# Новый SOC ПМ: и оперативные сервисы для экстренных случаев


**Софья Карева**

Менеджер продукта компании
«Перспективный мониторинг»


инфотекс ТЕХНОФЕСТ

Синий поток

# Содержание

# SOC ПМ сегодня

**15** лет

на рынке услуг SOC и исследования защищённости

**10** лет

корпоративный Центр ГосСОПКА класса «А»

**150**

и более операторов, исследователей и аналитиков

**4**

региональных опорных центра SOC по стране

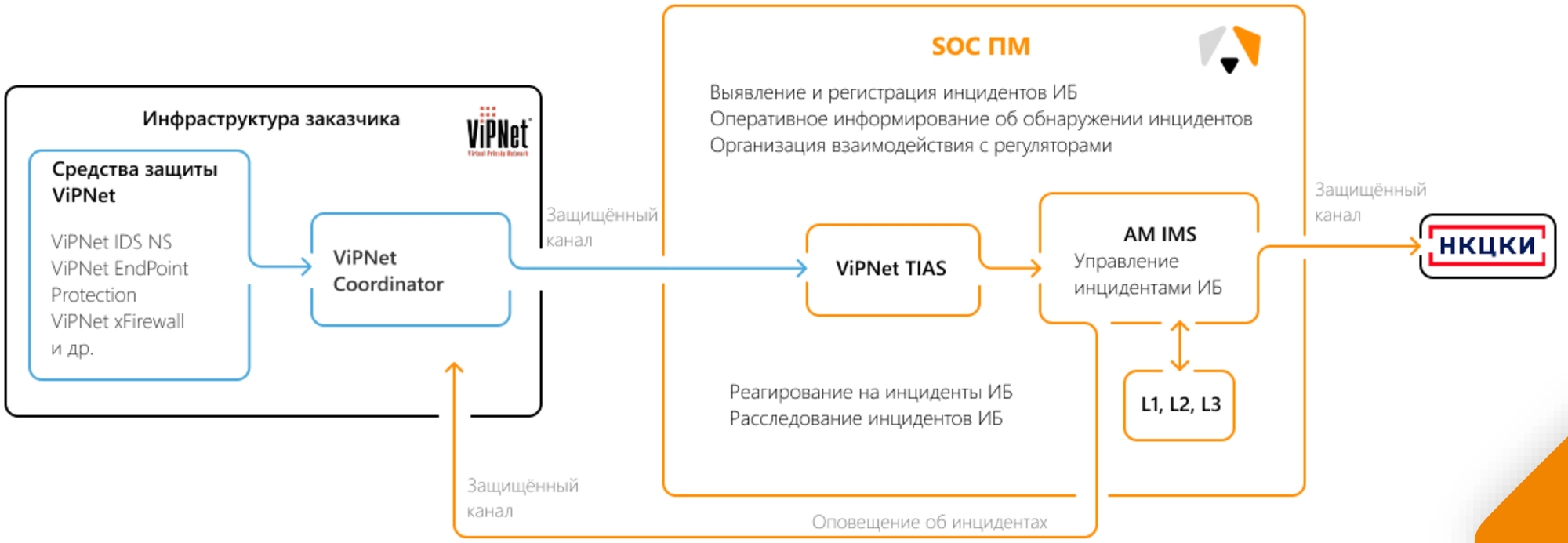
# Регионы присутствия

# Варианты мониторинга

## SOC на ViPNet

Решение «под ключ» с готовыми опциями

- Быстрое подключение от 1 недели
- Простая интеграция инфраструктуры в процессы мониторинга
- Легкая тарификация «по узлам» и оборудованию и ПО ViPNet

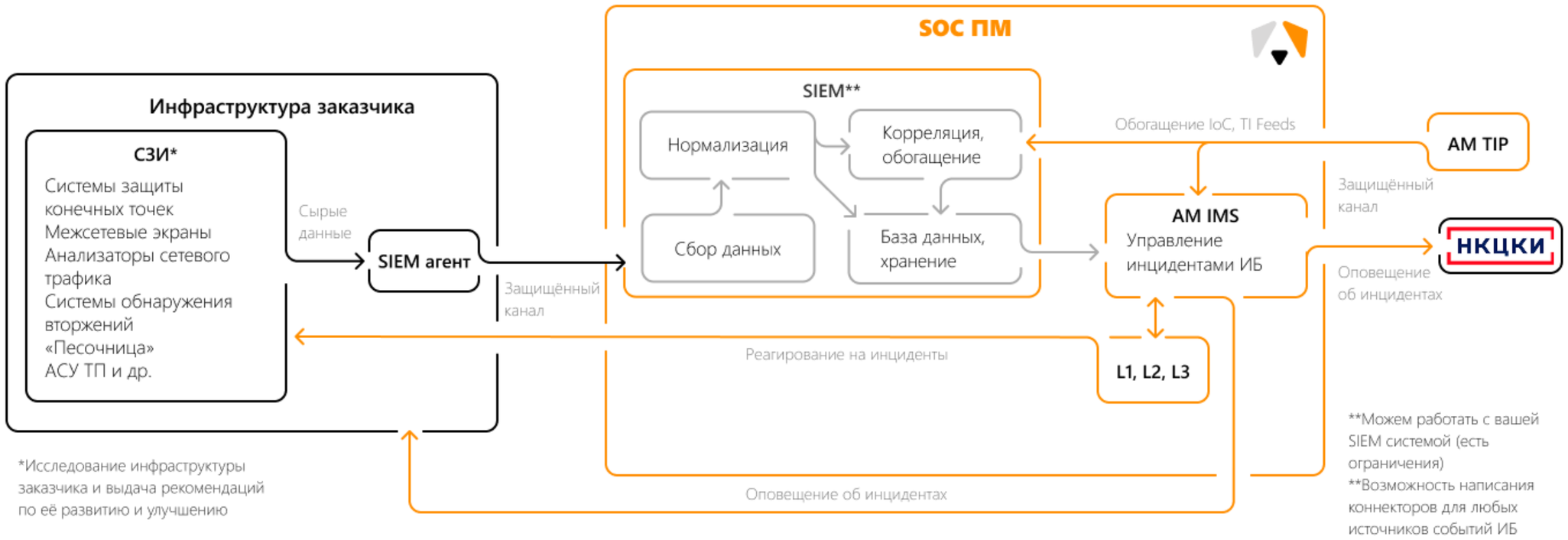


# Варианты мониторинга

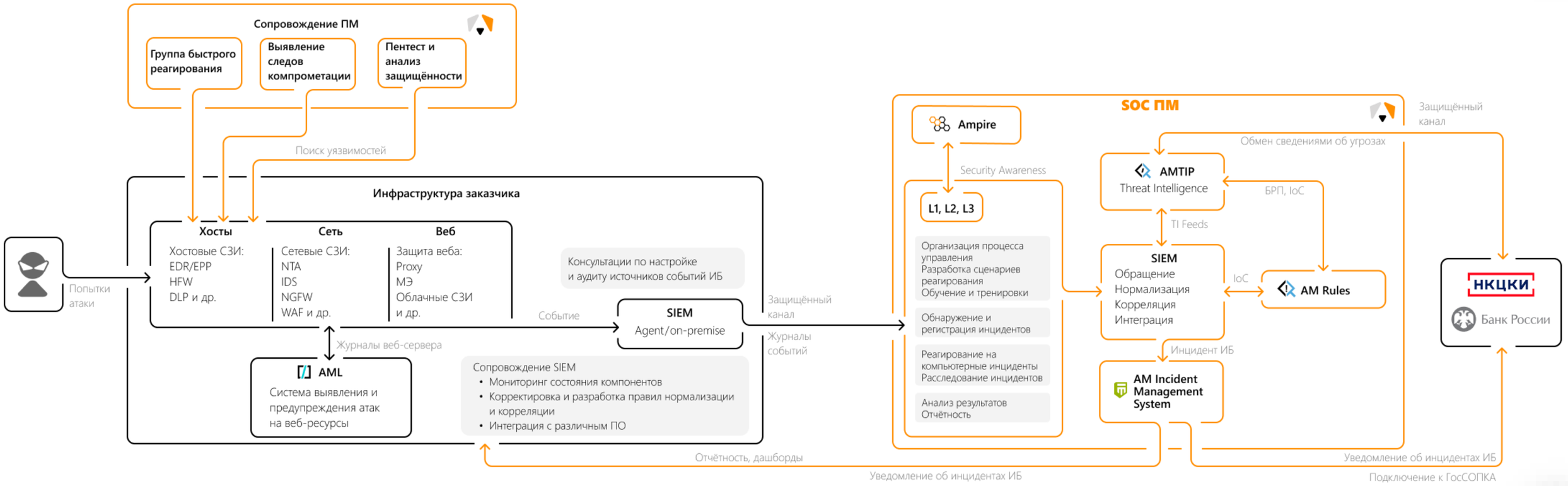
## Гибкий SOC

Индивидуальный подход к мониторингу

- Гибкий конфигуратор необходимых сервисов SOC
- Прозрачная тарификация индивидуального пакета услуг
- Лёгкое подключение дополнительных сервисов
- Возможность гибридного  формата взаимодействия



# Жизненный цикл инцидента



# Этапы работ

1 Исследование информационной системы

2 Определение перечня технических средств мониторинга (спецификации, схемы размещения и подключения)

3 Согласование оборудования и параметров соединения
Установка и настройка оборудования

4 Подключение к системам SOC ПМ по защищенным каналам

5 Контроль работы системы
Тестовая эксплуатация

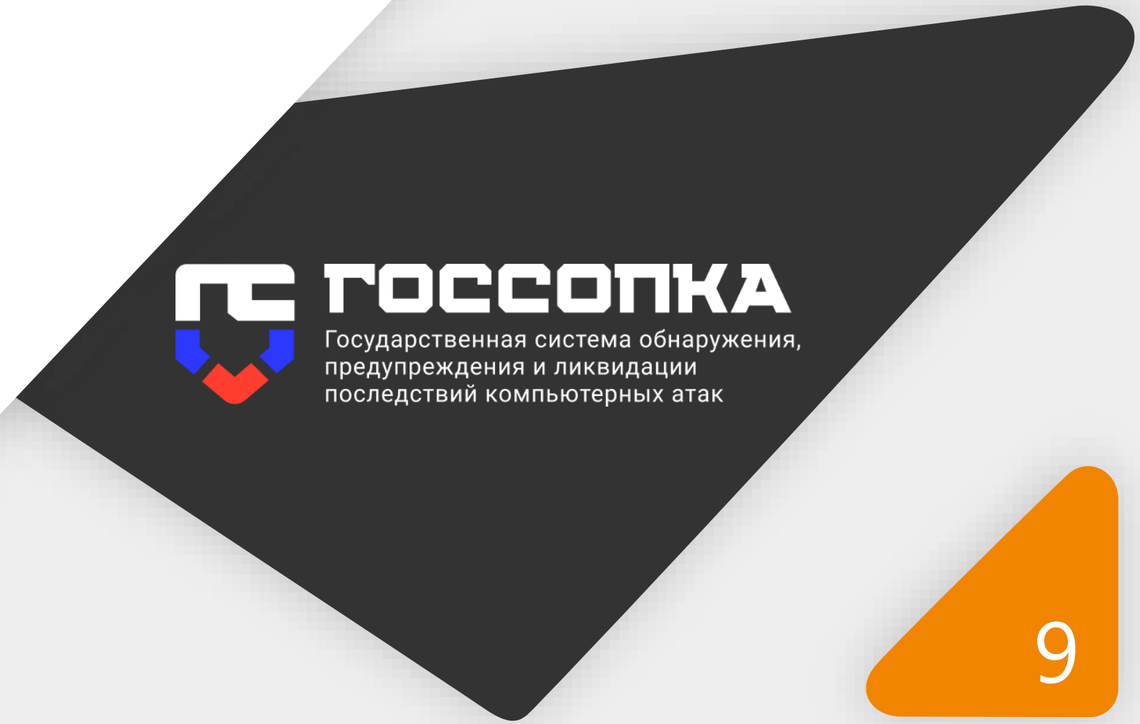
6 Разработка комплекса мер по реагированию на инциденты ИБ
Работа с сценариями обнаружения инцидентов ИБ

7 Сбор и анализ поступающих данных

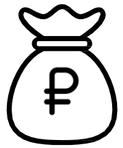
# Подключение к ГосСОПКА

ГосСОПКА — государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак, направленных на ИР РФ.

НКЦКИ организует сбор и обмен информацией об инцидентах между СКИИ, координирует мероприятия по реагированию, предоставляет методические рекомендации по предупреждению КА.

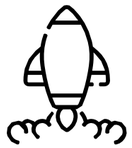


# Преимущества КЦ ГосСОПКА as Service



Оптимизация затрат на ИБ
за счет сервисной модели

Высокий уровень устойчивости
к киберугрозам



Быстрый старт и масштабируемость

Обеспечение непрерывного процесса
мониторинга угроз ИБ
и взаимодействия с ГосСОПКА

Экспертное сопровождение на всех
этапах

Качественный сервис вместо
длительного интеграционного
проекта

# Группа быстрого реагирования

SOS-сервис для быстрого реагирования на возникший инцидент ИБ

- Время прибытия на место
  2 часа в Москве
- Привезем свое ПО
  для анализа данных
- Возможность приобретения услуги
  как пакетом, так и разово
- Старт работ до фактического
  заключения договора на
  «джентельменских соглашениях»
- Удаленное подключение
  к инфраструктуре Заказчика
  до физического прибытия
  команды на место
- Прозрачная тарификация и сроки
  выполнения работ

## Мы нужны, если Заказчик:

- Обнаружил шифрование
  серверов или рабочих станций
- Выявил подозрительные входы,
  запуск неизвестных служб или
  скриптов
- Требует быстро определить
  масштаб заражения и не
  допустить развития атаки
- Заметил признаки компрометации
  доменной инфраструктуры
- Зафиксировал нарушение
  доступности критичных сервисов

# Группа быстрого реагирования

**0 Старт**

Удаленное подключение к инфраструктуре Заказчика и старт работ до прибытия команды

Результат: согласованы приоритеты, доступы и контур инцидента

**1 Подготовка**

- Сбор данных: опрос, схема сети, критичные системы
- Получение доступа к логам, SIEM и резервным копиям
- Фиксация гипотез и приоритетных узлов

**2 Локализация**

- Ограничение распространения угрозы
- Блокировка подозрительных учётных записей, IP и сессий
- Изоляция заражённых систем

**3 Сбор и анализ**

- Анализ журналов AD, серверов и рабочих станций
- Форензика дисков и памяти
- Выделение артефактов ВПО и IoC

**4 Реконструкция атаки**

- Подтверждение точки входа и цепочки событий
- Выявление закрепления и перемещений злоумышленника
- Определение затронутых данных

**5 Восстановление**

- Рекомендации по очистке и патчингу
- План запуска сервисов из резервных копий
- Технический отчёт и меры защиты

Что получает Заказчик: локализацию угрозы, подтверждённый масштаб компрометации, сценарий атаки и понятный план действий

# Compromise Assessment

## Выявление следов компрометации

Проведение углубленной проверки ИТ-инфраструктуры Заказчика с целью выявления признаков скрытого или ранее незамеченного компрометационного воздействия, а также оценки устойчивости организации к киберугрозам

- Своевременное обнаружение киберугроз
- Минимизация последствий возможных инцидентов ИБ
- Полноценная проактивная защита инфраструктуры
- Минимизация проведения повторной атаки
- Снижение рисков компрометации

# Compromise Assessment

Пошаговая логика проверки:
от triage до технического заключения

**0 Старт**

Подключение к инфраструктуре Заказчика,
согласование гипотез и перечня систем для проверки

Результат: подтверждены контур проверки,
критичные узлы и необходимые доступы

**1 Сбор артефактов**

- Получение triage с рабочих станций и серверов
- Выгрузка журналов, EDR/SIEM и сетевых событий
- Приоритизация критичных систем

**2 Проверка узлов**

- Анализ процессов, сервисов, задач и автозапуска
- IOC- и YARA-hunting
- Проверка подозрительной сетевой активности

**3 Анализ AD**

- Проверка привилегий, входов, GPO и сервисных учётных записей
- Поиск lateral movement и механизмов закрепления

**4 Подтверждение**

- Корреляция найденных артефактов и индикаторов
- Анализ вредоносных объектов при обнаружении
- Определение затронутых узлов

**5 Отчёт**

- Техническое заключение о наличии или отсутствии признаков компрометации
- Перечень рисков и рекомендации по снижению

Что получает Заказчик: объективную картину состояния инфраструктуры,
подтверждённые находки и рекомендации по дальнейшим действиям

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

# Спасибо за внимание!

Софья Карева,
Менеджер продукта

«Перспективный мониторинг»

amonitoring.ru

САНКТ ПЕТЕРБУРГ

инфотекс

# ТЕХНОФЕСТ

инфотекс Академия | Учебный центр Инфотекс | AMPIRE | TELEOFIS | КОМФОРТЕЛ оператор связи бизнес-класса | РУТОКЕН компания АКТИВ | TS Solution | AXOFT

Подписывайтесь на наши соцсети