
R·Vision
At the root of your security

Создание центров мониторинга ГосСОПКА на базе решения R-Vision

Октябрь 2017

Содержание

Правовая основа ГосСОПКА

1. Конституция РФ
2. ФЗ N187 «О безопасности критической информационной инфраструктуры Российской Федерации»
3. Указ Президента РФ N31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»
4. Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ N К 1274
5. Стратегия национальной безопасности РФ до 2020 года и другие нормативно-правовые акты РФ
6. Приказы и методические рекомендации ФСБ России и ФСТЭК России

Субъекты ГосСОПКА

1

Владельцы объектов критической информационной инфраструктуры и информационных ресурсов

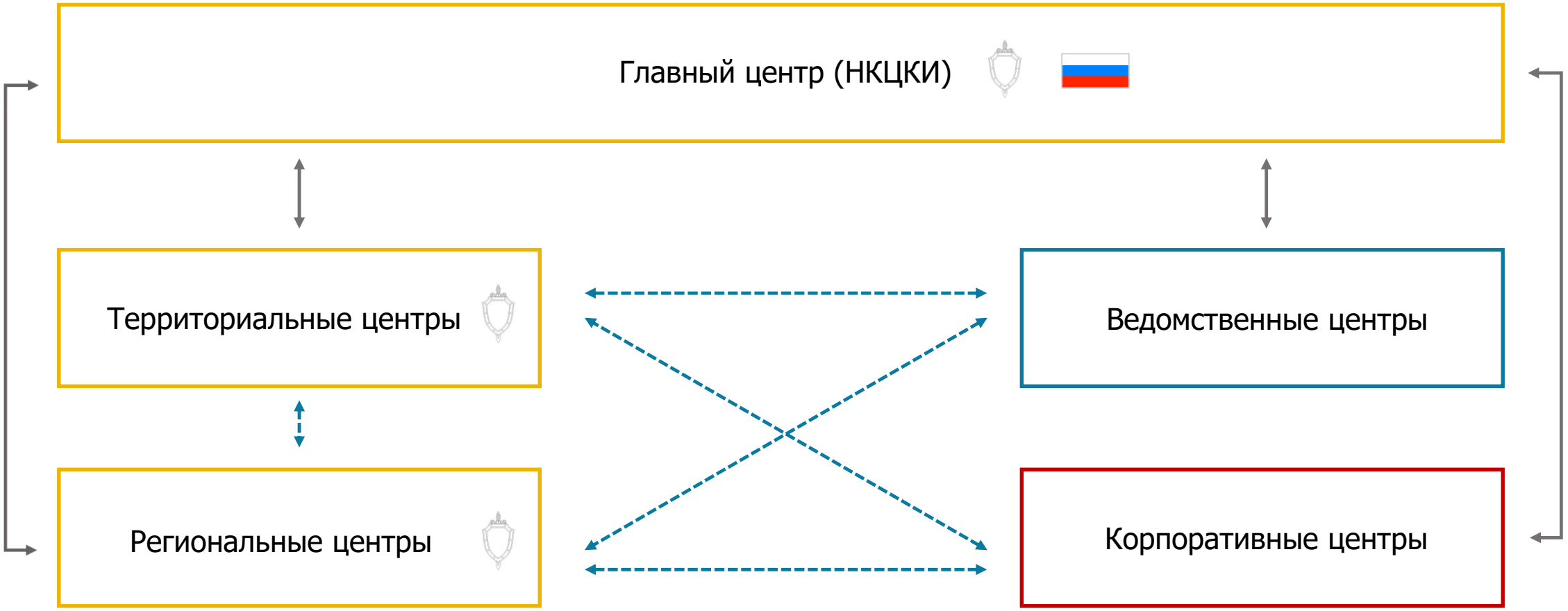
2

Операторы связи

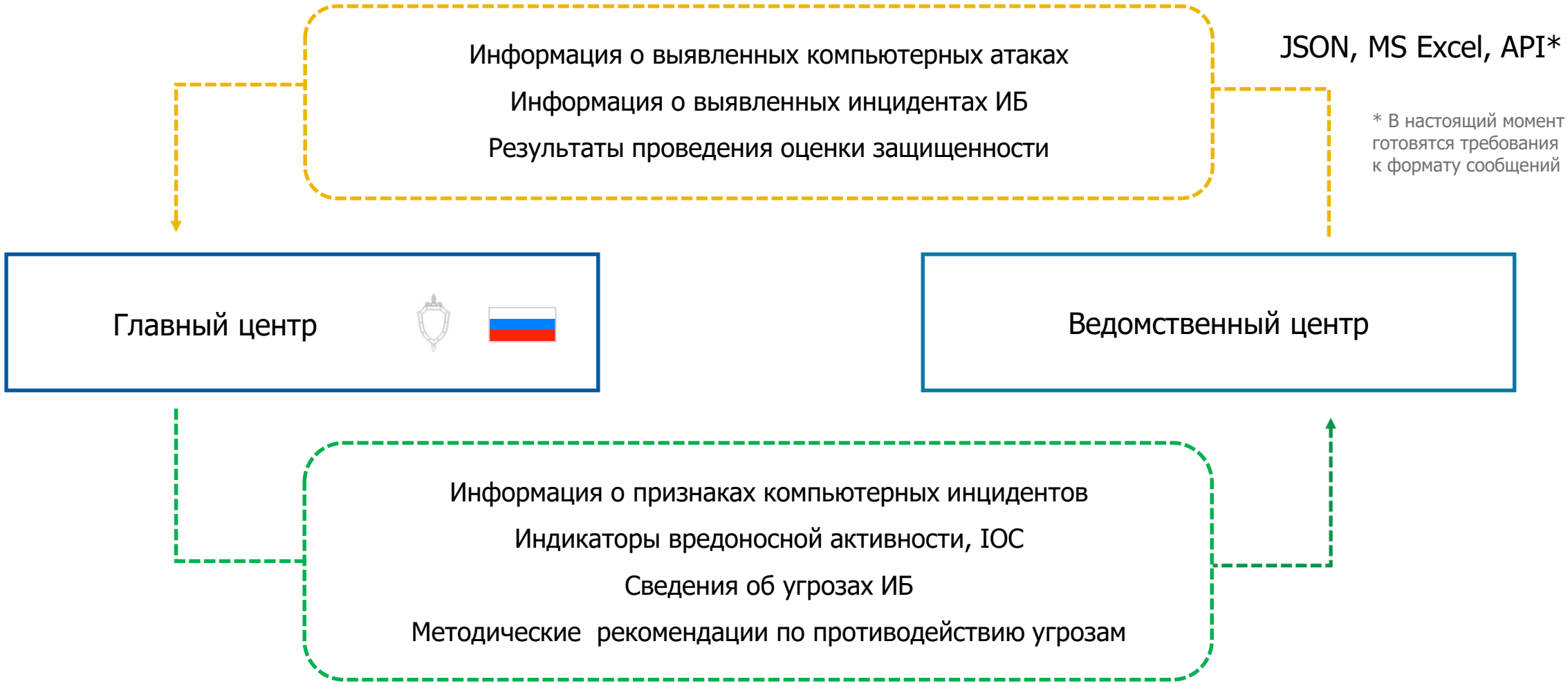
3

Организации-лицензиаты в области защиты информации

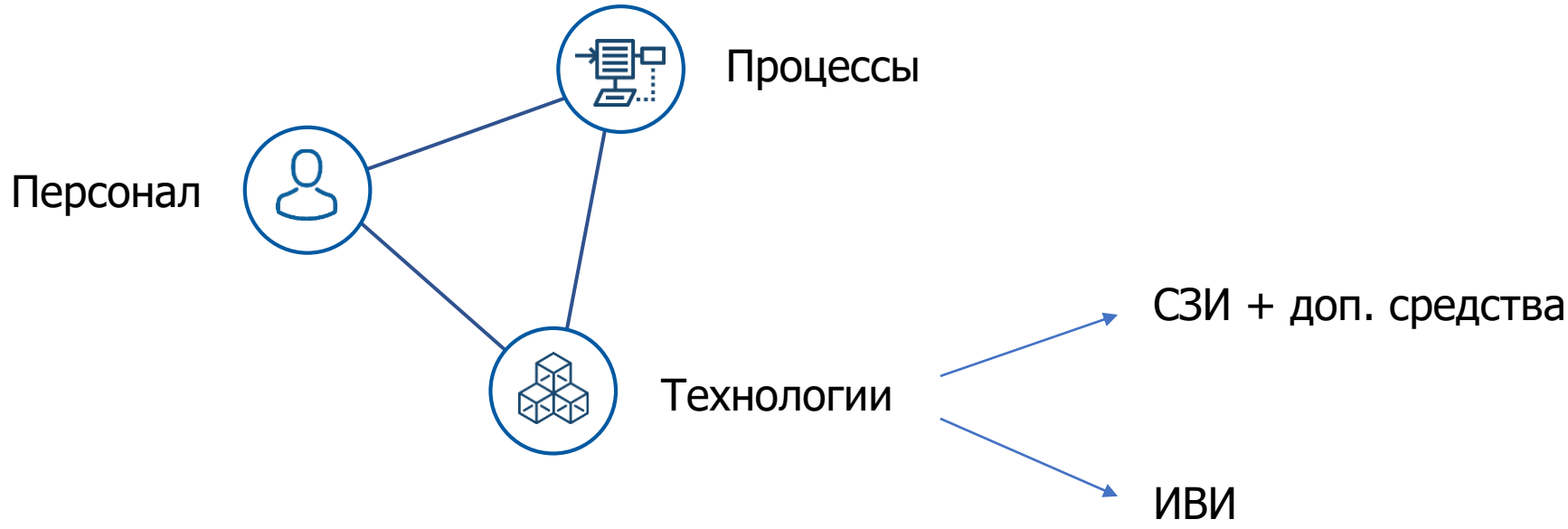
Структура ГосСОПКА



Обмен информацией в ГосСОПКА



Основные элементы центров мониторинга



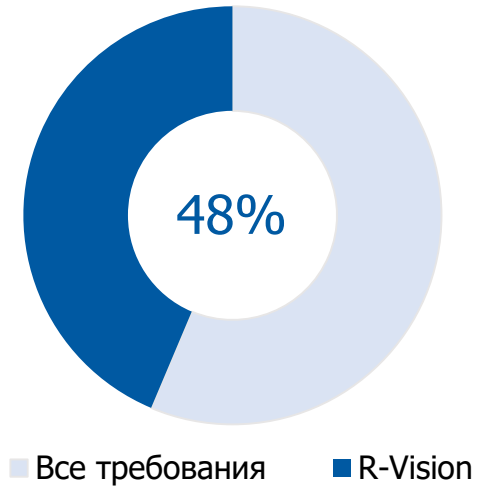
Функции центра мониторинга ГосСОПКА

1. Инвентаризация информационных ресурсов
2. Анализ уязвимостей информационных ресурсов
3. Анализ угроз информационной безопасности
4. Антивирусная защита информационных ресурсов
5. Повышение квалификации персонала информационных ресурсов
6. Прием сообщений о возможных инцидентах от персонала и пользователей информационных ресурсов
7. Обнаружение компьютерных атак
8. Анализ данных о событиях безопасности
9. Регистрация инцидентов
10. Реагирование на инциденты и ликвидация их последствий
11. Установление причин инцидентов
12. Анализ результатов устранения последствий инцидентов

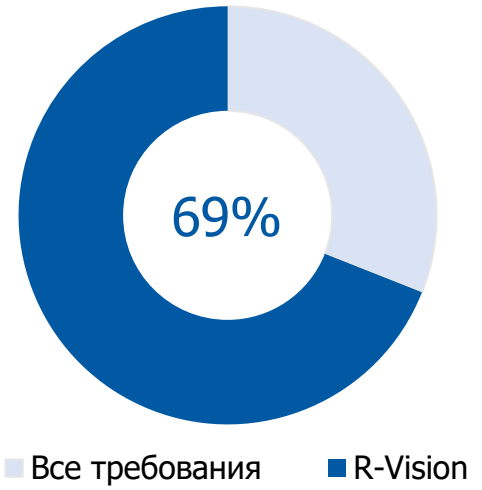
\+ Обмен информацией с Главным центром*

Соответствие метод. рекомендациям ФСБ России по созданию ведомственных центров ГосСОПКА

% соответствия R-Vision функциональным требованиям к ЦМ ГосСОПКА



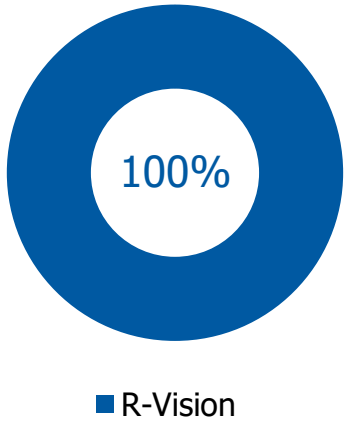
% присутствия в функциональных требованиях к ЦМ R-Vision



Соответствие метод.рекомендациям

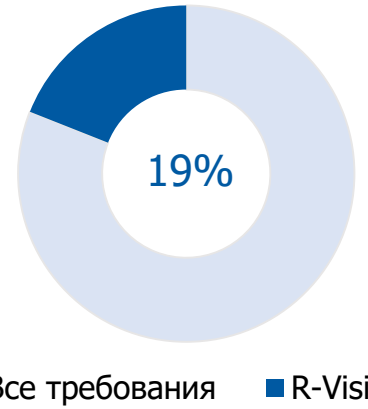
#1

Инвентаризация информационных ресурсов



#2

Анализ уязвимостей информационных ресурсов

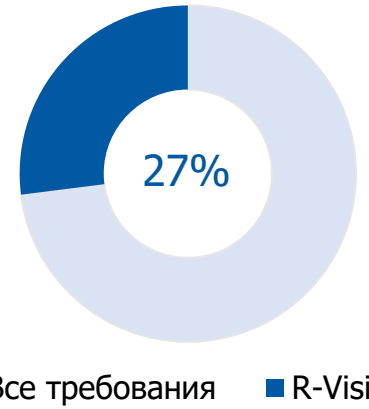


#3

Анализ угроз информационной безопасности

#4

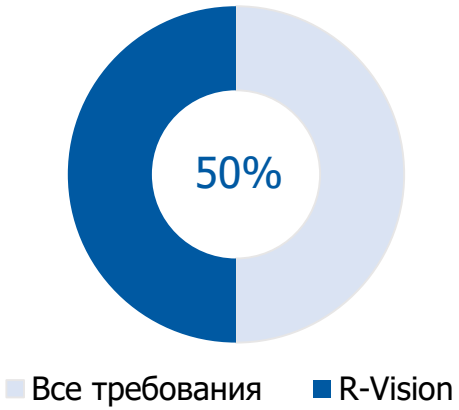
Антивирусная защита информационных ресурсов



Соответствие метод.рекомендациям

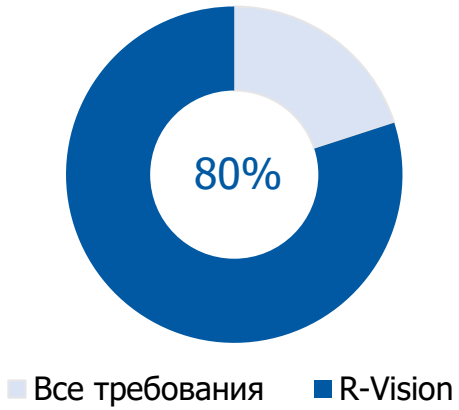
#5

Повышение квалификации персонала ИР



#6

Прием сообщений об инцидентах



#7

Обнаружение компьютерных атак

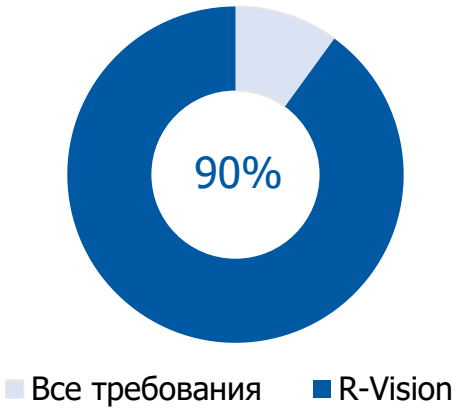
#8

Анализ данных о событиях безопасности

Соответствие метод.рекомендациям

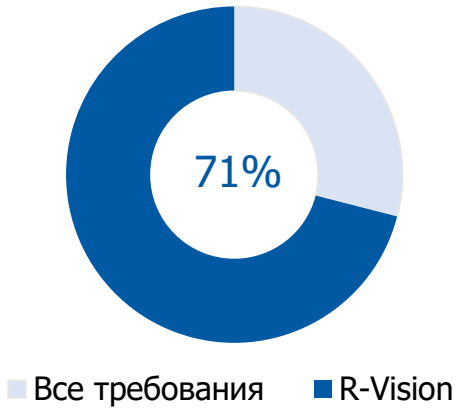
#9

Регистрация инцидентов



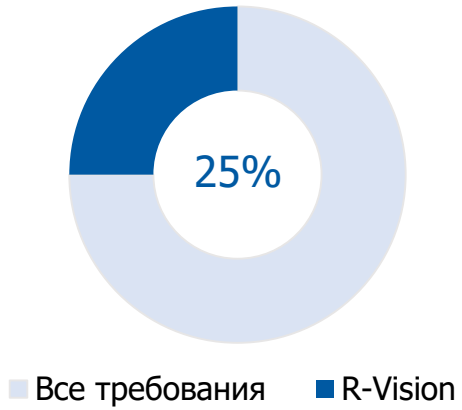
#10

Реагирование на инциденты, устранение последствий



#11

Установление причин инцидентов

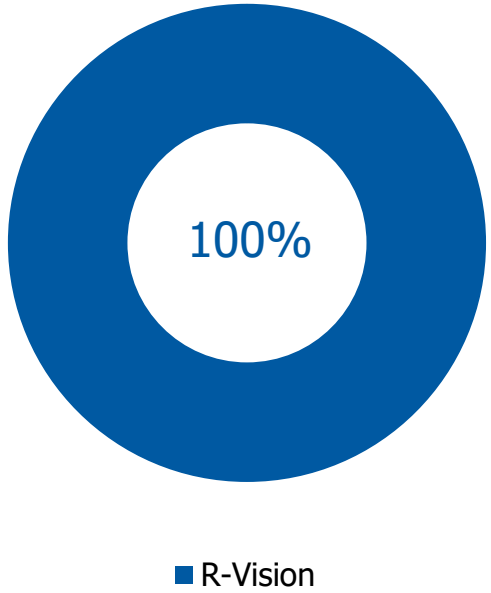


#12

Анализ результатов устранения последствий

#1

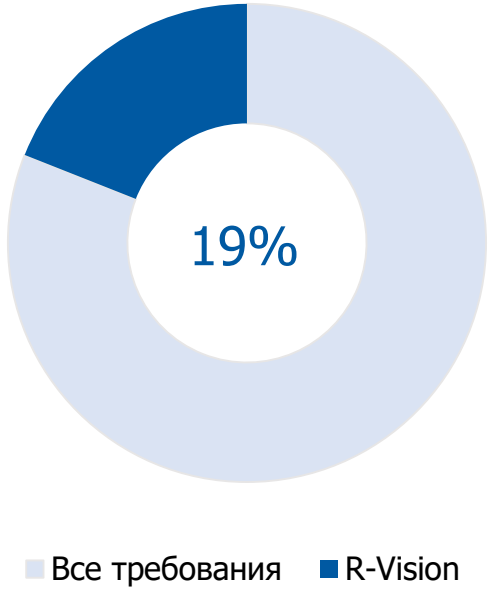
Инвентаризация информационных ресурсов



1. Собственный движок инвентаризации
2. Коннекторы к различным поставщикам инвентаризационной информации: CMDB-решениям, сканерам защищенности, антивирусам и др.
3. Обогащение информации о ИР с различных источников
4. Управление жизненным циклом ИТ-активов
5. Взаимосвязь информационных активов и оборудования

#2

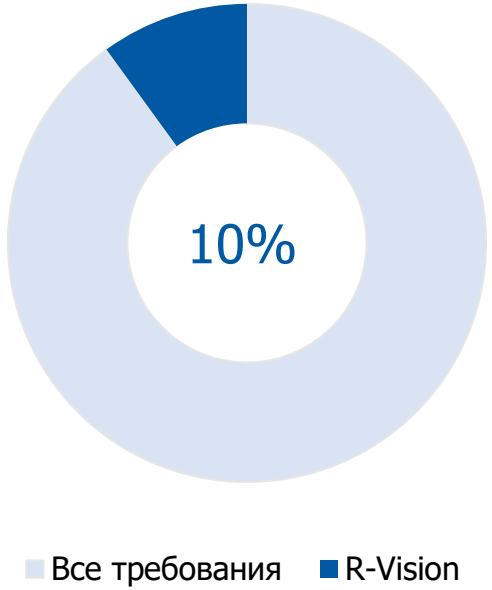
Анализ уязвимостей информационных ресурсов



1. Коннекторы ко всем распространённым сканерам защищенности
2. Анализ и управление уязвимостями
3. Поддержка базы угроз Vulners
4. Отображение информации об уязвимостях с различных источников
5. Взаимосвязь активов и уязвимостей

#3

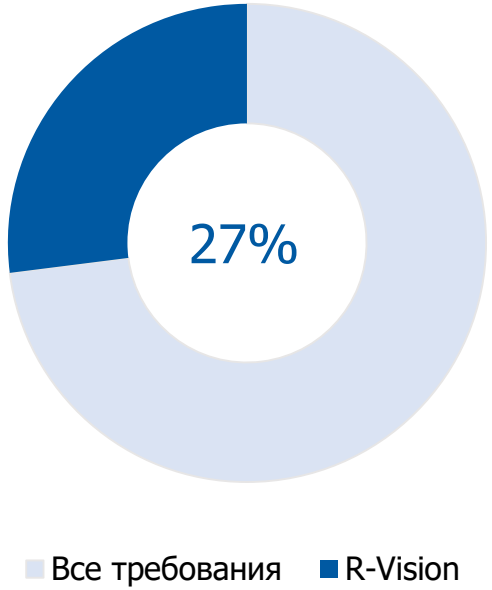
Анализ угроз информационной безопасности



1. Анализ сведений по обнаруженным уязвимостям ИР с различных источников
2. Поиск ПО на объектах ИР (на основе полученной информации по угрозам)
3. Моделирование угроз
4. Определение ложных срабатываний по уязвимостям
5. Визуализация и связь ИТ-активов и уязвимостей

#4

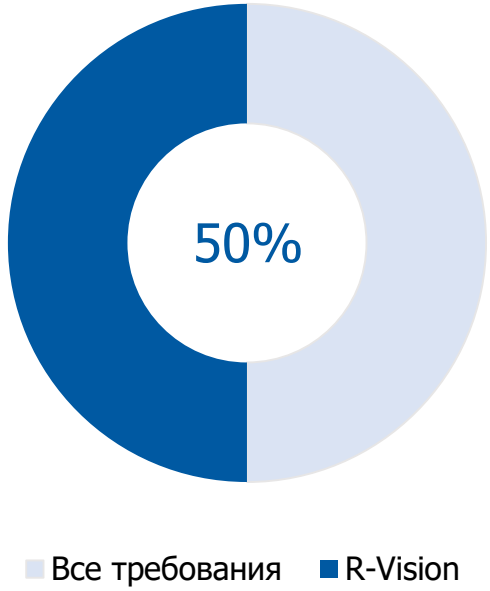
Антивирусная защита информационных ресурсов



1. Документационное обеспечение деятельности по АЗ
2. Единый центр документации
3. Учет требований регуляторов и собственных стандартов
4. Средство дополнительного контроля состояния агентов САЗ

#5

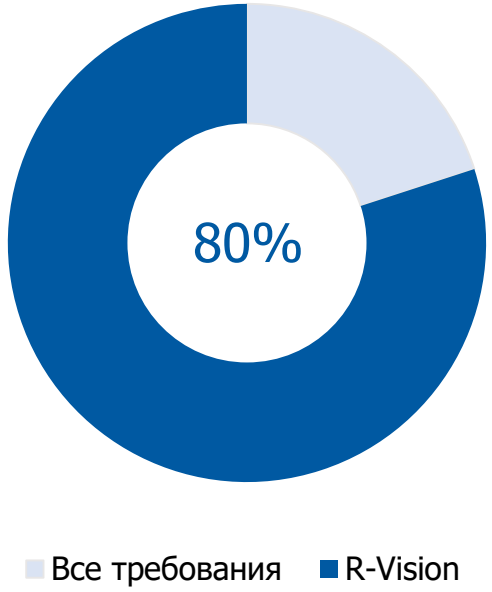
Повышение квалификации персонала информационных ресурсов



1. Интеграция с сервисом Antiphish.ru
2. Возможность локального размещения сервиса по обучению пользователей в организации
3. Наличие различных программ обучения с возможностью проверки знаний
4. Управление обучением, задание расписания, учет статистики, рейтингов, отчетность
5. Имитация действий злоумышленников, выявление наименее осведомленных пользователей

#6

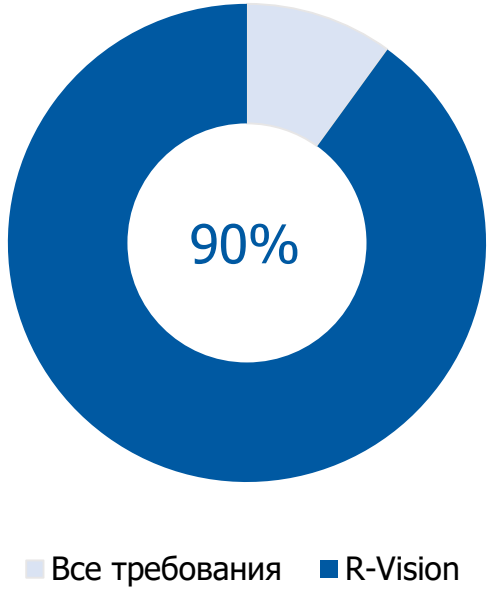
Прием сообщений об инцидентах



1. Обеспечение деятельности по приему, обработке и хранению сообщений об инцидентах в ЦМ
2. Прием сообщений от других сегментов ГосСОПКА
3. Прием сообщений об инцидентах операторами ЦМ (почта, телефон, веб-портал)
4. Встроенный почтовый сервер, прием сообщений в режиме online
5. Прием сообщений об инцидентах с аналогичной системы R-Vision, с SaaS сервиса JSOC

#9

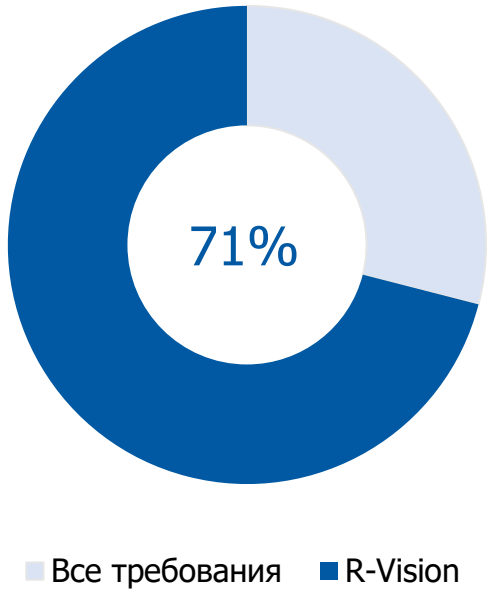
Регистрация инцидентов



1. Управление жизненным циклом инцидентов, накопление и обогащение информации в единой БД
2. Регистрация инцидентов через веб-форму Оператором ЦМ вручную
3. Регистрация инцидентов посредством интеграции с SIEM + 2х сторонний обмен статусами
4. Регистрация и обработка почтовых сообщений с различных СЗИ (в автоматическом режиме)
5. Парсинг сообщений по тегам и регулярным выражениям

#10

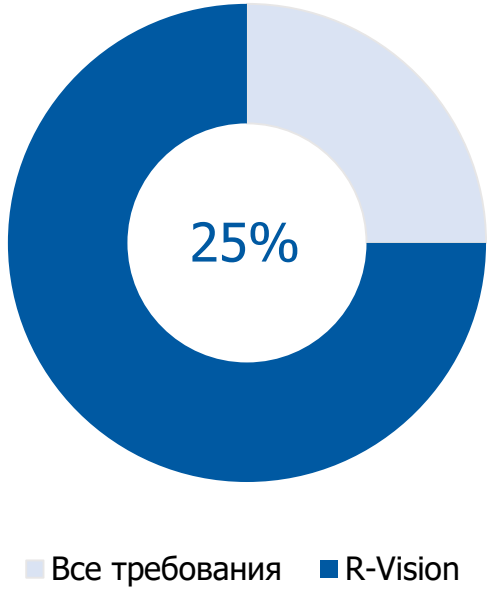
Реагирование на инциденты и ликвидация их последствий



1. Автоматизация функций по назначению, уведомлению ответственных, постановки задач и сроков
2. Наличие конструктора правил реагирования и сценариев реагирования, визуализация сценариев
3. Активные меры воздействия – скрипты реагирования и команды отправляемые на сетевые СЗИ
4. Контроль и управление задачами персонала ЦМ
5. Автоматизация функций по сбору свидетельств и доказательств

#11

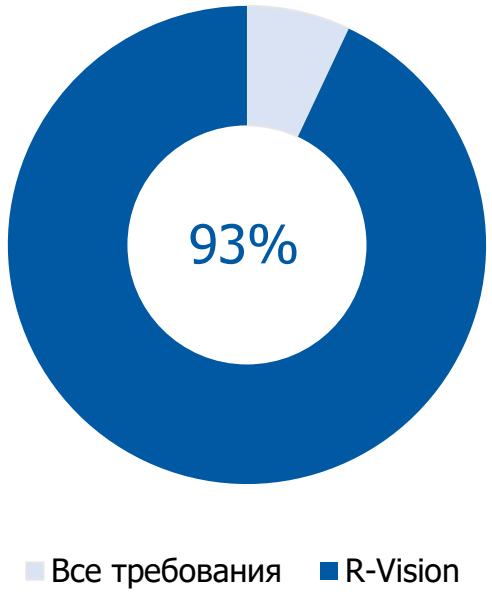
Установление причин инцидентов



1. Анализ сведений по инцидентам
2. Анализ свидетельств, полученных в том числе в автоматическом режиме
3. Анализ принятых мер
4. Анализ существующих процессов, методических документов
5. Анализ взаимосвязей инцидентов и информационных активов и их свойств

#12

Анализ результатов устранения последствий



1. Оценка предотвращенного ущерба от реализации инцидентов
2. Анализ действий персонала ЦМ
3. Оценка ущерба от реализации инцидентов
4. Анализ сроков реагирования на инциденты
5. Анализ принятых мер и их корректировка

?

Вопросы

8-800-350-77-57

sales@rvision.pro

Для лицензиатов ФСБ и ФСТЭК России: получить сведения о том, с помощью каких средств защиты и вспомогательных средств обеспечить выполнение функциональных требований для различных типов ЦМ, можно, обратившись к нам.

Информация сведена в файл MS Excel с указанием решений