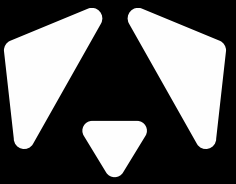


ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Подключение к ГосСОПКА. Техвопросы

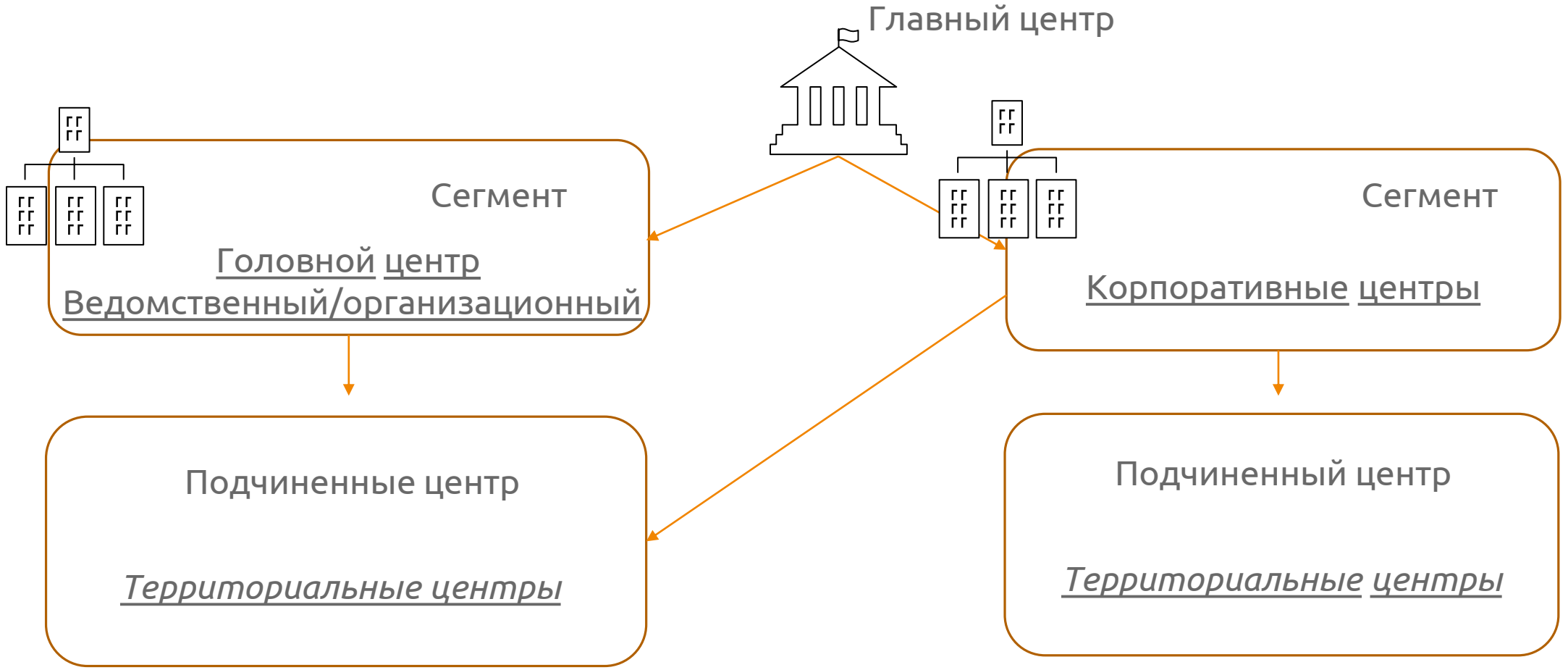
Алексей Васильев, Руководитель Центра мониторинга

Как получить действительно работающее решение

План

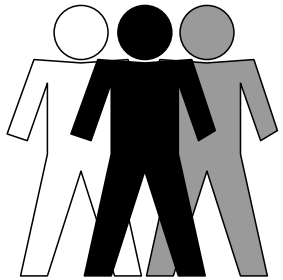
- Определение точки подключения
- Ресурсы
- Обмен сведениями
- Обнаружение атак
- Взаимодействие

Определение точки подключения



Необходимые ресурсы

Силы субъекта

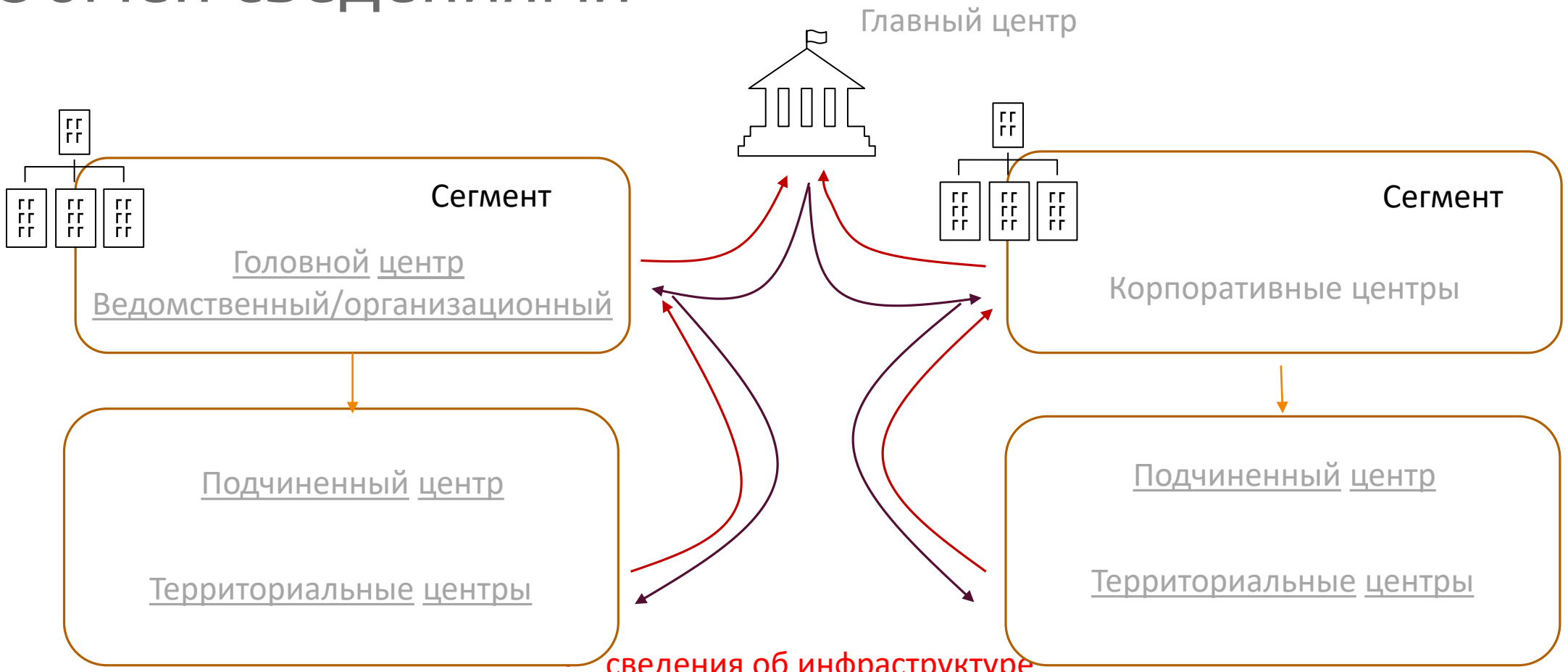


Персонал

Средства субъекта

Технологии,
технические,
программные,
лингвистические,
правовые,
организационные средства,
включая сети и средства связи,
средства сбора и анализа информации,
поддержки принятия управленческих решений

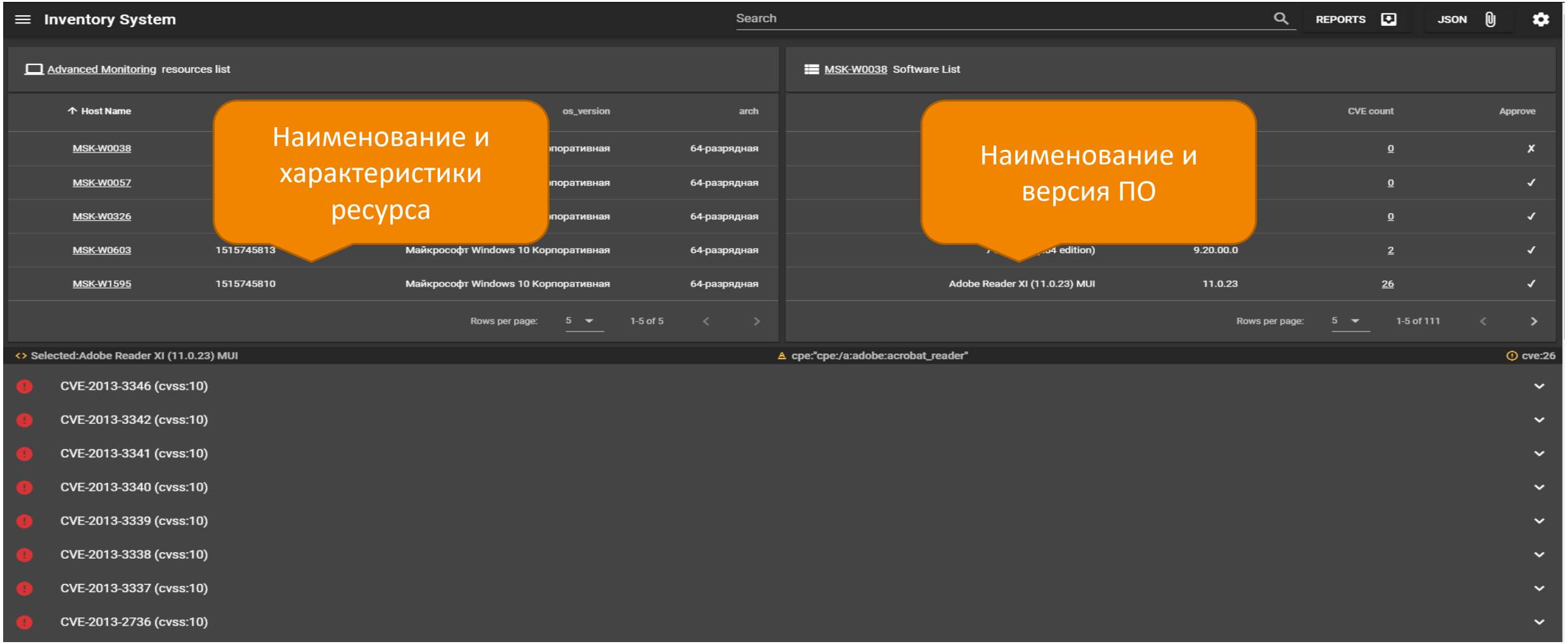
Обмен сведениями



- сведения об инфраструктуре
- компьютерных инцидентах
- индикаторы компрометации
- методические рекомендации

Сведения об инфраструктуре

Inventory System - Система инвентаризации



Сведения по уязвимостям ИР

Ввод в эксплуатацию

анализ проектной, конструкторской и эксплуатационной документации
анализ исходного кода

В месяц

сетевое и системное сканирование, анализ настроек
контроль выполнения требований безопасности

В квартал

контроль устранения ранее выявленных уязвимостей и недостатков

В год

тестирование на проникновение и нагрузочное тестирование

В 2 года

оценка соответствия мер защиты

Хранение сведений 3 года

Vulnerability Prevention – Сведения по уязвимостям ИР

- Анализ в реальном времени
- Экспертная поддержка
- Интерфейс взаимодействия для обработки уязвимостей и принятия решений

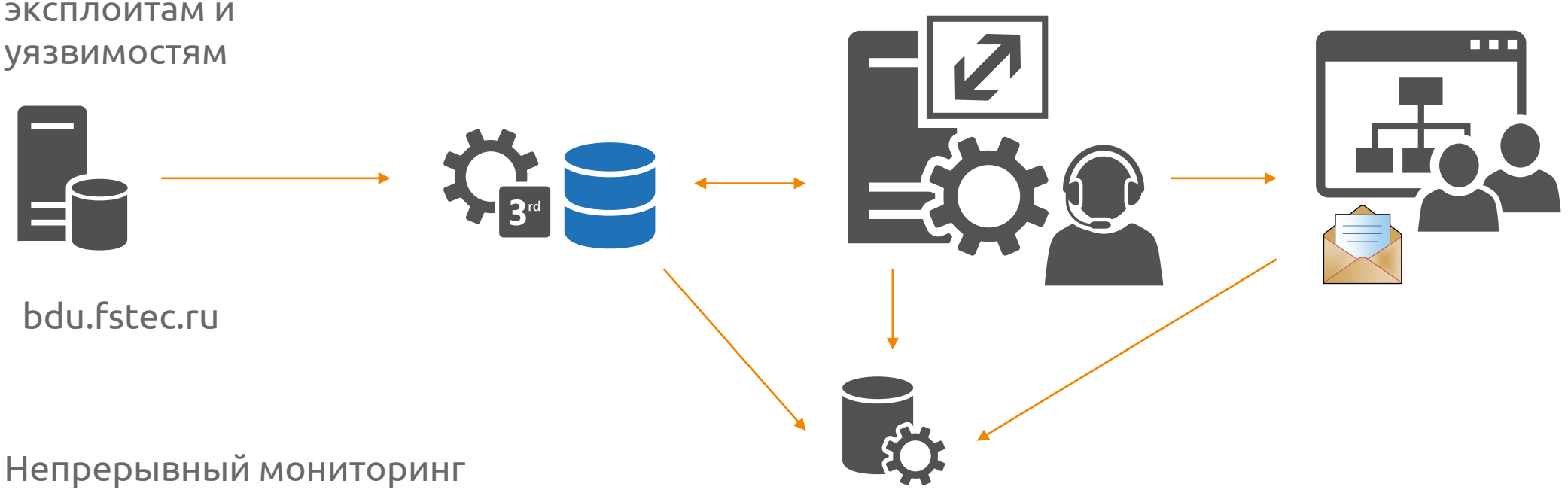
Обработка уязвимостей – Vulnerability Prevention

Вендоры
Информационные ресурсы по эксплойтам и уязвимостям

Формирование базы знаний

Информационно-аналитический центр

Пользователи системы
Реагирование



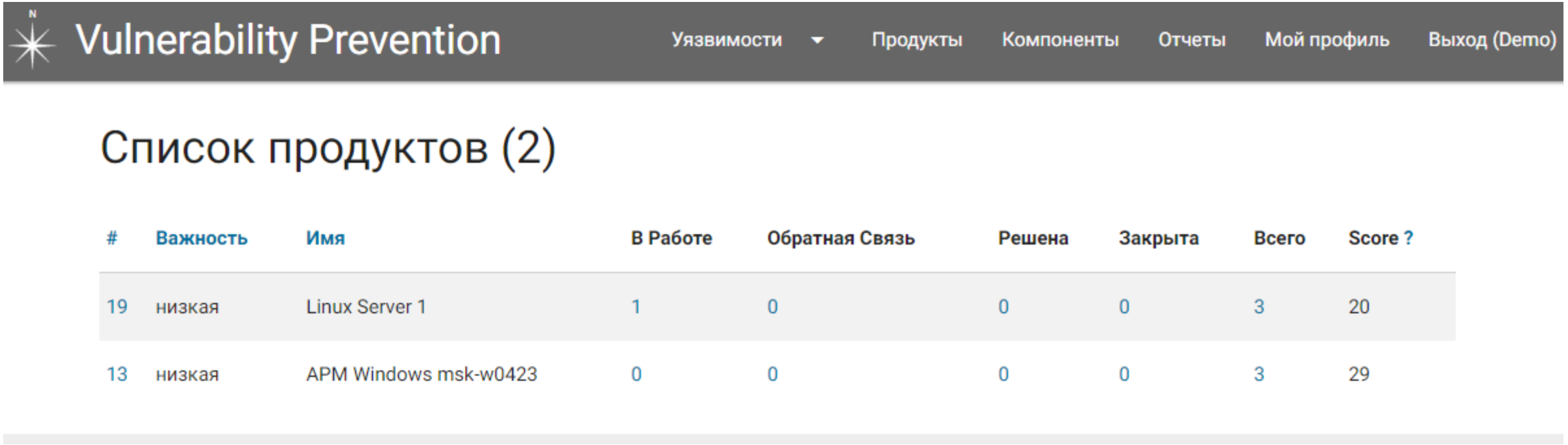
bdu.fstec.ru

Непрерывный мониторинг

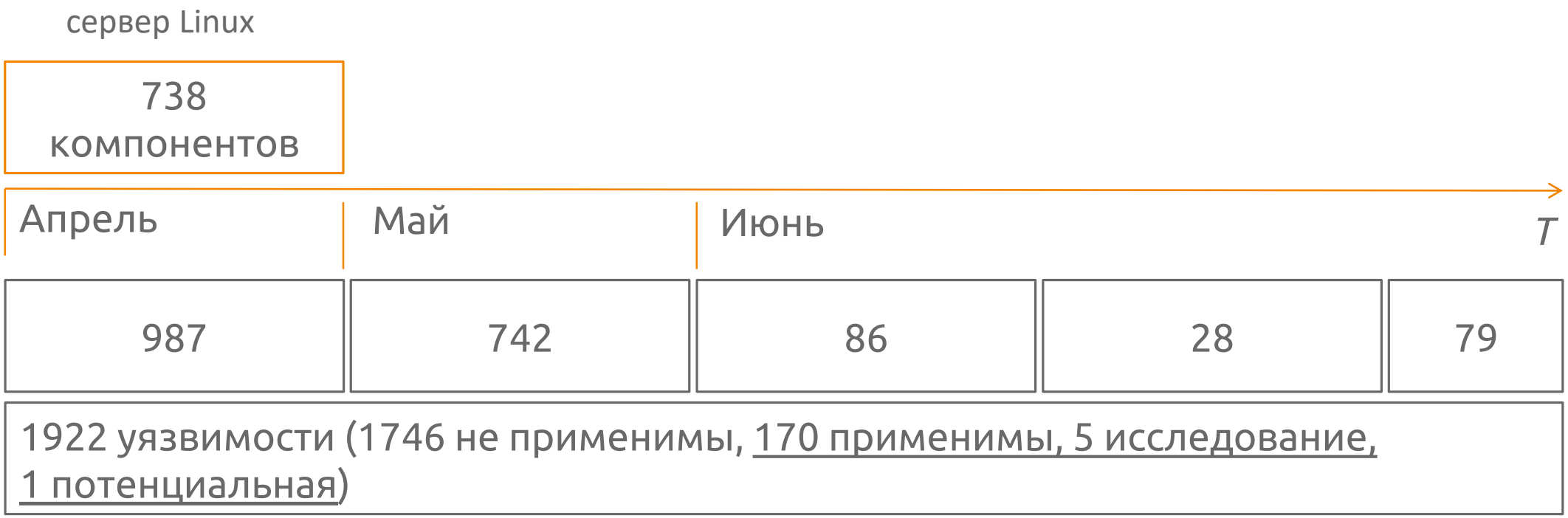
Хранение сведений 3 года

Сопоставление данных ИР и уязвимостей

Система управления уязвимостями

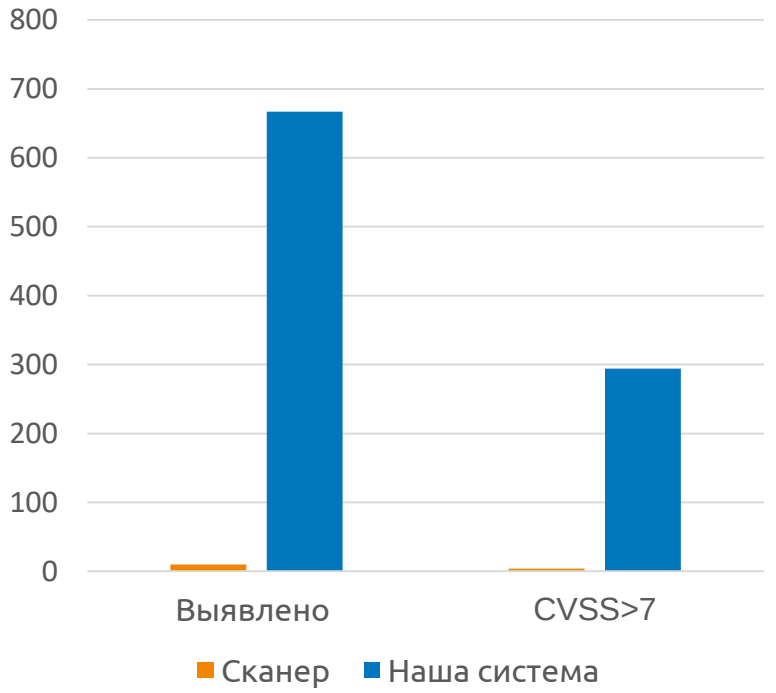


Пример процесса анализа уязвимостей сервера Linux (Vulnerability prevention)

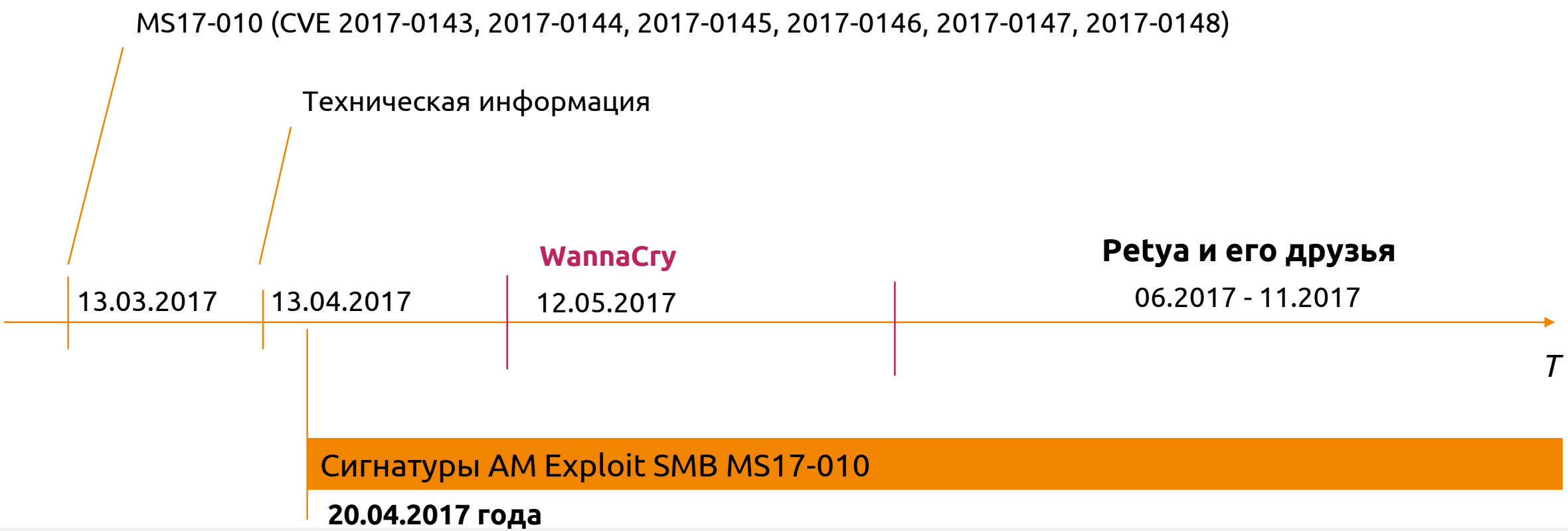


Сравнение результатов анализа уязвимостей

	Сканер	**Vulnerability Prevention**
Всего	10	667
Высокая критичность	4	294



Предупреждение угроз



Обнаружение компьютерных атак

False Positive
False Negative
True Positive
True Negative

Собирать все

Много шума

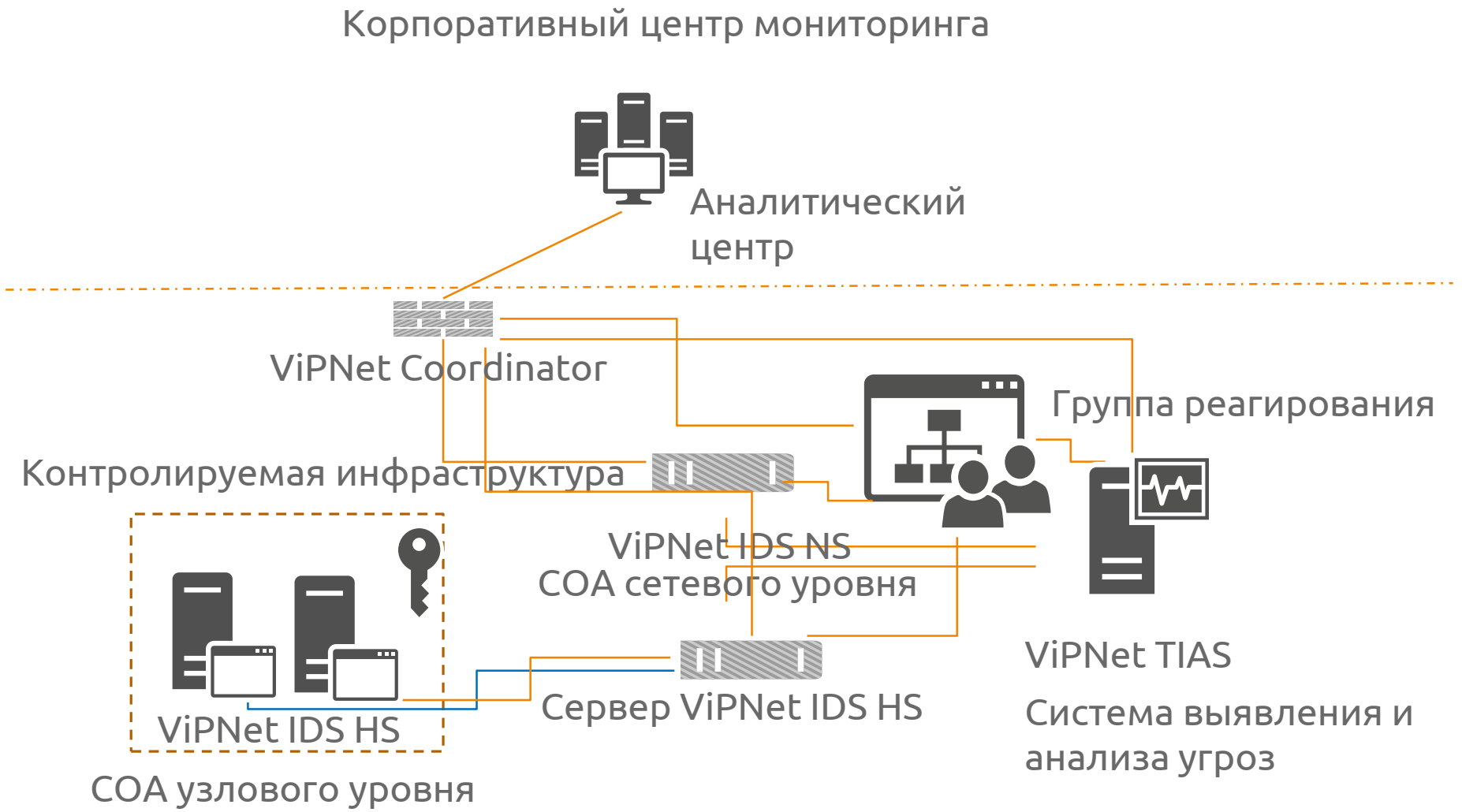
Детектируем, что знаем

Быстрое и точное реагирование

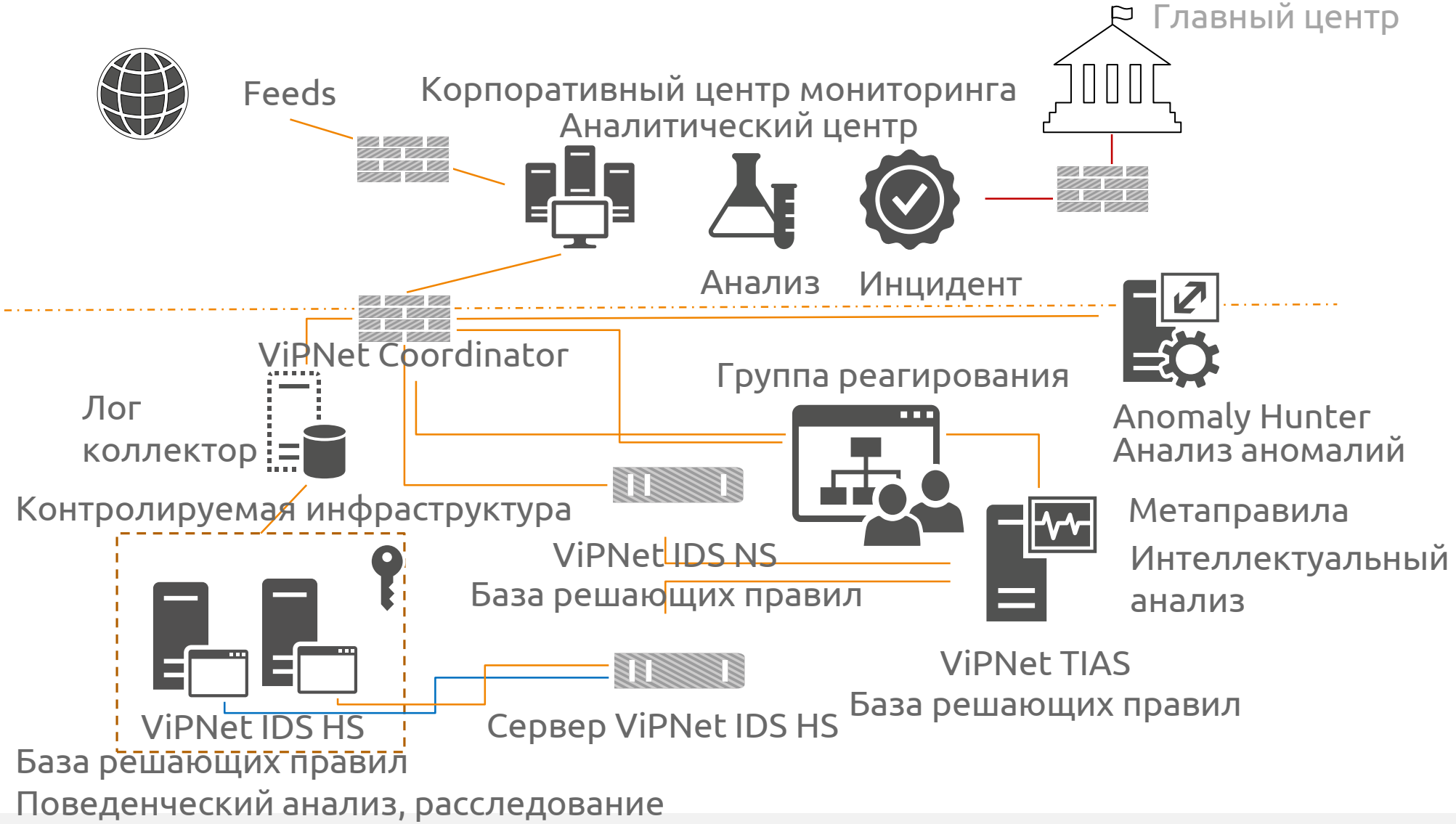
Анализируем новое

Постоянное обновление базы знаний

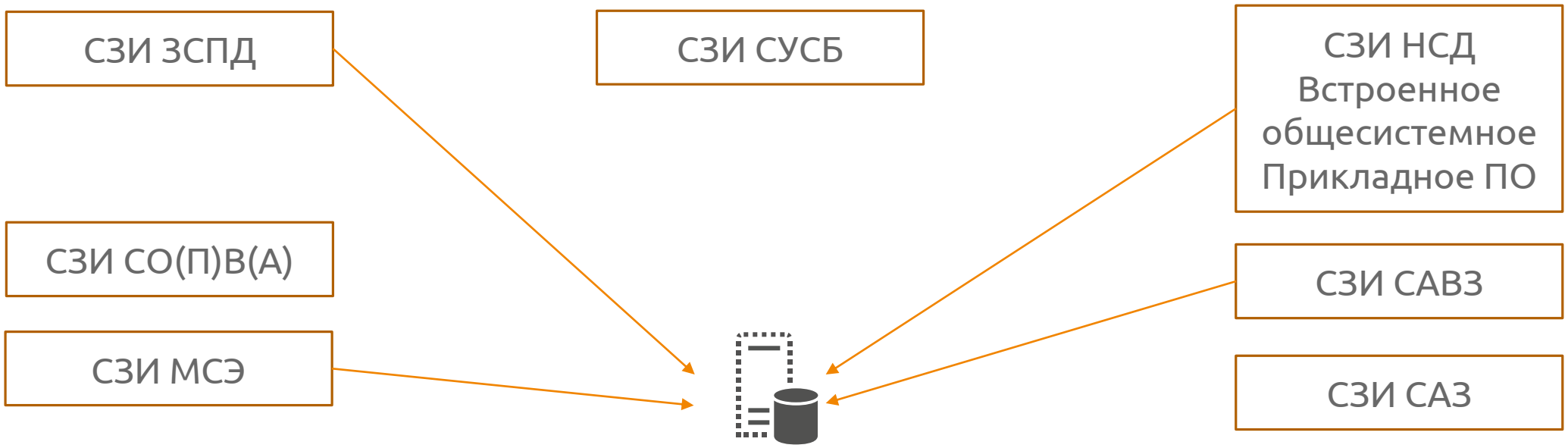
Обнаружение компьютерных атак



Анализ данных о событиях



Контролируемая инфраструктура и применяемые средства защиты информации

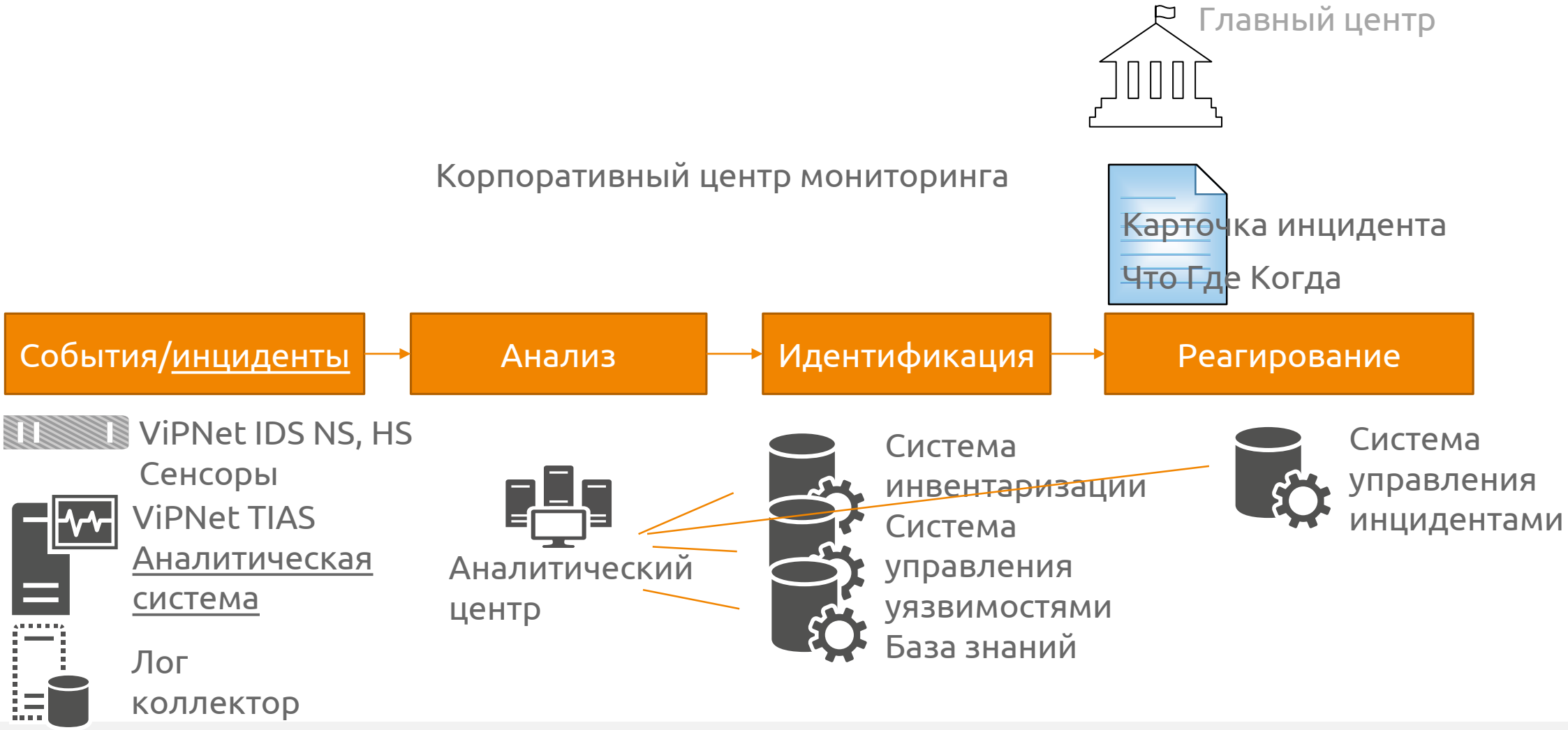


Лог коллектор

Правила корреляции

Постоянно обновляемая база решающих правил по новым угрозам для ViPNet IDS NS(более 5000), HS (более 800), правила корреляции и интеллектуальный модуль для ViPNet TIAS

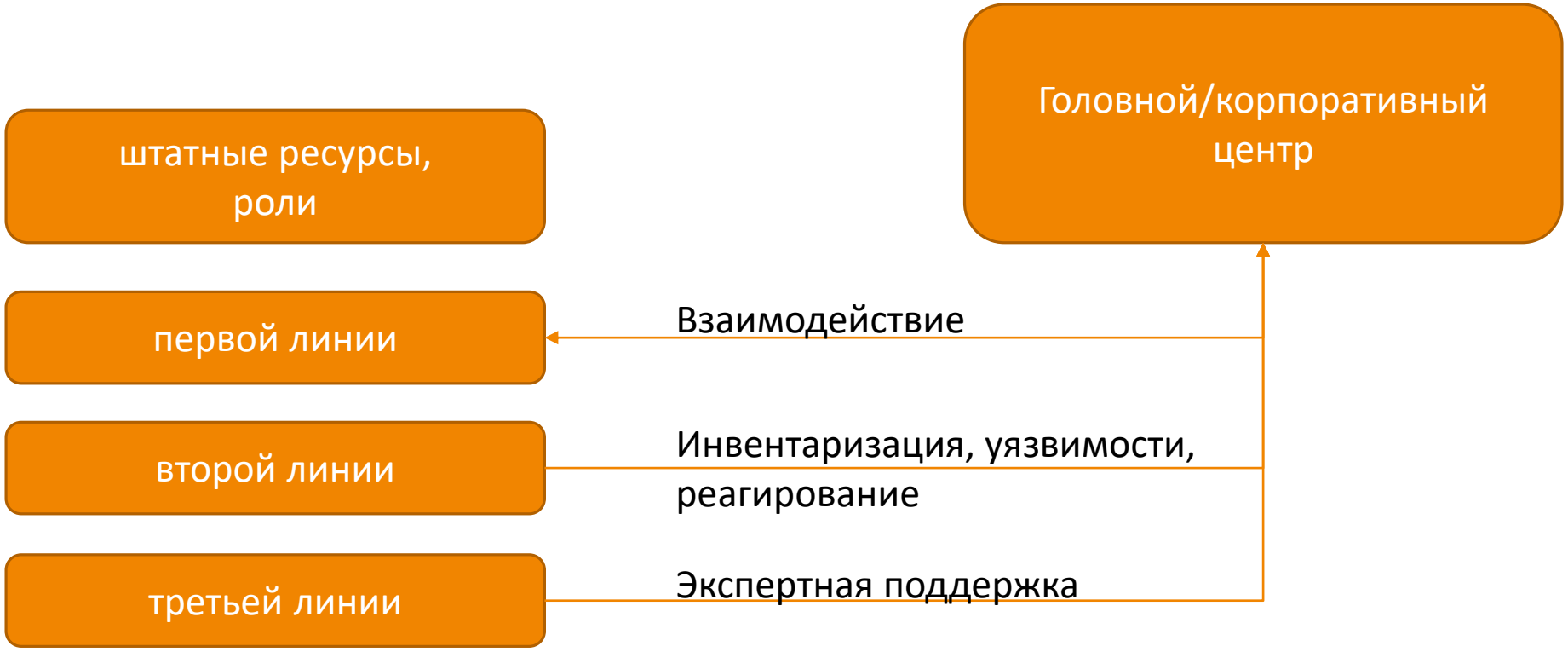
Регистрация инцидентов



Меры защиты

- анализ угроз безопасности информации и рисков их реализации
- контроль (анализ) защищенности информации
- управление конфигурацией средств защиты
- сбор и анализ информации
- поддержка принятия управленческих решений
- регистрация и анализ событий безопасности
- выявление инцидентов и реагирование на них
- обеспечение действий в нештатных ситуациях
- информирование и обучение персонала

Организационная структура сегмента



Спасибо за внимание!

Алексей Васильев

Начальник отдела разработки и эксплуатации систем мониторинга и аналитики

Руководитель Центра мониторинга

Aleksey.Vasilyev@amonitoring.ru