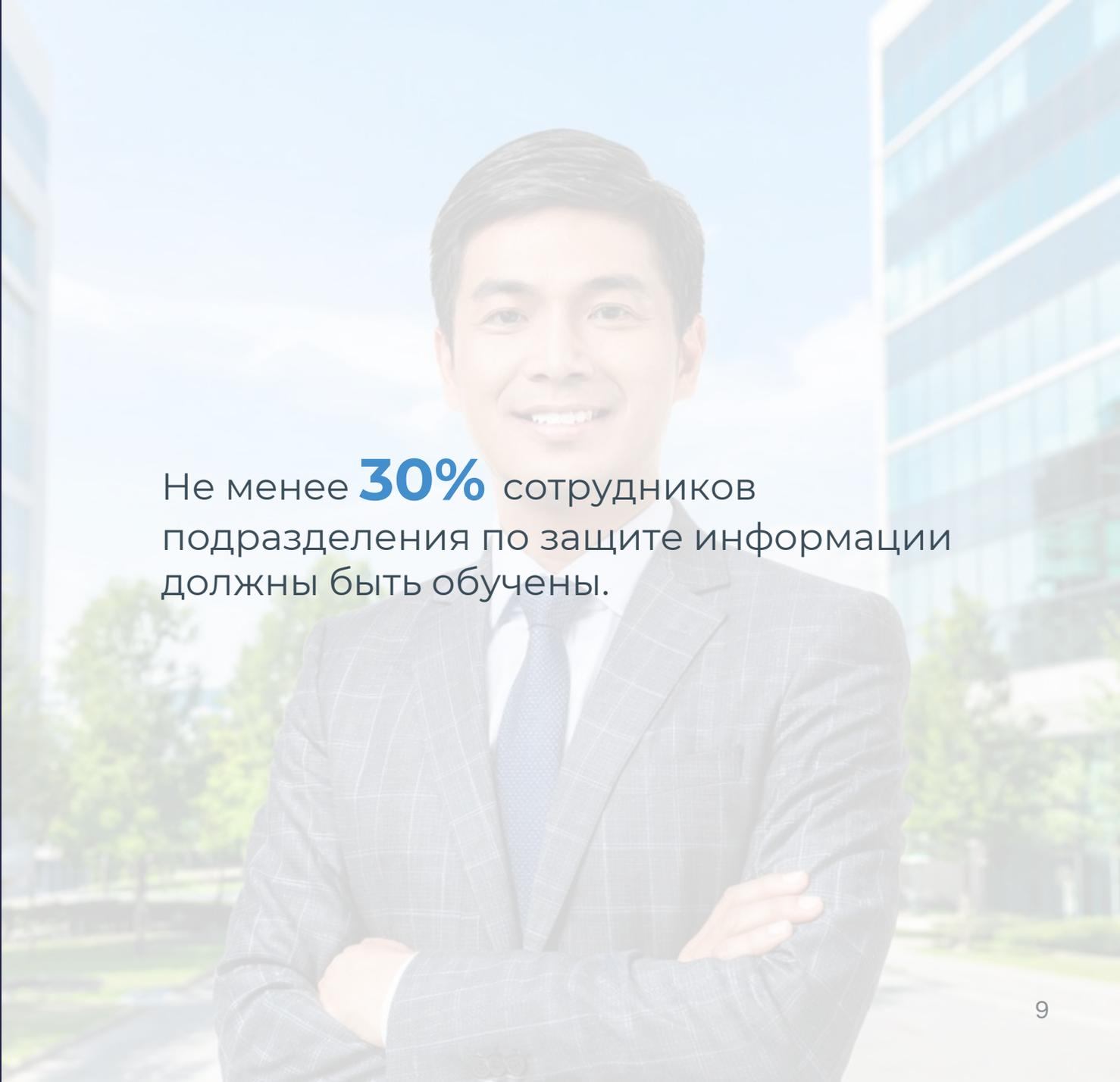
Не просто обеспечение соответствия требованиям, но и повышение эффективности процессов по ИБ!!!

Новый приказ ФСТЭК предусматривает:

- большее количество мер по защите информации;
- глубину проработки документов

## Требования к квалификации персонала

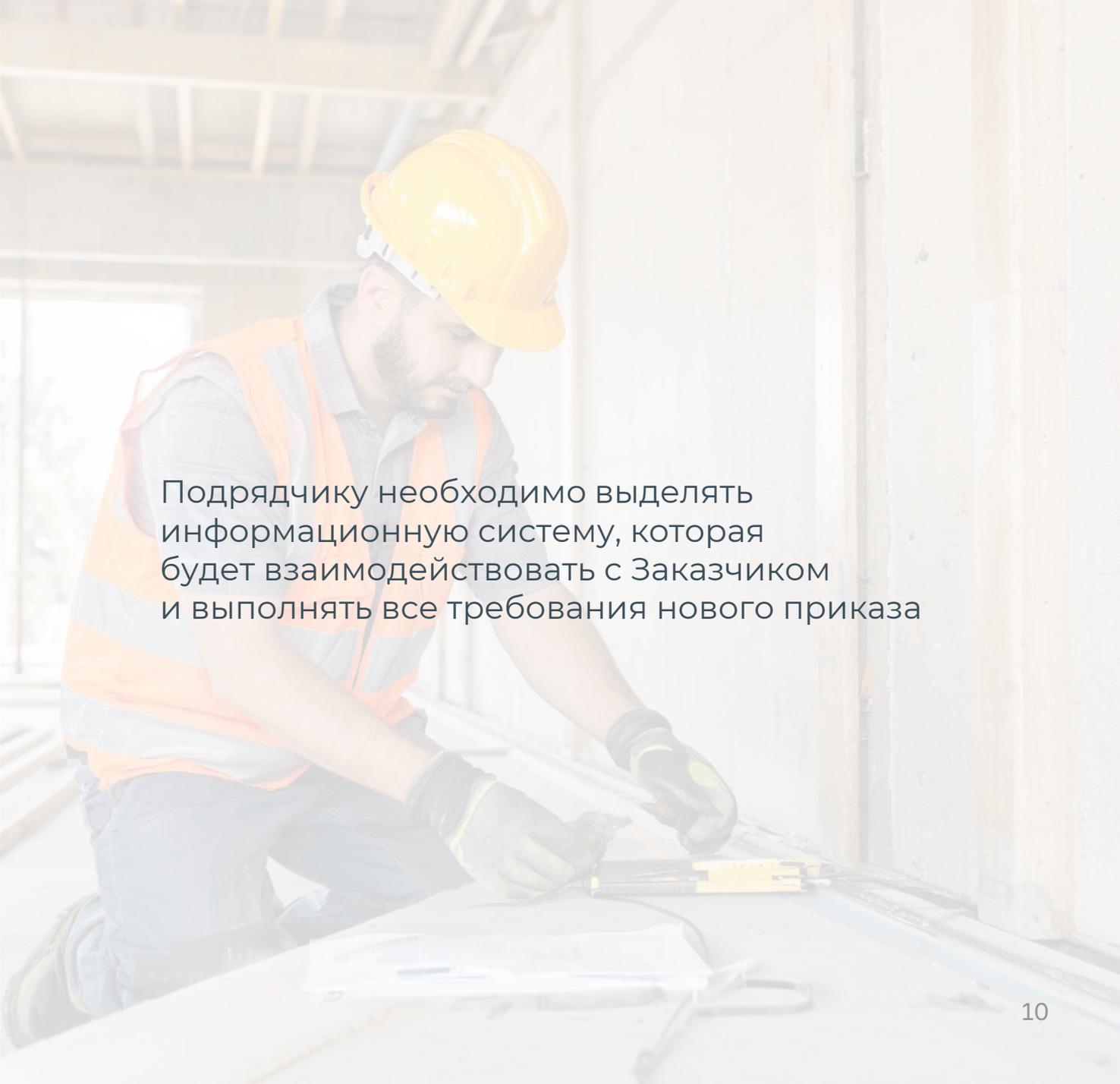
Требуется базовое образование по ИБ, либо профессиональная переподготовка

A photograph of a young man with dark hair, wearing a grey checkered suit jacket, a white shirt, and a blue tie. He is smiling and has his arms crossed. The background is a blurred modern building with large windows and some greenery.

Не менее **30%** сотрудников подразделения по защите информации должны быть обучены.

## Подрядчик тоже обязан

Требования приказа распространяются теперь и на подрядчиков, которые исполняют услуги для оператора ГИС

A construction worker wearing a yellow hard hat and an orange safety vest is kneeling on a construction site. He is focused on working with some equipment or materials on the ground. The background shows the wooden framework of a building under construction.

Подрядчику необходимо выделять информационную систему, которая будет взаимодействовать с Заказчиком и выполнять все требования нового приказа

## Показатели ФСТЭК России:

- показатель защищенности (Кзи)
- показатель уровня зрелости (Пзи)

**Наличие и выполнение плана  
по достижению нормального  
уровня показателей!!!**

## Новые механизмы контроля

Контроль состояния защищенности будет осуществляться ФСТЭК России по 2-ум новым показателям защищенности, помимо классического контроля при аттестации ГИС (5 р.д. для отправки во ФСТЭК).

# Больше СЗИ и их эффективное использование

Требования к используемым СЗИ расширены: много новых и расширение требований к старым

Контроль  
ИТ-  
конфигов

Контроль  
ИТ- активов

Анти-DDOS

РБПО

VM

ALO

Защита ИИ

Защита  
почты

PAM

SOC

Повышение  
уровня  
осведомленност  
и

Защита  
облаков и  
контейнеров

Защита  
мобильных  
устройств

MFA

## Требования к защите мобильных устройств:

- строгая аутентификация
- защита канала
- отсутствие несанкционированного доступа

### Личные мобильные устройства

Личные мобильные устройства использовать **МОЖНО**, но при выполнении требований приказа.

# Взаимодействия и мониторинг

В ИС должен функционировать мониторинг информационной безопасности, а также должно быть обеспечено взаимодействие с 2-мя федеральными ресурсами

Обязательные взаимодействия:

**1**

**ГОССОПКА  
(НКЦКИ)**

**2**

**ЦПУ ССОП  
(Роскомнадзор)**

## Методы контроля:

- выявление уязвимостей (ручное или автоматизированное)
- выявление несанкционированных подключенных устройств
- тестирование на проникновение
- киберучения и тренировки персонала

### Контроль аттестованной ИС

Контроль аттестованной ИС **не реже 1 раза в 3 года**, либо сразу после компьютерного инцидента **(5 р.д. для отправки во ФСТЭК)**.

# Классификация и меры

Классификация в целом осталась такой же, однако приложение с базовыми мерами убрали, будет отдельный методический документ

Стоит выделить:

- 1 Документам с грифом ДСП 1 уровень значимости при классификации
- 2 Возможность присвоения разных классов для разных сегментов ГИС

# «КСБ-СОФТ»

Обеспечение безопасной эксплуатации государственных информационных систем при сопровождении сторонними организациями с использованием технологий удаленного доступа

## Проблематика

- **Рост количества атак на целевые информационные системы через цепочку поставщиков (подрядчиков);**
- **Трудоемкое организационное обеспечение защищенного информационного взаимодействия с организациями-подрядчиками:**
  - Учет и актуализация сведений об ИТ-инфраструктуре организации, к которым предполагается осуществлять удаленный доступ сотрудников из организации-подрядчика;
  - Учет и контроль применяемых мер по защите информации, перечня и прав пользователей в организации-подрядчике;
  - Организация процесса согласования предоставления доступа для сотрудников организации-подрядчика;
  - Заключение соглашений об информационном взаимодействии с учетом требований безопасности и определения ответственности организации-подрядчика;
  - Обеспечение учета и выдачи необходимых СКЗИ (дистрибутивы, лицензии, парольно-ключевая информация) для безопасного подключения сотрудников организации-подрядчика к инфраструктуре защищаемых информационных систем.

# «КСБ-СОФТ»

Обеспечение безопасной эксплуатации государственных информационных систем при сопровождении сторонними организациями с использованием технологий удаленного доступа

Решение

 альфа:реестр

 альфа:коннект

 альфа:id

 альфа:крипто

1

**Формирование единой целостной картины по эксплуатируемым ИС/ГИС организации** с инвентаризацией и созданием единого реестра эксплуатируемых ИС/ГИС организации

2

**Координация участников информационного взаимодействия** при подключении внешних сотрудников к Вашим защищаемым ресурсам с учетом всех требований информационной безопасности и заключением соглашения об информационном взаимодействии

РАМ

3

**Организация единой точки входа** для защищаемых информационных систем, построенных на основе веб-технологий

4

**Организация учета и выдачи СЗКИ** при использовании Вашей защищенной виртуальной сети сотрудниками подрядной организации

## СКАДПУ НТ

### Шлюз доступа:

- модуль контроля сессий;
- менеджер паролей;
- модуль отказоустойчивости и катастрофоустойчивости.

Портал доступа

Кабинет оператора

Архив аудита

### Мониторинг и аналитика:

- модуль мониторинга и отчетности;
- модуль поведенческого анализа, включая детектирование аномалий, инцидентов, реагирование и расширенной статистики

АРЕ (Браузер по требованию)

Персональные сейфы

# ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ



## 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. А наличие сертификата ФСТЭК по УД-4 гарантирует неизменяемость данных для использования их в качестве доказательно базы



## 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, что особенно важно при подключении к объектам КИИ

# ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ



## 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

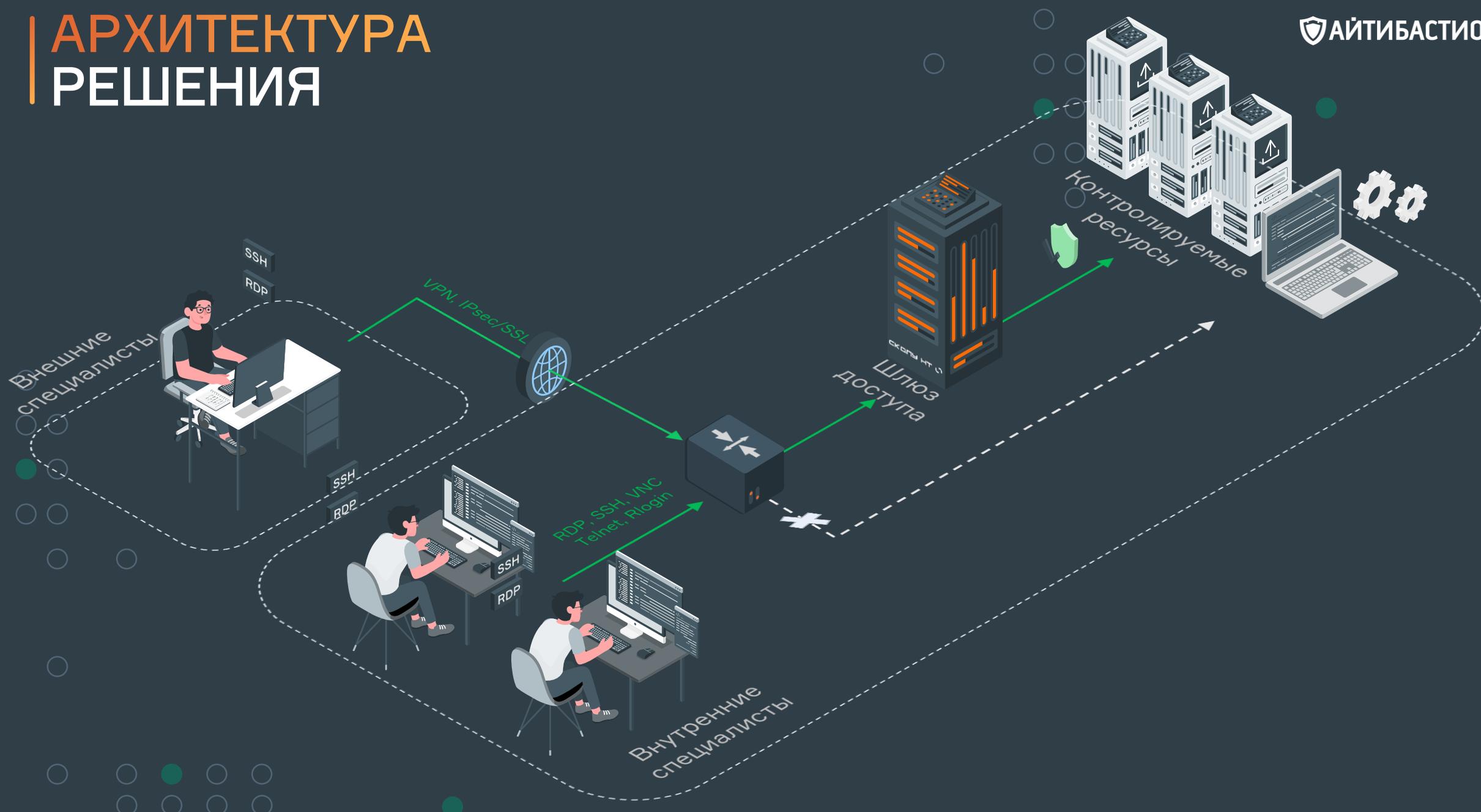
Возможность предоставления доступа по запросу как в момент подключения, так и заранее. Согласование доступа возможно с добавлением одного и более подтверждающих лиц.



## КОНТРОЛЬ НА СТОРОНЕ ИС

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

# АРХИТЕКТУРА РЕШЕНИЯ



# ЕДИНАЯ ТОЧКА ВХОДА

Скриншот веб-интерфейса АИТИБАСТИОН. В меню слева: Мои авторизации, Пароли, Аудит, Пользователи, Ресурсы, Управление паролями, Управление сессиями, Авторизации, Конфигурация, Система, Импорт/Экспорт. В центре: Сессии. Таблица сессий:

| Протоколы | Цель  | Имя авторизации | Описание уч. зап. |
|-----------|---|-----------------|-------------------|
| APP       | admin@chrome:APP                                      | Win-Auth        |                   |
| SSH       | Astra-terminal-agon@local@Terminal-Astra:SSH          | SSH-Auth        |                   |
| RDP       | Global-Domain-Winserver-admin@demo.agon@WinServer:RDP | Win-Auth        |                   |
| RDP       | Global-Domain-Winserver-agon@demo.agon@WinServer:RDP  | Win-Auth        |                   |
| RDP       | Graphic-Astra-agon@local@Graphic-Astra:RDP            | SSH-Auth        |                   |
| SSH       | Graphic-Astra-kira@local@Graphic-Astra:SSH_2          | SSH-Auth        |                   |
| SSH       | Graphic-Astra-shoora@local@Graphic-Astra:SSH_1        | Win-Auth        |                   |
| RDP       | Local-WinServer-12-agon@local@WinServer12:RDP         | Win-Auth        |                   |
| RDP       | Local-WinServer-administrator@local@WinServer:RDP     | SSH-Auth        |                   |
| SSH       | PashaFedora-agon@local@PashaFedora:SSH                | SSH-Auth        |                   |

```
flexandra@nb0083:~$ ssh admin@10.5.10.1
(admin@10.5.10.1) NODE1 - WARNING: Access to this system is restricted to duly a
uthorized users only. Any attempt to access this system without authorization or
fraudulently remaining within such system will be prosecuted in accordance with
the law.
Any authorized user is hereby informed and acknowledges that his/her actions may
be recorded, retained and audited.
admin's password:
| ID | Site (page 1/1) | Authorization
|----|-----|-----|
| 0 | Graphic-Astra-kira@local@Graphic-Astra:SSH_2 | SSH-Auth
| 1 | Graphic-Astra-shoora@local@Graphic-Astra:SSH_1 | Win-Auth
| 2 | PashaFedora-agon@local@PashaFedora:SSH | SSH-Auth
| 3 | Astra-terminal-agon@local@Terminal-Astra:SSH | SSH-Auth
Enter h for help, ctrl-D to quit
> _
```

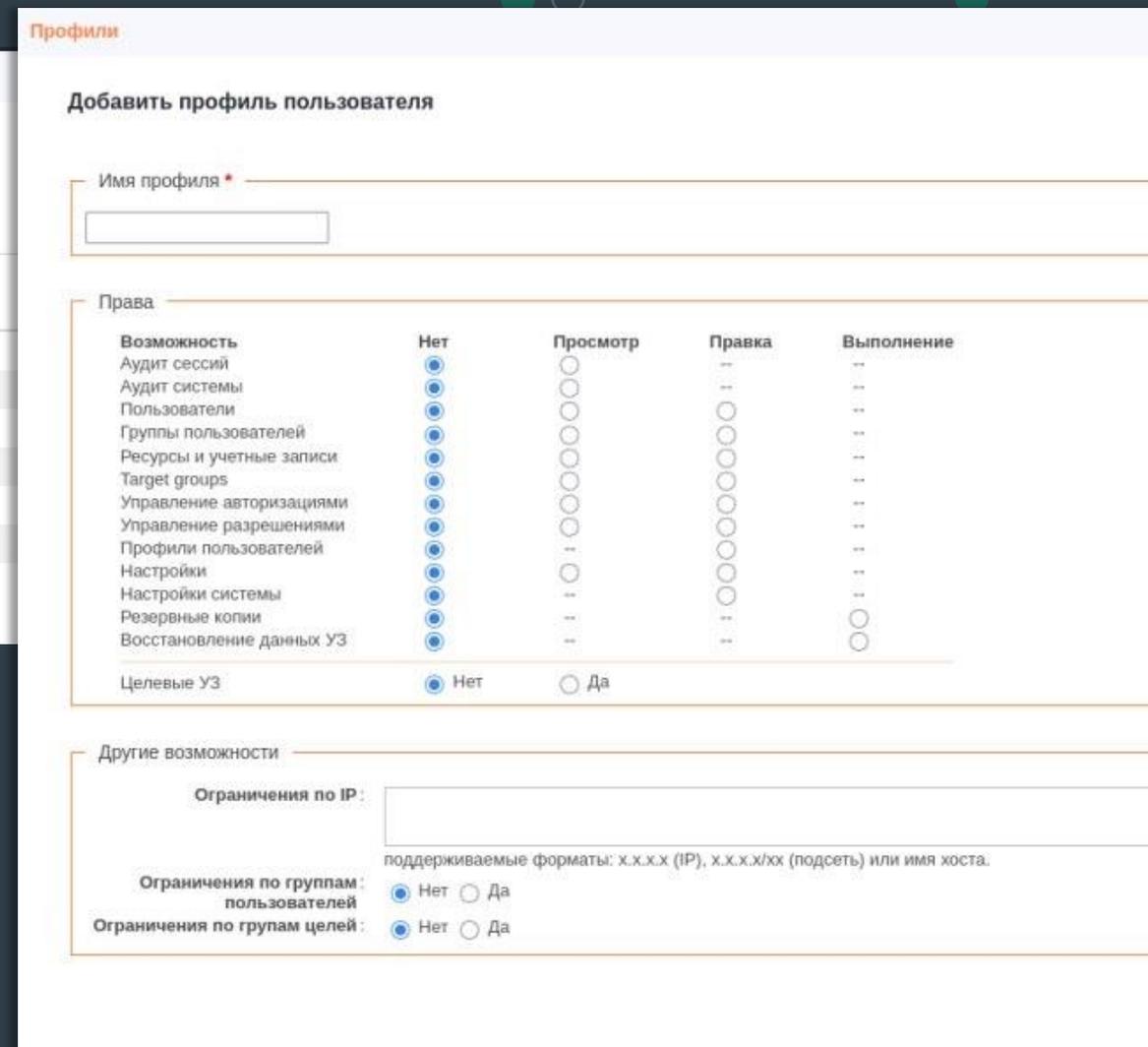
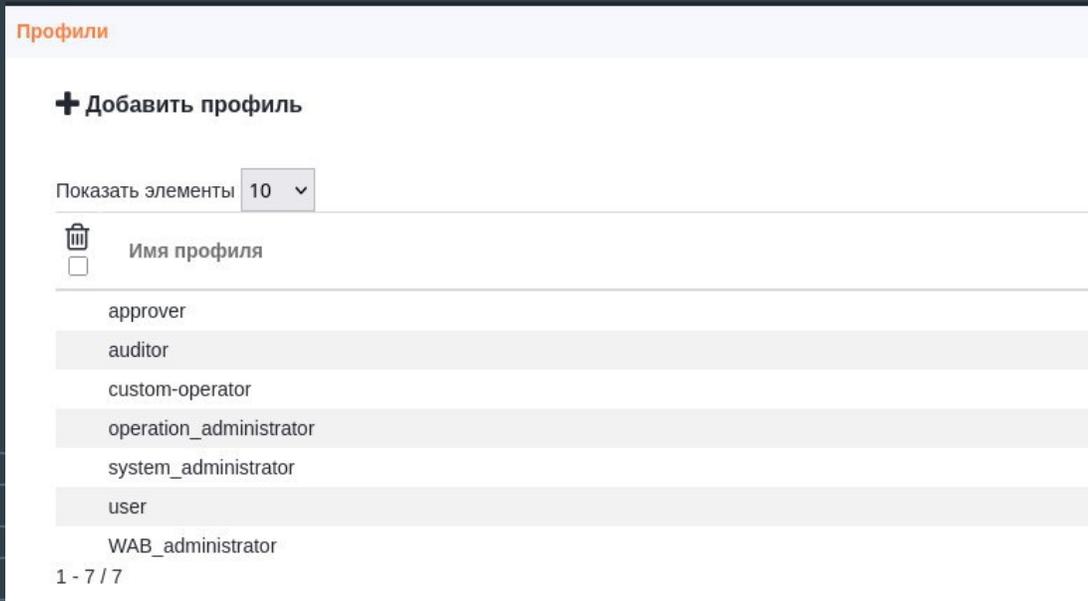
Скриншот rdesktop - 10.5.10.1. Таблица авторизации:

| Authorization | Target  | Protocol |
|---------------|---|----------|
| Win-Auth      | Global-Domain-Winserver-admin@demo.agon@WinServer:RDP | RDP      |
| Win-Auth      | Global-Domain-Winserver-agon@demo.agon@WinServer:RDP  | RDP      |
| SSH-Auth      | Graphic-Astra-agon@local@Graphic-Astra:RDP            | RDP      |
| Win-Auth      | Interactive@WinServer:RDP                             | RDP      |
| Win-Auth      | Local-WinServer-12-agon@local@WinServer12:RDP         | RDP      |
| SSH-Auth      | Local-WinServer-administrator@local@WinServer:RDP     | RDP      |
| Win-Auth      | admin@chrome:APP                                      | APP      |

## Организация доступов

С возможностью подключения пользователей через веб-интерфейс и стандартные клиенты подключения (терминвл, CMD, MSTSC, Remmina и пр.).

# ПРИСВОЕНИЕ И СОЗДАНИЕ РОЛЕЙ



Список ролей по умолчанию

Однозначная идентификация прав в системе «из коробки»

Уникальная роль

Точечное делегирование прав управления системой с разграничением групп, передаваемых под управление

# ЗАПИСЬ И ПРОСМОТР СЕССИИ

Просмотрщик RDP



Постоянное проигрывание

Полная запись: [Создать](#)

Список снимков экрана



Данные сессий

| Индекс | Дата время          | Действие   |                   |
|--------|---------------------|--|-------------------|
| 1      | 2025-08-13 12:36:28 | Beginning  | <a href="#">↓</a> |
|        | 2025-08-13 12:36:31 | type="NEW_PROCESS" command_line="C:\Windows\system32\TSTheme.exe -Embedding"       |                   |
|        | 2025-08-13 12:36:31 | type="COMPLETED_PROCESS" command_line="C:\Windows\system32\TSTheme.exe -Embedding" |                   |
|        | 2025-08-13 12:36:31 | type="NEW_PROCESS" command_line="taskhostw.exe install \$(Arg0)"                   |                   |
|        | 2025-08-13 12:36:31 | type="COMPLETED_PROCESS" command_line="taskhostw.exe install \$(Arg0)"             |                   |

Поиск:

**Видеозапись сессии**  
С фрагментацией по интервалам времени или запускаемым процессам в сессии

**Мета-информация сессии**  
С индексацией процессов, фиксацией клавиатурного ввода, заголовков окон, нажатия клавиш и др.

## Политики замены паролей

### Редактировать политику смены паролей

Имя политики: demo-change

Описание: --

Период замены: 20 0 \*\*\*

Минимальная длина пароля: 12

Минимальное число символов: 3

К-во маленьких букв: 3

К-во больших букв: 3

Число цифр: 3

Запрещенные символы: #

Тип ключа SSH: RSA

Размер ключа SSH: 2048

### История смены паролей

Аккаунт: Global-Domain-Winserver-agon  
Домен: demo.agon

Показать элементы 10 ▾

| Дата                | Тип учетной записи | Пароль/Отпечаток ключа SSH |
|---------------------|--------------------|----------------------------|
| 2025-08-15 19:10:04 | password           | \0aG86E                    |
| 2025-08-15 00:20:10 | password           | zV\$o+F3                   |
| 2025-08-14 00:20:12 | password           | <QdO;k0                    |
| 2025-08-13 13:17:02 | password           | rhB{F4R\                   |
| 2025-08-13 12:56:58 | password           | (F8]25Ki                   |
| 2025-08-13 00:20:10 | password           | 0F.1&qV                    |
| 2025-07-23 00:20:10 | password           | im:16A>L                   |
| 2025-07-22 00:20:10 | password           | 1So=F41                    |
| 2025-07-21 00:20:10 | password           | Gb0g-3C                    |
| 2025-07-20 00:20:10 | password           | 9IZ53um                    |

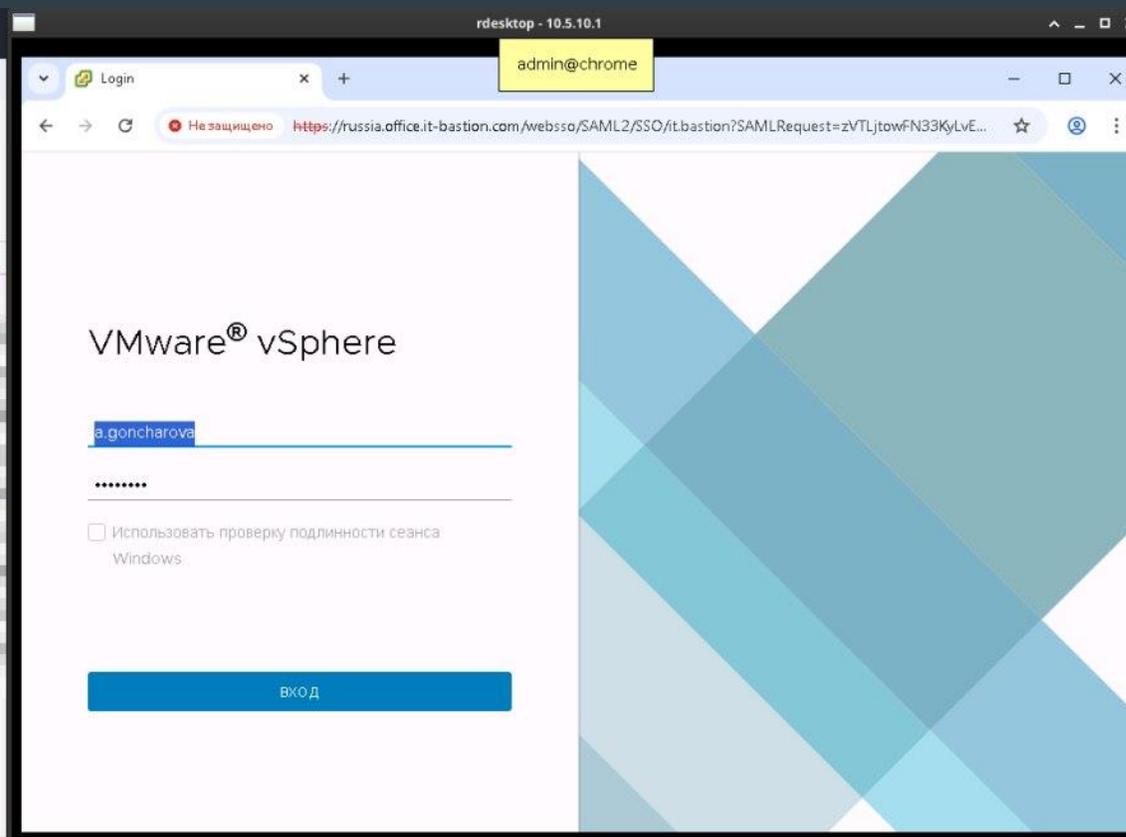
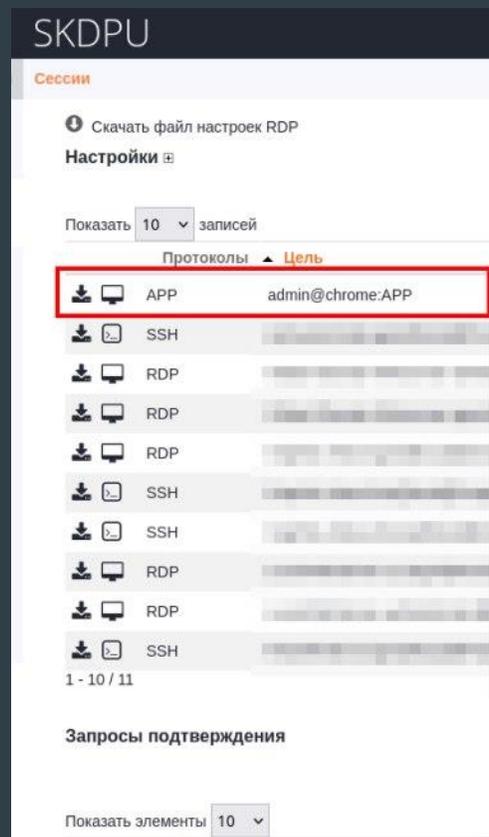
1 - 10 / 222

- **Дополнительная защита учетных записей целевых устройств**  
Возможность менять пароли средствами PAM-системы на целевых системах как по расписанию, так и по факту отключения пользователя от сессии (однозразовый пароль сессии).

# КОНТРОЛЬ ПРИЛОЖЕНИЙ И УЗ В НИХ

Подключение к конечным приложениям

С подстановкой учётной записи без раскрытия её пользователю и полной фиксацией действий



# СКДПУ НТ APE (БРАУЗЕР ПО ТРЕБОВАНИЮ) \*MVP

Добавление конечного WEB приложения

Ограничение на использование иных приложений и запрет действий.

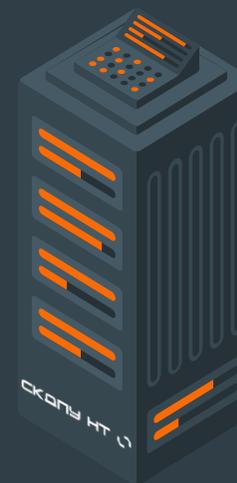
Использование данных для входа из СКДПУ НТ

Хранение УЗ на СКДПУ НТ, обеспечение защиты доступа и ротации УЗ.

- Фиксация событий
- Расширенные возможности логирования с видео и метаданными.
- Базируется на ос Astra Linux
- Отечественная ОС, уход от зарубежных решений.



СКДПУ НТ  
Шлюз доступа

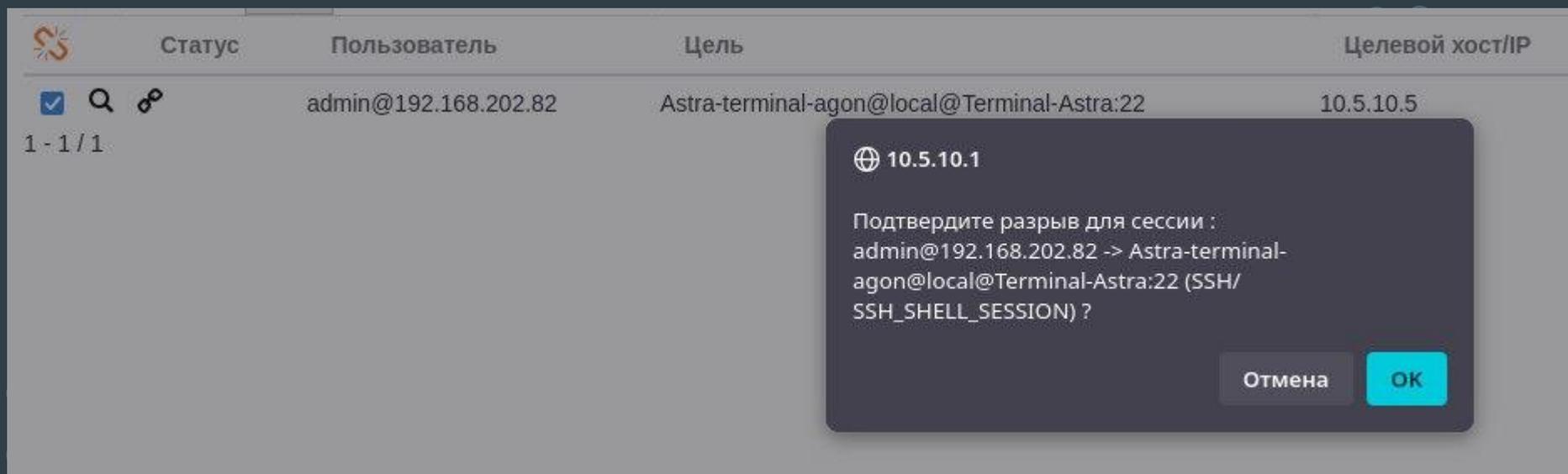


Astra Linux  
APE



Конечный  
WEB ресурс

# РАЗРЫВ СОЕДИНЕНИЯ



Блокировка пользовательской сессии  
вручную администратором или с автоматическим паттерном реагирования

```
2025-08-13 12:40:59 type="KILL_PATTERN_DETECTED" pattern="rm"  
2025-08-13 12:40:59 type="SESSION_DISCONNECTION" duration="0:06:16"
```

# ПОДТВЕРЖДЕНИЕ ДОСТУПА

Запрос обоснования  
необходимости подключения  
у пользователя

Подтверждение подключения  
одним или более администратором

rdesktop - 10.5.10.1

Information

Вы должны получить подтверждение чтобы получить доступ к целевой системе.

Duration \*  Format: [hours]h[mins]m

Ticket Ref.

Comment

(\*) required fields

Запрос разрешения

Запрос разрешения: agon -- Global-Domain-Winserver-agon@demo.agon@WinServer:RDP

Дата начала \*

Время начала \*

Длительность \*

Ссылка на тикет:

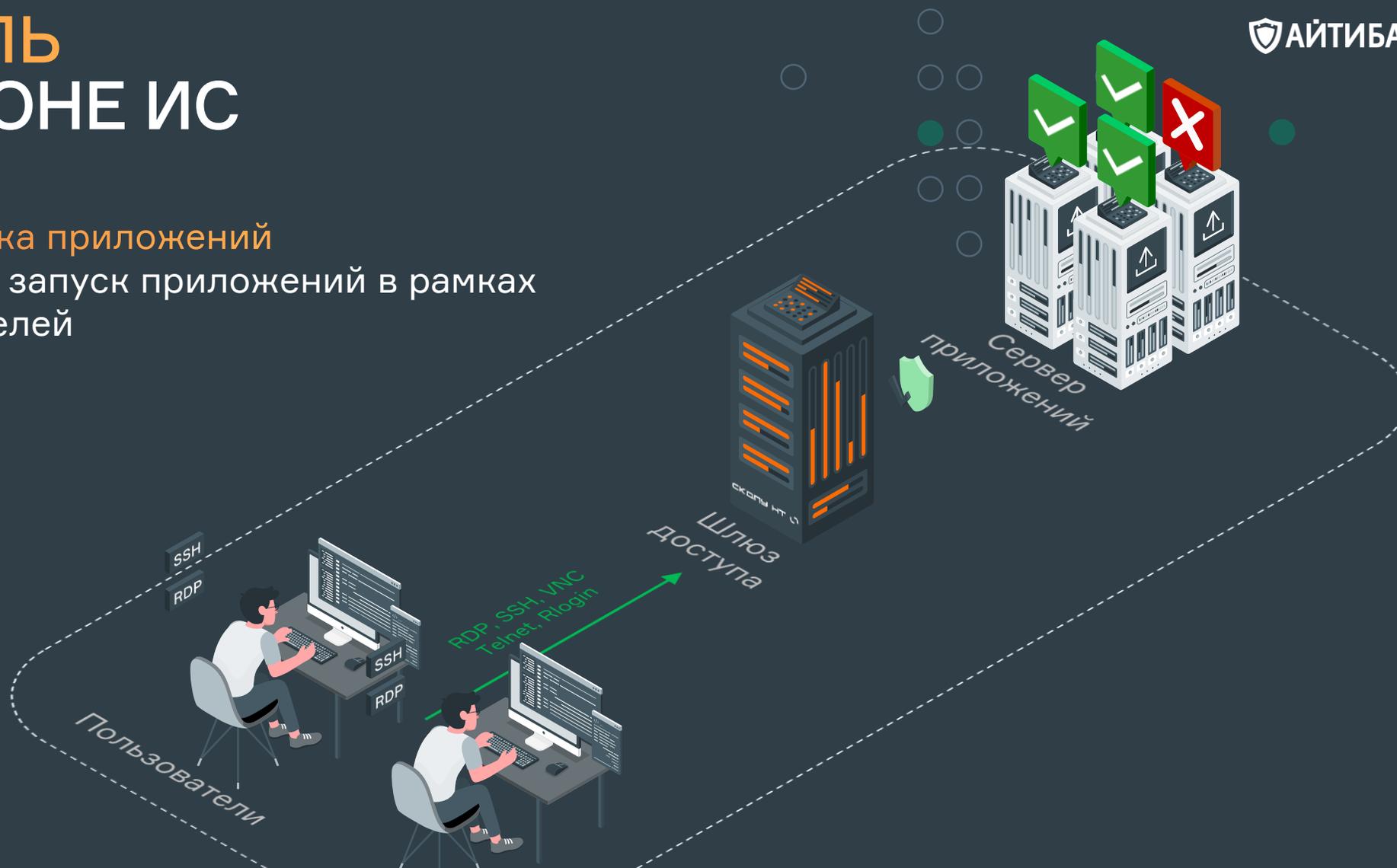
Комментарий:

Формат: "[часы]h[мин]m" (не обязательно указывать все)

# КОНТРОЛЬ НА СТОРОНЕ ИС

## Блокировка запуска приложений

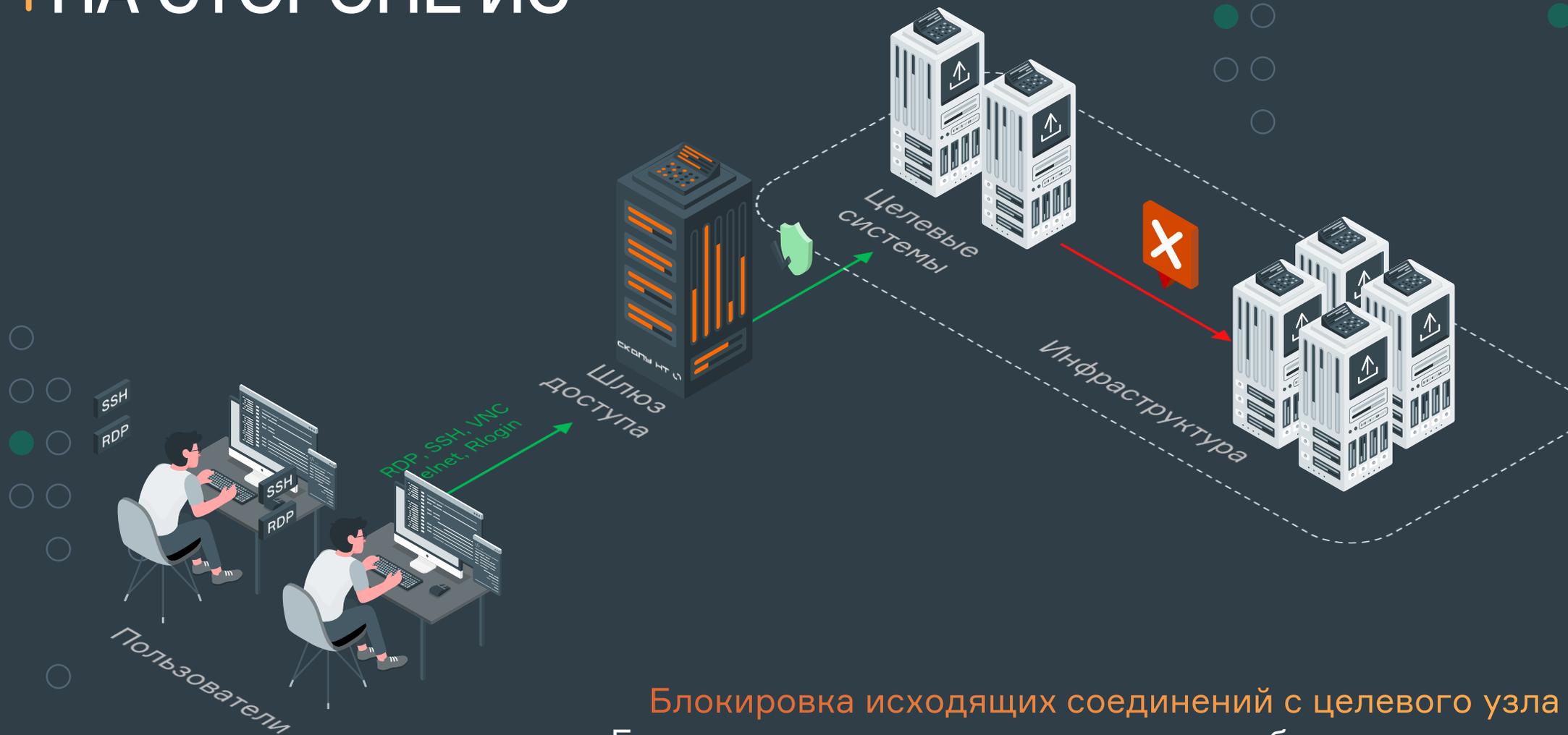
Можем запрещать запуск приложений в рамках сессий пользователей



38:48 MSK

The process 'iexplore.exe' was interrupted in accordance with security policies. (insert key or left click to hide)

# КОНТРОЛЬ НА СТОРОНЕ ИС



Блокировка исходящих соединений с целевого узла  
Блокируем заданные соединения, чтобы пользователь  
не имел доступ во всю внутреннюю сеть

# ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ СКДПУ ИТ МОНИТОРИНГ И АНАЛИТИКА



## 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 МАСШТАБИРОВАНИЕ

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.

# РАМ-ПЛАТФОРМА СКДПУ ИТ МОНИТОРИНГ И АНАЛИТИКА

Единая точка мониторинга и аудита для нескольких площадок.  
Графическое представление событий в сессиях.

### 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

### Активность пользователей

### Использование

- отчет по ситуации
- более активные персоны
- менее активные персоны
- более длительные сессии
- более долго работающие персоны
- более занятые целевые системы
- срочные сеансы
- много файлов
- много документов
- более частые процессы
- процессы кто использует
- по шлюзам
- по целевой системе
- более 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

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

Цифровой профиль пользователя | 7 дней | Показать | Выберите дату... | Напечатать | Редактировать

**Избранное** ★

ID: admin  
 Зарегистрирован: 16-10-2023 13:58:00  
 Последняя активность: 06-03-2024 11:24:00  
 Группа: Интеграторы

Уровень доверия: 700

### Активности

|                 | Сегодня       | Текущая неделя | Текущий месяц | Текущий квартал | Текущий год   | Всего               |
|-----------------|---------------|----------------|---------------|-----------------|---------------|---------------------|
| Сессии:         | 0             | 0              | 15            | 70              | 70            | 208                 |
| Шлюзы:          | 0             | 0              | 2             | 3               | 3             | 5                   |
| Цели:           | 0             | 0              | 4             | 6               | 6             | 15                  |
| Учётные записи: | 0             | 0              | 3             | 4               | 4             | 7                   |
| Время работы:   | --            | --             | 0:40:21       | 2:00:21         | 2:00:21       | 7:58:44             |
| Загружено:      | 0В (0 файлов) | 0В (0 файлов)  | 0В (0 файлов) | 0В (0 файлов)   | 0В (0 файлов) | 0В (0 файлов)       |
| Скачано:        | 0В (0 файлов) | 0В (0 файлов)  | 0В (0 файлов) | 0В (0 файлов)   | 0В (0 файлов) | 29.05KB (10 файлов) |

Построение поведенческой модели пользователей и реакция на отклонение от типичного поведения в сессии

Обширная библиотека отчётов для ретроспективного анализа сессий и состояния инфраструктуры

# РАМ-ПЛАТФОРМА СКДПУ ИТ МОНИТОРИНГ И АНАЛИТИКА

## График эффективности

В цифровом профиле пользователя оценить общую эффективность работы на протяжении времени



# РАМ-ПЛАТФОРМА СКДПУ ИТ МОНИТОРИНГ И АНАЛИТИКА

## Настройки детекторов аномалий

Детектирование потенциально опасных команд

Детектор разрывов сессий

Контроль привычного времени работы

Контроль изменения уровня доверия

Контроль стандартных команд

Контроль привычных сетевых адресов работы

Контроль эффективности работы

Индикаторы взрывной активности

Детектор новых доступов

Детектор проблем с правами доступа к файлам

Детектор использования средств удаленного досту

Детектор входов без средств контроля

Анализатор ошибок авторизации

Детектор забытых персон

Количество переданных файлов

Детектор сканеров

CLM-1001562

Дата регистрации: 27-06-2023 20:16:55

Персона: abezboro

Сессия: root win1-RDP  
С помощью: skdrp70 продолжительность: 0:01:08

Тип инцидента: Подозрительные команды

Уровень: Низкий

Влияние: 20

Статус: Новые

Назначен: Нет владельца

Адрес клиента: 172.16.128.186

Данные: black: "Burp."

Подробности:

| Дата и время записи | Тип события | Данные            |
|---------------------|-------------|-------------------|
| 27-06-2023 20:16:55 | KBD_INPUT   | data Burp/<enter> |

CLM-1000045

Дата регистрации: 13-03-2023 16:44:59

Персона: abezboro

Сессия: root win1-RDP  
С помощью: skdrp70 продолжительность: 0:03:40

Тип инцидента: Подозрительные команды

Уровень: Низкий

Влияние: 2

Статус: Новые

Назначен: Нет владельца

Адрес клиента: 172.16.128.186

Данные: gray: ".tor-"

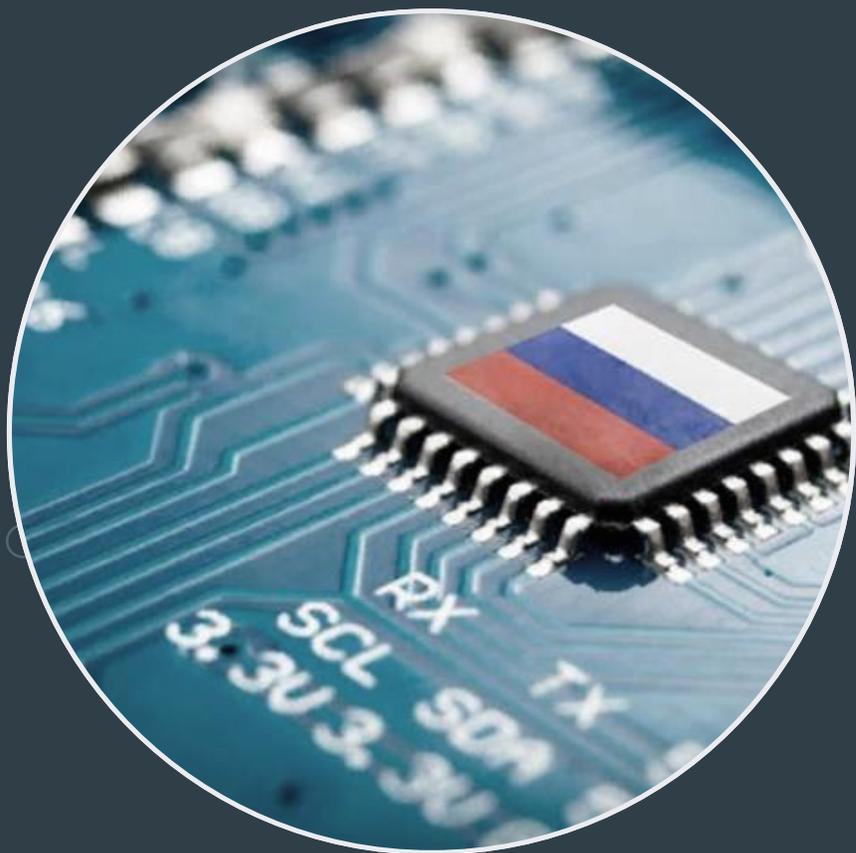
Подробности:

| Дата и время записи | Тип события | Данные  |
|---------------------|-------------|---|
| 13-03-2023 16:44:59 | NEW_PROCESS | command_line 'C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=crashpad-handler "--user-data-dir=C:\Users\root\AppData\Local\Google\Chrome\User Data" /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\root\AppData\Local\Google\Chrome\User Data\Crashpad\..." |

Индивидуальные модели реагирования  
Подключение функций реагирования на инциденты и интеграция в единую систему реагирования

Взаимодействие с SOAR/IRP

```
17 do
18 incident=$(echo "${incident}" | base64 --decode)
19 session_id=$(echo "${incident}" | jq -r '.data.event.session_id')
20 event_type=$(echo "${incident}" | jq -r '.data.event.event_type')
21 incident_id=$(echo "${incident}" | jq -r '.data.incident')
22 incident_link=$(echo "${incident}" | jq -r '.incident_link')
23
24 if [ "$event_type" == "NEW_PROCESS" ]; then
25     curl -k -X PUT \
26     -H "X-Auth-Key: $xtoken" \
27     -H "X-Auth-User: $xuser" \
28     -H "Content-Type: application/json" \
29     -d "{\"reason\": \"${incident_id}\${incident_link}\"} \" \
30     "https://${api_address}/api/sessions?session_id=${session_id}&action=kill"
31 fi
32 done
33
```



Сертификация

# ФСТЭК России

Работа продукта на базе отечественной  
операционной системы Astra Linux SE



# СКДПУ ИТ СУММАРНЫЙ ЭФФЕКТ



## ТРЕБОВАНИЯ РЕГУЛЯТОРОВ

Соблюдение предписаний и рекомендаций государственных регуляторов в сфере ИБ



## ДОКАЗАТЕЛЬНАЯ БАЗА

Защита собственных специалистов от неправомерных претензий в случае инцидентов ИБ или аварий



## ОПЕРАТИВНЫЙ АУДИТ

Анализ действий пользователей, сбор событий при сбоях или инцидентах ИБ



## ИМПОРТО- НЕЗАВИСИМОСТЬ

Отсутствие в ПО зарубежных компонентов, непосредственно взаимодействующих с критической инфраструктурой



## ПОДРЯДЧИКИ

Контроль за действиями подрядчиков.  
Контроль соблюдения SLA



## ОТЧЁТНОСТЬ

Быстрый доступ к аналитике, отчётам и потенциальным инцидентам



## СОБЛЮДЕНИЕ ПОЛИТИК

Исполнение корпоративных стандартов в области информационной безопасности



## ЗАЩИТА ДОСТУПА

Контроль доступа к информационной инфраструктуре в реальном времени

# Благодарю за внимание!

Гончарова Александра  
инженер поддержки продаж



[a.goncharova@it-bastion.com](mailto:a.goncharova@it-bastion.com)



+7 499 322 3667



[it-bastion.com](http://it-bastion.com)



## Способы контроля состояния защиты информации в цифрах:

- Не менее **30%** работников подразделения по ЗИ должны быть обучены
- Расчет Кзи **не реже 1 раза в 6 месяцев, Пзи не реже 1 раза в 2 года.** Направляются во ФСТЭК России **не позднее 5 р.д.** после дня их расчета
- Устранять уязвимости в срок **от 24 часов до 7 дней**, в зависимости от уровня опасности
- При выявлении уязвимостей, которые отсутствуют в БДУ, отправить их во ФСТЭК России **не позднее 5 р.д.** со дня их обнаружения
- **Ежегодно** направлять отчет по мониторингу ИБ во ФСТЭК России
- Интервалы восстановления инфраструктуры **от 24 часов до 4 недель** в зависимости от класса защиты ИС

## Способы контроля состояния защиты информации в цифрах:

- **Не реже 1 раза в 2 года** проверки/тренировки по восстановлению информации из резервных копий
- Оценка уровня знаний пользователей **не реже 1 раза в 3 года** или после компьютерного инцидента
- Контроль уровня защищенности информации в аттестованной системе должен проводиться **не реже 1 раза в 3 года** или после компьютерного инцидента. Результаты направляются во ФСТЭК России **не позднее 5 р.д.** после дня их получения
- Сертифицированные **СЗИ от 4 до 6 класса** в зависимости от класса защиты ИС

# Работайте с нами!



<https://ksb-soft.ru/>



428000, г. Чебоксары,  
пр-т Максима Горького,  
18 Б, пом. 9



8 800 3333-872



[info@ksb-soft.ru](mailto:info@ksb-soft.ru)



Телеграм-канал  
«Мнение интегратора»

