
КОНТРОЛЬ
РЕАГИРОВАНИЕ
АВТОМАТИЗАЦИЯ
Incident Response Platform

R-Vision Incident Response Platform (IRP)

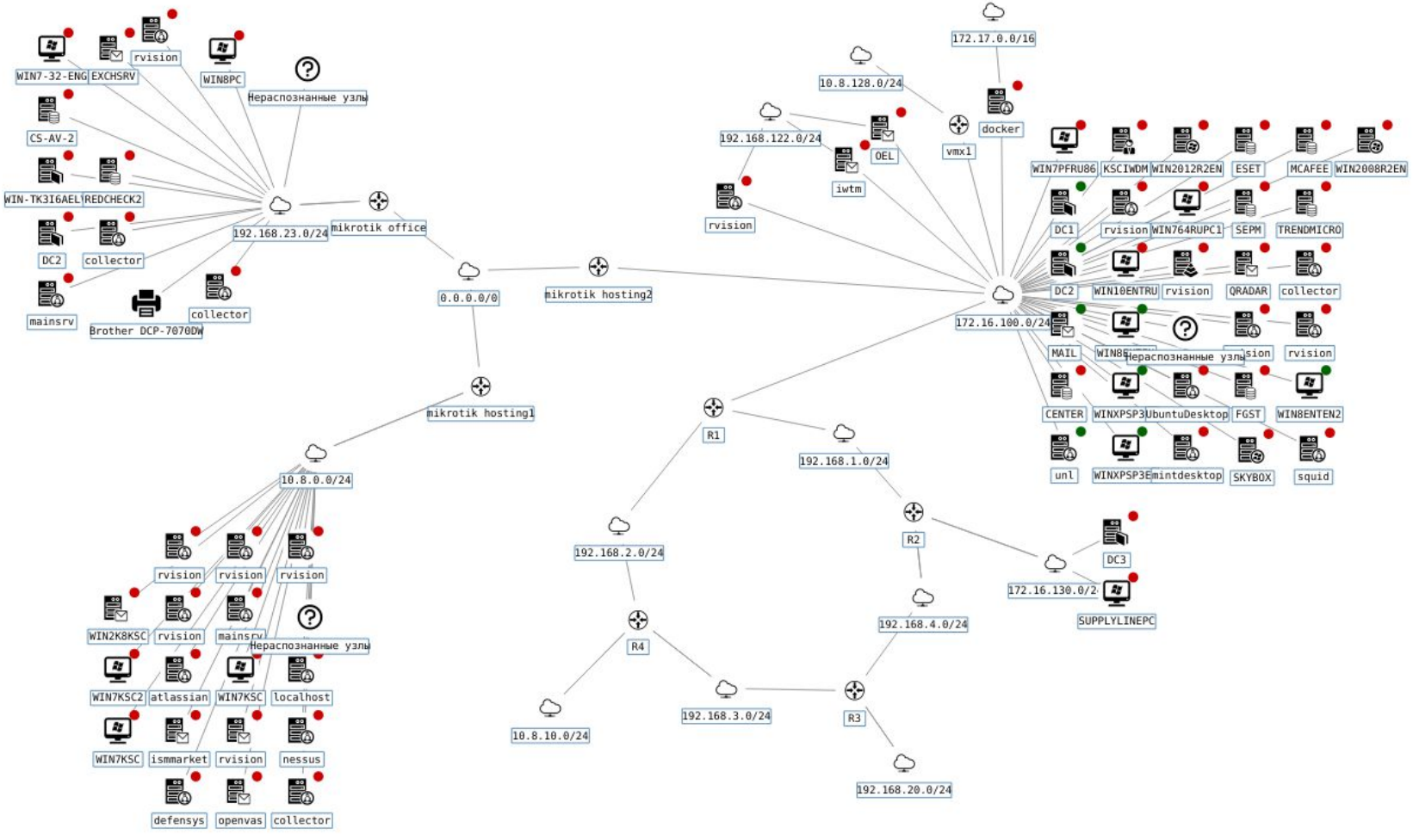
Единая точка консолидации информации обо всех инцидентах информационной безопасности в компании (корпоративный SOC)

Платформа для совместной работы группы реагирования на инциденты ИБ с возможностью сбора, анализа и хранения сведений, относящихся к инцидентам ИБ

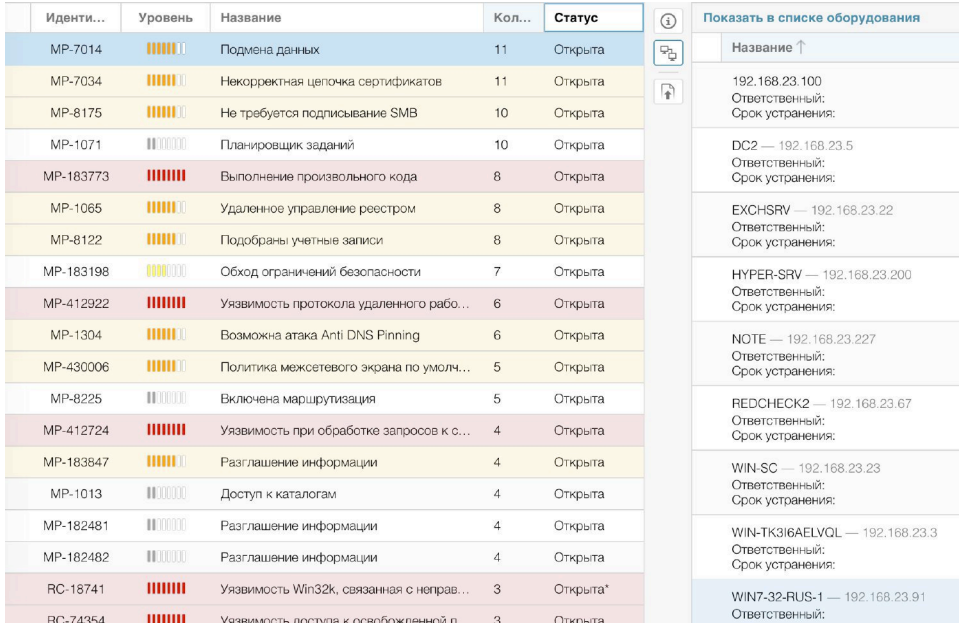
Центр координации деятельности сотрудников компании, распределения задач и учета выполненных мероприятий по реагированию на инциденты ИБ

#1 Интеграция

#2 Контроль ИТ-инфраструктуры



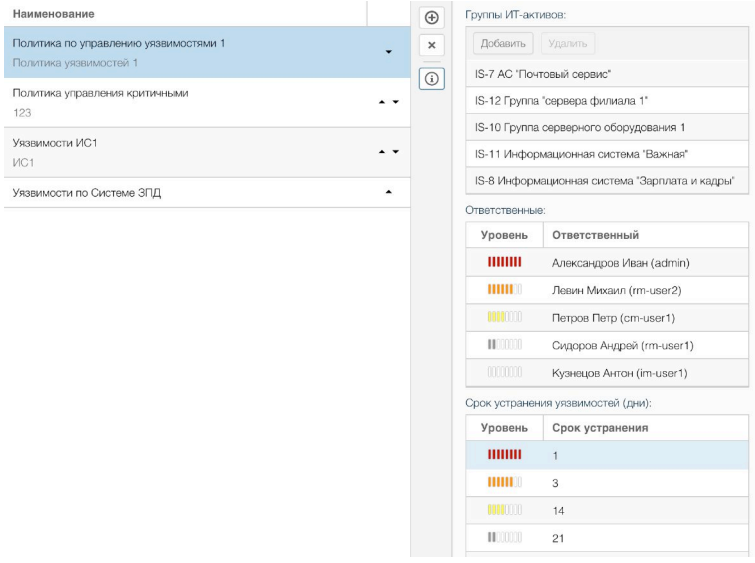
#3 Управление уязвимостями



Идентиф...	Уровень	Название	Кол...	Статус
MP-7014		Подмена данных	11	Открыта
MP-7034		Некорректная цепочка сертификатов	11	Открыта
MP-8175		Не требуется подписывание SMB	10	Открыта
MP-1071		Планировщик заданий	10	Открыта
MP-183773		Выполнение произвольного кода	8	Открыта
MP-1065		Удаленное управление реестром	8	Открыта
MP-8122		Подобраны учетные записи	8	Открыта
MP-183198		Обход ограничений безопасности	7	Открыта
MP-412922		Уязвимость протокола удаленного рабо...	6	Открыта
MP-1304		Возможна атака Anti DNS Pinning	6	Открыта
MP-430006		Политика межсетевого экрана по умолч...	5	Открыта
MP-8225		Включена маршрутизация	5	Открыта
MP-412724		Уязвимость при обработке запросов к с...	4	Открыта
MP-183847		Разглашение информации	4	Открыта
MP-1013		Доступ к каталогам	4	Открыта
MP-182481		Разглашение информации	4	Открыта
MP-182482		Разглашение информации	4	Открыта
RC-18741		Уязвимость Win32k, связанная с неправ...	3	Открыта*
RC-74354		Уязвимость доступа к освобожденной п...	3	Открыта

Показать в списке оборудования

Название
192.168.23.100 Ответственный: Срок устранения:
DC2 — 192.168.23.5 Ответственный: Срок устранения:
EXCHSRV — 192.168.23.22 Ответственный: Срок устранения:
HYPER-SRV — 192.168.23.200 Ответственный: Срок устранения:
NOTE — 192.168.23.227 Ответственный: Срок устранения:
REDCHECK2 — 192.168.23.67 Ответственный: Срок устранения:
WIN-SC — 192.168.23.23 Ответственный: Срок устранения:
WIN-TK3I6AELVQL — 192.168.23.3 Ответственный: Срок устранения:
WIN7-32-RUS-1 — 192.168.23.91 Ответственный:



Наименование

Политика по управлению уязвимостями 1
Политика уязвимостей 1

Политика управления критичными
123

Уязвимости ИС1
ИС1

Уязвимости по Системе ЗПД

Группы ИТ-активов:

Добавить | Удалить

IS-7 АС "Почтовый сервис"
IS-12 Группа "сервера филиала 1"
IS-10 Группа серверного оборудования 1
IS-11 Информационная система "Важная"
IS-8 Информационная система "Зарплата и кадры"

Ответственные:

Уровень	Ответственный
	Александров Иван (admin)
	Левин Михаил (rm-user2)
	Петров Петр (cm-user1)
	Сидоров Андрей (rm-user1)
	Кузнецов Антон (im-user1)

Срок устранения уязвимостей (дни):

Уровень	Срок устранения
	1
	3
	14
	21

VULNERS.COM

Nessus® vulnerability scanner

nexpose®

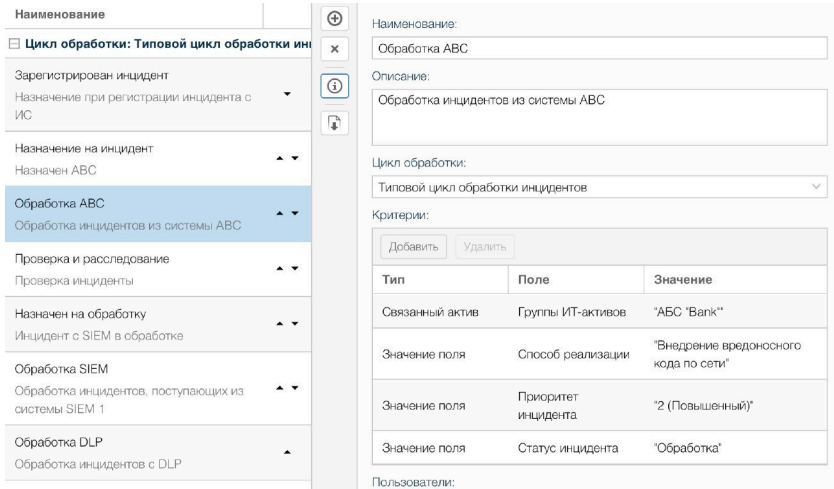
MAXPATROL
КОМПЛЕКСНЫЙ МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

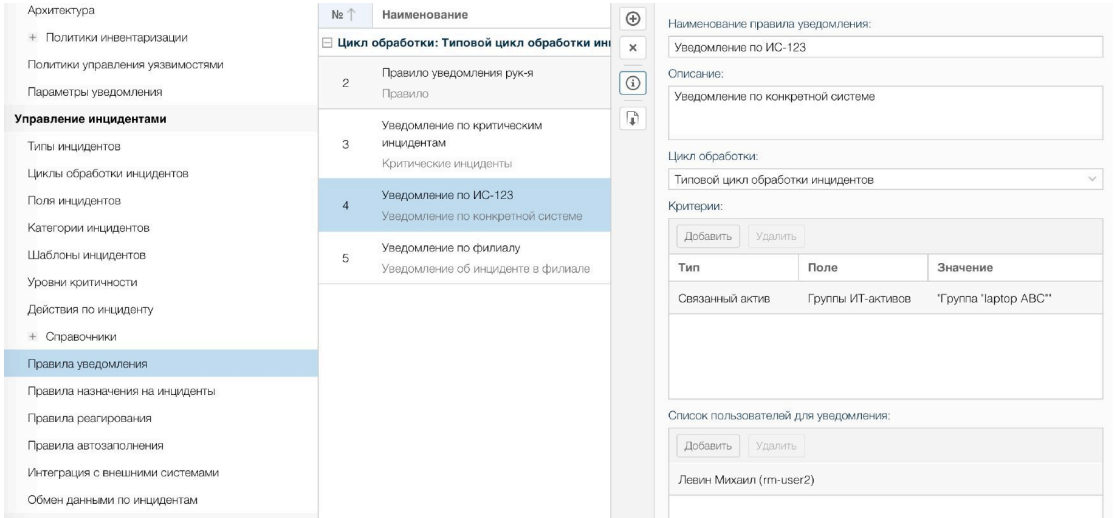
RedCheck

OpenVAS Open Vulnerability Assessment System

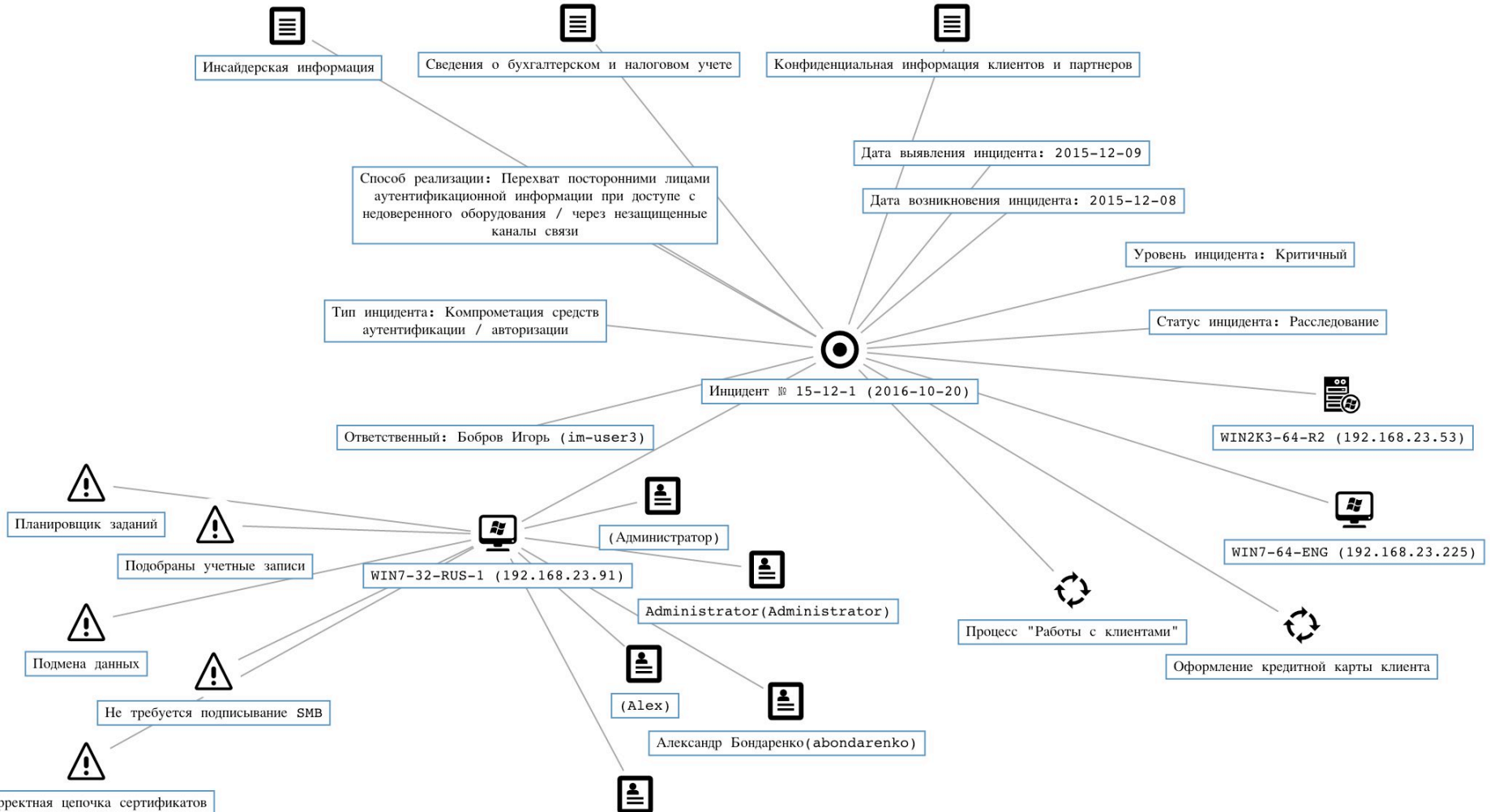
QUALYS®

#4 Управление инцидентами

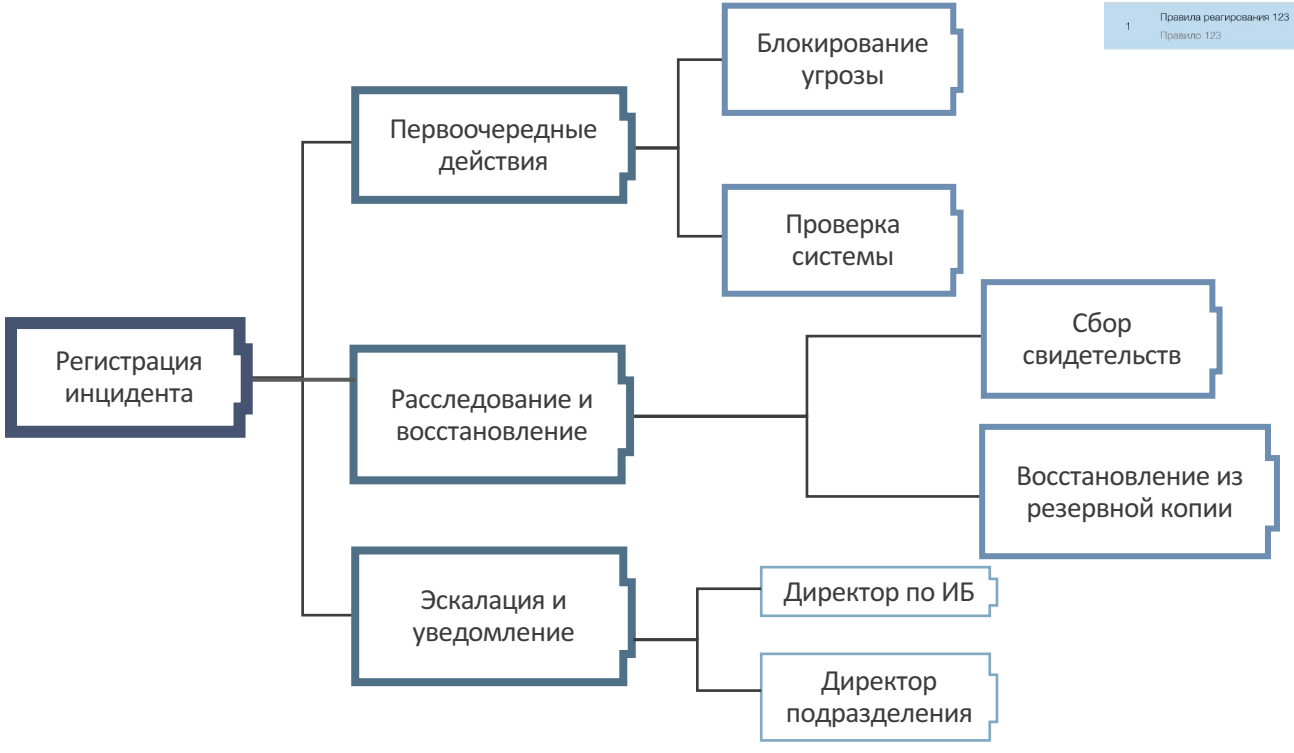


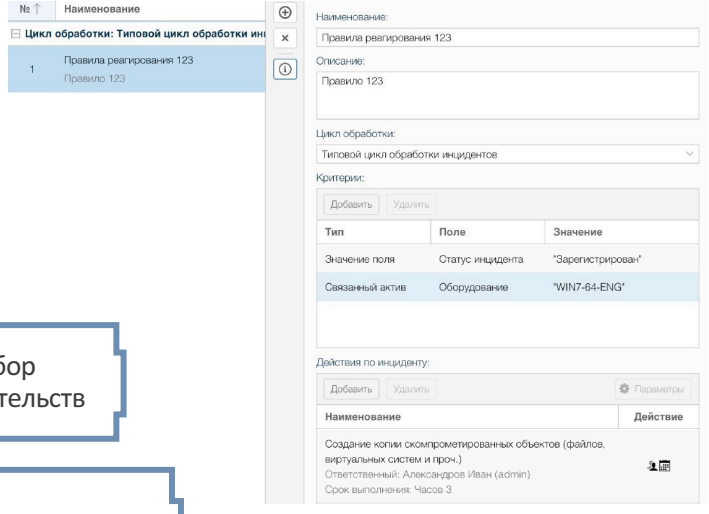


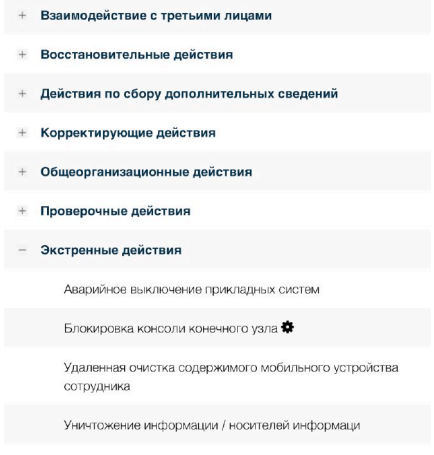
#5 Визуализация и графы связей



#6 Автоматизация реагирования



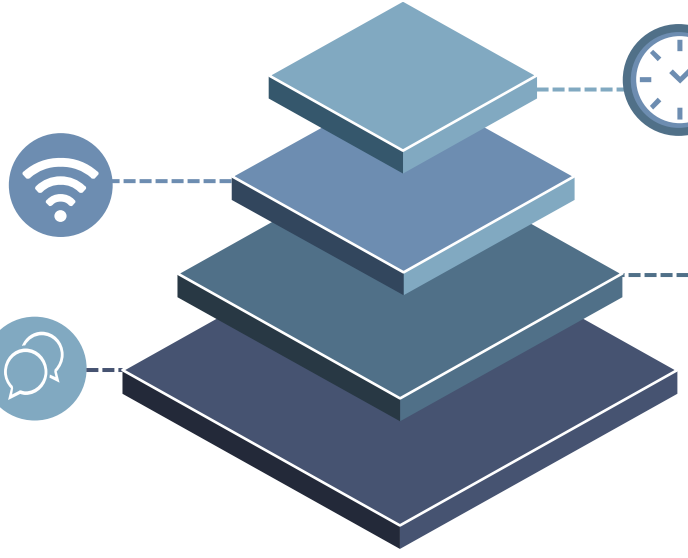




#7 Платформа для взаимодействия с внешними SOC, CERT, ГосСОПКА

Обмен информацией

Обмен данными с внешними источниками (SOC, TI)



Оперативный контроль

Контроль сроков реагирования на инциденты

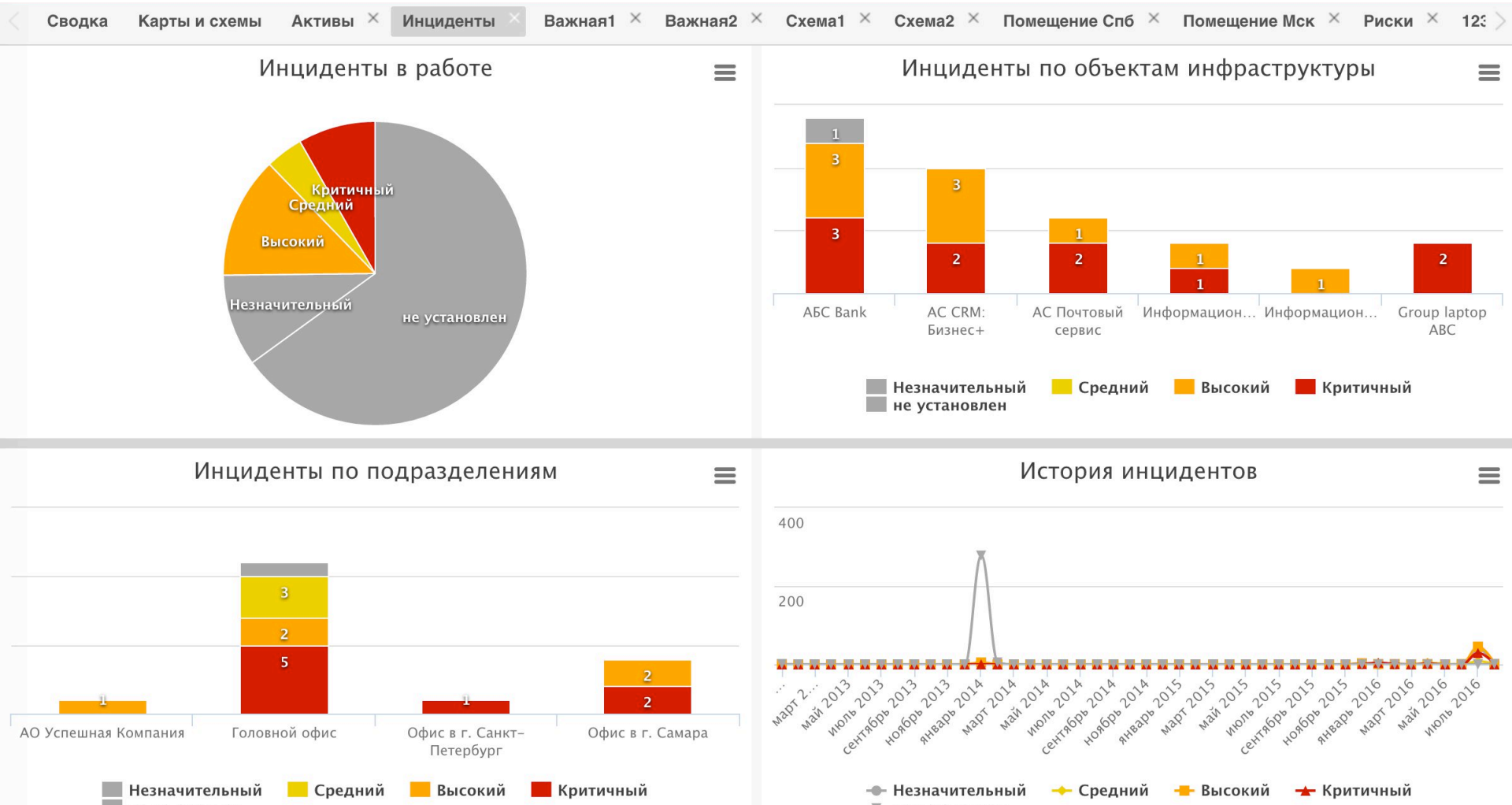
Совместная работа

Рабочие области по инцидентам, коммуникации и обмен данными, учет действий по инциденту

Автоматизация реагирования

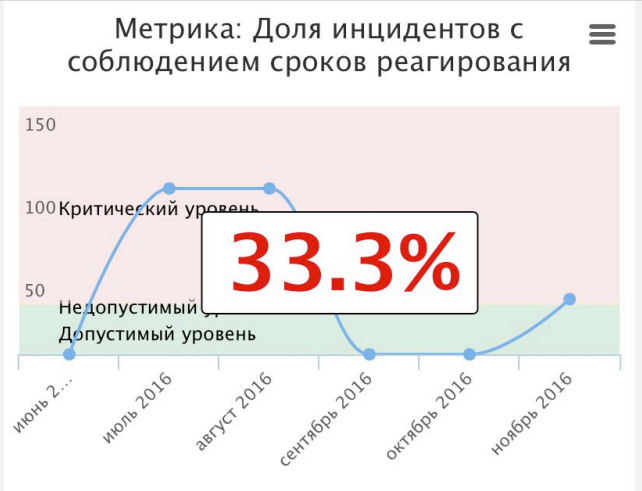
Правила реагирования по типам инцидентов, распределение задач, уведомление, эскалация

#8 Диаграммы. Графики. Схемы



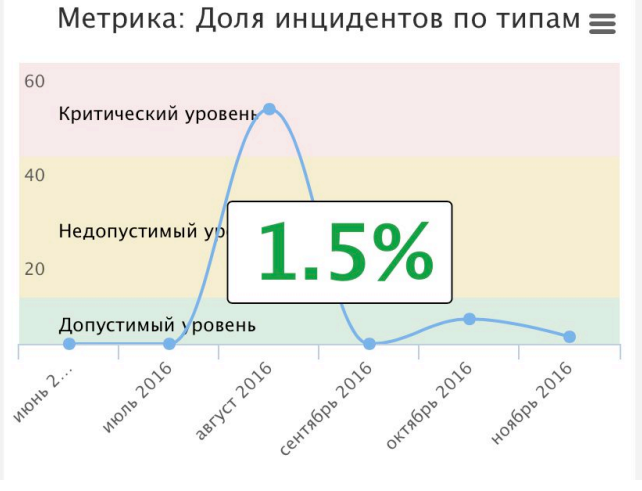
#9 Метрики

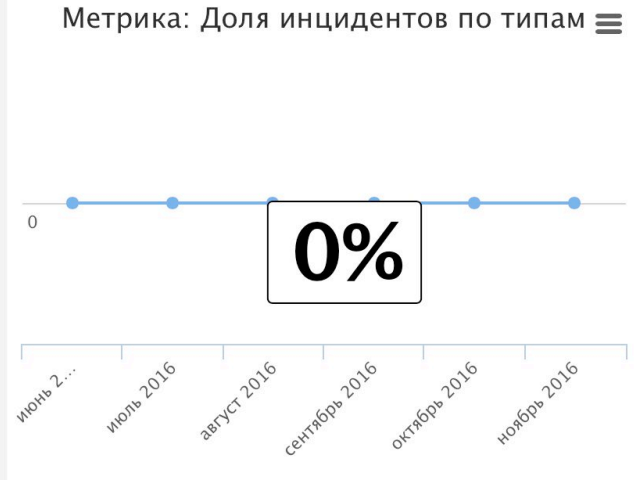

Метрика: Ущерб от реализации инцидентов
200000
100000
190 222 руб.
май 2016
июнь 2016
июль 2016
август 2016
сентябрь 2016
октябрь 2016
ноябрь 2016


Метрика: Доля инцидентов с соблюдением сроков реагирования
150
100
50
Критический уровень
Допустимый уровень
33.3%
июнь 2...
июль 2016
август 2016
сентябрь 2016
октябрь 2016
ноябрь 2016

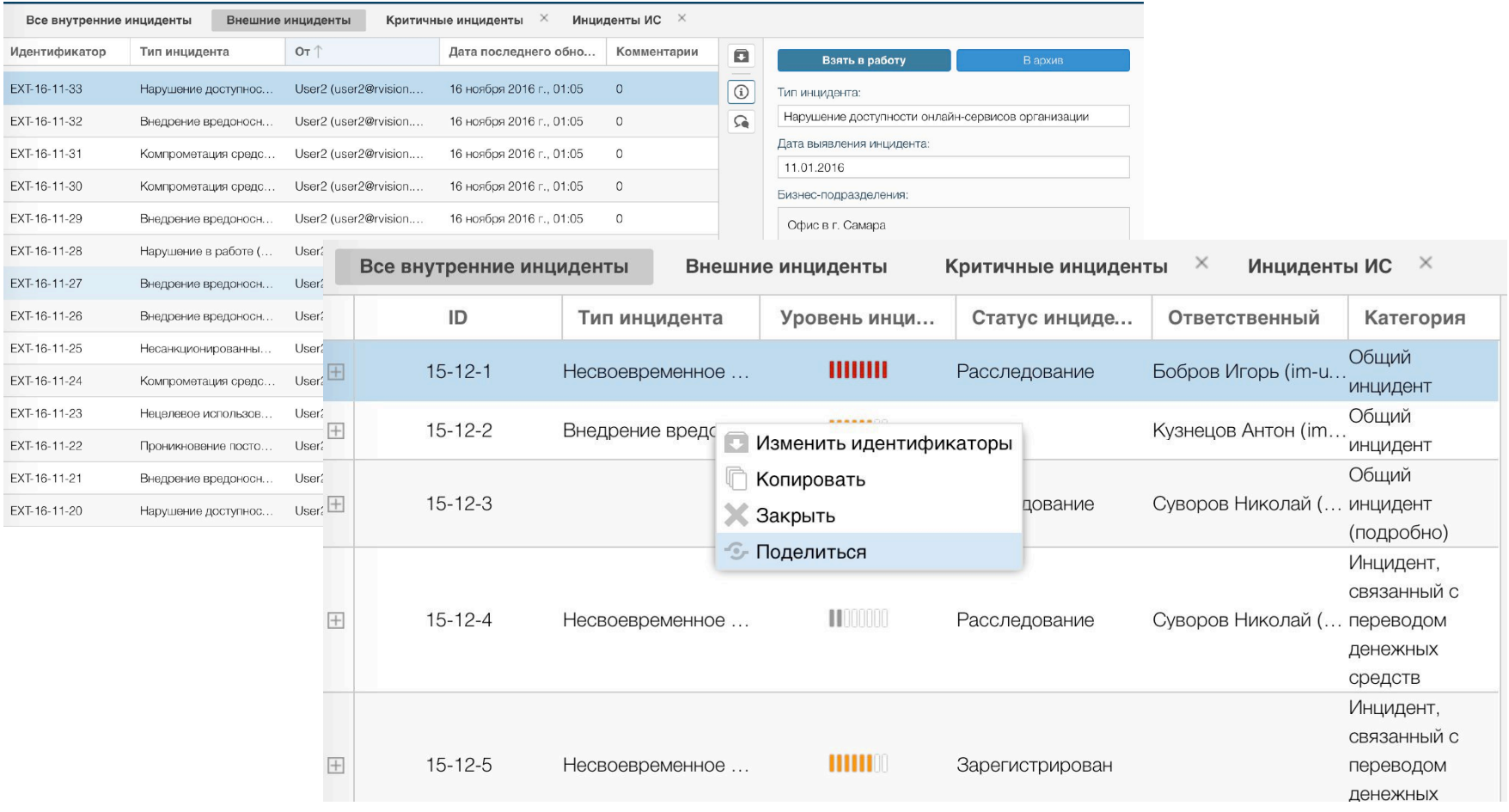

Метрика: Доля инцидентов по типам
60
40
20
1.5%
июнь 2...
июль 2016
август 2016
сентябрь 2016
октябрь 2016
ноябрь 2016


Метрика: Предотвращенный ущерб от инцидентов
30000
20000
10000
26 111 руб.
июнь 2...
июль 2016
август 2016
сентябрь 2016
октябрь 2016
ноябрь 2016

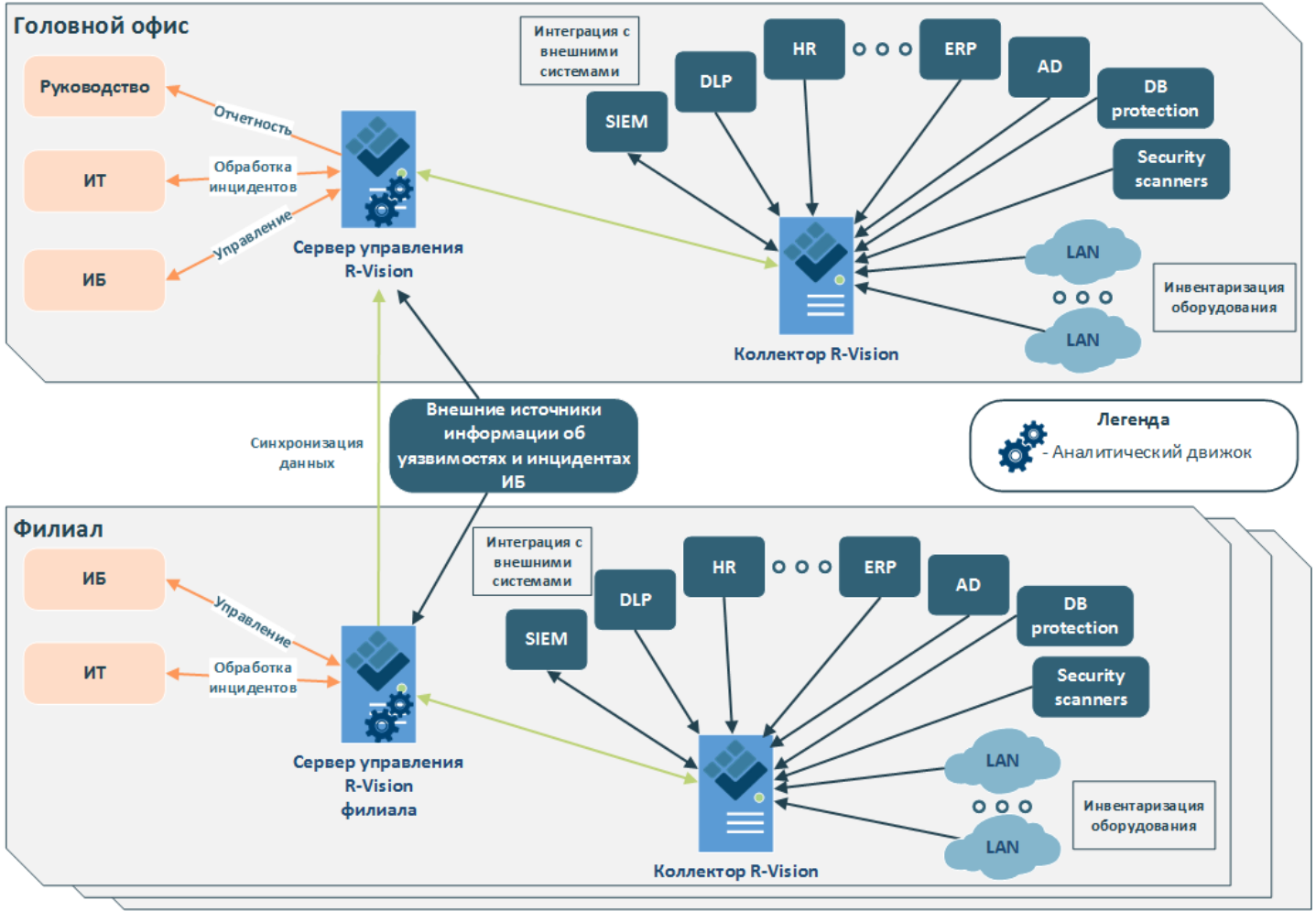

Метрика: Доля инцидентов по типам
60
40
20
Критический уровень
Допустимый уровень
1.5%
июнь 2...
июль 2016
август 2016
сентябрь 2016
октябрь 2016
ноябрь 2016


Метрика: Доля инцидентов по типам
0
0%
июнь 2...
июль 2016
август 2016
сентябрь 2016
октябрь 2016
ноябрь 2016

#10 Обмен информацией по инцидентам



#11 Организация SOC на базе R-Vision IRP




R·Vision
At the root of your security