

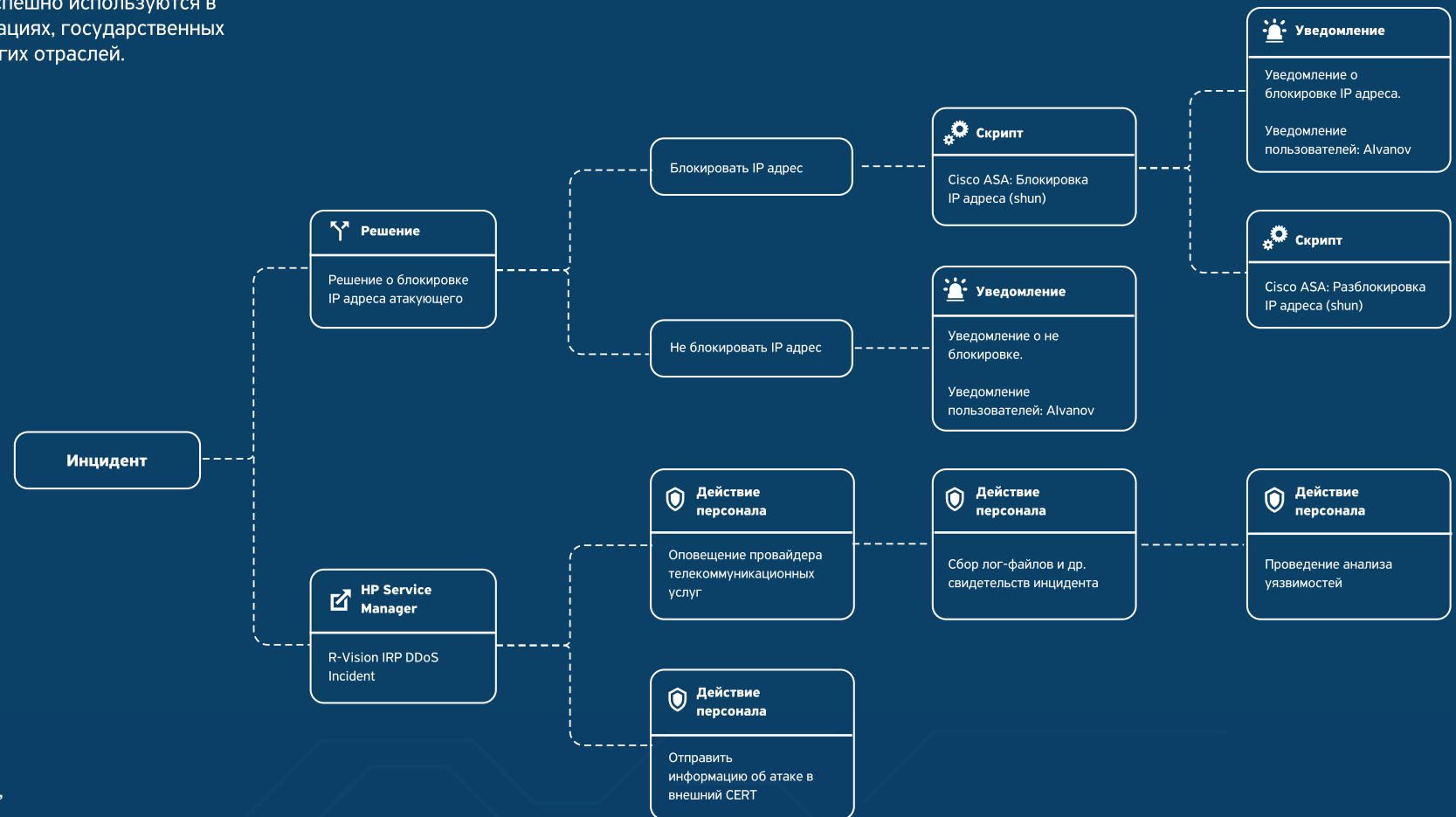


О компании R-Vision

Компания R-Vision с 2011 года ведет разработки инновационных программных решений, которые позволяют эффективно автоматизировать деятельность по мониторингу, регистрации и реагированию на инциденты информационной безопасности и значительно повысить возможности внутренней команды по отражению кибератак. Решения R-Vision успешно используются в российских кредитно-финансовых организациях, государственных структурах, компаниях нефтегазовой и других отраслей.


R-Vision Incident Response Platform


Платформа автоматизации процессов обработки и реагирования на инциденты информационной безопасности



 www.rvision.pro

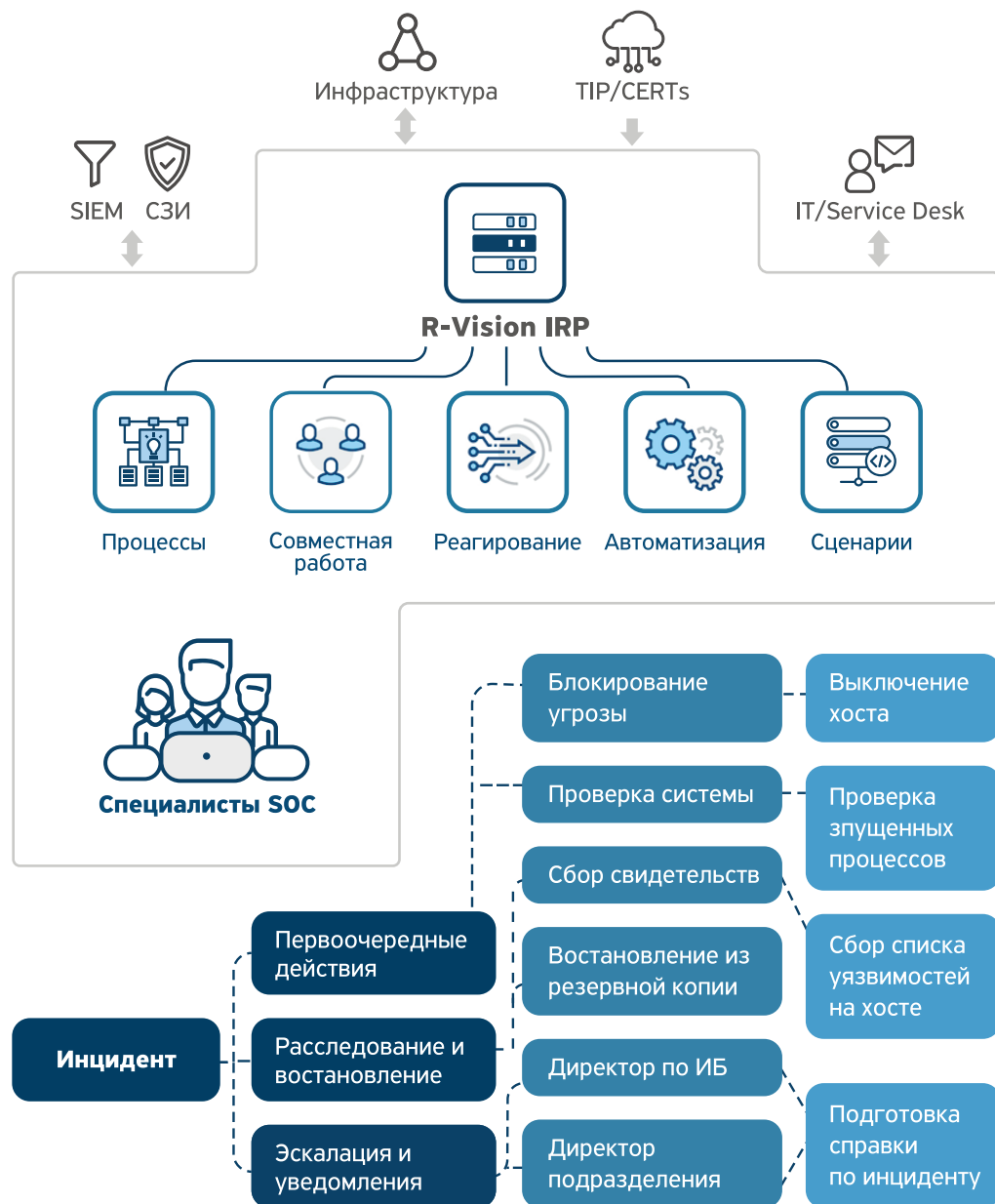
 sales@rvision.pro

 8 (499)-322-80-40
8 (800)-350-77-57

 143026, г. Москва, Территория инновационного центра «Сколково», ул. Нобеля д.7

R-Vision Incident Response Platform (IRP)

Платформа автоматизации процессов обработки и реагирования на инциденты информационной безопасности, управления жизненным циклом инцидентов и координации деятельности команды SOC.



АВТОМАТИЗАЦИЯ РЕАГИРОВАНИЯ

- ⚙️ Цикл обработки инцидентов ИБ
- ⚙️ Правила реагирования
- ⚙️ Сценарии реагирования
- ⚙️ Действия
- ⚙️ Приоритезация по степени критичности
- ⚙️ Классификация
- ⚙️ Эскалация
- ⚙️ Уведомление
- ⚙️ Технические меры реагирования (запуск скриптов, отправка команд)
- ⚙️ SLA, сроки реагирования

Агрегация информации обо всех инцидентах ИБ в единой системе

Контроль ИТ-активов и их свойств, включая уязвимости, контроль привилегий пользователей (аудит прав доступа пользователей к информационным ресурсам на основе членства в группе Active Directory и полномочий)

Интеграция с различными средствами защиты информации (SIEM-системы, сканеры уязвимостей, антивирусы, DLP-системы, NGFW/IPS, сервисы, Threat Intelligence - сервисы) и поддержка интеграции с ITSM-системами, Service Desk – системами и др.

Управление командой реагирования, распределение задач между участниками и контроль выполнения

Визуализация информации на различных уровнях представления, отображение связей между информационными и физическими активами, а также инцидентами, отображение метрик, связанных с процессом управления инцидентами ИБ. Формирование и экспорт отчетов в различные форматы

ПРЕИМУЩЕСТВА ДЛЯ ИБ



Облегчает координацию деятельности команды реагирования SOC



Сокращает время реагирования на инциденты ИБ и ускоряет сбор данных при проведении расследований, что минимизирует риски для бизнеса



Обеспечивает визуализацию данных для оперативного принятия решений при обработке инцидентов ИБ



Повышает эффективность работы персонала SOC при обработке инцидентов ИБ и эффективность существующей системы защиты