
R·Vision
At the root of your security

R-Vision: наши продукты

R-Vision Incident Response Platform (IRP)
Платформа для автоматизации центра обработки и реагирования на инциденты ИБ (SOC)

R-Vision Security Governance, Risk & Compliance (SGRC)
Система контроля деятельности по управлению ИБ, оценке соответствия требованиям и оценке рисков ИБ

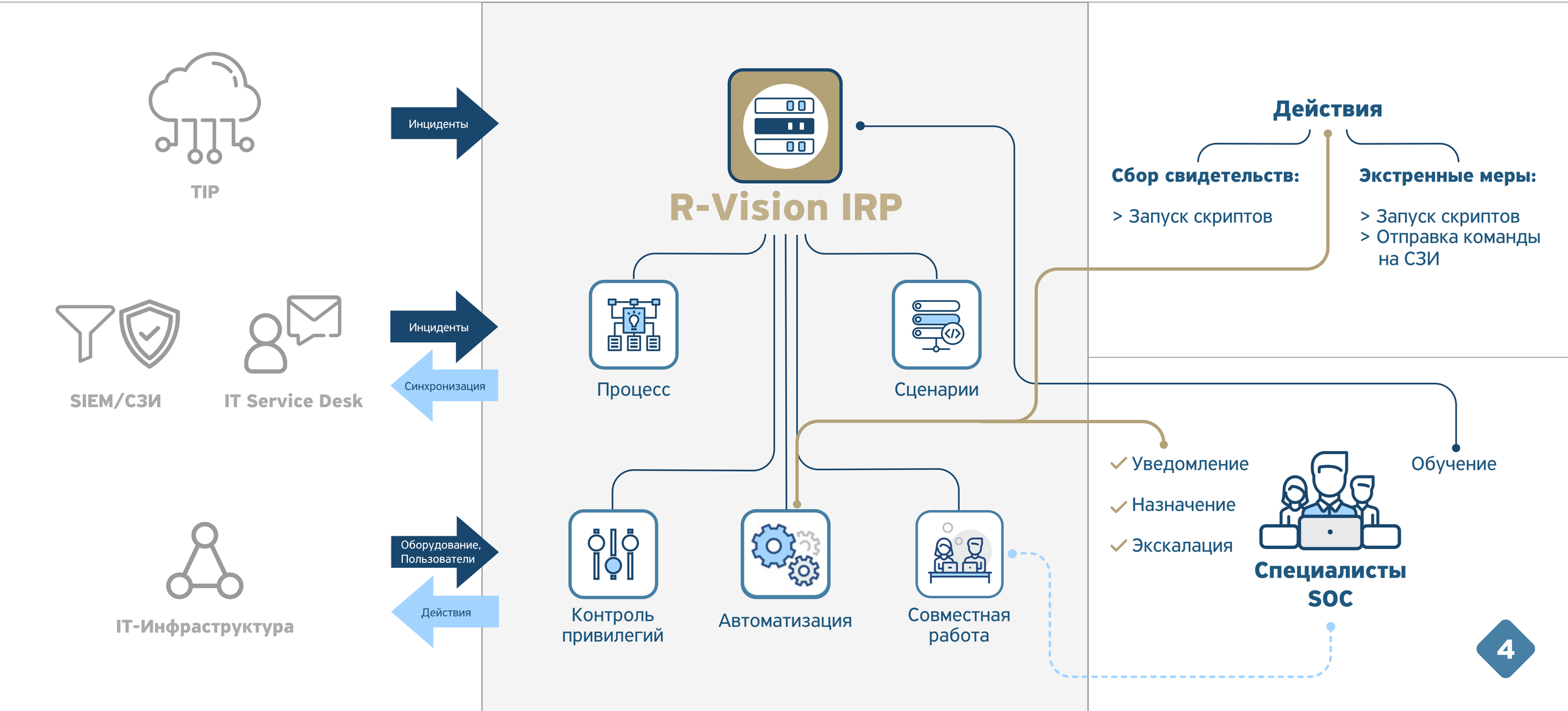
R-Vision IRP: о продукте

R-Vision Incident Response Platform (IRP) — необходимый элемент SOC – платформа автоматизации процессов обработки и реагирования на инциденты ИБ, управления жизненным циклом инцидентов и координации деятельности команды SOC

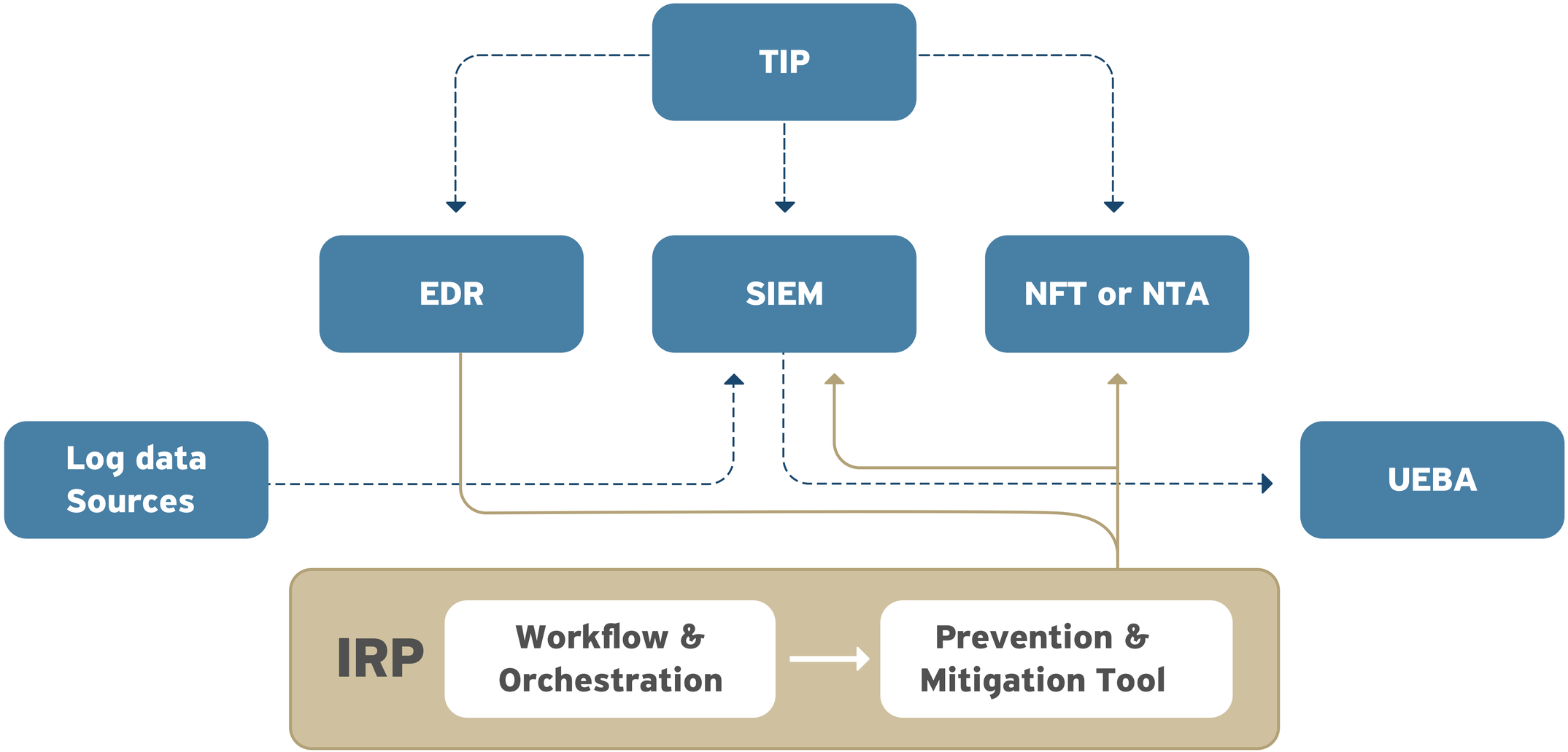
Агрегация информации из:

- **Threat intelligence**
- **CERTs**
- **ИТ-инфраструктура**
- **Средства защиты**
- **Информационные системы**

R-Vision IRP: о продукте



Комплекс решений для построения SOC



IRP как класс решений

IRP = workflow + автоматизация + оркестрация

Включает:

- **План обработки инцидентов**
- **Сценарии реагирования**
- **Сбор дополнительных сведений, свидетельств**
- **Объединение/обогащение данных контекстом**
- **Аналитика результатов для адаптации мер защиты**

Оркестрация как процесс SOC

To Tie it, Together - Orchetration

R-Vision IRP: основные функции

Агрегация

информации обо всех инцидентах ИБ в единой системе

Интеграция

с различными решениями (SIEM, VS, AV, ITSM и др. системами)

Визуализация

информации на различных уровнях представления

Контроль

ИТ-активов, привилегий пользователей в ИС, метрик ИБ

Автоматизация

- реагирования на инциденты
- жизненного цикла инцидентов
- контроля уязвимостей
- рабочего процесса (workflow) команды реагирования

Отчетность

формирование и экспорт отчетов

R-Vision IRP: интеграция и агрегация данных

Импорт

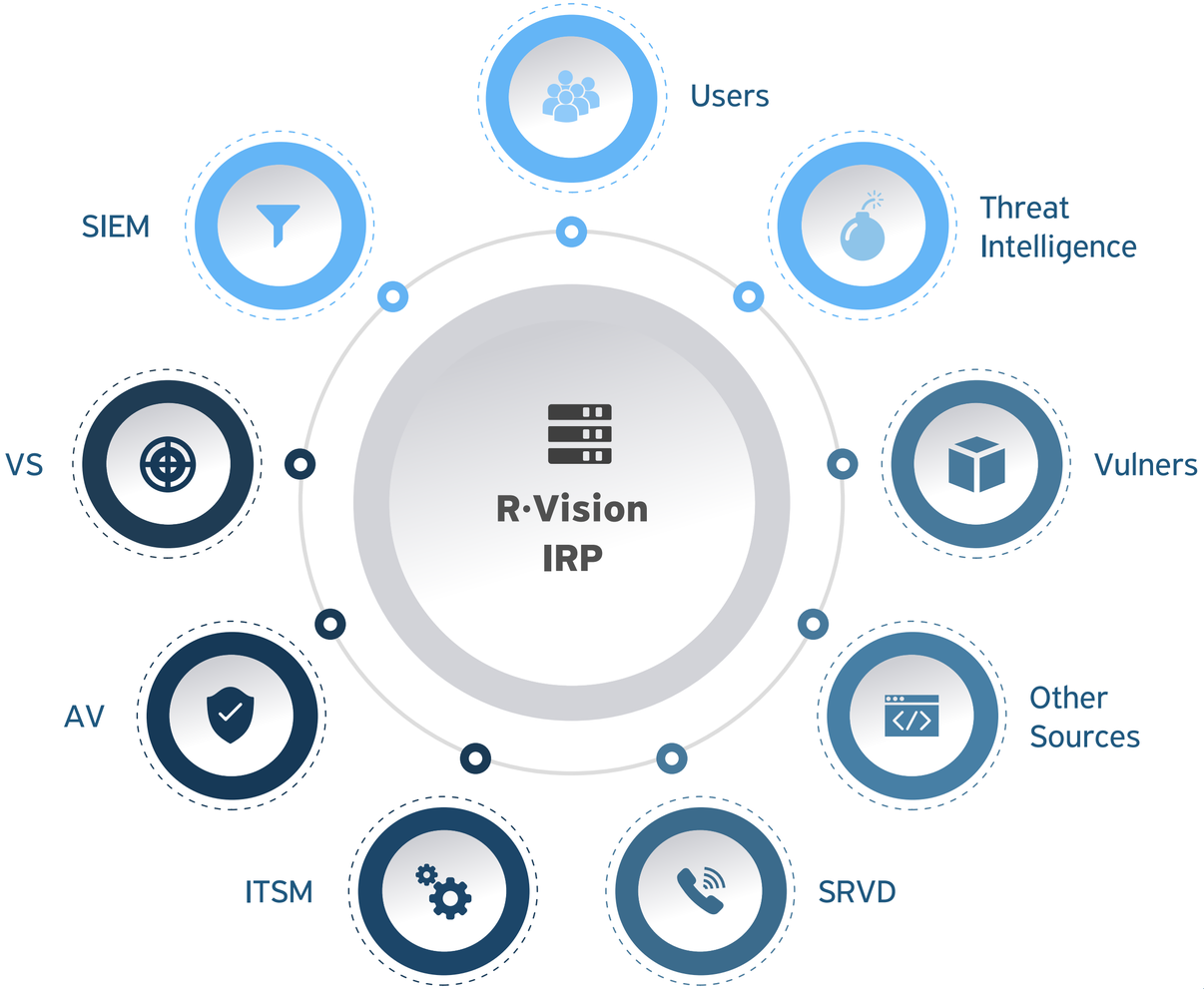
- Инвентаризационных данных
- Инцидентов ИБ
- Сведений об уязвимостях
- Threat Intelligence Feeds
- Детальных сведений о хостах (статусов агентов ПО)

Обмен

- Данными с другими SOC/CERT
- Между копиями R-Vision

Агрегация

- Накопление и хранение в единой базе сведений по инцидентам, уязвимостям, активам



R-Vision IRP: автоматизация

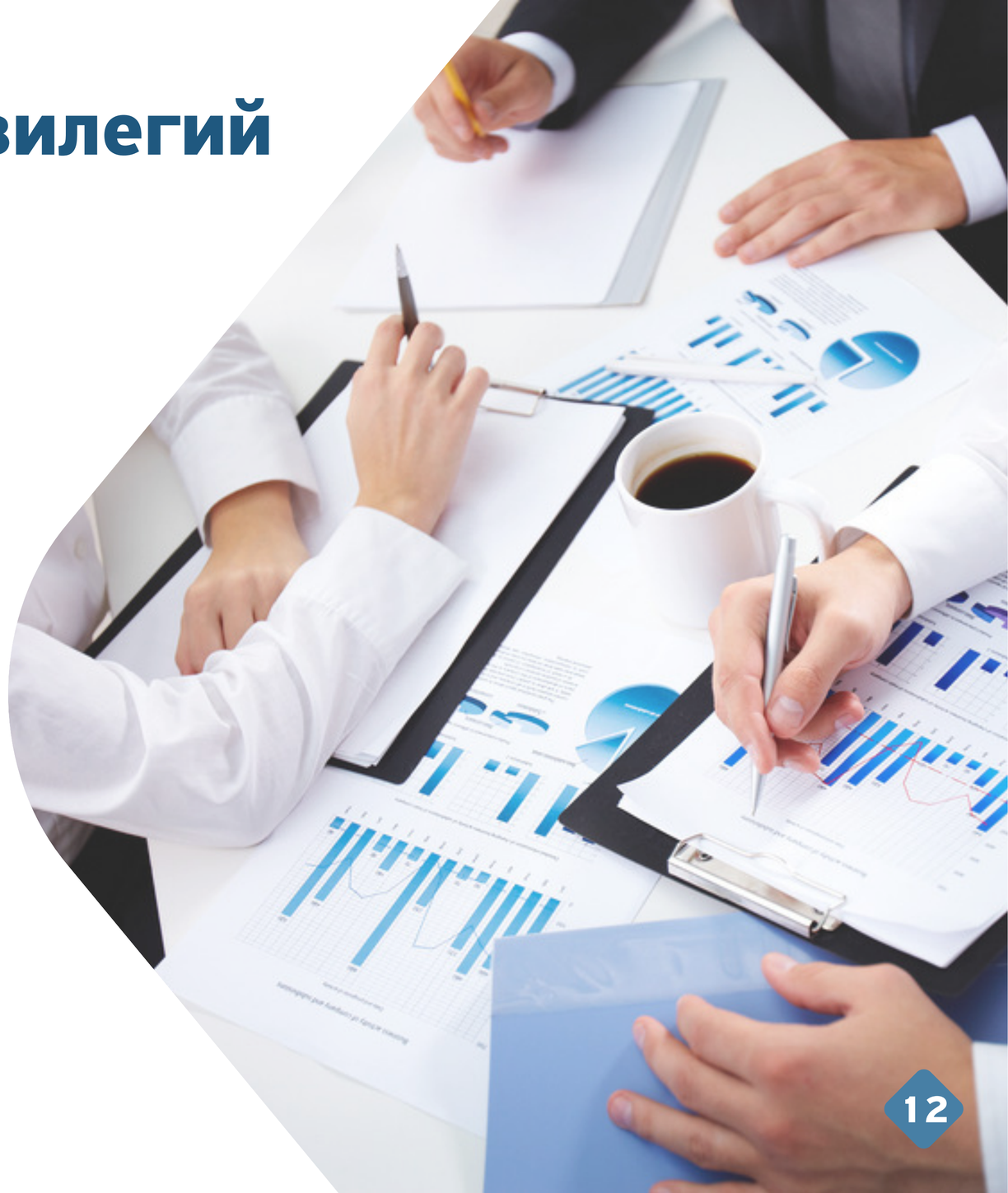
IRP vs SIEM vs SD

Решаемые задачи	IRP	SIEM	ServiceDesk
Сбор событий, логов		✓	
Сбор/формирование инцидентов	✓	✓	
Управление жизненным циклом инцидентов (workflow)	✓		✓*
Контроль инфраструктуры (включая инвентаризацию)	✓	✓*	
Визуализация (метрики, KPI)	✓		✓*
Автоматизированный сбор информации при обработке инцидентов	✓		
Возможность автоматического реагирования на инциденты по одному клику	✓		
Интеграция с разными СЗИ, ПО, CERT, SOC для сбора аналитики, фидов, данных	✓		
Обмен определенной информацией по инцидентам между компаниями	✓		

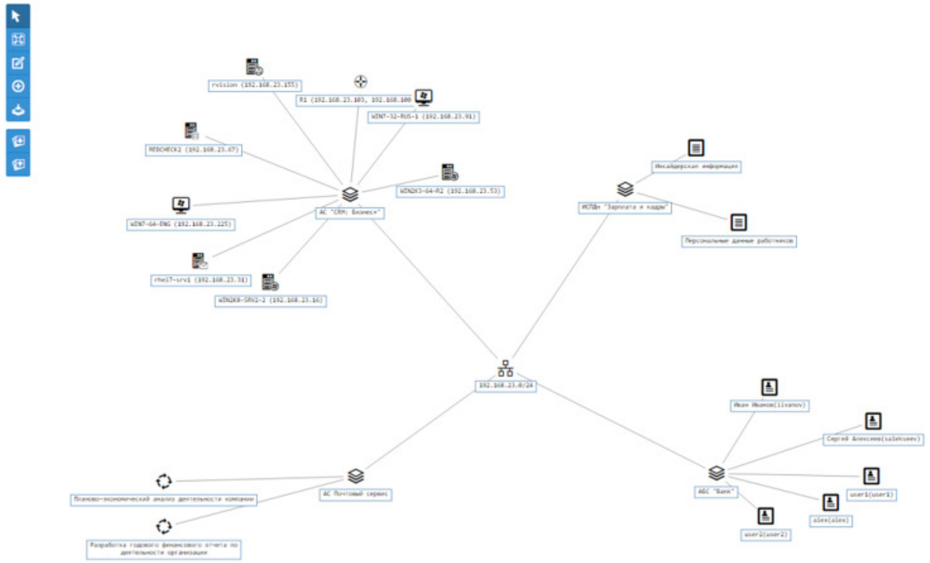
R-Vision IRP: контроль привилегий

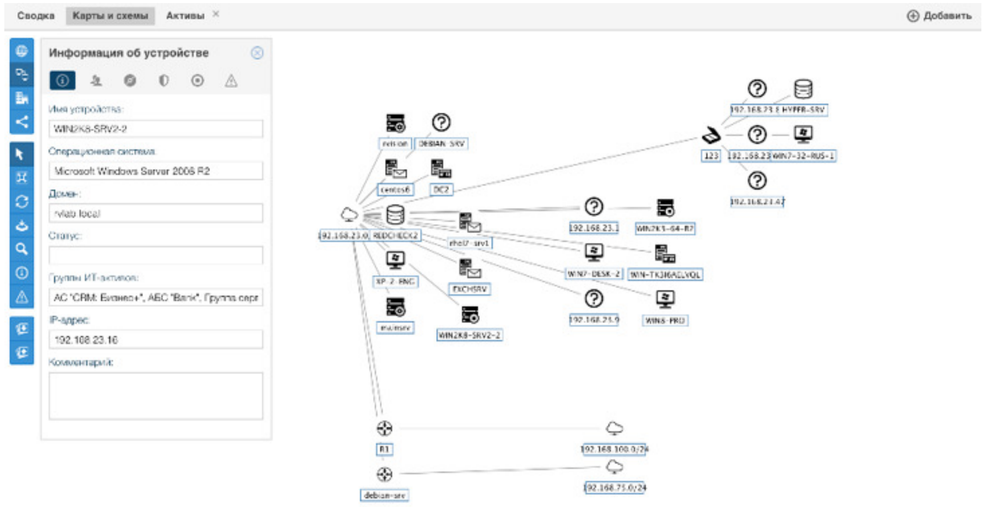
Основные функции:

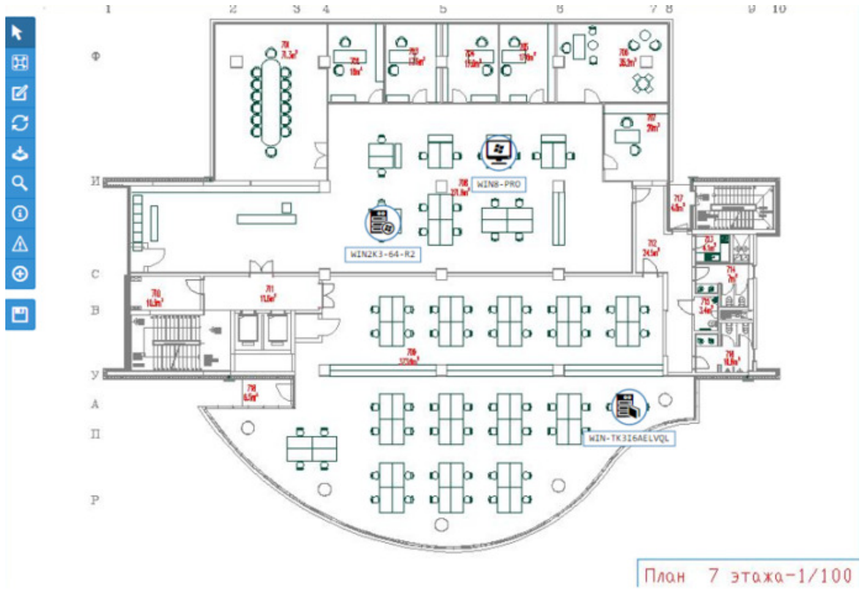
- **Аудит прав доступа пользователей к информационным ресурсам на основе членства в группах Active Directory и полномочий**
- **Обнаружение несоответствия установленных прав доступа на основе фактических прав доступа**
- **Контроль изменения прав доступа**
- **Визуализация и представление информации в различных форматах**
- **Формирование отчетности**



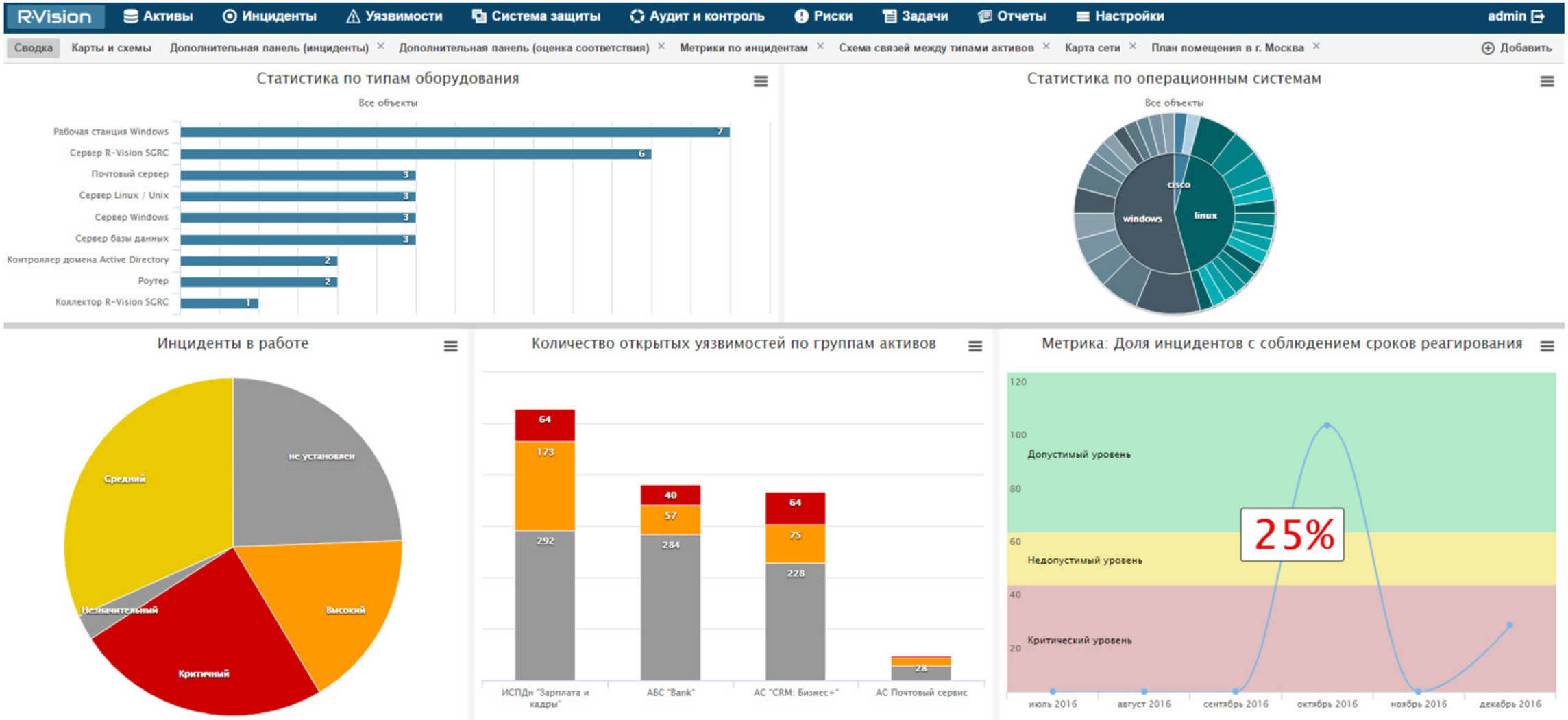
R-Vision IRP: ИТ-активы



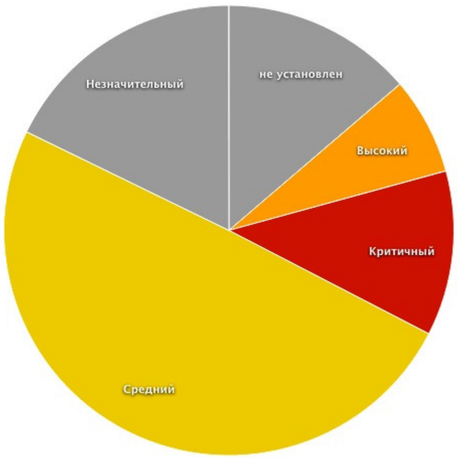


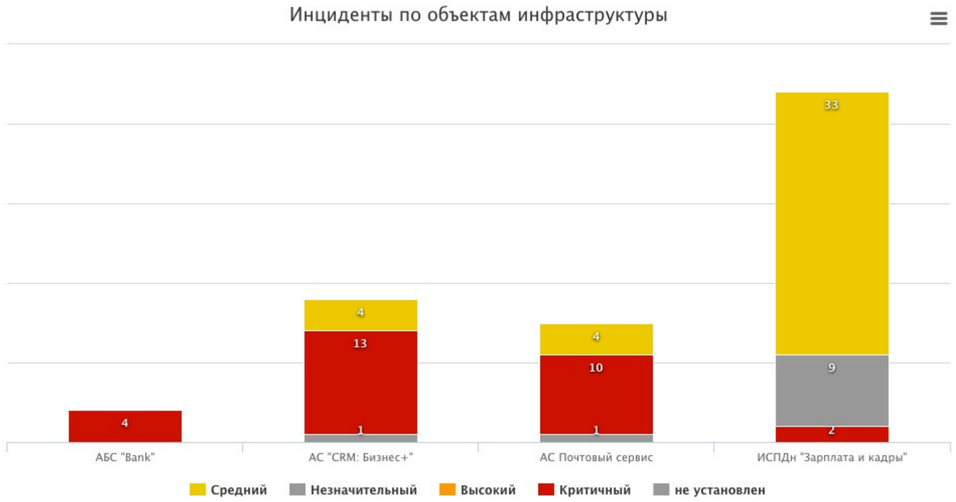


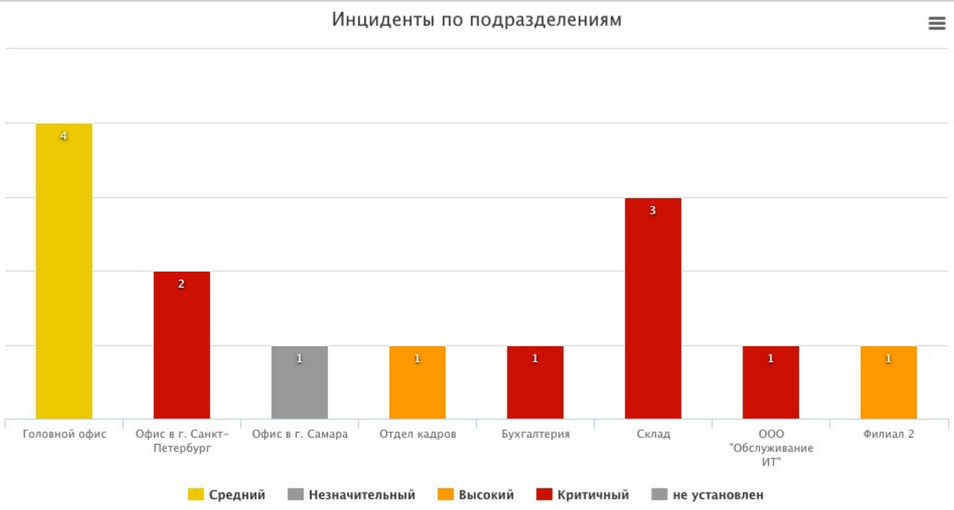
R-Vision IRP: сводная информация

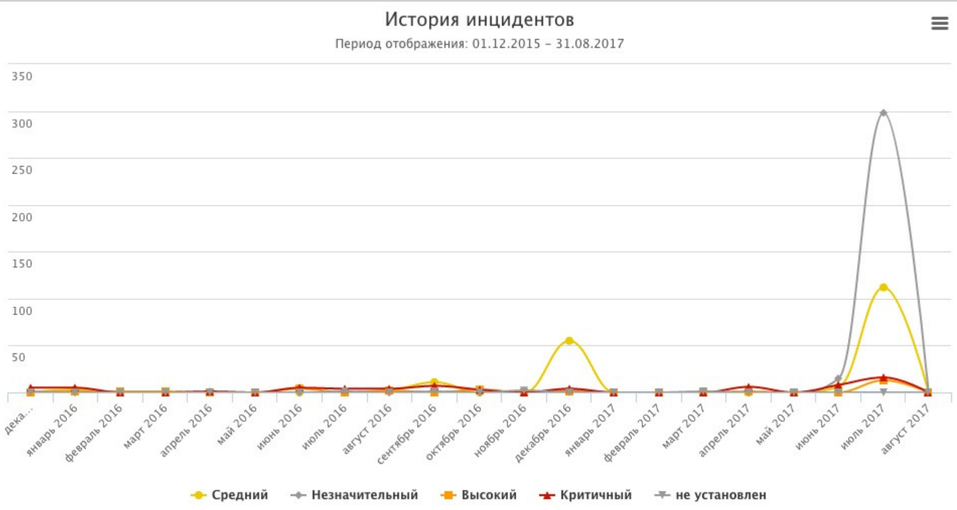


R-Vision IRP: инциденты

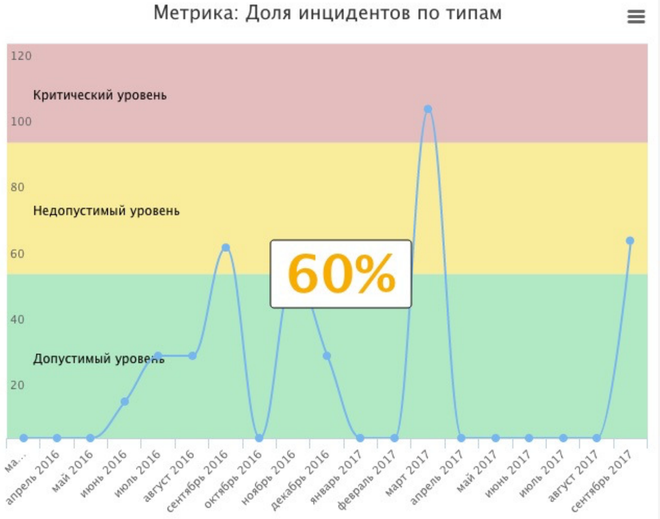


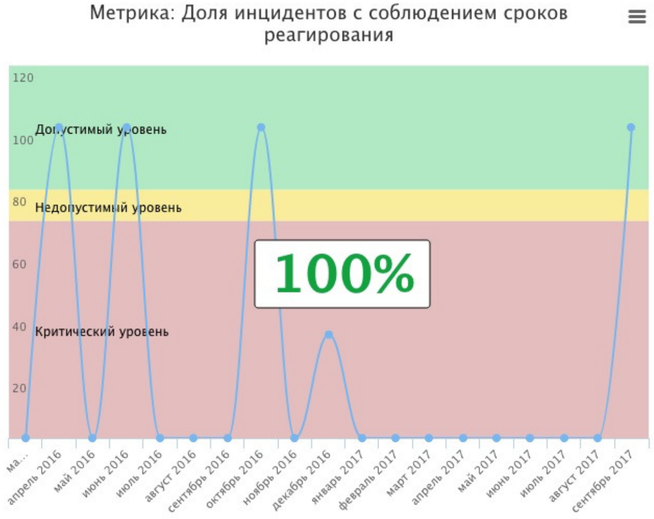


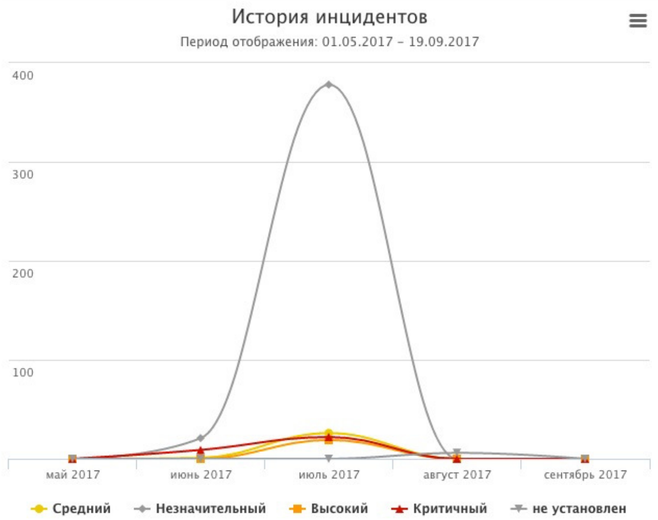




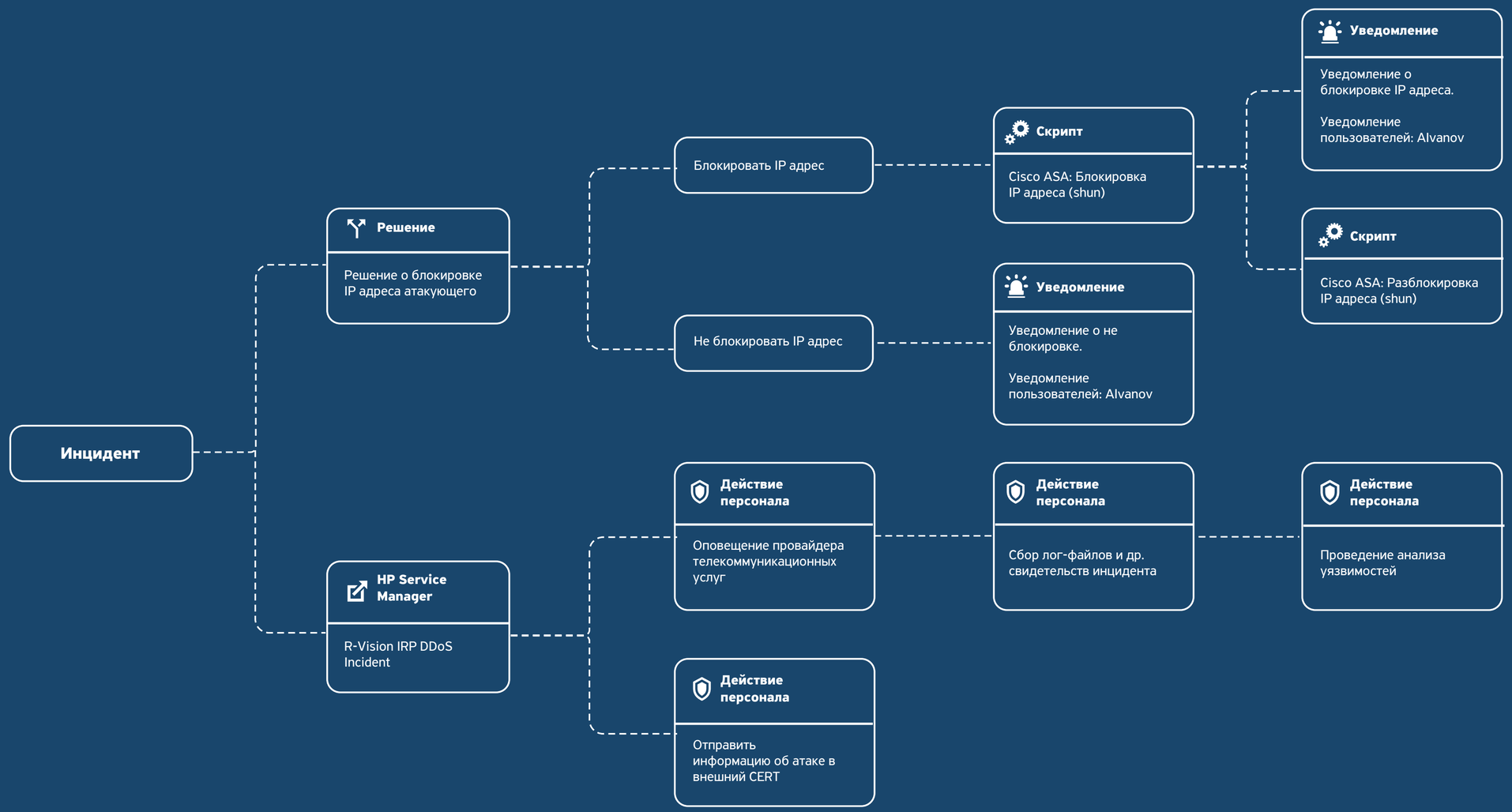
R-Vision IRP: количественные метрики







R-Vision IRP: сценарии реагирования



R-Vision IRP: преимущества

- Ускорение времени ответной реакции на инциденты ИБ и последующая минимизация рисков для бизнеса
- Координация деятельности команды реагирования
- Повышение эффективности работы персонала SOC при обработке инцидентов ИБ
- Сокращение времени для сбора данных при расследовании инцидентов ИБ
- Визуализация данных для оперативного ринятия решений при обработке инцидентов ИБ

R·Vision
At the root of your security

Благодарим за внимание!

www.rvision.pro

sales@rvision.pro

+7 (499) 322 80 40
8 (800) 350 77 57

Подписывайтесь на наш Дайджест ИБ: rvision.pro/blog