

kaspersky



Kaspersky Industrial
Cybersecurity
Conference 2020

Константин Родин

Руководитель технического центра,
ООО «АйТи Бастион»

#KasperskyICS

Чат конференции: <https://kas.pr/kicscon>



kaspersky

Реализация контроля удаленного доступа администраторов к элементам инфраструктуры. Интеграция с KICS

IT-Bastion
2020



Kaspersky Industrial
Cybersecurity
Conference 2020

- Российская компания (без участия иностранного капитала);
- Более 70 крупных заказчиков и успешно реализованных проектов;
- Более 60 партнеров – интеграторов;
- Разработчик СКДПУ ИТ – Системы контроля действий поставщиков ИТ-услуг.

Заказчики



ПРАВИТЕЛЬСТВО МОСКВЫ



МИНИСТЕРСТВО ТРАНСПОРТА
РОССИЙСКОЙ ФЕДЕРАЦИИ



Очевидные проблемы и риски удаленного доступа

Персонал

Присутствие, подготовка и дежурные смены

Доступ и доверие

Многие сотрудники – многие печали

Удаленный доступ

Не всегда можно, но часто нужно

Регуляторы

Соответствие требованиям нескольких ФЗ

Задачи



Какие задачи ставятся при организации
безопасного удаленного доступа

- **Снижение простоев за счет оперативного обслуживания**
- **Снижение требований к персоналу**
- **Автоматизация контроля SLA**
- **Защита собственных специалистов**

- Управление рисками безопасности и соответствие требований регуляторов
- Сбор и фиксация данных для возможных расследований в будущем
- Управление доступом и правами, контроль изменений.
- Разграничение зон ответственности между ИТ и ИБ.

1. Увеличение количества обслуживаемых ИС – увеличение штата сотрудников «на местах»;
2. Человек с доступом к ИС – потенциальная угроза;
3. Человек с доступом к ИС «удаленно» – потенциальная угроза вдвойне;
4. Инфраструктура объектов КИИ – требует соответствия требованиям по КИИ
5. ИБ решение не должно мешать решениям ИТ
(в нормальных условиях)

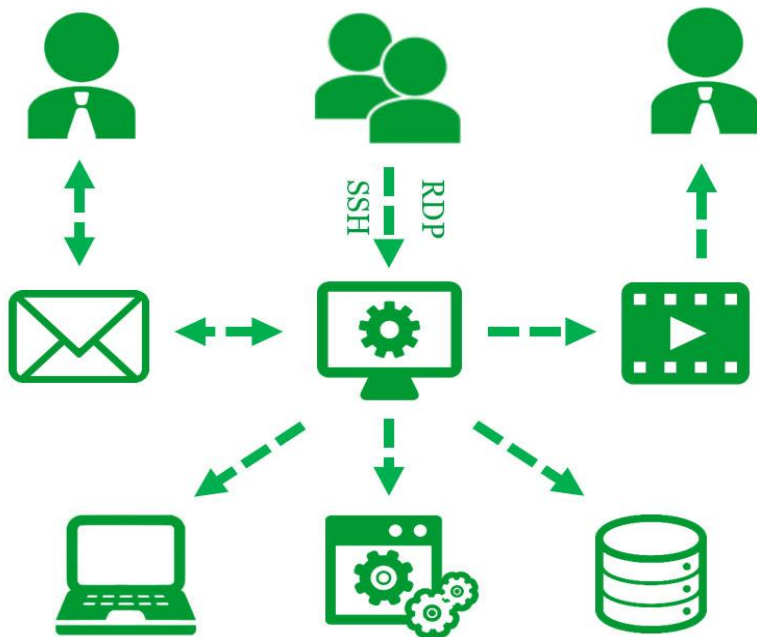
Сценарии использования

The background features a detailed technical schematic of a piping system. It includes various components such as pumps, valves, tanks, and flow lines, all rendered in a light teal color against a darker teal background. A large, dark silhouette of a hand is superimposed over the center of the diagram, with its fingers pointing towards the text. The overall aesthetic is technical and industrial.

- Узел удаленного доступа
- Запись и онлайн мониторинг действий
- Контролируемый доступ по согласованию;
- Удалённый доступ в нерабочее время;
- Выявление опасных команд и приложений;
- Контроль работы подрядчиков и аутсорсеров;
- Управление доступом и политикой паролей

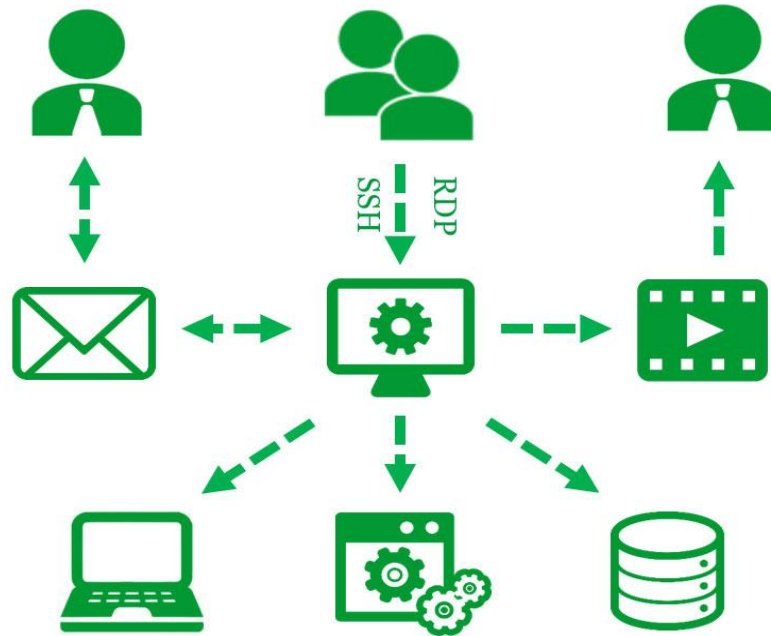
Узел удаленного доступа

12



- Исполнитель видит только разрешенные варианты входа
- Можно не выдавать настоящие пароли
- Запись всех действий
- Личный и автоматизированный контроль

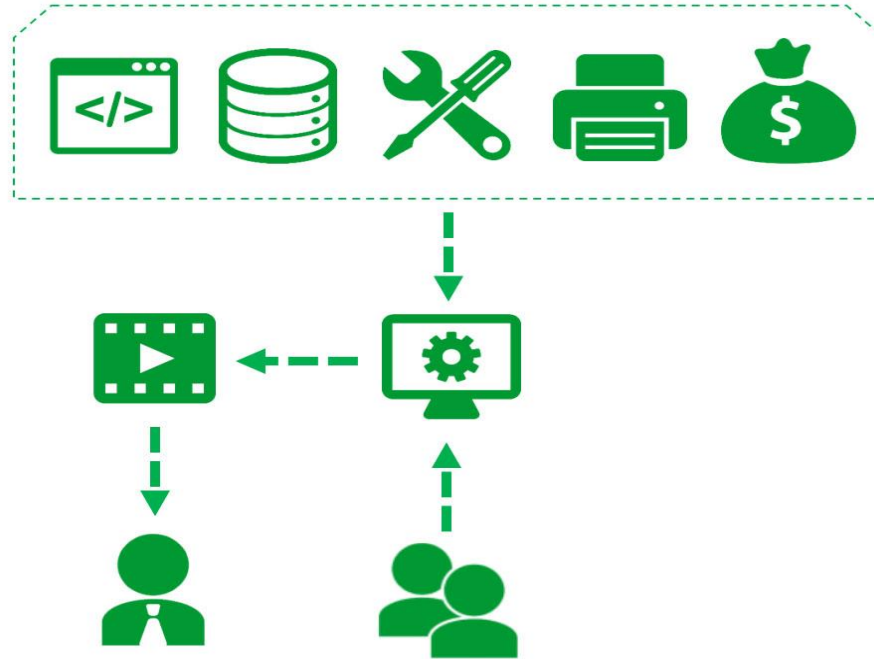
Доступ по согласованию



- Уведомление ответственных лиц
- Голосование за доступ на определенное время
- Возможность отозвать разрешение

Публикация приложений

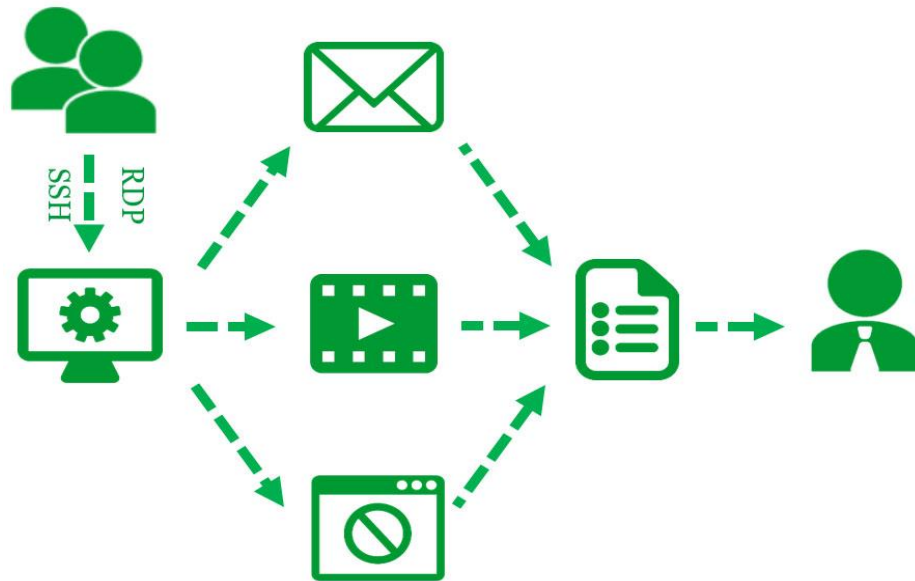
14



- Доступ только к одному приложению
- Контроль нажатия кнопок и ввода текста в диалогах.
- Контроль администраторов приложений

Контроль подрядчиков и аутсорсеров

15



- Скрытие паролей и ключей от исполнителя
- Автоматизированный контроль состава команд
- Отчеты для контроля SLA
- Согласования для доступа

Интеграция

The image features a detailed technical schematic of a hydraulic or pneumatic system. The diagram is rendered in a light teal color against a darker teal background. It includes various components such as pumps, valves, cylinders, and connecting lines. A large, dark silhouette of a hand is superimposed over the center of the diagram, with its fingers pointing towards the right. The word 'Интеграция' (Integration) is written in large, white, bold Cyrillic letters across the top left portion of the image.

- SIEM
- AV\DLP\Sandbox (контроль файлов)
- Многофакторная авторизация
- Однонаправленные шлюзы
- Оркестраторы и автоматизация

и **KICS**

Соединение есть, контроля нет

18

- Интеграция по API
- Контроль все-таки есть

ID	DL-1000193
Дата регистрации	2020-08-13 16:16:54
Тип	DIRECT_LOGIN
Уровень	Высокий
Статус	Новые
Назначен	Нет владельца
Данные	Remote TCP connection from: 172.16.30.63:58348 to: 10.100.101.63:3389

:

аписи	Тип события	Данные
6:33	DIRECT_LOGIN	dst_mac: 00:0c:29:b6:55:8e id: 483587 src_ip_port: 58348 ipv4_type: 2 ether_type: 1 proto: TCP src_mac: 64:d1:54:f1:65:fb dst_ip_port: 3389 title: Обнаружено неразрешенное сетевое взаимодействие dst_ip_addr: 10.100.101.63 src_ip_addr: 172.16.30.63

- **Возможность войти напрямую с сохранением контроля**
- **Анализ и детектирование сессий в обход СКДПУ НТ**
- **Без агентское решение контроля для критических ИС**

Свойства



Ключевые свойства решения СКДПУ НТ

ЕДИНАЯ ТОЧКА ДОСТУПА

Единая точка доступа в инфраструктуру (SSO). Гибкая ролевая модель доступов с возможностью интеграции в существующую инфраструктуру (LDAP, AD, Radius).

БЕЗ УСТАНОВКИ АГЕНТОВ

Подключение к ЦУ без необходимости установки агентов, особенно важна при подключении к объектам КИИ.

РАБОТА ПО ЗАЯВКАМ И ПОДТВЕРЖДЕНИЯМ ДОСТУПА

Возможность просмотра открытой сессии в режиме реального времени, а так же её прерывания в ручном режиме или по обнаружению подозрительных действий или команд.



ЗАПИСЬ СОБЫТИЙ ДОСТУПА

Полная запись видео и метаданных сессий с созданием долгосрочного архива. Максимальный объем информации в рамках сессий, с возможностью её передачи во внешний SIEM.

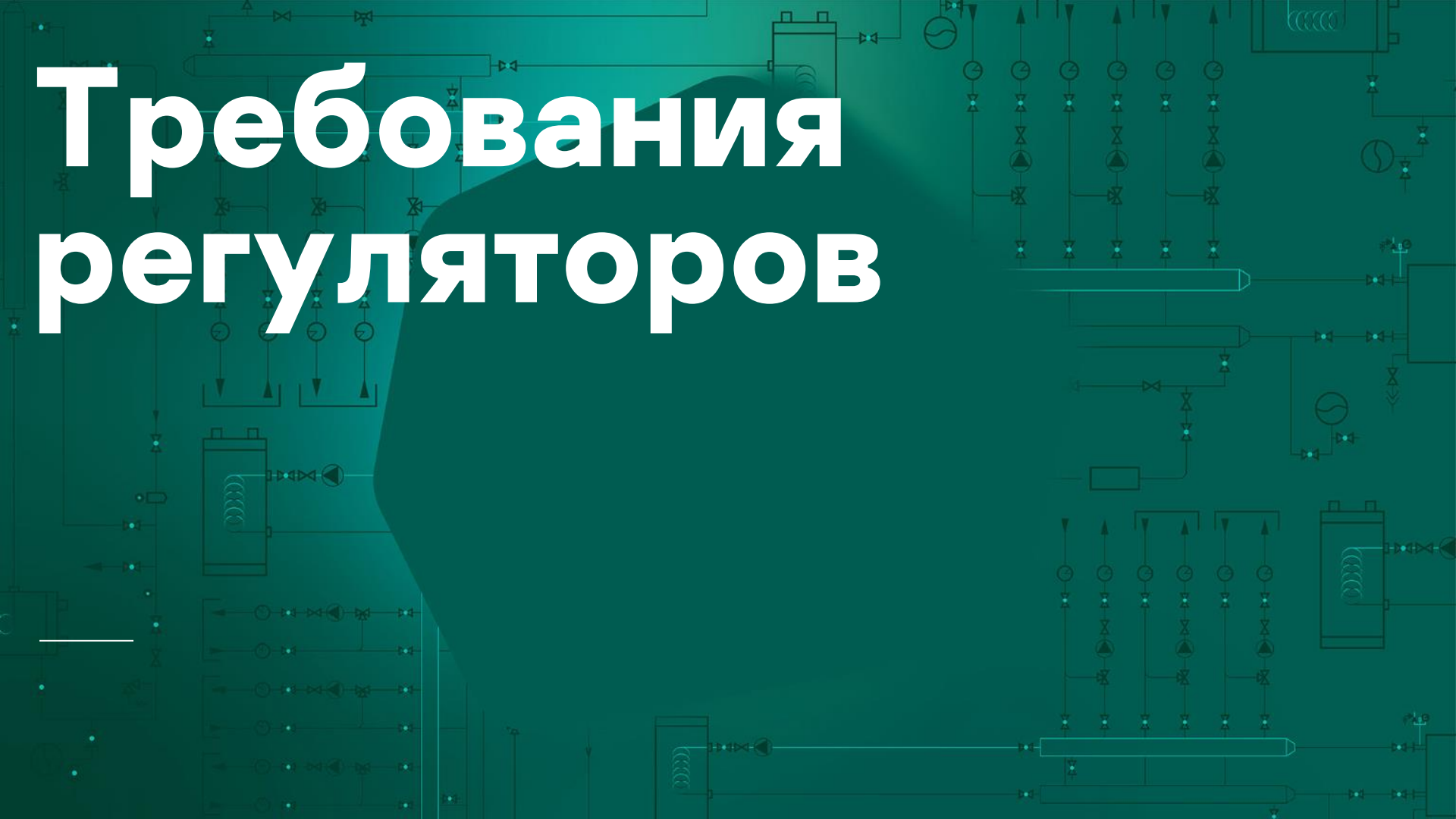
УПРАВЛЕНИЕ ПАРОЛЯМИ

Управление паролями целевых учетных записей без необходимости установки агентов на целевые устройства по настраиваемым политикам.

ПРОСМОТР И ПРЕРЫВАНИЕ СЕССИЙ

Возможность просмотра открытой сессии в режиме реального времени, а так же её прерывания в ручном режиме или по обнаружению подозрительных действий или команд.

Требования регуляторов

The background of the image is a complex technical diagram in shades of teal and green. It features a network of lines representing pipes or electrical connections, with various symbols such as pumps, valves, and tanks. A large, dark silhouette of a human brain is positioned in the center, overlapping the diagram. The text 'Требования регуляторов' is written in a large, bold, white sans-serif font across the upper left portion of the image.

Контроль администраторов и ...

Простота запуска и работы

Шлюз протоколов удаленного доступа

Поведенческий анализ

Поиск и сигнализация об отклонениях от обычного порядка

Масштабируемость

На мощность, надежность и гео-распределение

Интеграция

с разными уже существующими средствами

Спасибо за внимание

info@it-bastion.com

+7(499) 322-3767