

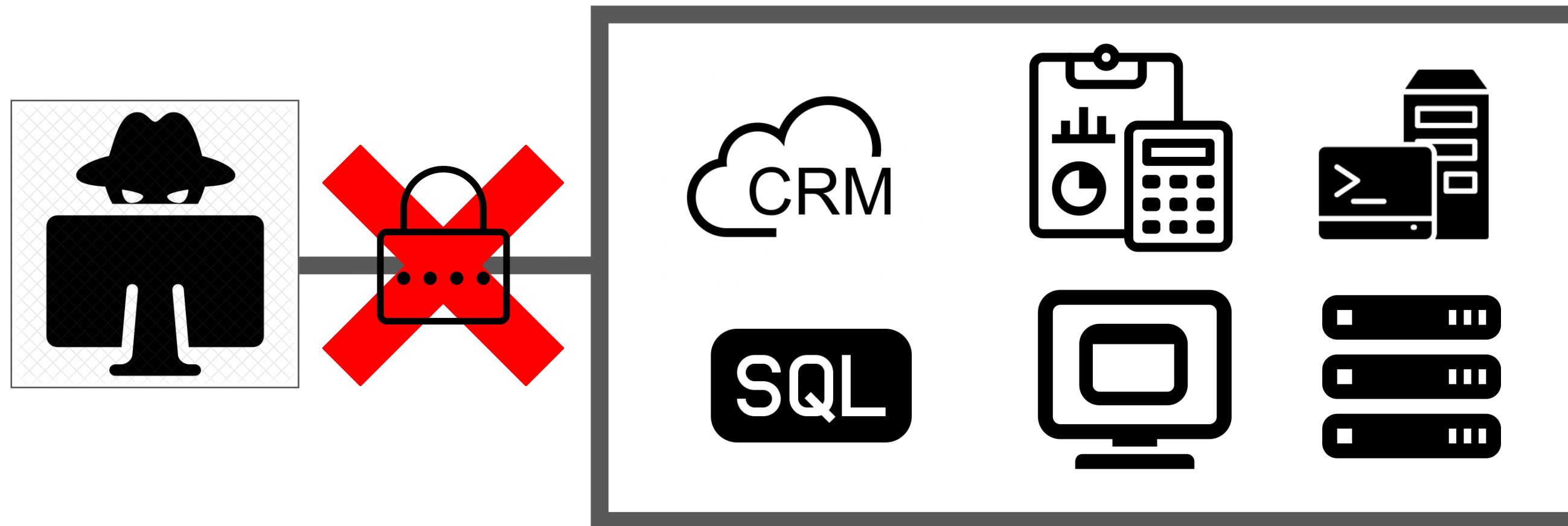
sRacе: масштабируемая РАМ система с широким функционалом

Обеспечение контролируемого и безопасного доступа к ИТ-инфраструктуре



Информация - цель киберпреступников

Данные ИТ-сервисов цель атак киберпреступников



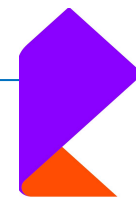
**Главная точка атаки –
неконтролируемые привилегии**

Проблема

Несанкционированный привилегированный доступ к ИТ-системам приводит к росту числа успешных кибератак. Следствием этого является утеря данных, утечка конфиденциальной информации, финансовые и репутационные потери Компаний

infosecurity

Практически 100% продвинутых кибератак связаны с кражей и использованием привилегированных учетных записей



Ростелеком
Солар

100% российских средних и крупных компаний сталкиваются с нарушением прав доступа и вызванными ими кибератаками



Ростелеком
Солар

55% нарушений прав доступа приводят к утечке конфиденциальной информации компании

verizon✓

Злоупотребление привилегированным доступом - второй по частоте инцидент информационной безопасности

В большинстве компаний никто не может быть уверен в безопасности привилегированных учетных данных

Почему РАМ нужен именно сейчас

- ❑ Лавинообразный рост числа сотрудников и внешних подрядчиков которым нужен удаленный доступ
- ❑ Рост ИТ-составляющей в бизнес-процессах компаний
- ❑ Высокий ценовой порог РАМ-решений для большинства компаний

РАМ-система - самый действенный инструмент для предупреждения кибератак

Gartner

К 2024 году 50% организаций внедрят привилегированный доступ

Gartner

Внедрение РАМ - «приоритет №1» в проектах безопасности на ближайшие годы

Kuppingercorle
ANALYSTS

Рынок РАМ-решений вырастет
вырастет с 2,2 млрд.\$ в 2020 до
4,5 млрд.\$ к 2025

Проблема

Традиционные РАМ-системы

- ❑ Прежде всего системы хранения и обеспечения жизненного цикла привилегированных учетных записей
- ❑ В основном ориентированы на работу с администраторами ИТ-систем, контроль их действий и расследования инцидентов связанных с компрометацией привилегированного доступа
- ❑ Имеют ограниченный набор поддерживаемых «из коробки» контролируемых ИТ-систем.

**Процесс внедрения это длительный
трудоемкий процесс который не всегда
удается довести до конца.**

«Идеальный РАМ» глазами заказчиков

- ❑ Поддержка всех ИТ систем в организации
- ❑ Безопасность
- ❑ Простота внедрения
- ❑ Простота использования

Основной функционал по управлению привилегиями работает надежно

Просто интегрировать новые объекты администрирования

Просто разворачивать и быстро внедряется

Не только безопасный, но и простой в использовании

Можно использовать с другими ИБ-решениями.

Затраты на сопровождение и масштабирование минимальны, сотрудников не нужно обучать работать с системой

Система настолько проста, что с ней могут работать не только ИТ-специалисты, но и бизнес-пользователи

Решение

sPace - система организации контролируемого доступа привилегированных пользователей, обеспечивающая не только безопасность, но и простоту эксплуатации

sPace это:

- ☐ Защита привилегированных учетных данных и снижение рисков кибератак, вызванных их компрометацией
- ☐ «Демократизация» РАМ - снижение порога «вхождения» и минимизация уровня пользовательского опыта, необходимого для работы с РАМ
- ☐ Обеспечение контролируемого доступа не только для администраторов, но и для любого привилегированного доступа
- ☐ Автоматизация управления доступом и повышение продуктивности сотрудников

Принцип минимальных привилегий

- ❑ Привилегированный доступ предоставляется для решения определенной **Задачи** на конкретной целевой системе
- ❑ Доступ предоставляется по запросу с использованием механизма согласования **Нарядов-Допусков**
- ❑ В случае отсутствия согласованного и действующего Наряда-Допуска доступ Пользователя к целевым системам невозможен
- ❑ sPASE позволяет гранулировать доступ и предоставлять **разные права** для решения **различных задач** на конкретной целевой системе
- ❑ Доступ к конкретной задаче предоставляется путем запуска **Сценариев**

Наряд-Допуск

Задача + Пользователь + Полномочия + Период действия

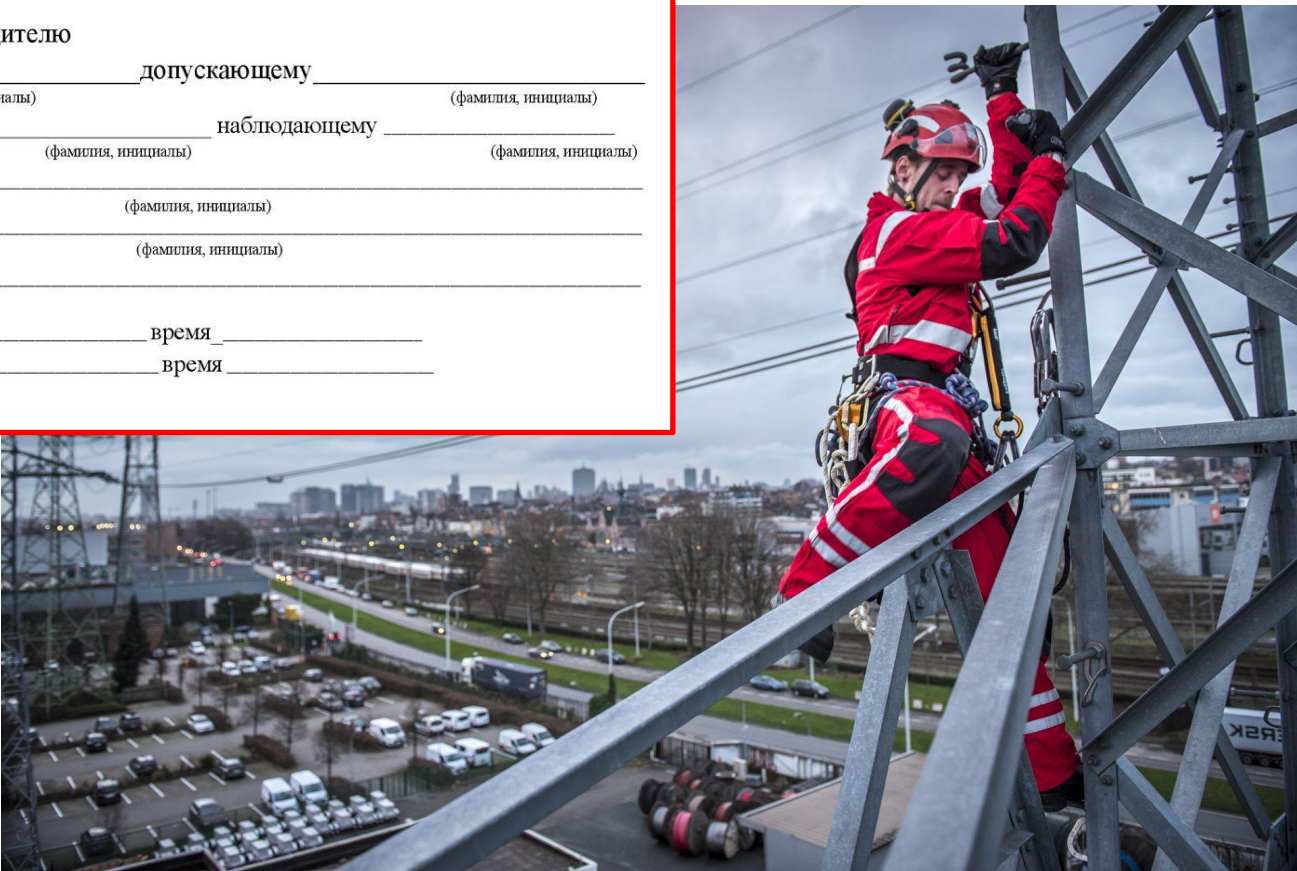
ФОРМА НАРЯДА-ДОПУСКА ДЛЯ РАБОТЫ В
ЭЛЕКТРОУСТАНОВКАХ
И УКАЗАНИЯ ПО ЕГО ЗАПОЛНЕНИЮ

Лицевая сторона наряда (стр. 1)

Организация _____
Подразделение _____

НАРЯД-ДОПУСК № _____
для работы в электроустановках

Ответственному руководителю работ _____ допускающему _____
(фамилия, инициалы) (фамилия, инициалы)
Производителю работ _____ наблюдающему _____
(фамилия, инициалы) (фамилия, инициалы)
с членами бригады _____
(фамилия, инициалы)
_____ (фамилия, инициалы)
поручается _____
Работу начать: дата _____ время _____
Работу закончить: дата _____ время _____



Создание наряда-допуска

Задача :
Администрирование БД Oracle

Доступ для :
test-user (test-user@spacedemo)

Учетные записи :
Введите значения

Период действия :
19.01.2022 16:41 11.02.2022 16:51

Дополнительные настройки времени :
Не задано

Дополнительные действия по истечении НД :
Завершить сеансы Наряда-допуска

Обоснование :
Срочная необходимость

Основание :
Авария на сервере БД

Отключить запись ВСАС

Объекты администрирования :
Oracle Test DB

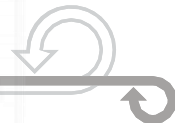
Согласующие :
test-user (test-user)
Федоров Александр (afedorov)

Уведомления email для :
Иванов Семен (test-space-001@...)

Настроить

Согласовать

Закрыть



Задача

Объект + Сценарий запуска + Инструмент

Сценарий 1

```
Описание сценария
Имя: after_launch_si.au3

#include <WinAPI.au3>
#include <MsgBoxConstants.au3>
#include <Date.au3>
#include <File.au3>
#include <StringConstants.au3>

Local Const $ParentFolder = PathFull(@ScriptDir & ".\..\")
Local Const $Regmetadataname = "RegMetaData.exe"
Local Const $Regmetadata = $ParentFolder & $Regmetadataname
Local Const $hlpapi = DllOpen("iphlpapi.dll")
Local Const $DELIMITER = ""

<#if pid??>
Local $IPid = "${pid}"
<#else>
Local $IPid = "${r"${pid}"}"
<#if>
<#if vasilid??>
```

Сценарий 2

```
Описание сценария
Имя: after_launch_si.au3

#include <WinAPI.au3>
#include <MsgBoxConstants.au3>
#include <Date.au3>
#include <File.au3>
#include <StringConstants.au3>

Local Const $ParentFolder = PathFull(@ScriptDir & ".\..\")
Local Const $Regmetadataname = "RegMetaData.exe"
Local Const $Regmetadata = $ParentFolder & $Regmetadataname
Local Const $hlpapi = DllOpen("iphlpapi.dll")
Local Const $DELIMITER = ""

<#if pid??>
Local $IPid = "${pid}"
<#else>
Local $IPid = "${r"${pid}"}"
<#if>
<#if vasilid??>
```

Сценарий 3

```
Описание сценария
Имя: after_launch_si.au3

#include <WinAPI.au3>
#include <MsgBoxConstants.au3>
#include <Date.au3>
#include <File.au3>
#include <StringConstants.au3>

Local Const $ParentFolder = PathFull(@ScriptDir & ".\..\")
Local Const $Regmetadataname = "RegMetaData.exe"
Local Const $Regmetadata = $ParentFolder & $Regmetadataname
Local Const $hlpapi = DllOpen("iphlpapi.dll")
Local Const $DELIMITER = ""

<#if pid??>
Local $IPid = "${pid}"
<#else>
Local $IPid = "${r"${pid}"}"
<#if>
<#if vasilid??>
```

ЗАДАЧА 1 – Настройка базы

ЗАДАЧА 2 - Анализ данных

ЗАДАЧА 3 – Настройка сервера



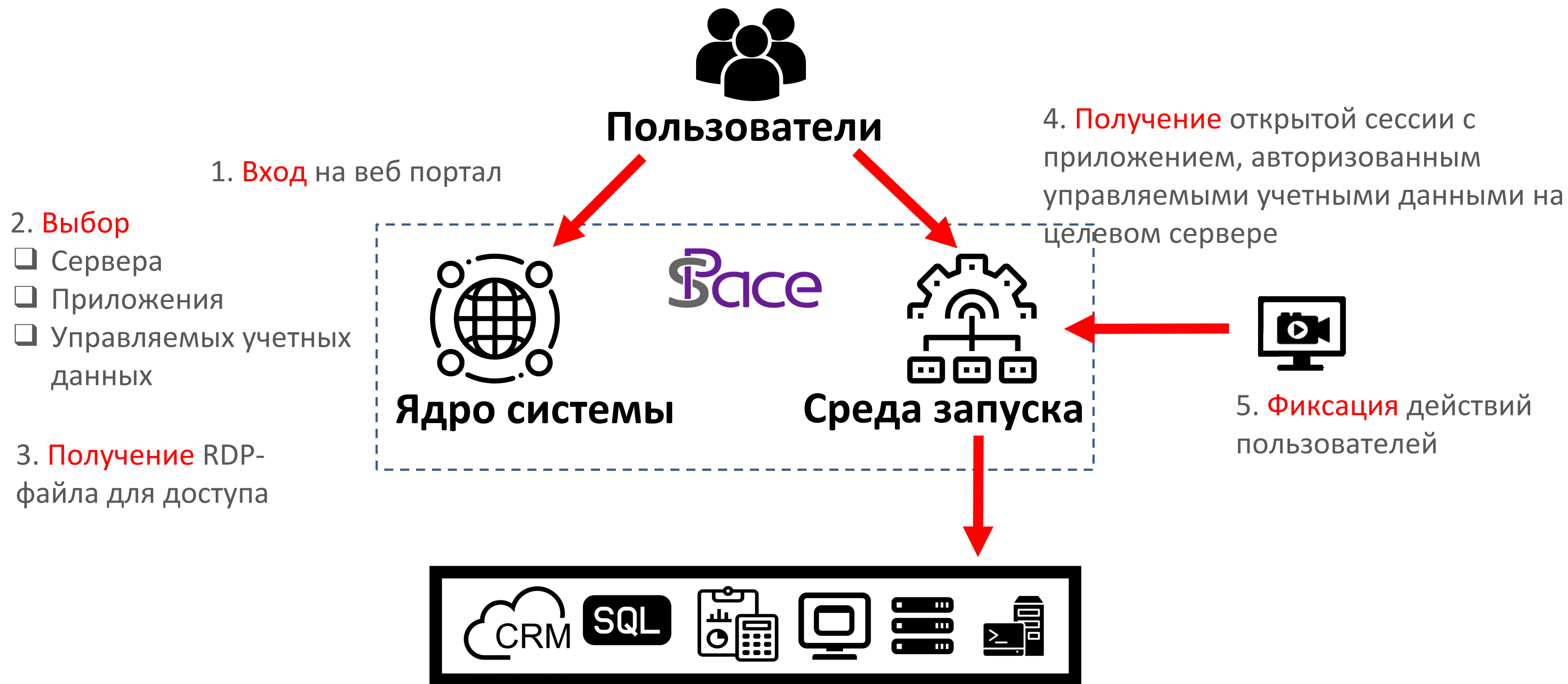
Как устроен sPACE



РАМ система

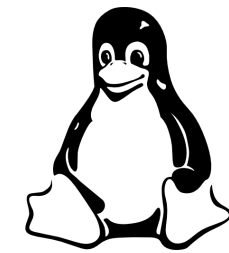


Техническая реализация доступа



Ядро системы

ЯДРО - главный управляющий элемент системы

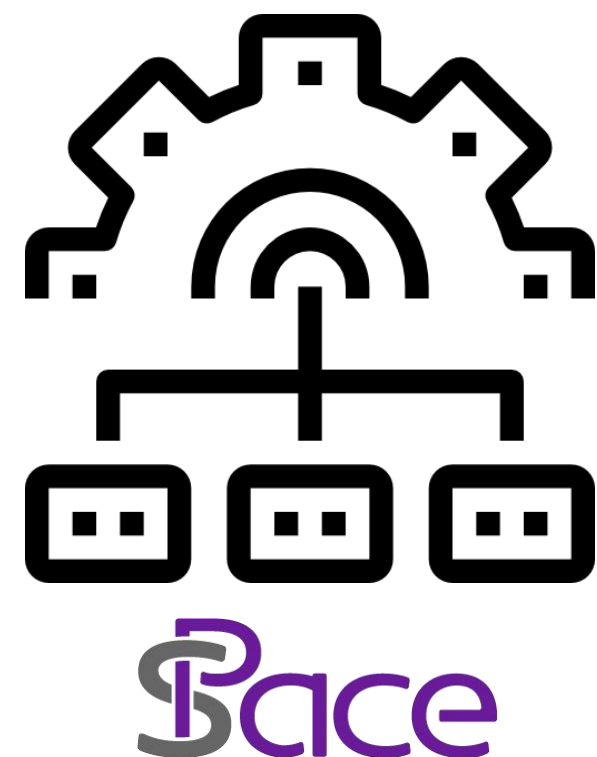
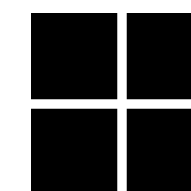


- ☐ Единый веб портал для пользователей, аудиторов и администраторов
- ☐ Встроенная защищенная база данных
- ☐ Служба защищенной очереди
- ☐ Служба хранения данных аудита
- ☐ Поддержка инсталляции на Ubuntu/Debian/CentOS/Astra Linux

Поддерживается распределенная установка ядра

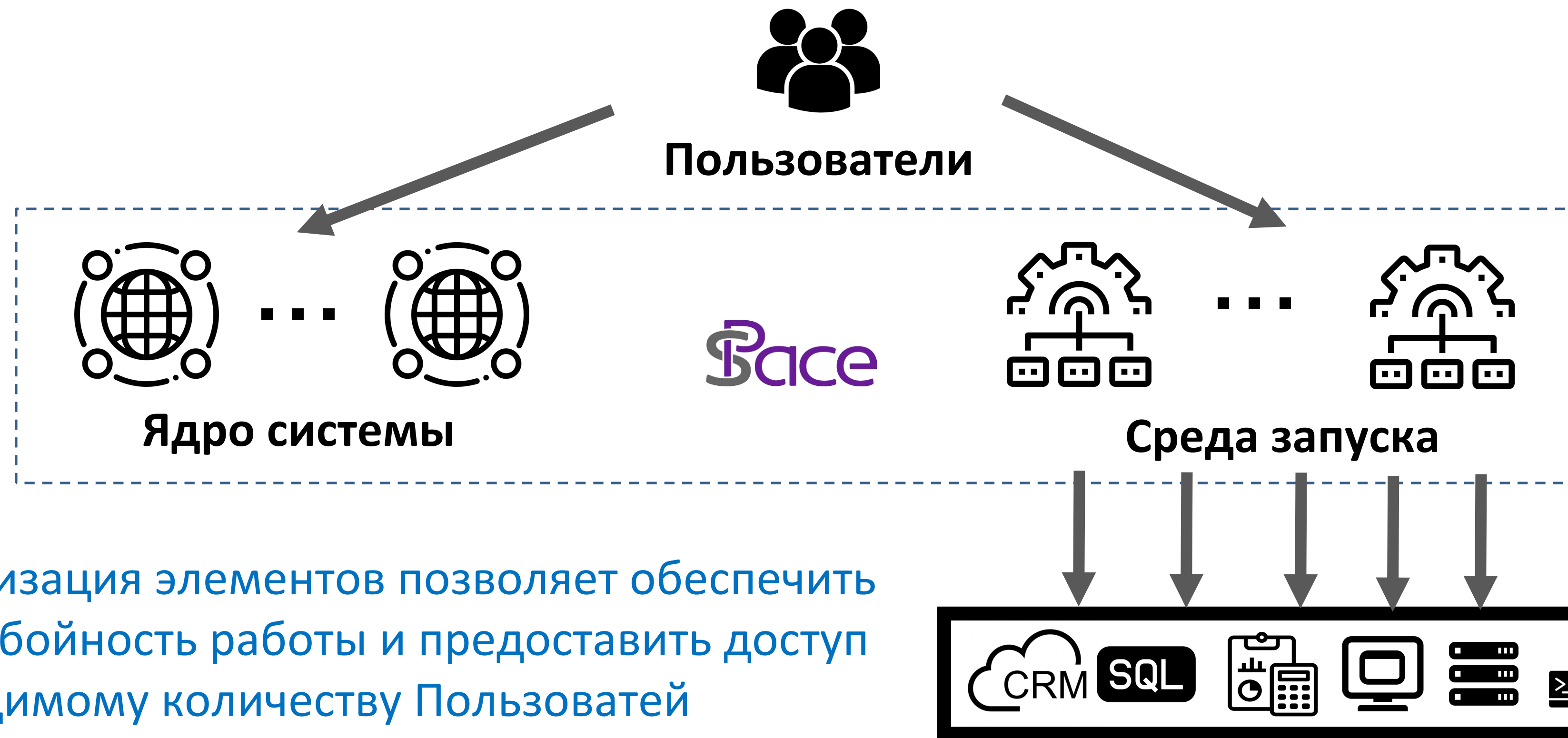
Среда запуска

Защищенная СРЕДА ЗАПУСКА инструментов



- ☐ Доверенная среда исполнения инструментов администрирования
- ☐ Безопасный проброс учетных данных целевых систем
- ☐ Широкие возможности масштабирования
- ☐ Запись сеансов и keylog
- ☐ Поддержка всех актуальных версий Windows Terminal Server

Масштабирование системы



Кластеризация элементов позволяет обеспечить бесперебойность работы и предоставить доступ необходимому количеству Пользователей

Управление привилегиями

❑ Изоляция учетных данных и обеспечение их полного жизненного цикла

Учетные данные к ИТ-системам хранятся в системе и неизвестны пользователям, автоматическая подстановка учетных данных при подключении сеансов, обеспечение полного жизненного цикла хранимых учетных данных (назначение, ротация, отзыв)

❑ Автоматизация процессов предоставления доступа сотрудников и внешних подрядчиков к ИТ-системам компании

Для доступа, в том числе удаленного, достаточно рабочей станции с веб-браузером и RDP-клиентом.

Реализован полный цикл запроса, предоставления и отзыва доступа привилегированным пользователям

❑ Реализация принципа наименьших привилегий

Предоставление доступа конкретному сотруднику к целевой системе для решения актуальной проблемы/задачи в определенное время

Контроль доступа

☐ Запись пользовательской активности

Автоматическое формирование журнала сеансов, выполнение записи экранов пользователей, запись лога нажатий клавиатуры

☐ Аудит действий пользователей

Просмотр и экспорт записей завершенных сессий, он-лайн просмотр текущих сессий и их прерывание в случае необходимости

☐ Внутренний мониторинг системы

Контроль состояния модулей системы

☐ Поддержка двухфакторной аутентификации

Поддержка двухфакторной аутентификации, интеграция с Rutoken и Google Authenticator

Преимущества sPASE

- ❑ Быстрая интеграция на основе запуска открытых для редактирования сценариев в рамках бизнес-задач
- ❑ Простой механизм наделения привилегиями с использованием нарядов-допусков
- ❑ Удобство и простота эксплуатации
- ❑ Развитый API для интеграции с другими инструментами ИБ
- ❑ Распределенная архитектура (масштабирование, автоматическая балансировка нагрузки и устойчивость к отказам)
- ❑ Нетребовательность к ИТ-ресурсам - низкая стоимость эксплуатации и масштабирования

Что дает sPace

- ❑ **Защиту доступа** к критически важным ИТ системам и **снижение риска** кибератак, вызванных компрометацией привилегированных учетных данных
- ❑ **Автоматизацию управления доступом** и повышение продуктивности сотрудников
- ❑ **Контролируемый доступ** не только для ИТ-специалистов, но и для критических бизнес-пользователей, работающих с «чувствительной» информацией
- ❑ **Минимизацию** финансовых **потерь и штрафов** регуляторов из-за неконтролируемых привилегий



Игорь Базелюк

bazelyuk@web-control.ru

+7 (495) 925-77-94

www.web-control.ru

e-mail: info@web-control.ru

www.s-space.ru

e-mail: info@s-space.ru

