

ПЕРСПЕКТИВНЫЙ  
МОНИТОРИНГ

# Подключение к ГосСОПКА. Техвопросы

Алексей Васильев, Руководитель Центра мониторинга

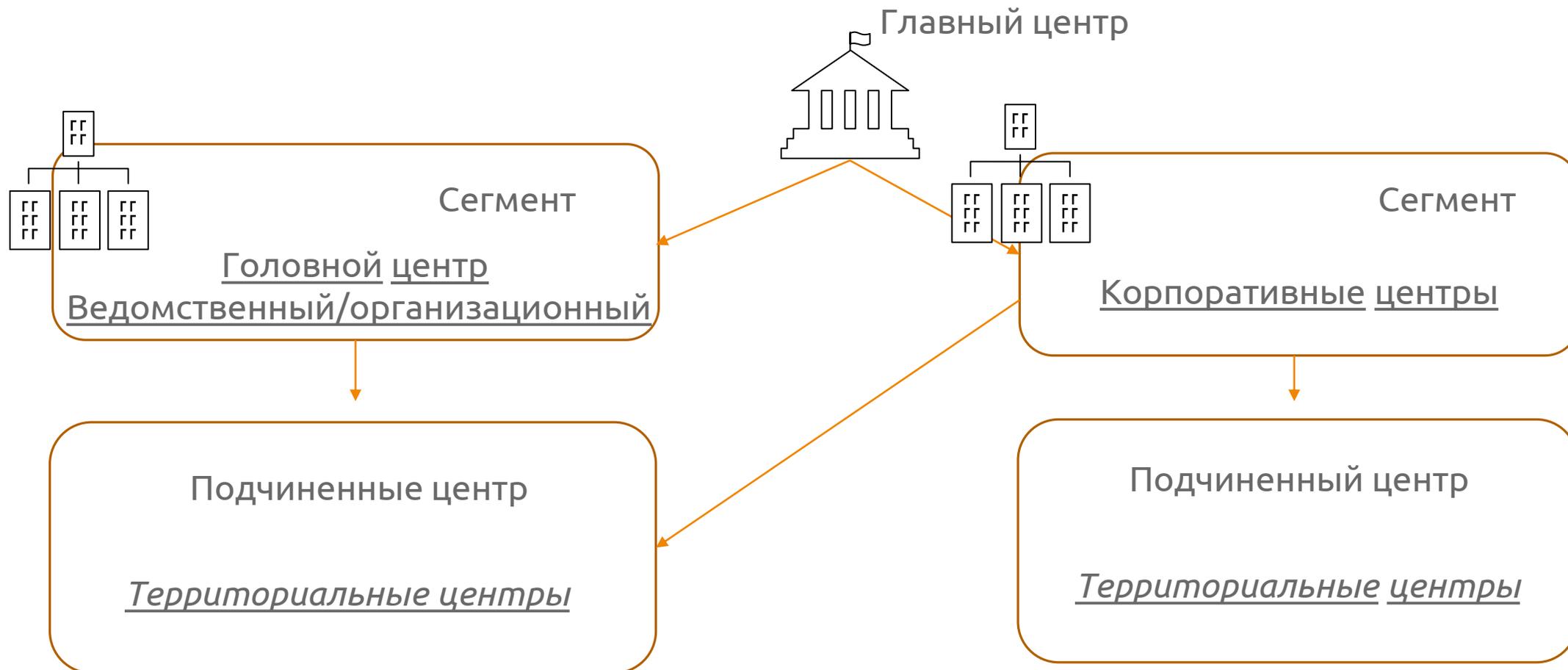
---

# Как получить действительно работающее решение

## План

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

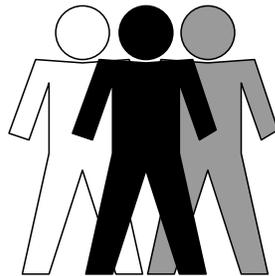
# Определение точки подключения





# Необходимые ресурсы

Силы субъекта



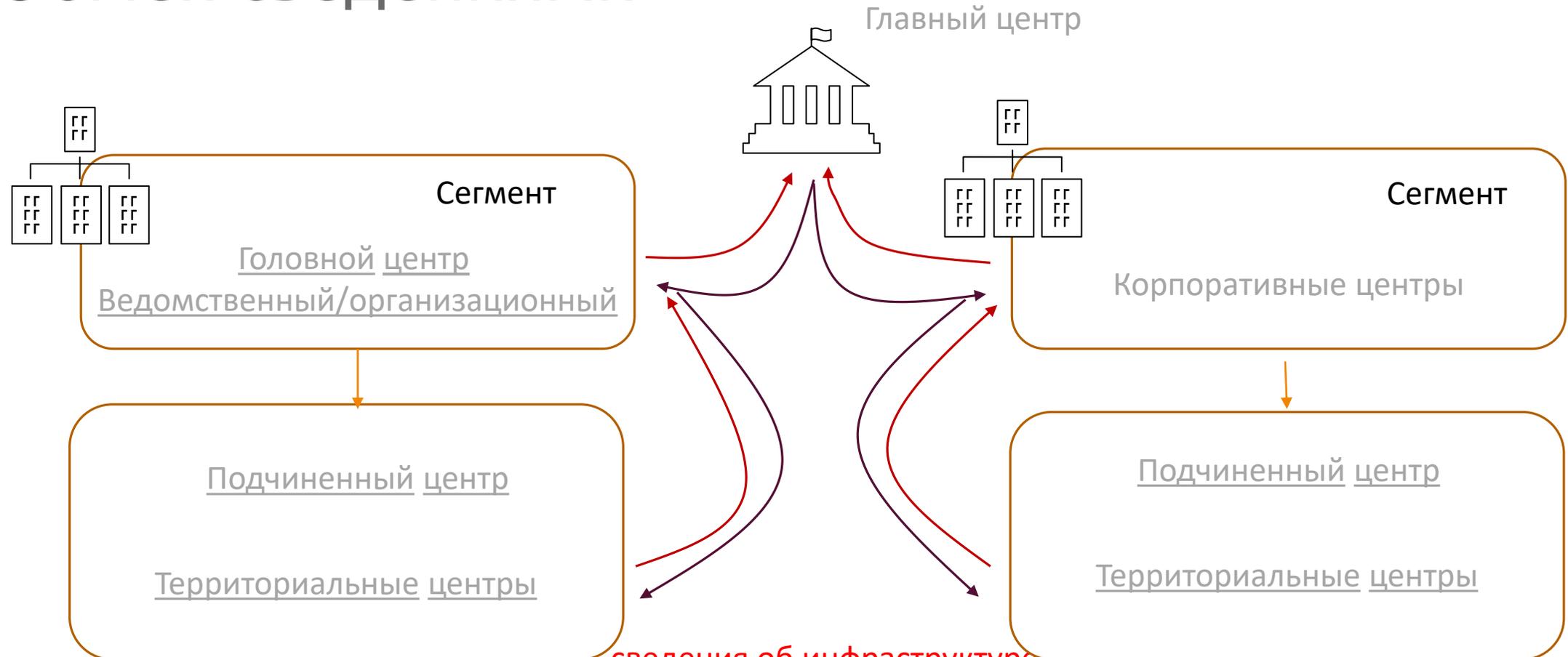
Персонал

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

Inventory System

Search

REPORTS

JSON

Advanced Monitoring resources list

Host Name	os_version	arch
MSK-W0038	Корпоративная	64-разрядная
MSK-W0057	Корпоративная	64-разрядная
MSK-W0326	Корпоративная	64-разрядная
MSK-W0603	1515745813 Майкрософт Windows 10 Корпоративная	64-разрядная
MSK-W1595	1515745810 Майкрософт Windows 10 Корпоративная	64-разрядная

Наименование и характеристики ресурса

MSK-W0038 Software List

Software Name	Version	CVE count	Approve
MSK-W0038		0	X
MSK-W0057		0	✓
MSK-W0326		0	✓
MSK-W0603	7 (64 edition)	2	✓
MSK-W1595	Adobe Reader XI (11.0.23) MUI	26	✓

Наименование и версия ПО

Selected: Adobe Reader XI (11.0.23) MUI

cpe:"cpe:/a:adobe:acrobat\_reader"

cve:26

- ! CVE-2013-3346 (cvss:10)
- ! CVE-2013-3342 (cvss:10)
- ! CVE-2013-3341 (cvss:10)
- ! CVE-2013-3340 (cvss:10)
- ! CVE-2013-3339 (cvss:10)
- ! CVE-2013-3338 (cvss:10)
- ! CVE-2013-3337 (cvss:10)
- ! CVE-2013-2736 (cvss:10)



# 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



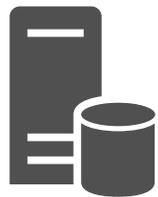
# Vulnerability Prevention – Сведения по уязвимостям ИР

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



# Обработка уязвимостей – Vulnerability Prevention

Вендоры  
Информационные  
ресурсы по  
эксплоитам и  
уязвимостям

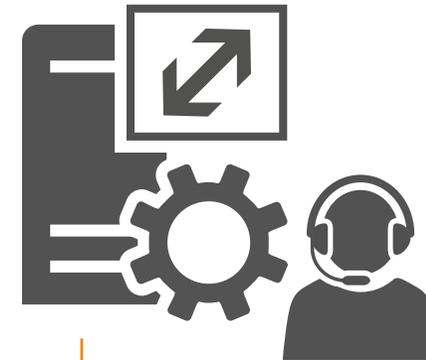


bdu.fstec.ru

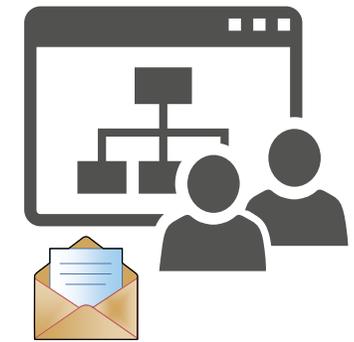
Формирование  
базы знаний



Информационно-  
аналитический  
центр

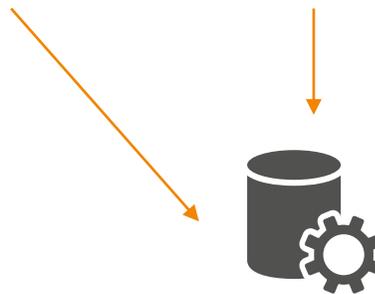


Пользователи  
системы  
Реагирование



Непрерывный мониторинг

Хранение сведений 3 года



Сопоставление данных  
IP и уязвимостей

# Система управления уязвимостями



Vulnerability Prevention

Уязвимости ▾

Продукты

Компоненты

Отчеты

Мой профиль

Выход (Demo)

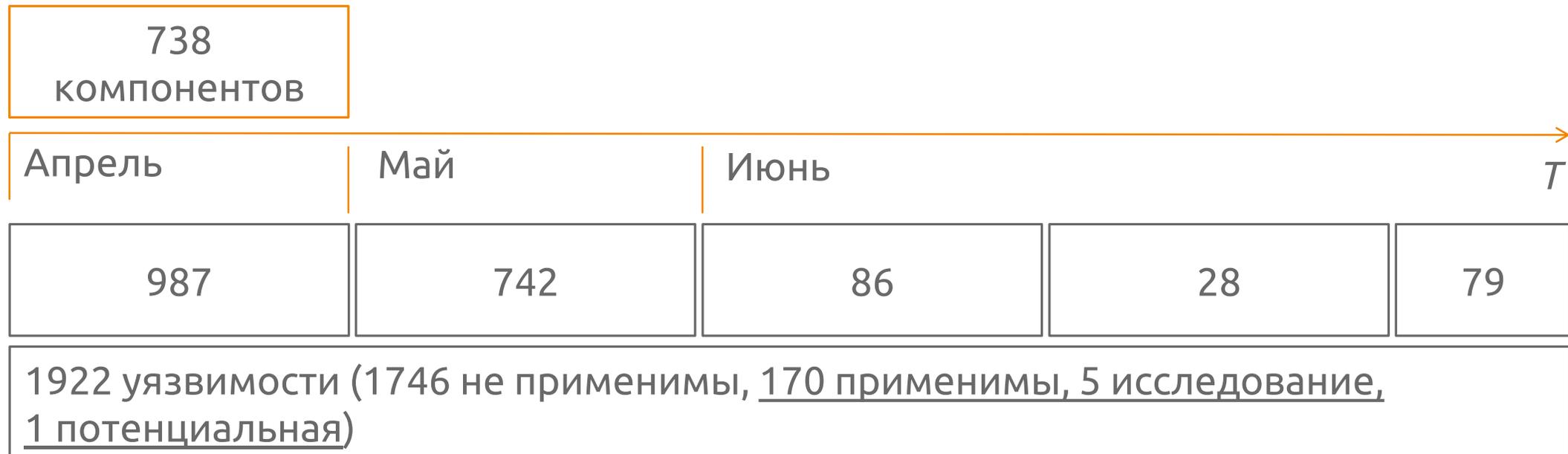
## Список продуктов (2)

#	Важность	Имя	В Работе	Обратная Связь	Решена	Закрыта	Всего	Score ?
19	низкая	Linux Server 1	1	0	0	0	3	20
13	низкая	APM Windows msk-w0423	0	0	0	0	3	29

# Пример процесса анализа уязвимостей сервера Linux (Vulnerability prevention)



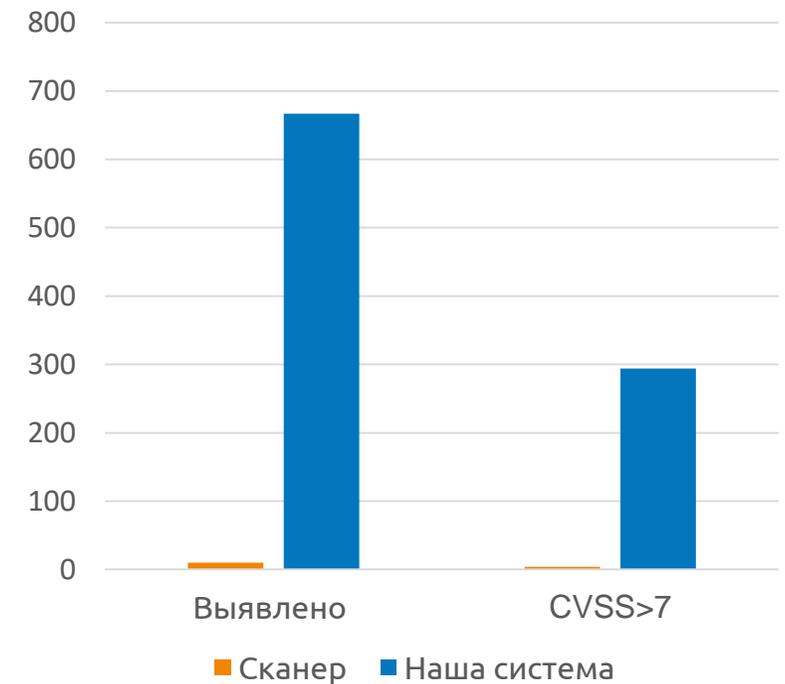
сервер Linux



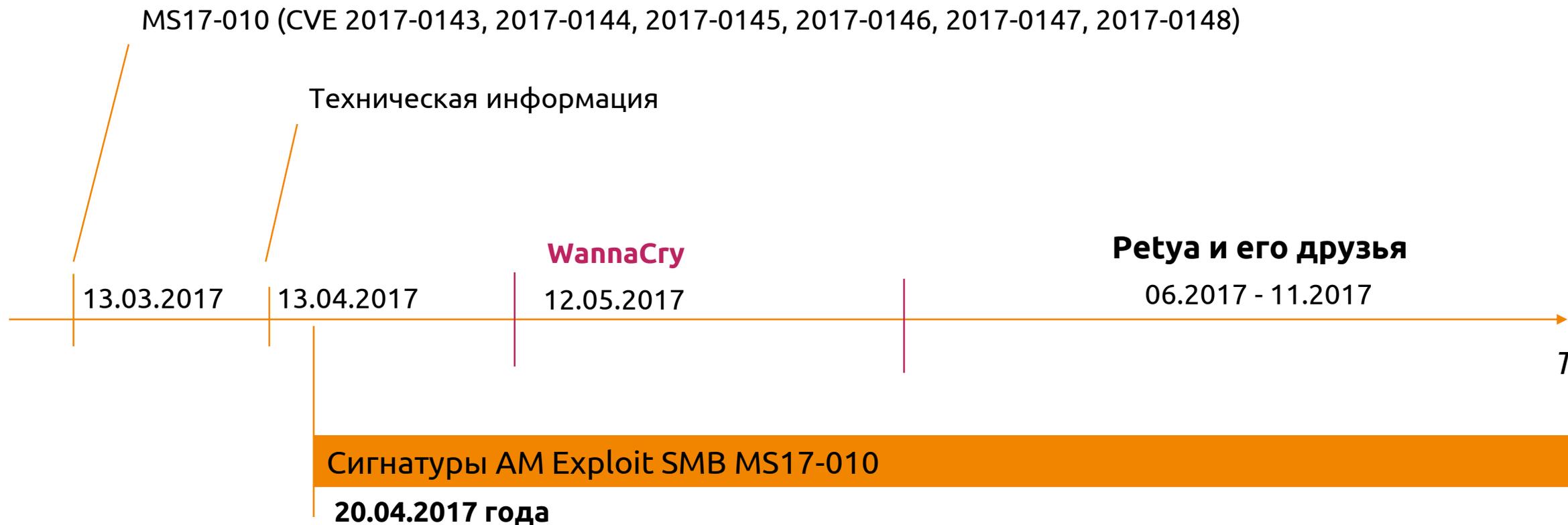
# Сравнение результатов анализа уязвимостей



	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

Детектируем,  
что знаем

Анализируем  
новое

Много шума

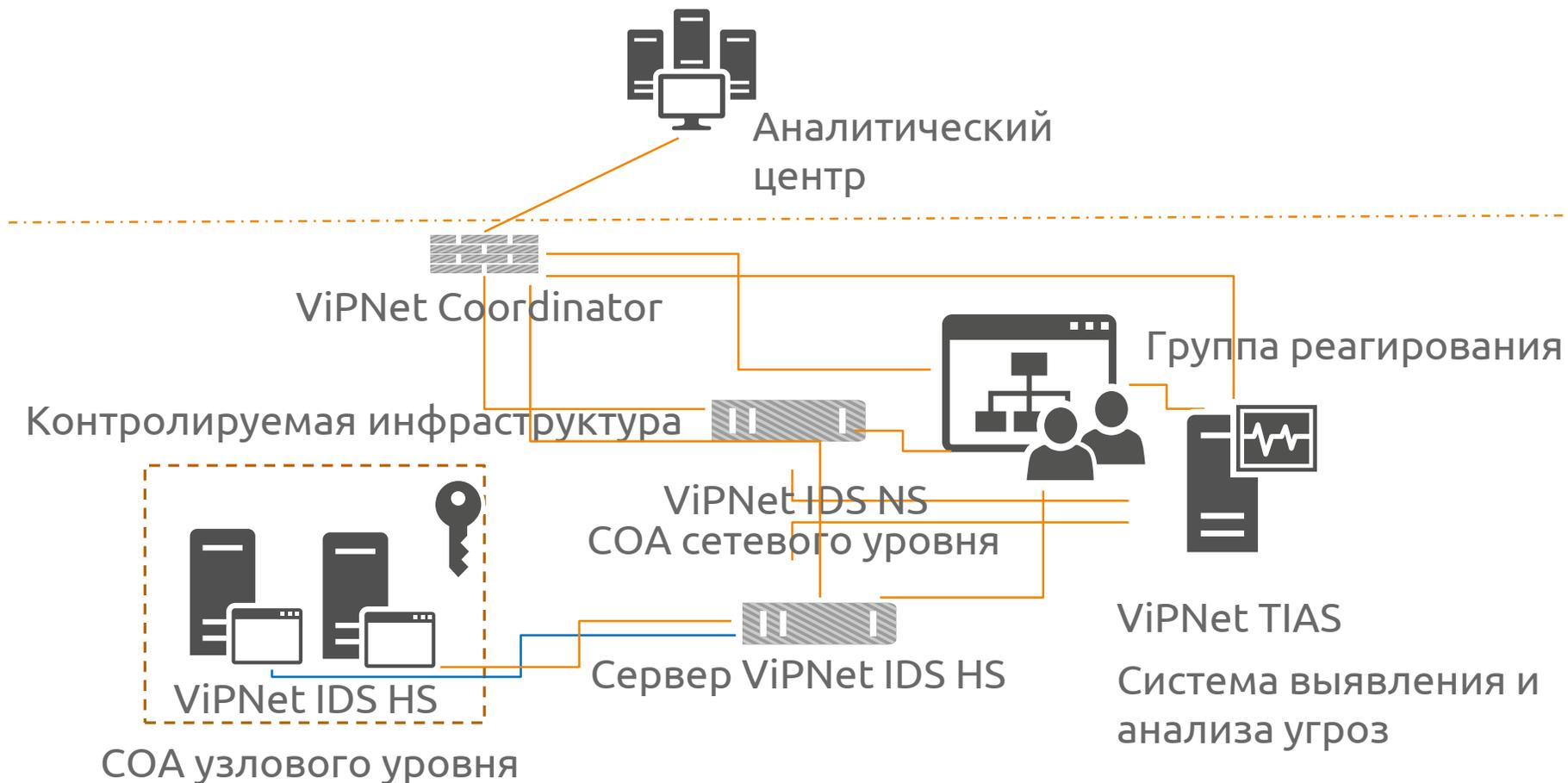
Быстрое и точное реагирование

Постоянное обновление базы знаний

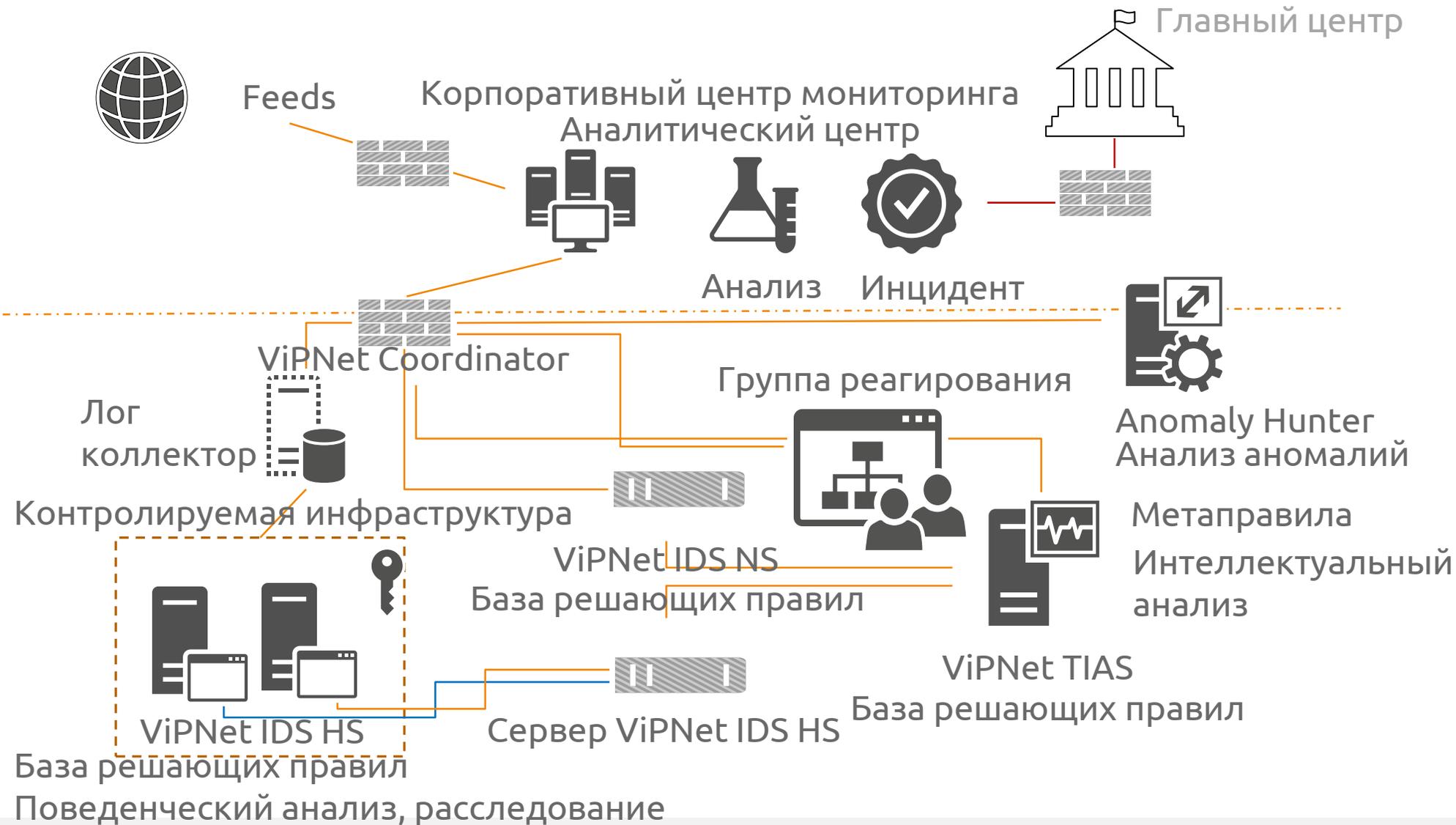
# Обнаружение компьютерных атак



Корпоративный центр мониторинга

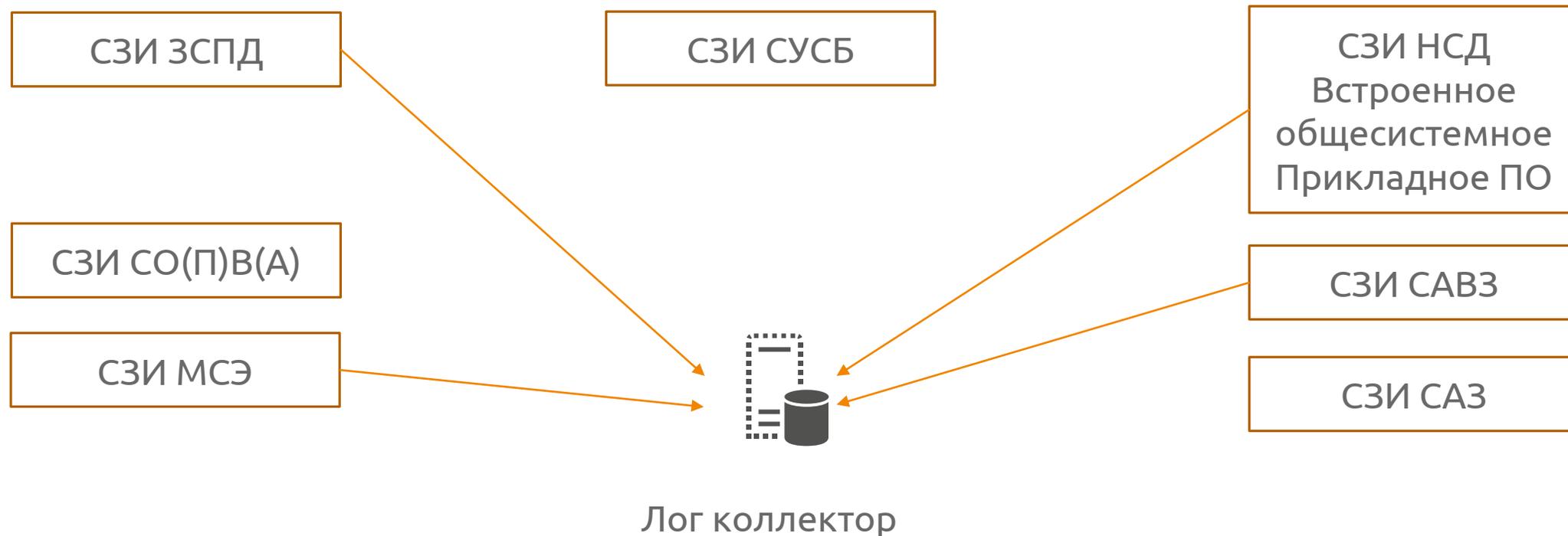


# Анализ данных о событиях





# Контролируемая инфраструктура и применяемые средства защиты информации



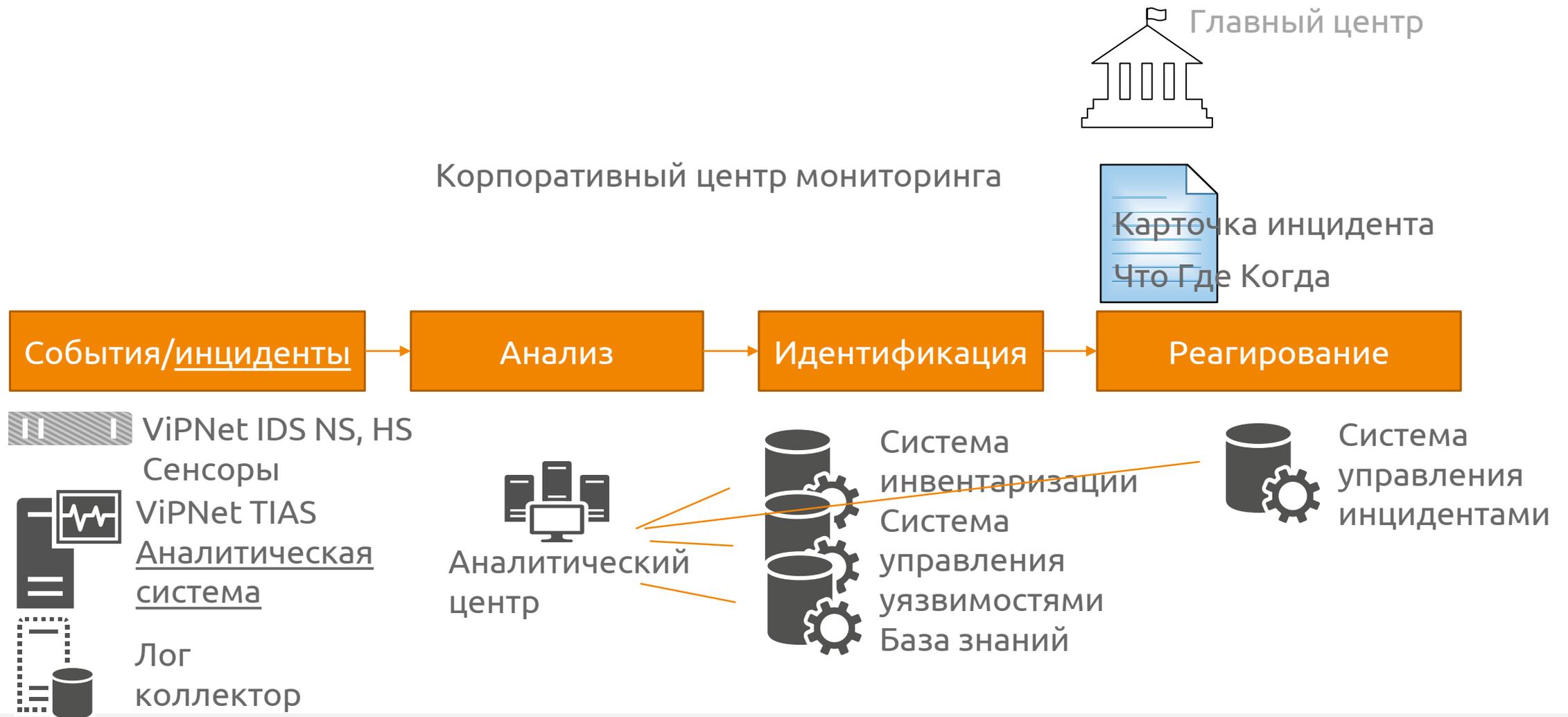


# Правила корреляции



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](mailto:Aleksey.Vasilyev@amonitoring.ru)