КСБ-СОФТ АЙТИБАСТИОН

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%

PAM-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»

Телеграм-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

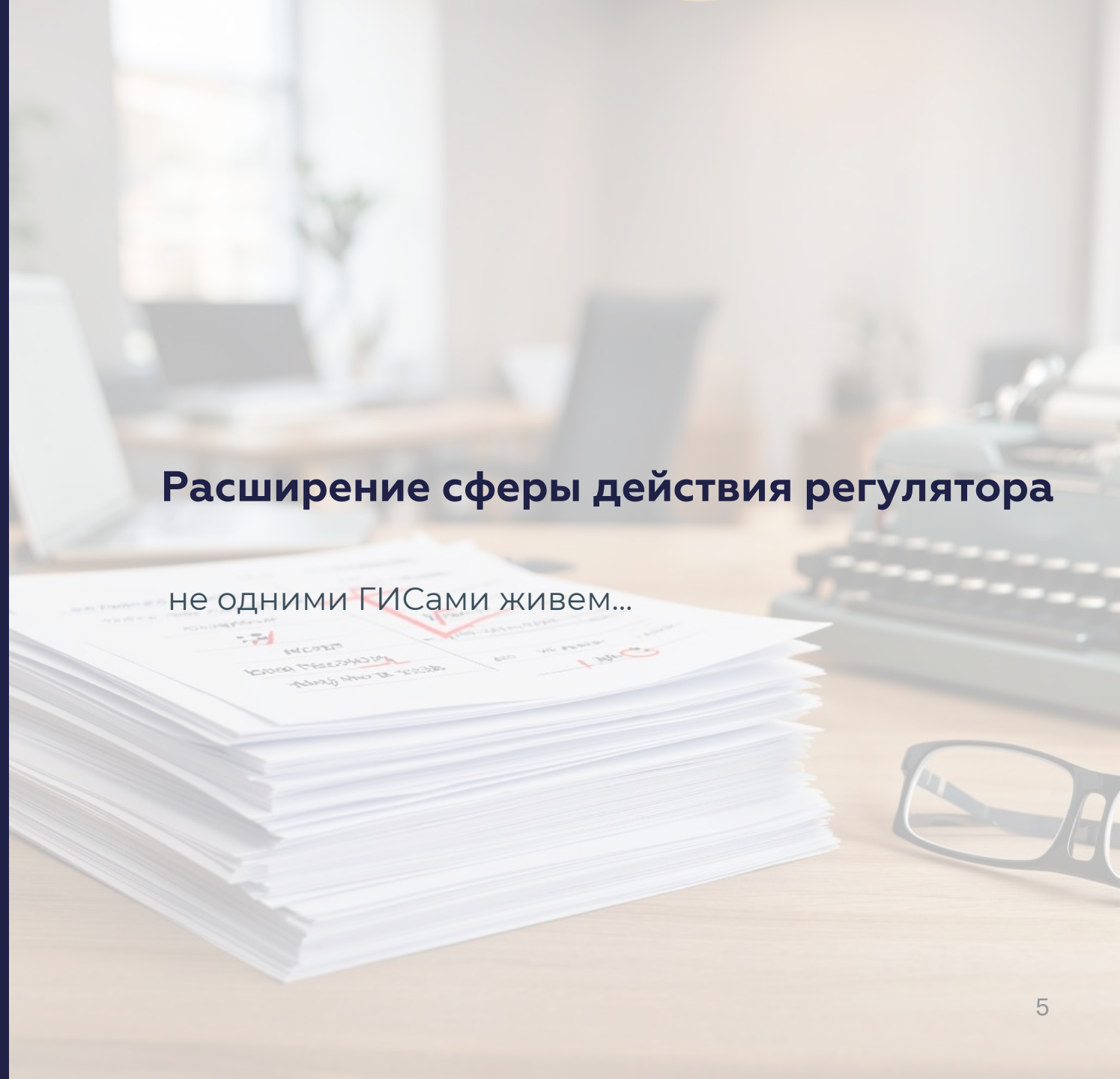
Портфолио КСБ-СОФТ

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 потребуется 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

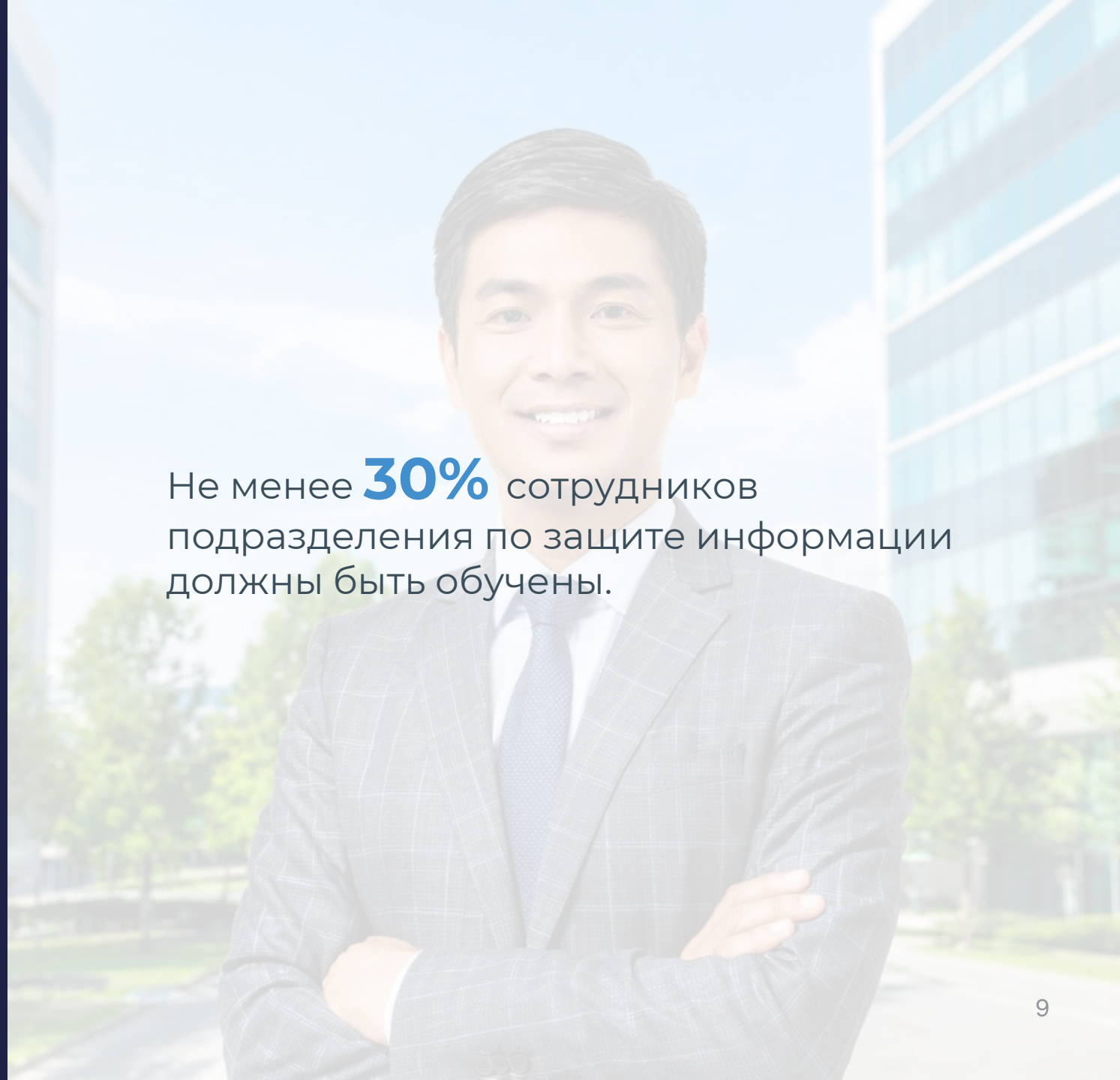
Не просто обеспечение соответствия требованиям, но и повышение эффективности процессов по ИБ!!!

Новый приказ ФСТЭК предусматривает:

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

Требования к квалификации персонала

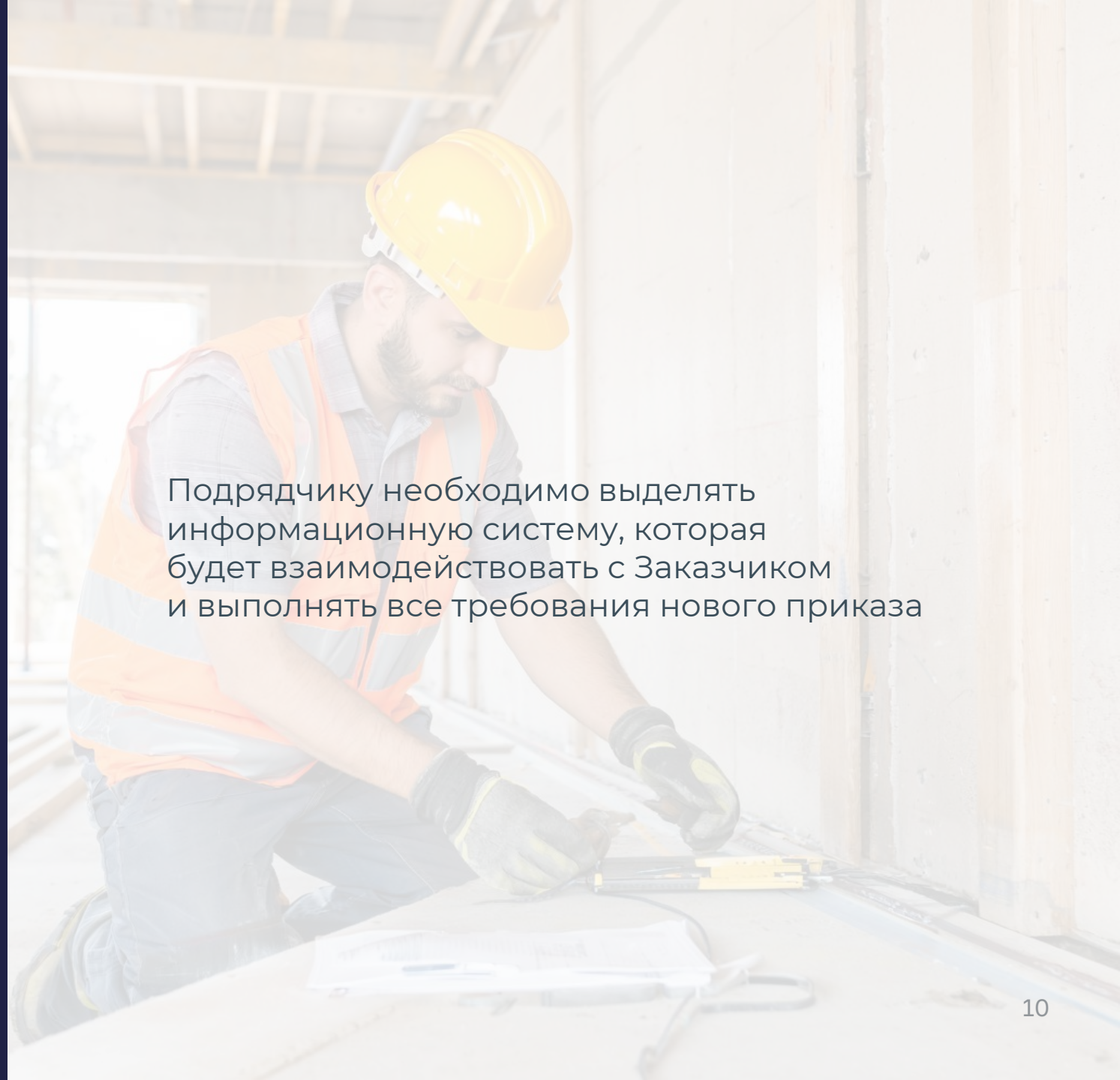
Требуется базовое образование по ИБ, либо профессиональная переподготовка



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

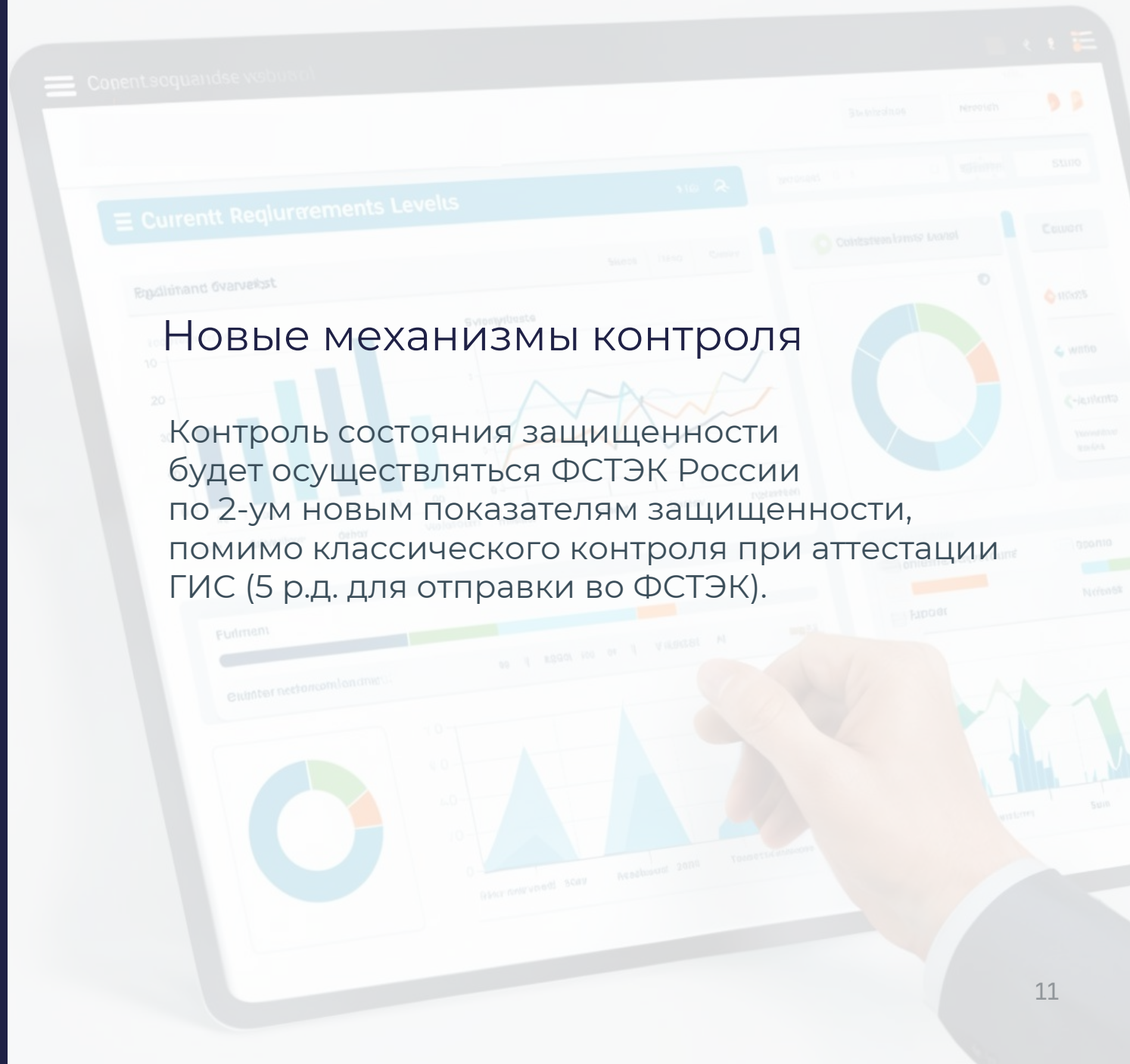


Подрядчику необходимо выделять информационную систему, которая будет взаимодействовать с Заказчиком и выполнять все требования нового приказа

Показатели ФСТЭК России:

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

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



Новые механизмы контроля

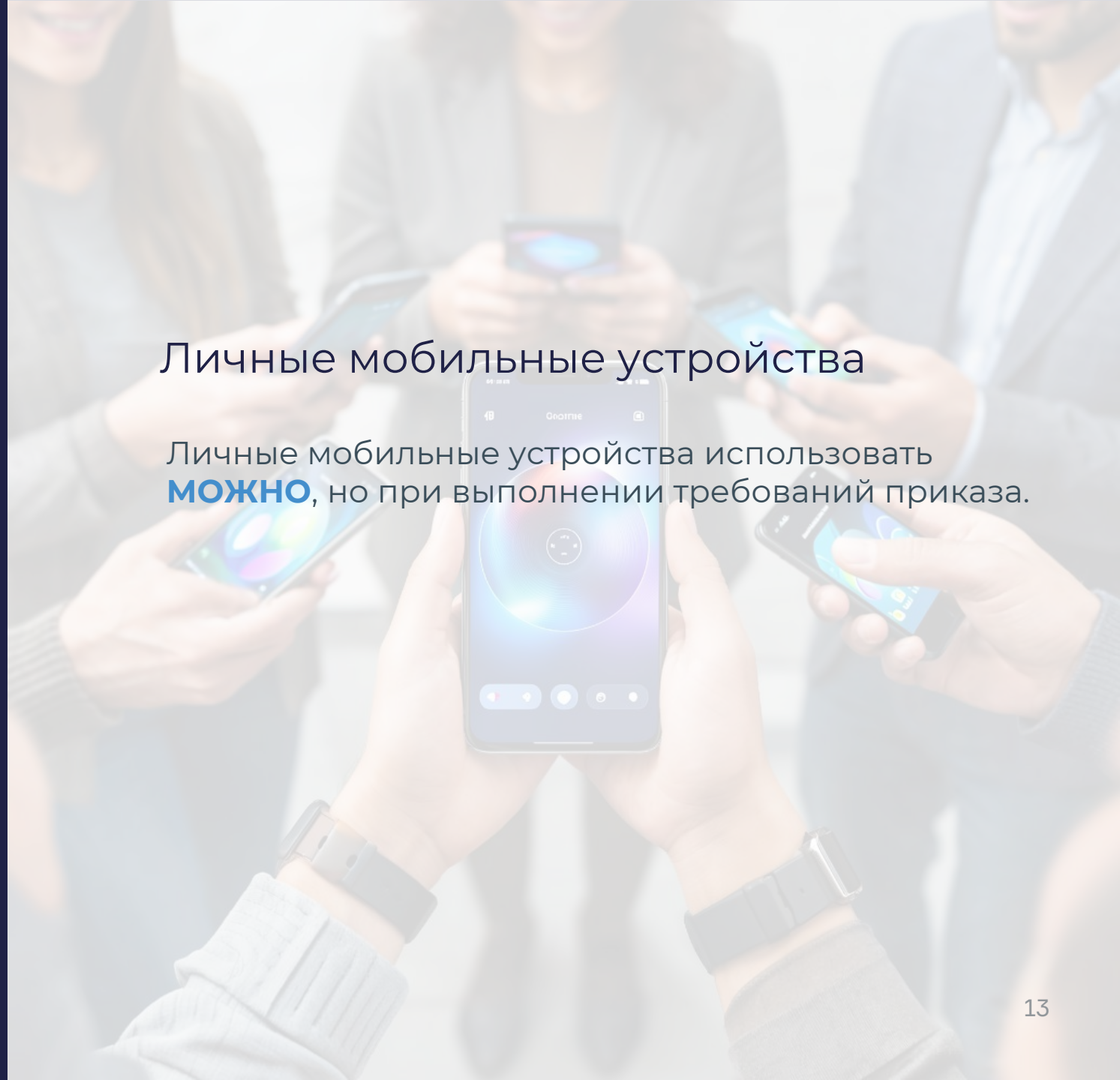
Контроль состояния защищенности будет осуществляться ФСТЭК России по 2-ум новым показателям защищенности, помимо классического контроля при аттестации ГИС (5 р.д. для отправки во ФСТЭК).

Больше СЗИ и их эффективное использование

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

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

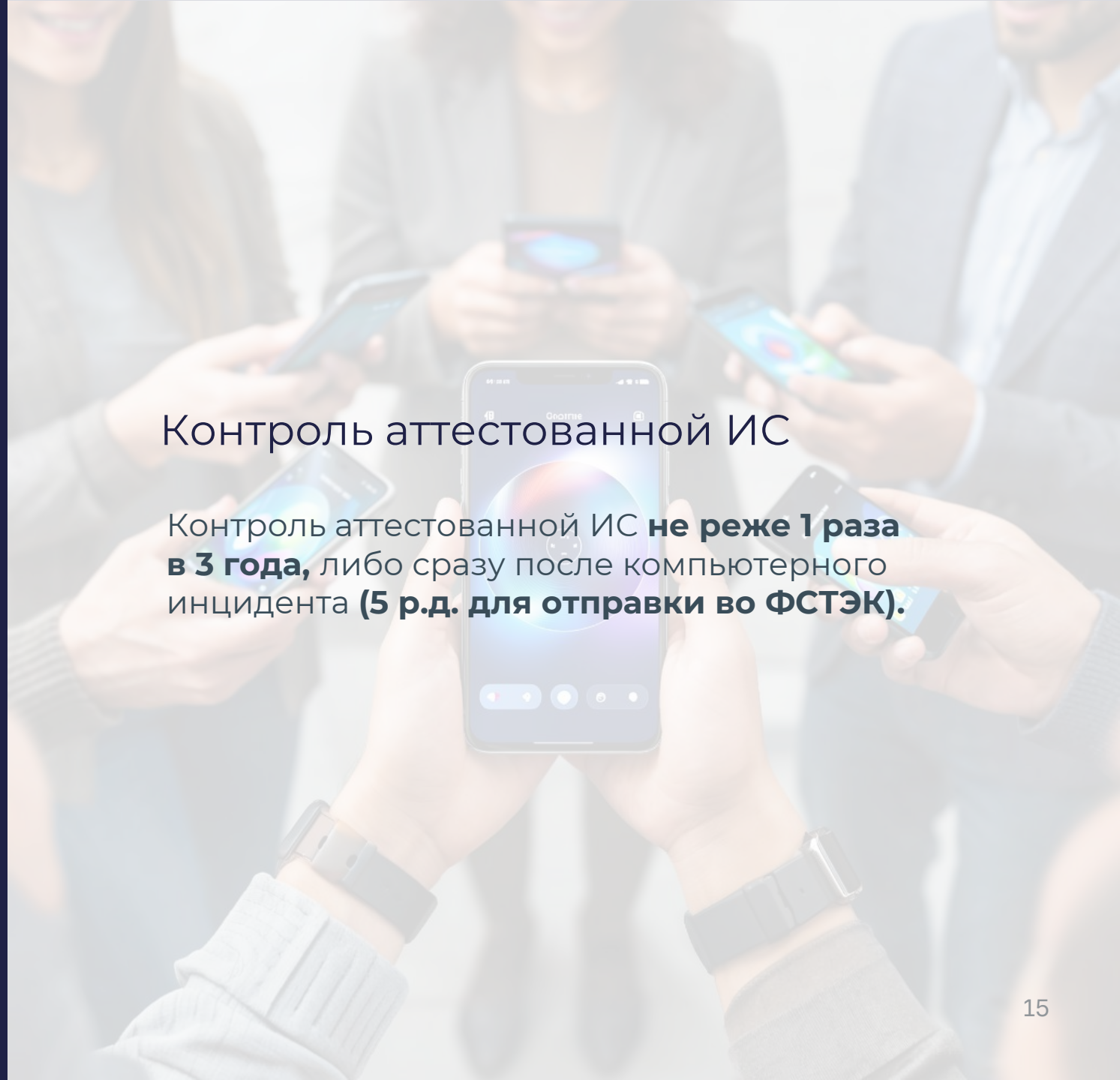
ГОССОПКА (НКЦКИ)

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

PAM

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

МОДУЛЬНАЯ ПЛАТФОРМА

АЙТИБАСТИОН

СКАУТ NT

Шлюз доступа:

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

Мониторинг и аналитика:

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

Портал доступа

Кабинет оператора

Архив аудита

APE (Браузер по требованию)

Персональные сейфы

www.it-bastion.com

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

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. А наличие сертификата ФСТЭК по УД-4 гарантирует неизменяемость данных для использовании 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

www.it-bastion.com

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

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.

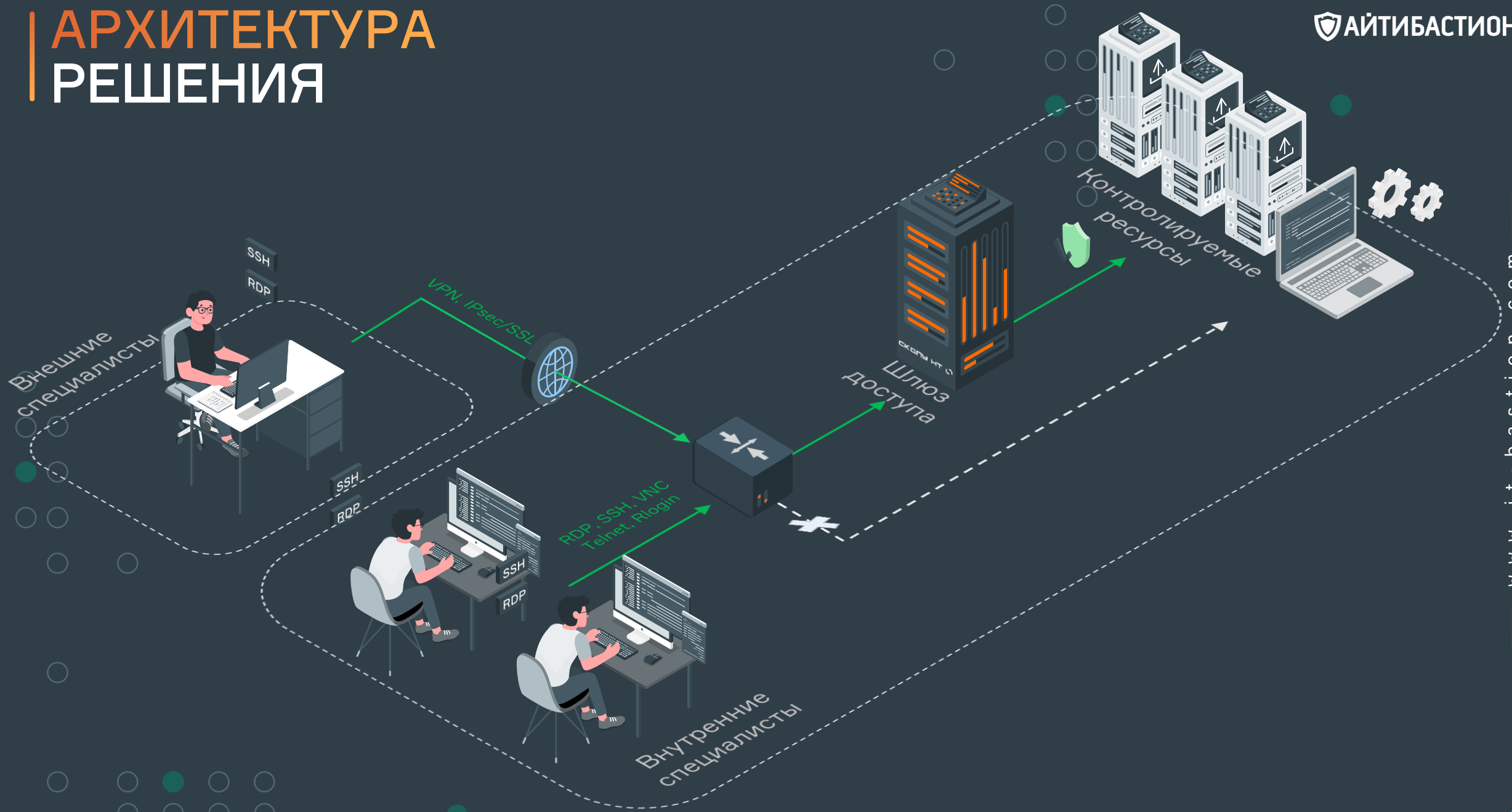
КОНТРОЛЬ НА СТОРОНЕ ИС

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

www.it-bastion.com

АРХИТЕКТУРА РЕШЕНИЯ

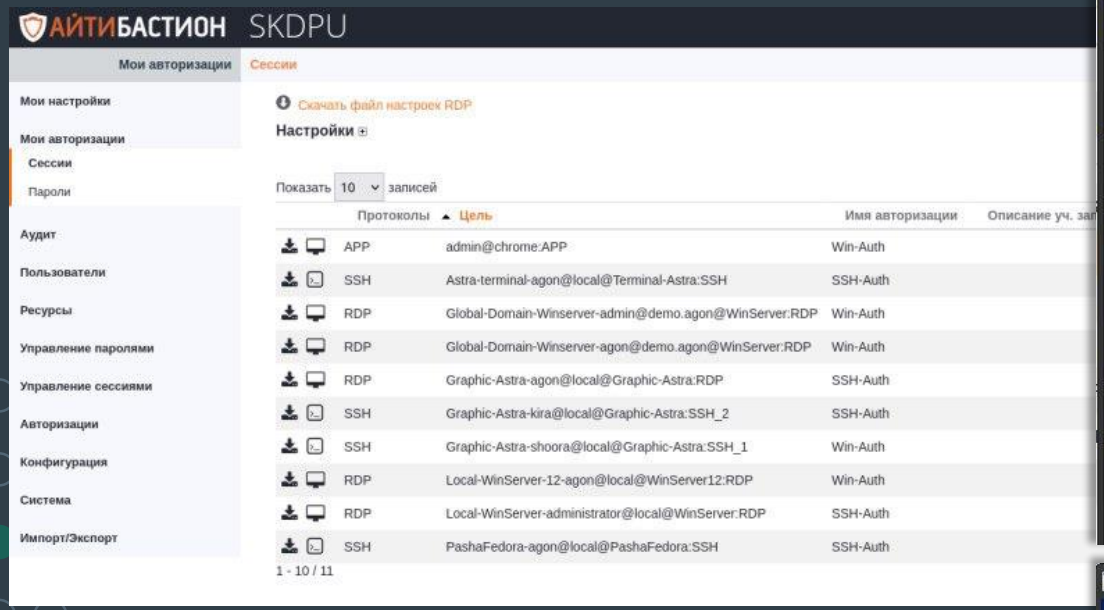
АЙТИБАСТИОН

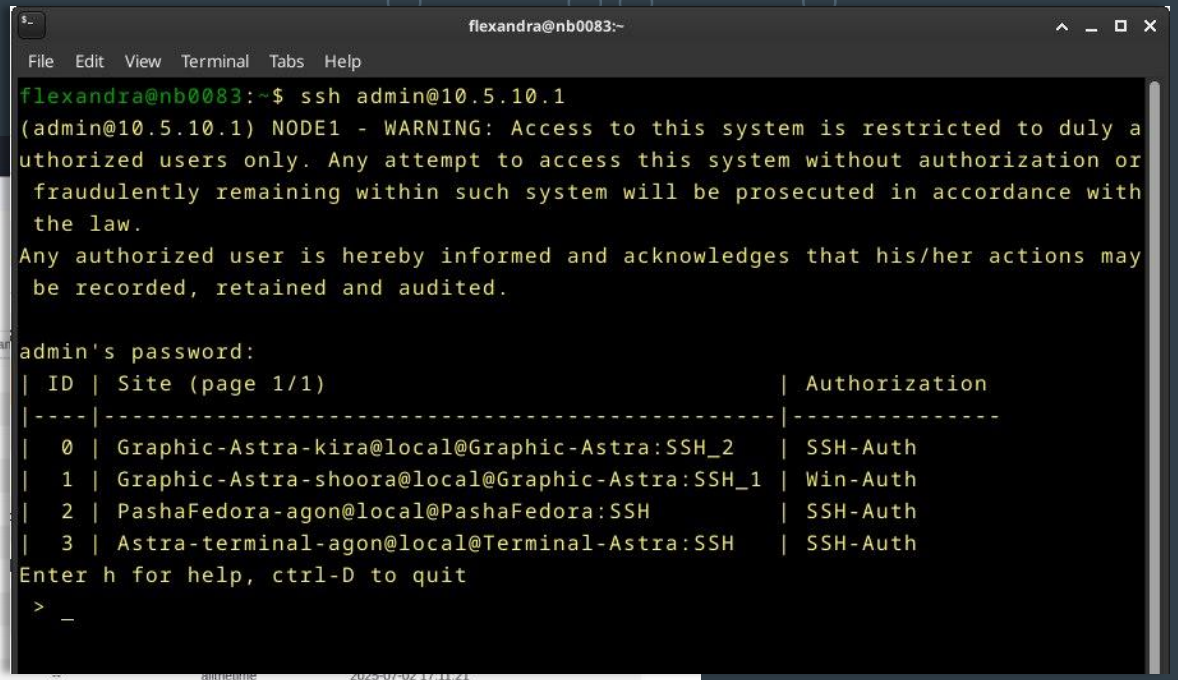


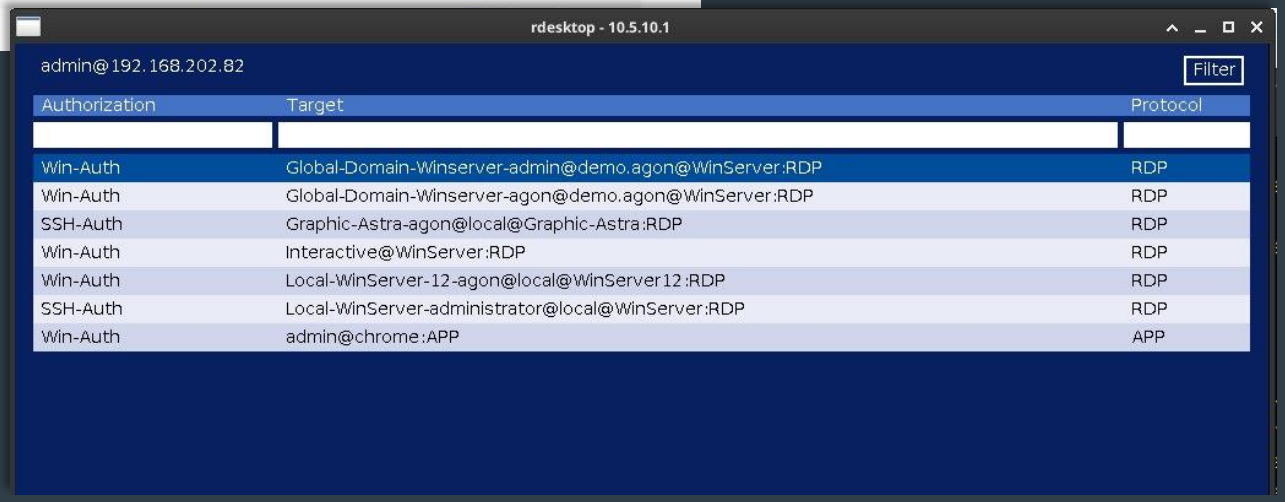
www.it-bastion.com

ЕДИНАЯ ТОЧКА ВХОДА

АЙТИБАСТИОН







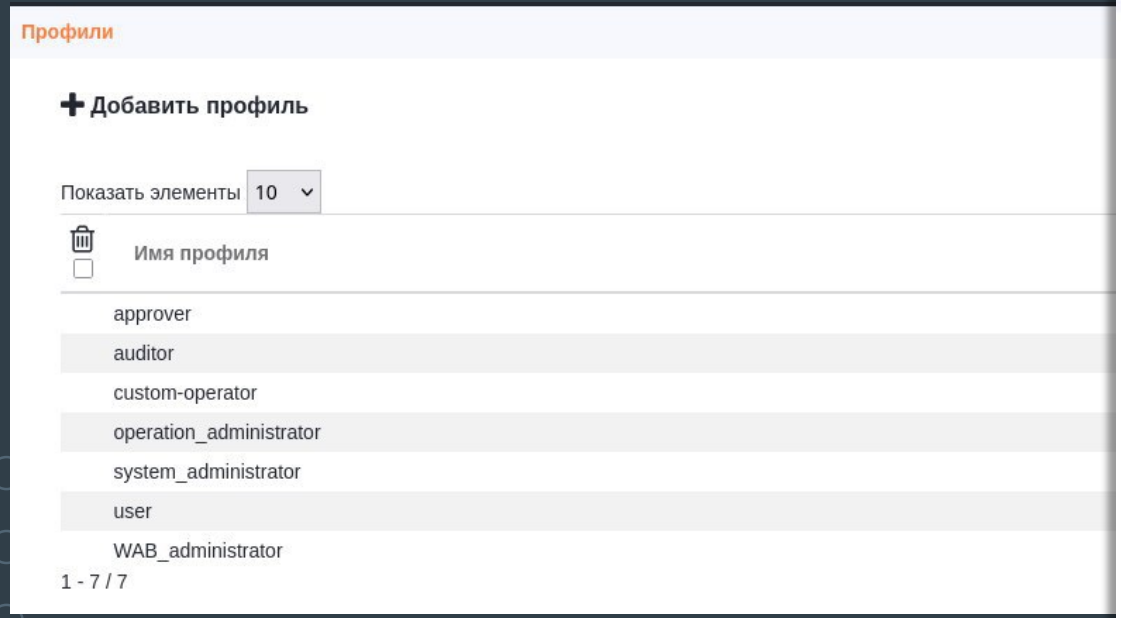
Организация доступов

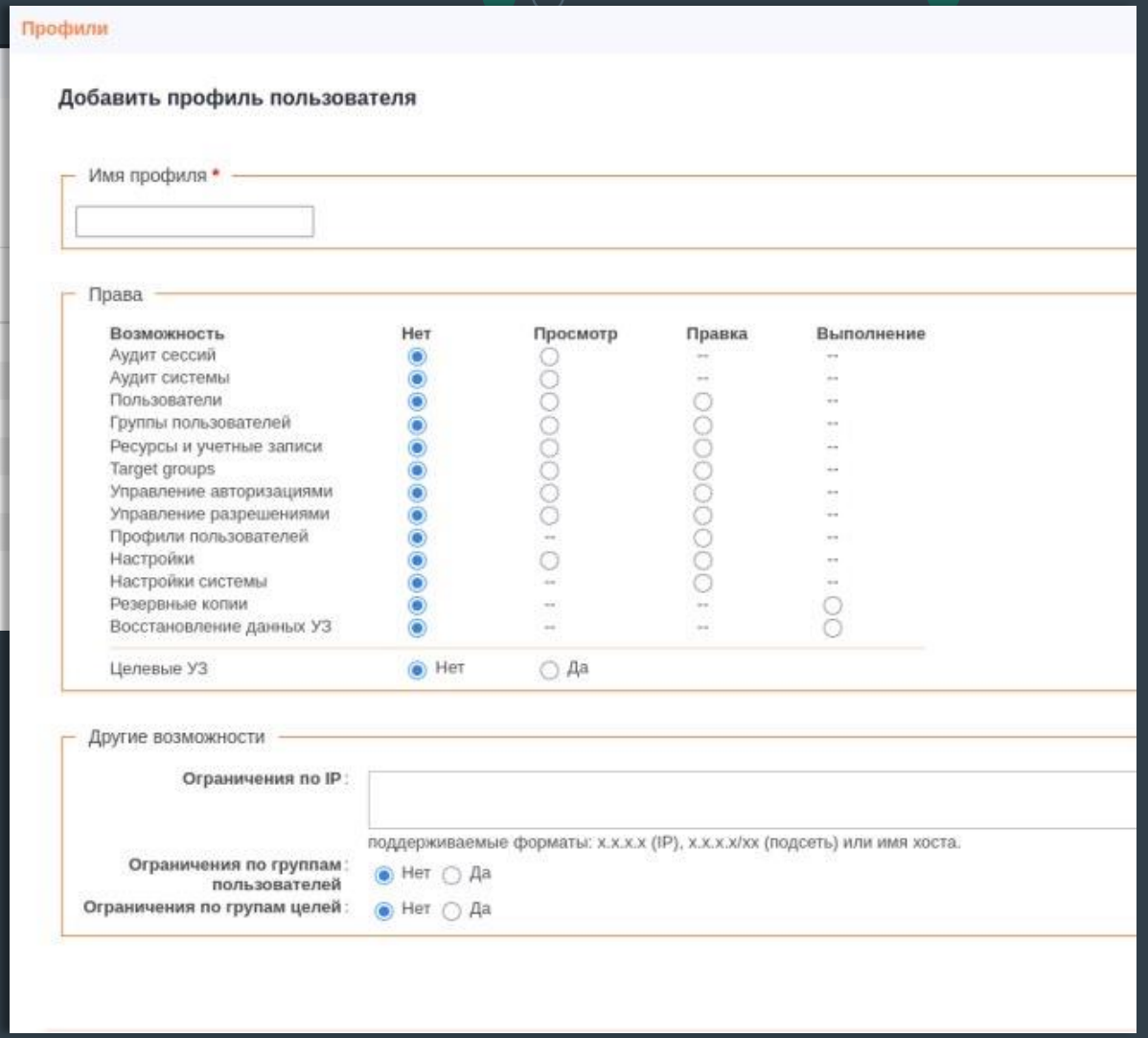
С возможностью подключения пользователей через веб-интерфейс и стандартные клиенты подключения (терминвл, CMD, MSTSC, Remmina и пр.).

www.it-bastion.com

ПРИСВОЕНИЕ И СОЗДАНИЕ РОЛЕЙ

АЙТИБАСТИОН





Список ролей по умолчанию

Однозначная идентификация прав в системе «из коробки»

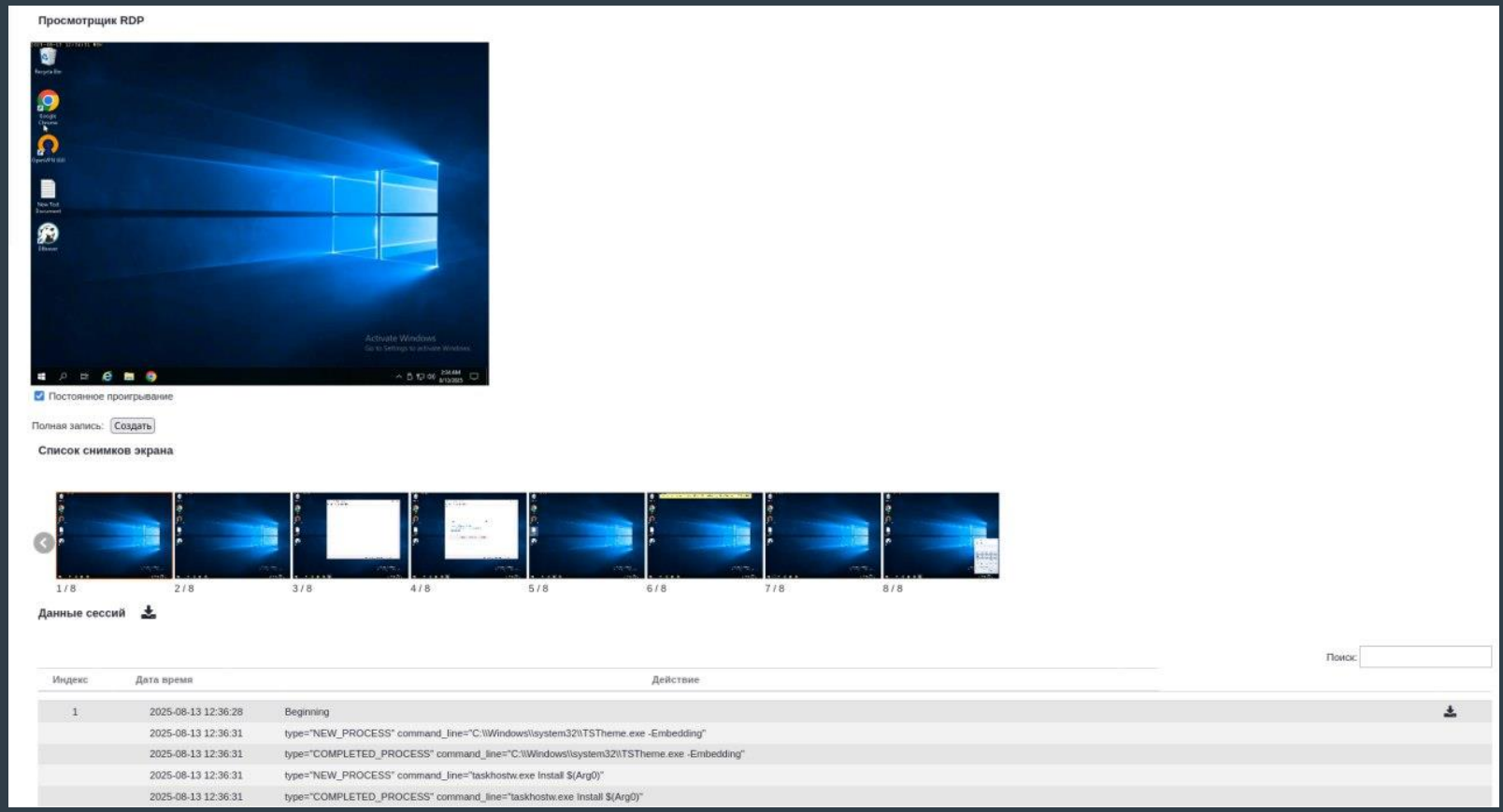
Уникальная роль

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

www.it-bastion.com

ЗАПИСЬ И ПРОСМОТР СЕССИИ

АЙТИБАСТИОН



Видеозапись сессии

С фрагментацией по интервалам времени или запускаемым процессам в сессии

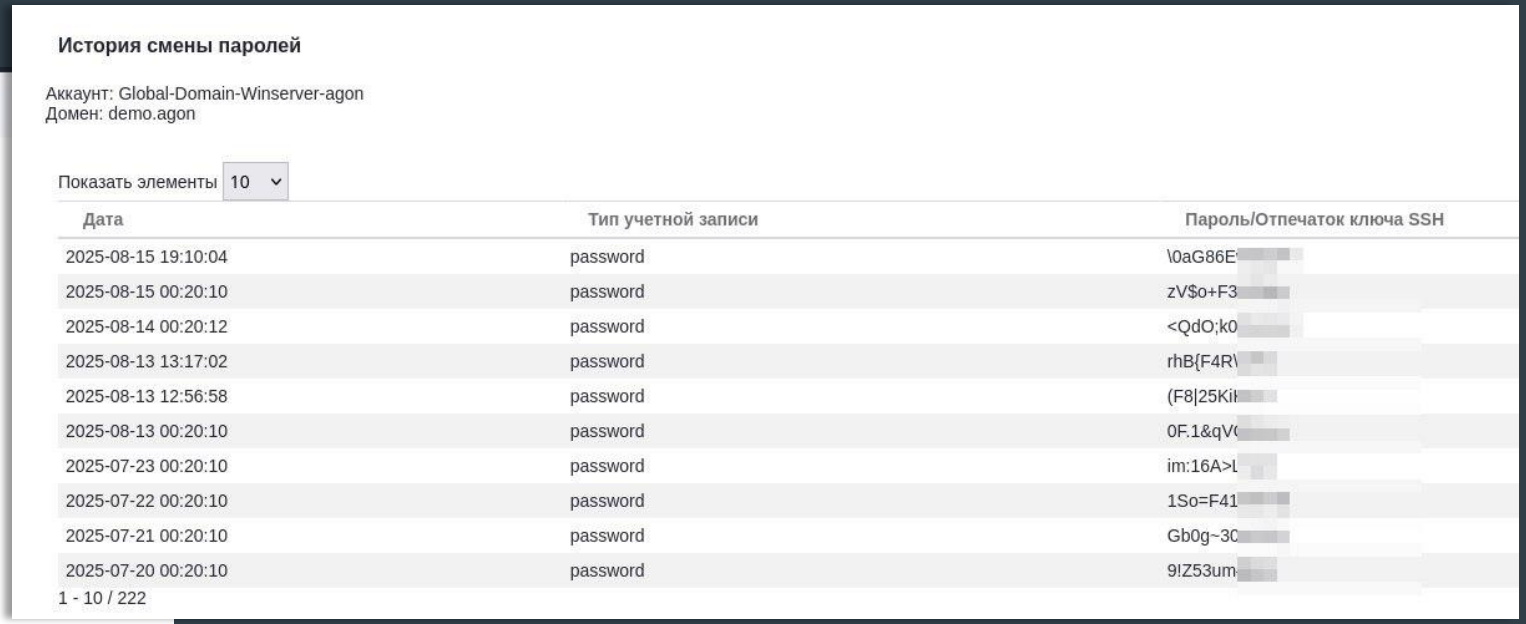
Мета-информация сессии

С индексацией процессов, фиксацией клавиатурного ввода, заголовков окон, нажатия клавиш и др.

www.it-bastion.com

УПРАВЛЕНИЕ ПАРОЛЯМИ

АЙТИБАСТИОН



- 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).

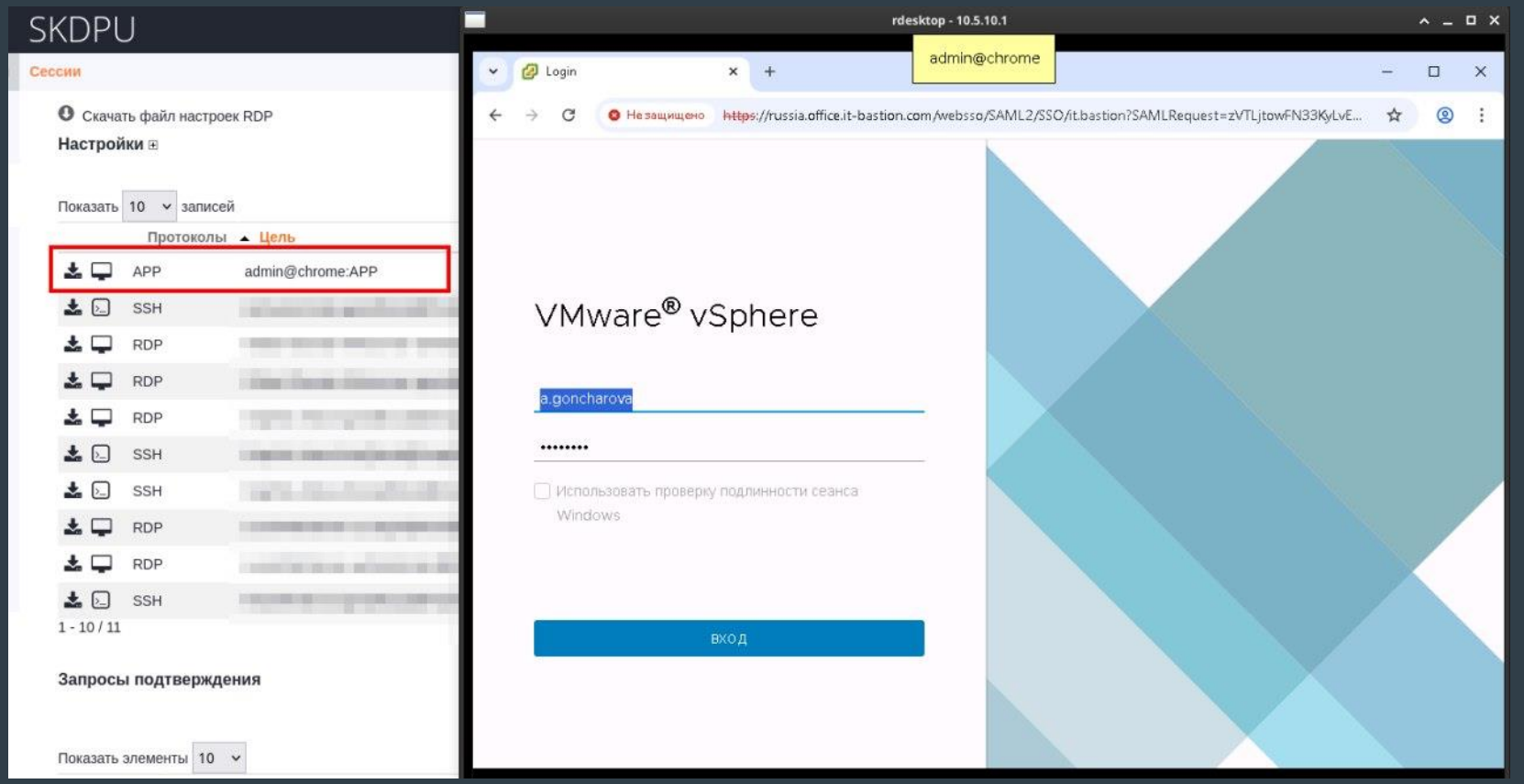
www.it-bastion.com

КОНТРОЛЬ ПРИЛОЖЕНИЙ И УЗ В НИХ

АЙТИБАСТИОН

Подключение к конечным приложениям

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



www.it-bastion.com

СКДПУ НТ
APE (БРАУЗЕР ПО ТРЕБОВАНИЮ) *MVP

АЙТИБАСТИОН

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.

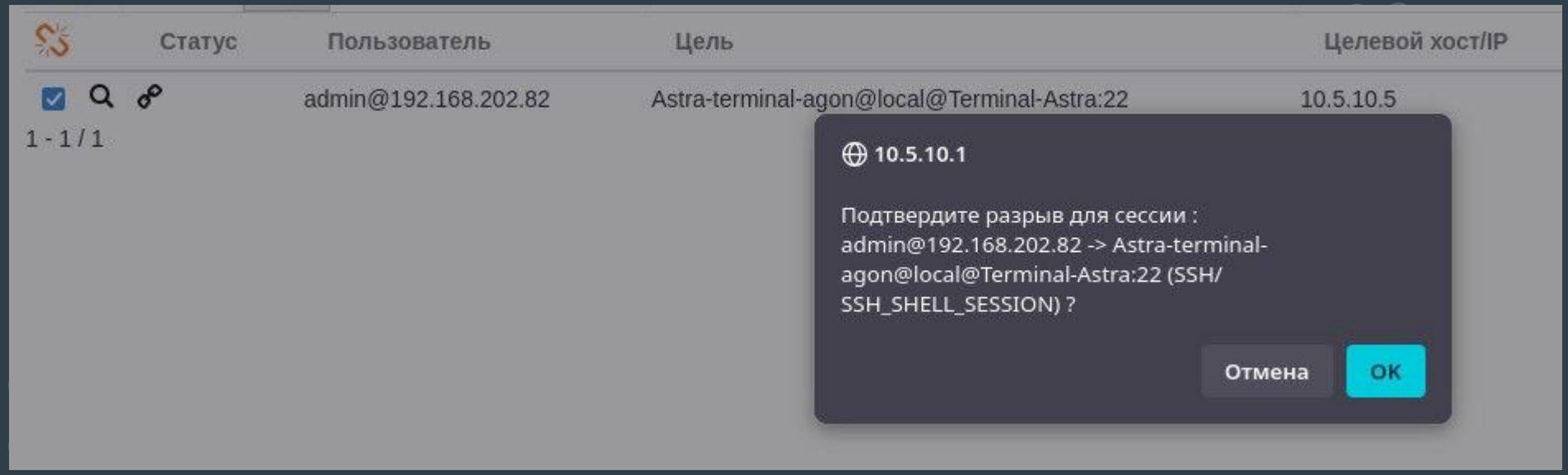
СКДПУ НТ
Шлюз доступа

Astra Linux
APE

Конечный
WEB ресурс

РАЗРЫВ СОЕДИНЕНИЯ

АЙТИБАСТИОН



Блокировка пользовательской сессии
вручную администратором или с автоматическим паттерном реагирования

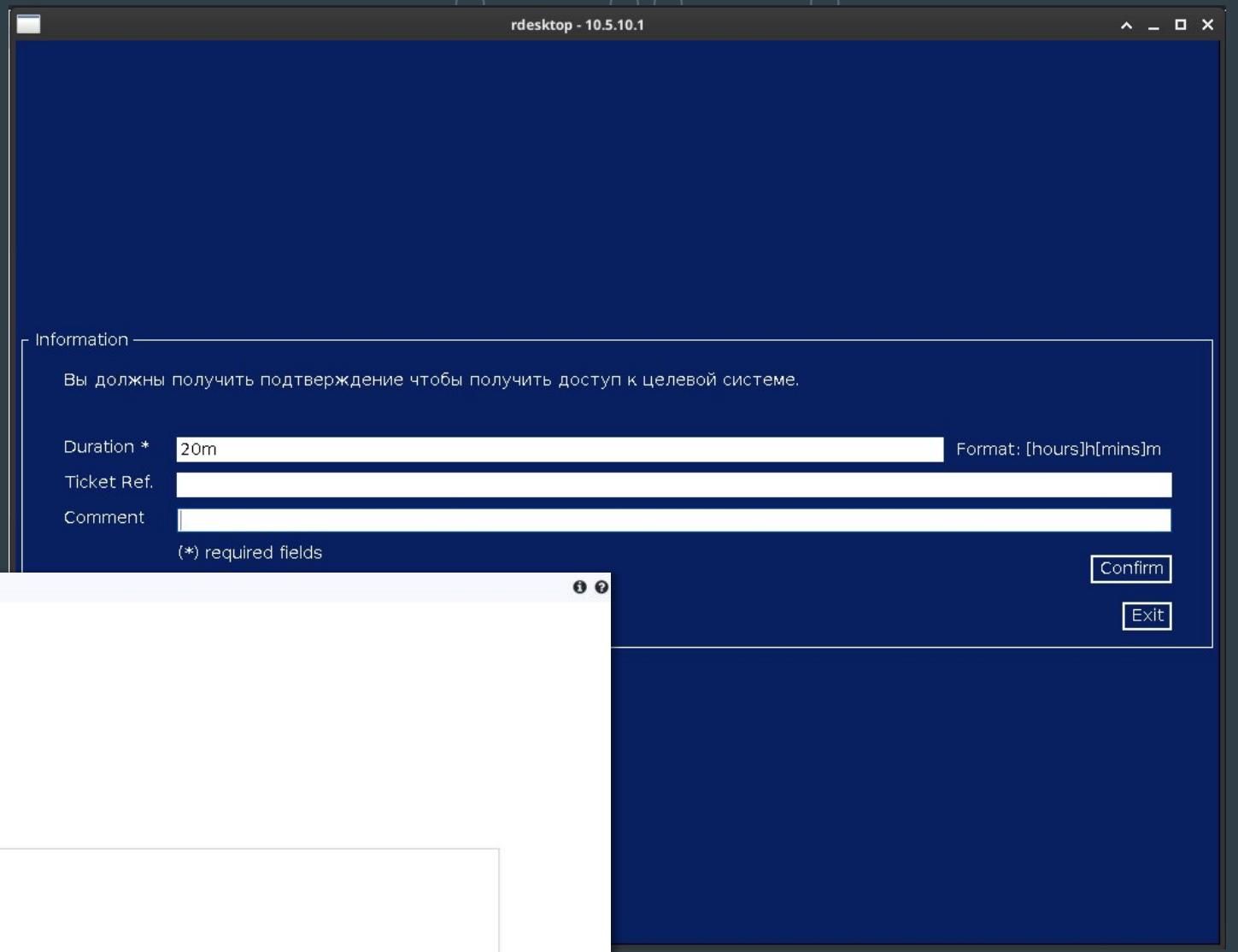
```
2025-08-13 12:40:59 type="KILL_PATTERN_DETECTED" pattern="rm"
2025-08-13 12:40:59 type="SESSION_DISCONNECTION" duration="0:06:16"
```

ПОДТВЕРЖДЕНИЕ ДОСТУПА

АЙТИБАСТИОН

Запрос обоснования необходимости подключения у пользователя

Подтверждение подключения одним или более администратором

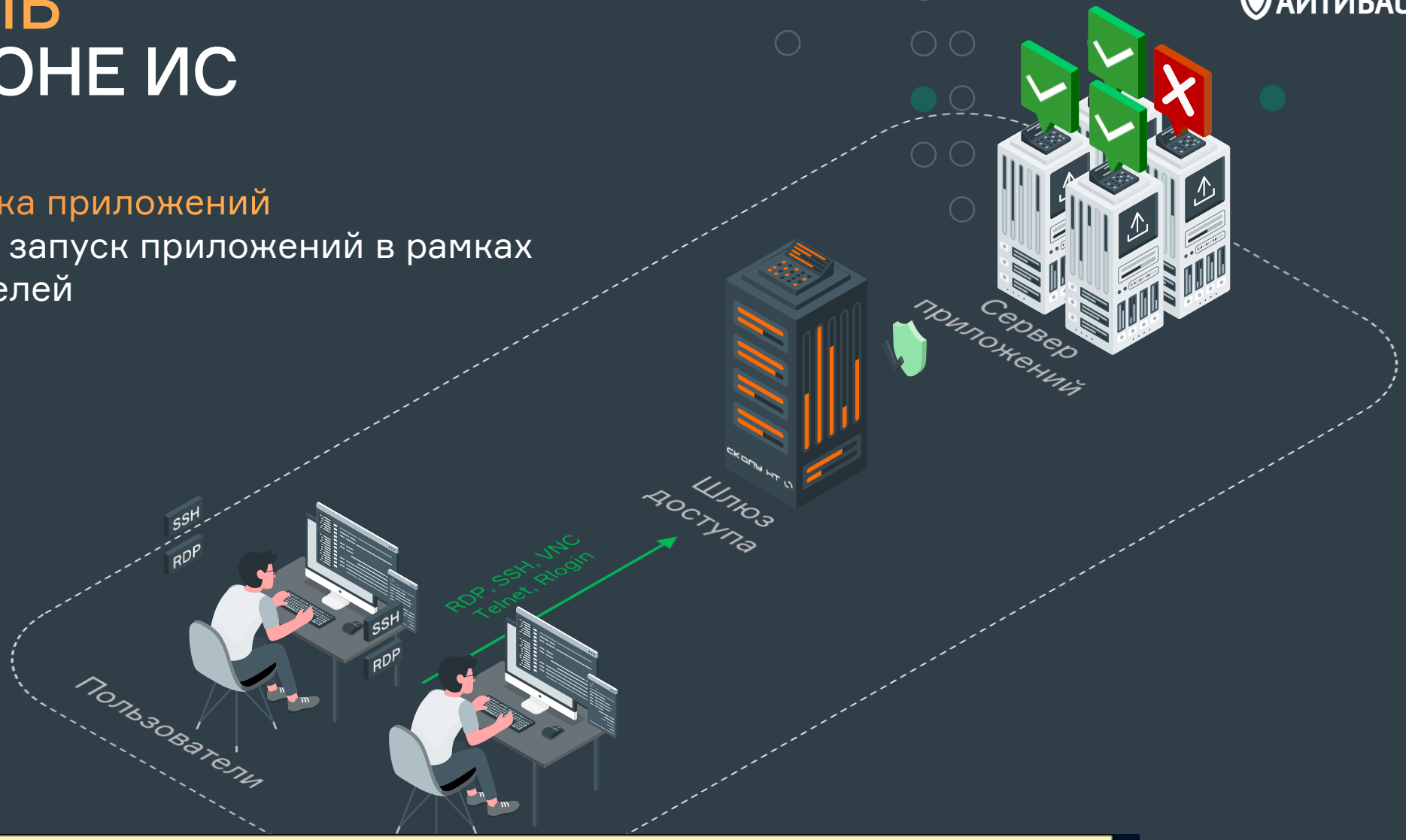


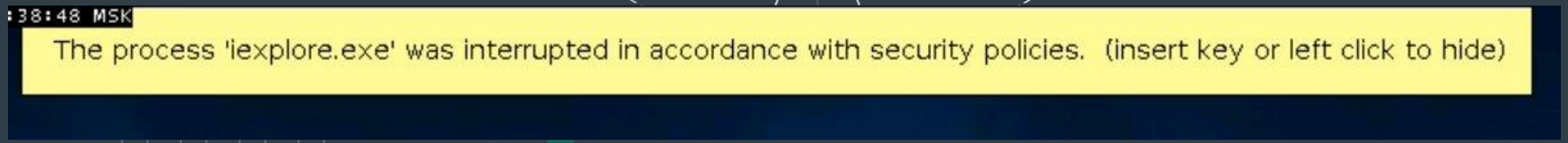
КОНТРОЛЬ НА СТОРОНЕ ИС

АЙТИБАСТИОН

Блокировка запуска приложений

Можем запрещать запуск приложений в рамках сессий пользователей

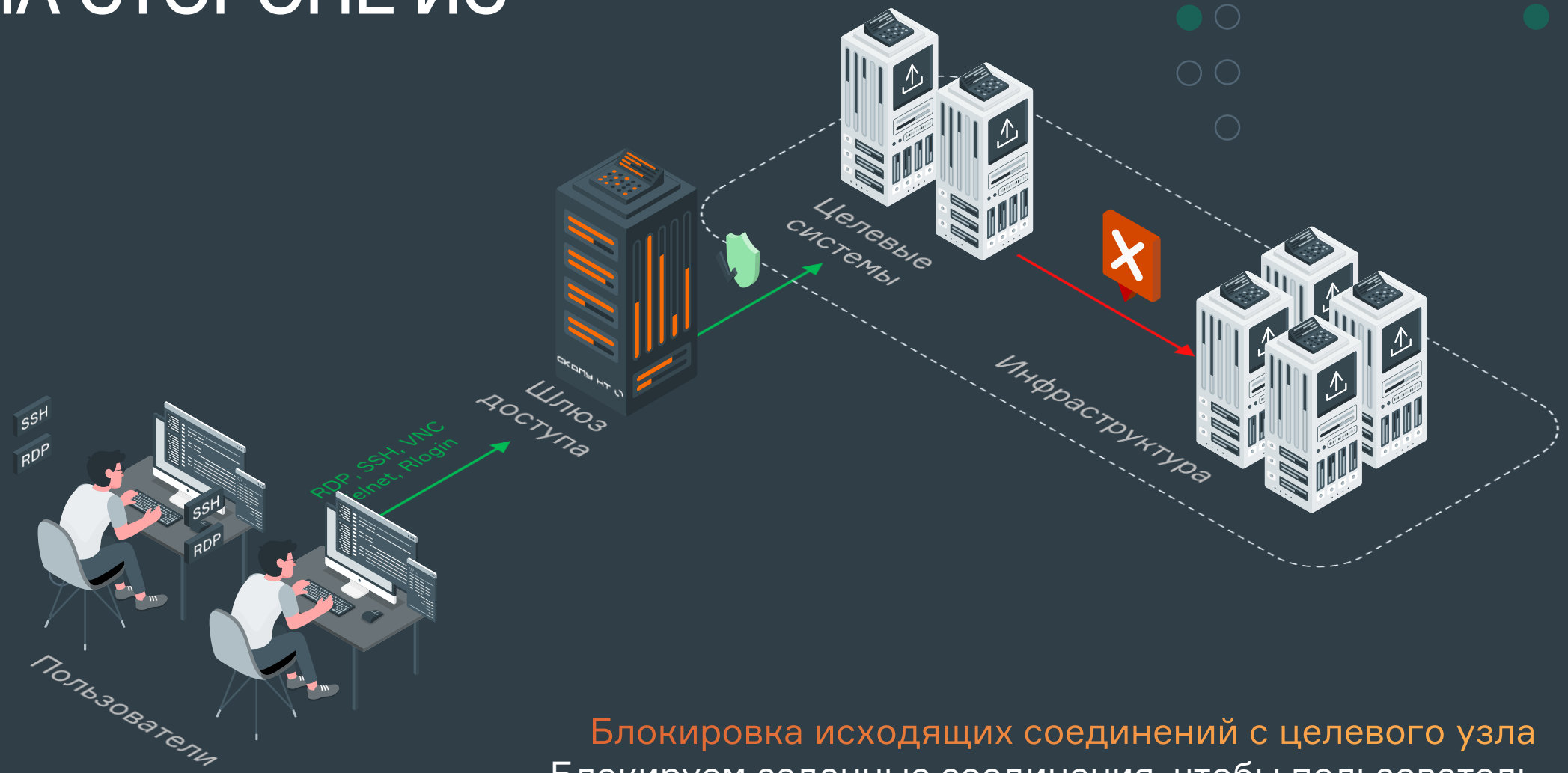




www.it-bastion.com

КОНТРОЛЬ НА СТОРОНЕ ИС

АЙТИБАСТИОН



Блокировка исходящих соединений с целевого узла

Блокируем заданные соединения, чтобы пользователь не имел доступ во всю внутреннюю сеть

www.it-bastion.com

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ
СКДПУ НТ МОНИТОРИНГ И АНАЛИТИКА

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 МАСШТАБИРОВАНИЕ

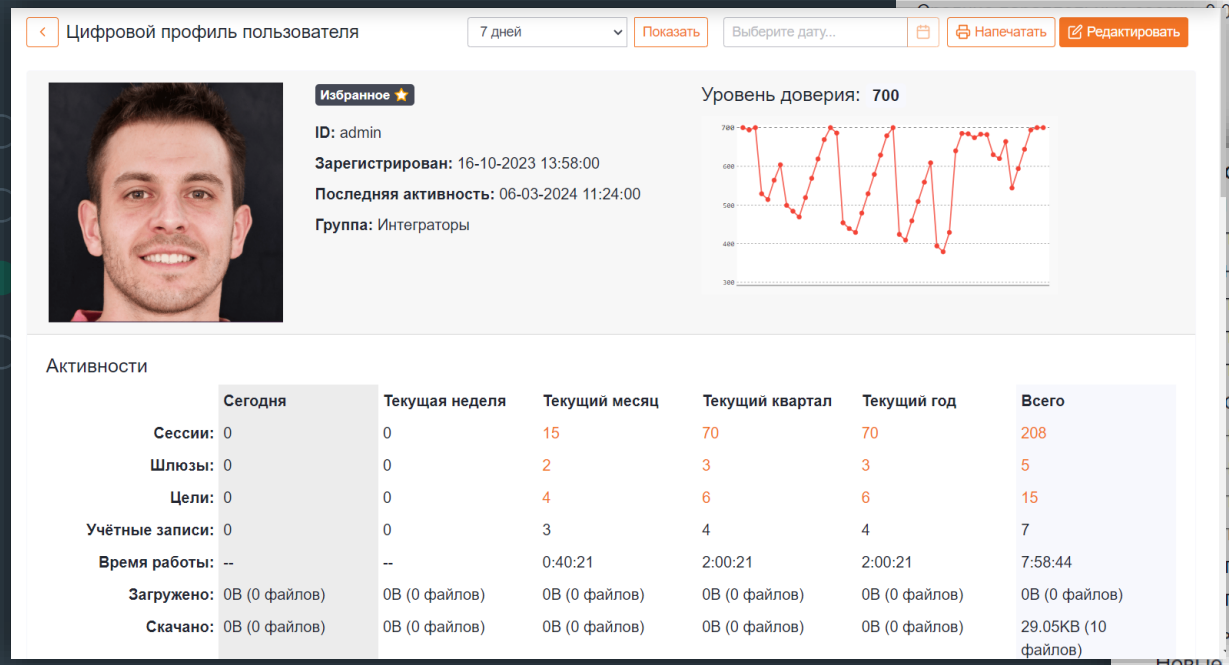
Возможность построения действительно отказоустойчивых инсталляций, в т.ч. распределенных между городами и странами. Легкая возможность наращивать мощности как вертикально, так и горизонтально без привязки к территориальному расположению узлов.

www.it-bastion.com

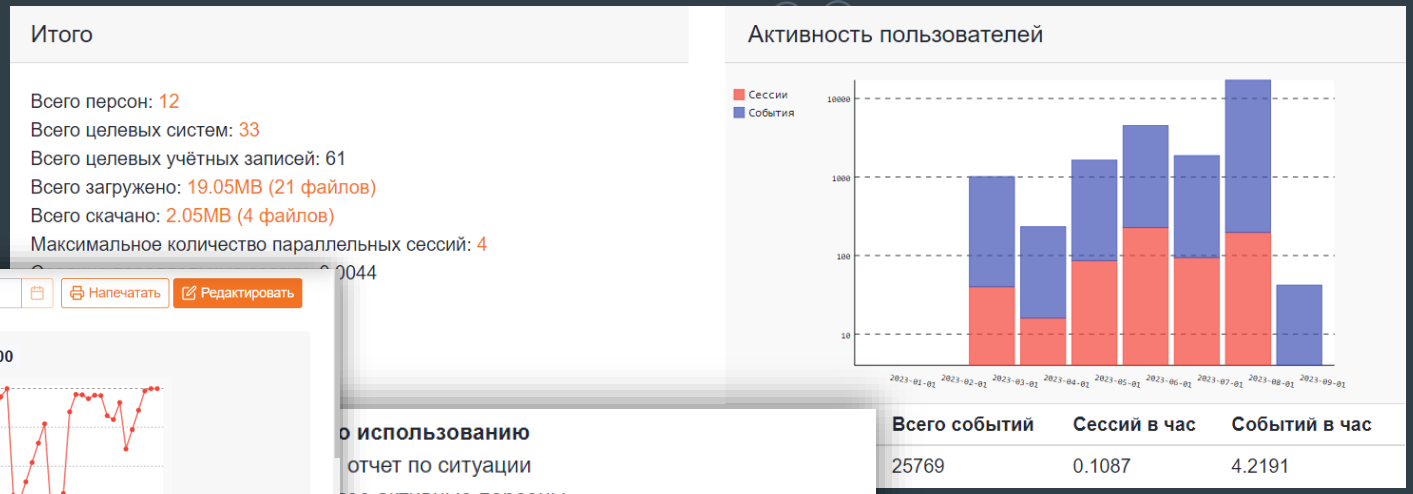
РАМ-ПЛАТФОРМА СКДПУ НТ
МОНИТОРИНГ И АНАЛИТИКА

АЙТИБАСТИОН

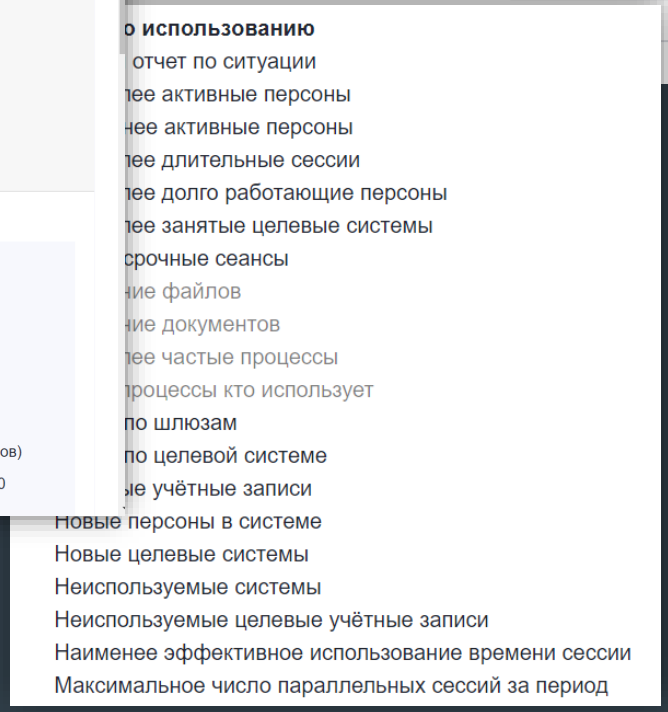
Единая точка мониторинга и аудита для нескольких площадок.
Графическое представление событий в сессиях.



	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:	0B (0 файлов)	0B (0 файлов)	0B (0 файлов)	0B (0 файлов)	0B (0 файлов)	0B (0 файлов)
Скачано:	0B (0 файлов)	0B (0 файлов)	0B (0 файлов)	0B (0 файлов)	0B (0 файлов)	29.05KB (10 файлов)



Всего событий	Сессий в час	Событий в час
25769	0.1087	4.2191



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

Обширная библиотека отчётов для ретроспективного анализа сессий и состояния инфраструктуры

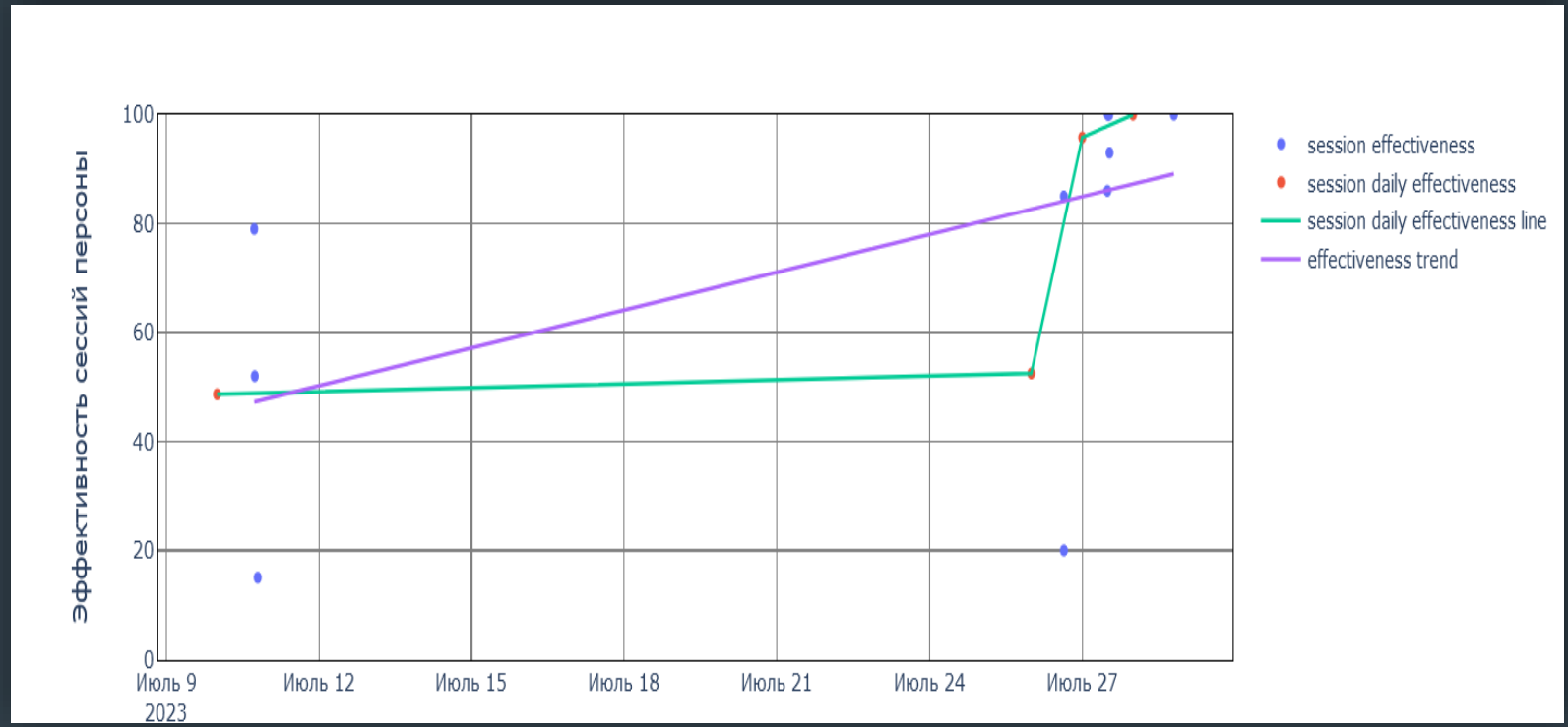
www.it-bastion.com

РАМ-ПЛАТФОРМА СКДПУ НТ
МОНИТОРИНГ И АНАЛИТИКА

АЙТИБАСТИОН

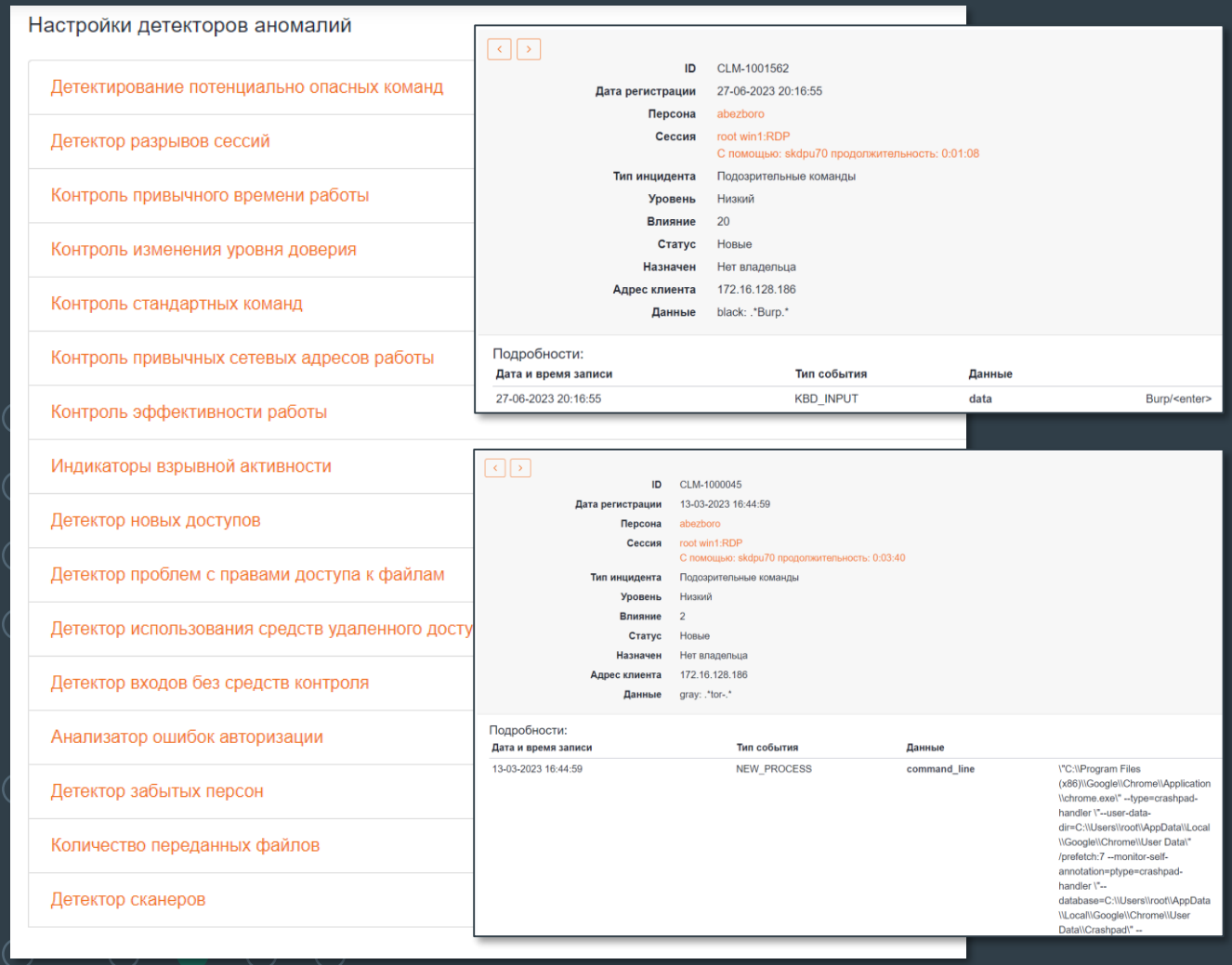
График эффективности

В цифровом профиле пользователя оценить общую эффективность работы на протяжении времени



РАМ-ПЛАТФОРМА СКДПУ НТ
МОНИТОРИНГ И АНАЛИТИКА

АЙТИБАСТИОН



Индивидуальные модели реагирования

Подключение функций реагирования на инциденты и интеграция в единую систему реагирования

Взаимодействие с SOAR/IRP

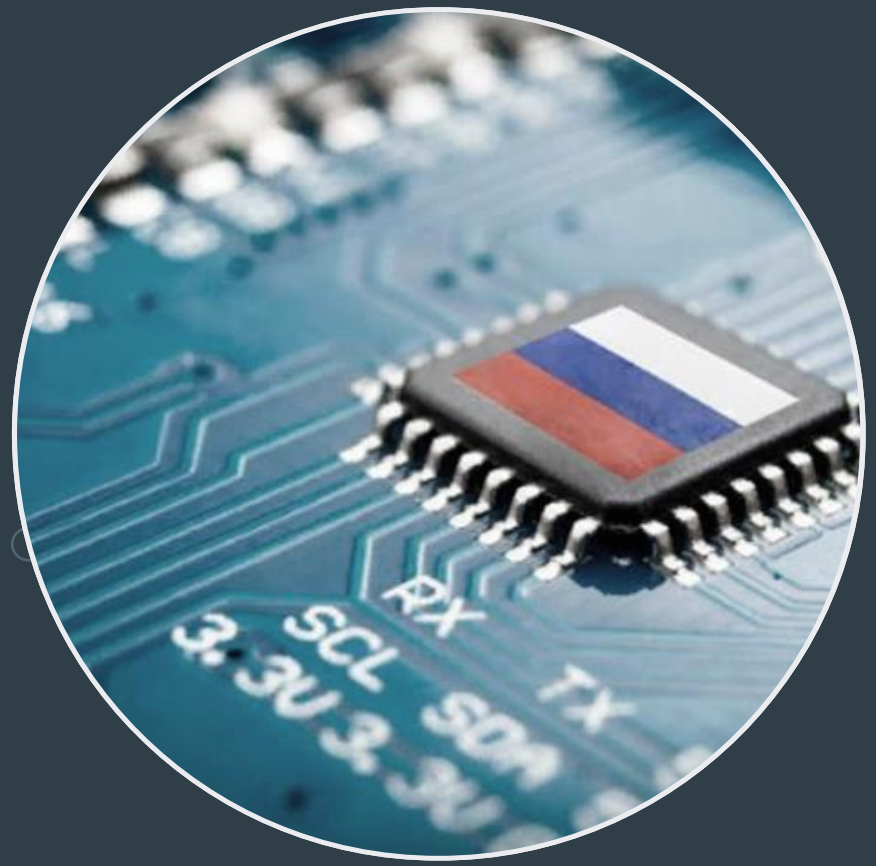
```
do
incident=$(echo "${incident}" | base64 --decode)
session_id=$(echo "${incident}" | jq -r '.data.event.session_id')
event_type=$(echo "${incident}" | jq -r '.data.event.event_type')
incident_id=$(echo "${incident}" | jq -r '.data.indent')
incident_link=$(echo "${incident}" | jq -r '.incident_link')

    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
```

www.it-bastion.com

СЕРТИФИКАЦИЯ
СКДПУ НТ

АЙТИБАСТИОН



Сертификация

ФСТЭК России

Работа продукта на базе отечественной операционной системы Astra Linux SE

ASTRA LINUX®

www.it-bastion.com

СКДПУ НТ
СУММАРНЫЙ ЭФФЕКТ

АЙТИБАСТИОН

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

www.it-bastion.com

АЙТИБАСТИОН

Благодарю за внимание!

Гончарова Алекандра
инженер поддержки продаж

a.goncharova@it-bastion.com

+7 499 322 3667

it-bastion.com

www.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

Телеграм-канал
«Мнение интегратора»