servicepipe

Пинг-понг: кто отвечает за сетевую безопасность?

Павел Акифьев

Руководитель пресейл-направления
Servicepipe

О компании

servicepipe

servicepipe

Компания основана
в 2015 году
ведущими экспертами
из крупных российских
зарубежных
ИТ-компаний

100+

Технических
экспертов
в команде, включая
специалистов
highload и big data

Собственная
георасспредёленная
отказоустойчивая
платформа
фильтрации
с узлами в России
и Германии

500+

Клиентов, включая
ведущие компании
в различных
секторах: банки,
маркетплейсы, СМИ,
телеком и другие

Sk Участник

Резидент
ИНТЦ МГУ

Продукты в реестре
отечественного ПО

Минцифры
России

О чем поговорим

servicepipe

1. Основные вызовы ИТ и ИБ департаментов
2. Проблематика во взаимодействии во время инцидентов
3. Путь от конфликтующих департаментов до слаженной команды на примере реального кейса

Основные вызовы ИТ и ИБ департаментов

servicepipe

1. Рост мощности и числа DDoS-атак

2. Конфликты при расстановке приоритетов: доступность против безопасности

3. Необходимость быстрой адаптации к новым угрозам (например, Zero-day)

Проблематика ИТ и ИБ департаментов

servicepipe

ИТ департамент

Ответственность

Эксплуатация и поддержка серверов, сетевой инфраструктуры и приложений.

Основная цель — обеспечить доступность и производительность сервисов для внешних и внутренних клиентов.

ИБ департамент

Ответственность

Защита информации, противодействие кибератакам и соответствие нормативным требованиям.

Основная цель — предотвращение утечек данных и защита от киберугроз.

Основная проблема

1. Отсутствие внутренних регламентов:
   - Нет согласованных зон ответственности между ИТ и ИБ, что приводит к конфликтам в управлении инцидентами.
   - Разные подходы к приоритетам: ИТ фокусируется на доступности и производительности, а ИБ — на безопасности.
2. Разрыв в коммуникации
   - Недостаточное взаимодействие между командами, что замедляет принятие решений при инцидентах сетевой безопасности.
   - Отсутствие совместных процессов и ПО для предотвращения угроз и их оперативного устранения.

При появлении DDoS-атаки

servicepipe

ИТ департамент

Фокус:

- Расширить каналы связи
- Восстановить работоспособность сервисов, перенаправляя трафик
- Проверить состояние серверов, сети и приложений на наличие перегрузок
- В экстренных случаях временно отключают доступ к атакуемым ресурсам

ИБ департамент

Фокус:

- Укрепить сетевой периметр
- Оценка и анализ угроз
- Разработка временных политик безопасности для предотвращения дальнейшего ущерба

Появляются разногласия, которые приводят к задержкам в принятии решений. Отсутствие согласованности между департаментами — мешает оперативно реагировать на угрозы и эффективно решать проблему.

Кейс

servicepipe

Заказчик: облачная платформа

Ситуация

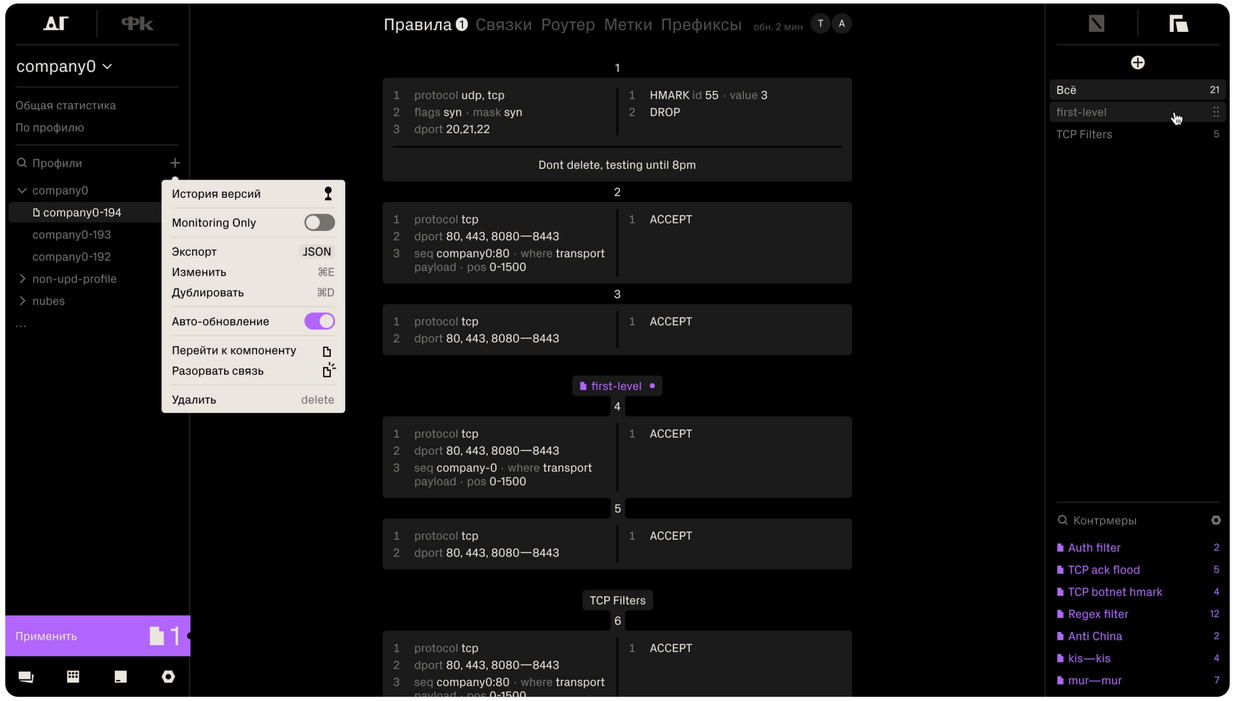
Появление DDoS-атаки привело к простоям сервисов, жалобам клиентов и финансовым потерям.

Осознание

В компании решили объединить усилия для нейтрализации дальнейших сетевых киберинцидентов и учитывать потребности и требования каждого департамента.

Решение

Внедрение единой системы управления сетевым трафиком, политиками безопасности и мониторинга.



Единая система управления DosGate:
роли и взаимодействие ИТ и ИБ департаментов

servicepipe

ИТ департамент

Настройка сетевых маршрутов и резервирования:

- Использование API DosGate для автоматизации управления трафиком.
- Трафик автоматически заворачивается на очистку только в случае атаки.
- Резервирование всех компонентов системы в режиме Active + Active.

ИБ департамент

Управление политиками безопасности:

- Настройка детализированных фильтров и правил защиты для обнаружения и блокировки вредоносного трафика.
- Автоматическое реагирование системой на DDoS-атаки L3-L7.
- Использование API DosGate для автоматизации управления политиками безопасности.

Единая система управления DosGate:
роли и взаимодействие ИТ и ИБ департаментов

servicepipe

ИТ департамент

Управление доступностью и производительностью:

- Контроль нагрузки на сеть и инфраструктуру, обеспечение бесперебойной работы сервисов.

Мониторинг сетевого оборудования через DosGate:

- Уведомления о проблемах с аппаратной частью.
- Реакция на резкое увеличение нагрузки на CPU или перегрузку сети.

ИБ департамент

Управление политиками безопасности:

- Отчетность об атаках, вредоносных IP-адресов.
- Уведомления по почте или в телеграм о наличии аномального трафика в сетевой инфраструктуре.

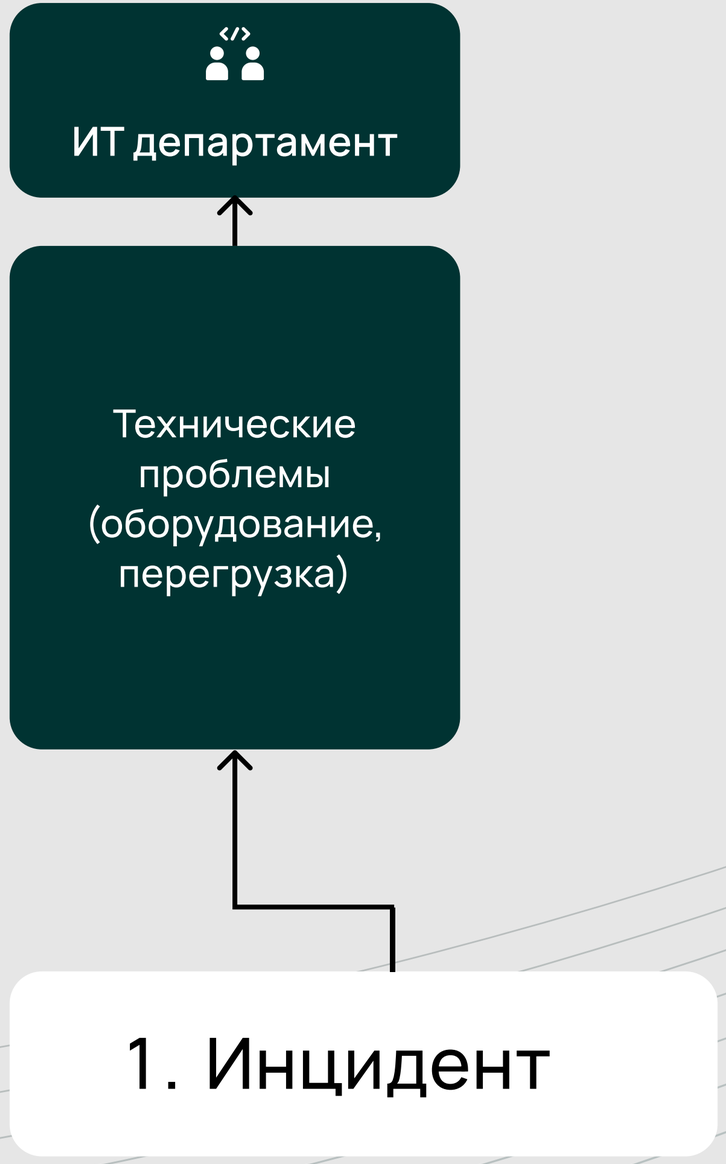
Общее взаимодействие

servicepipe

1. Инцидент

Общее взаимодействие

servicepipe

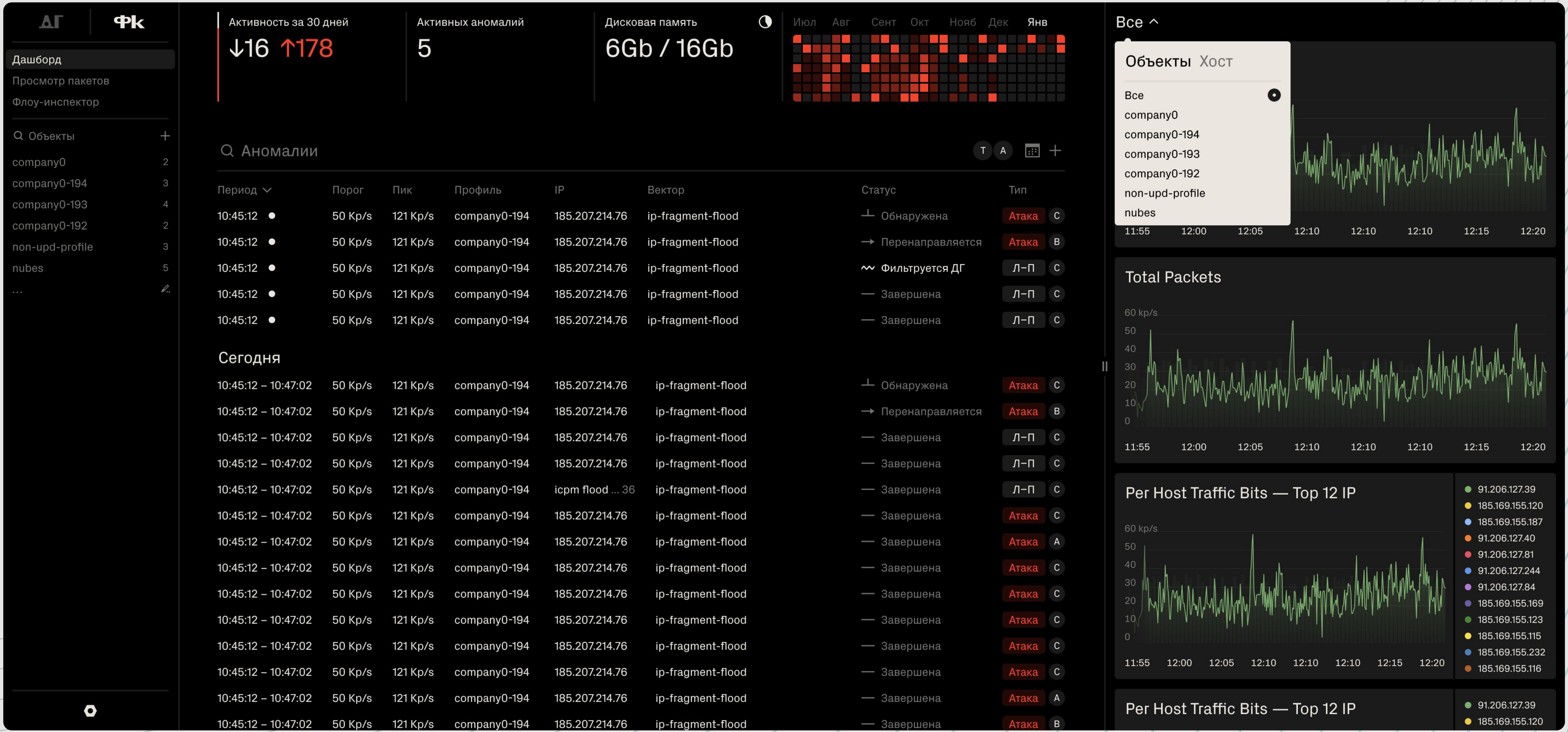


Общее взаимодействие

servicepipe

Общее взаимодействие

1. Единый механизм уведомлений



Общее взаимодействие

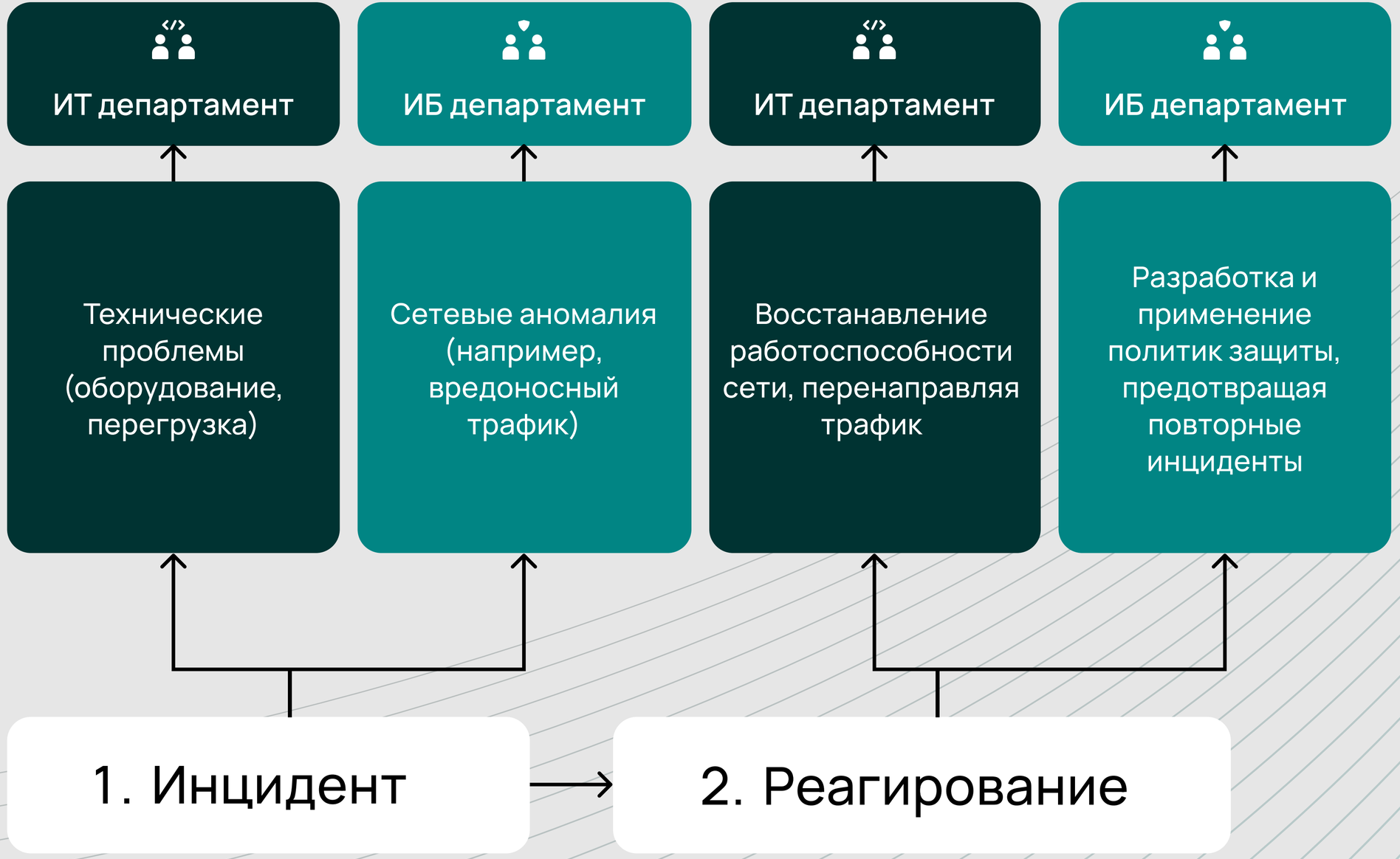
servicepipe

Общее взаимодействие

servicepipe

Общее взаимодействие

servicepipe

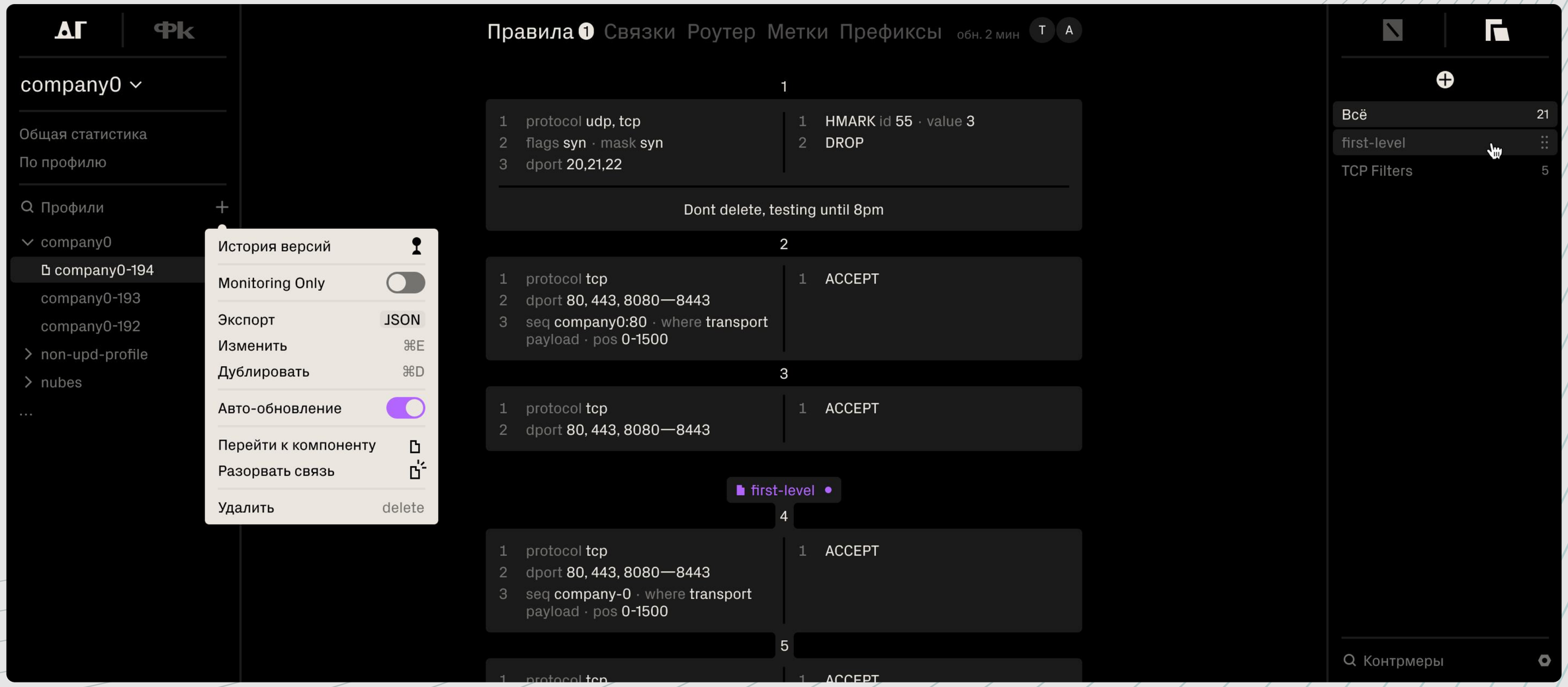


Общее взаимодействие

servicepipe

2. Совместное реагирование:

Взаимодействие DosGate с различными внутренними сервисами, например с SIEM и системами мониторинга



Общее взаимодействие

servicepipe

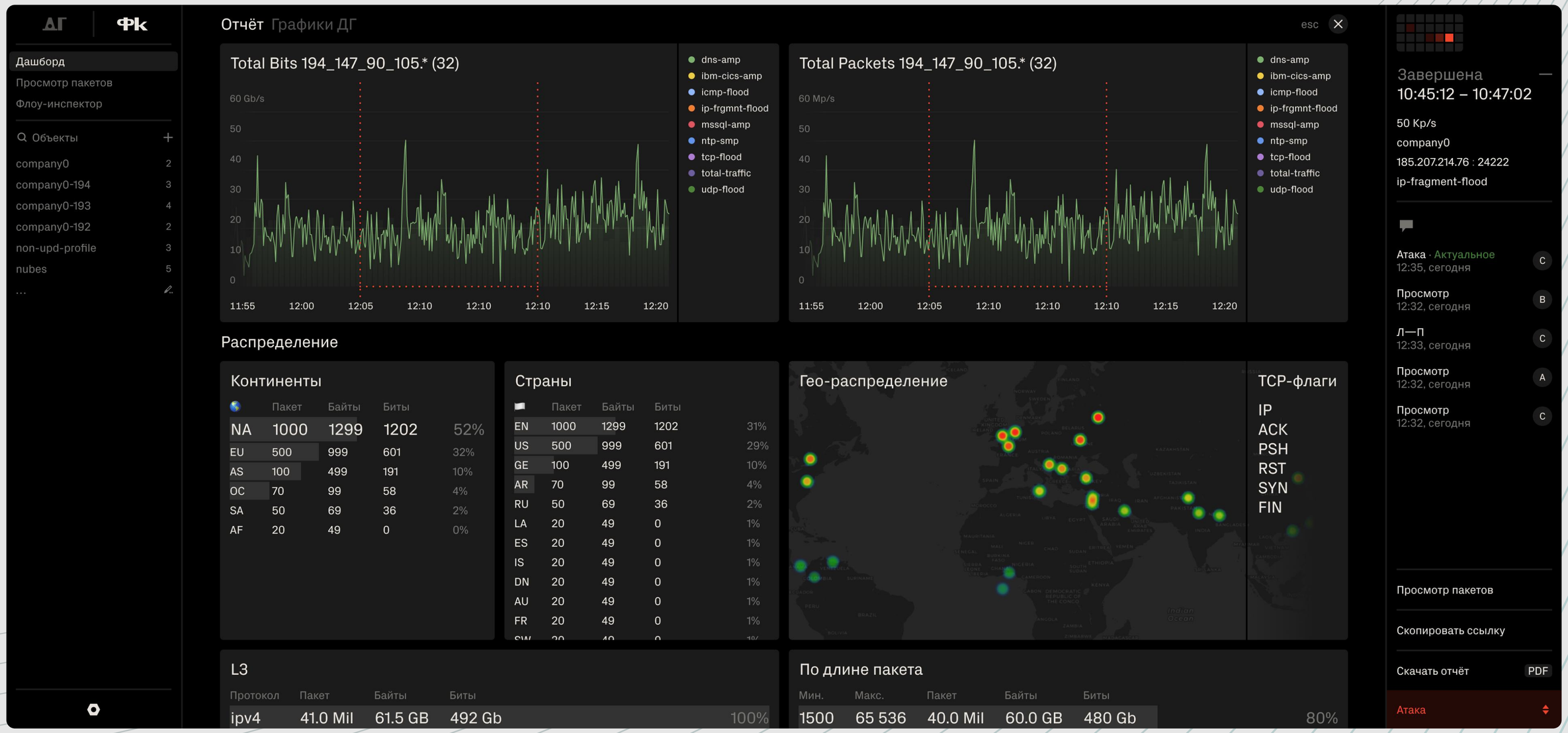
Общее взаимодействие

servicepipe

Общее взаимодействие

servicepipe

3. Общий мониторинг в реальном времени:



Общее взаимодействие

servicepipe

DosGate

становится связующим звеном между двумя департаментами, помогая реализовать слаженную и эффективную защиту сетевой инфраструктуры.

DosGate — это

servicepipe

- Защита от L3–L7 DDoS-атак до 400 Gbps и 400 Mpps на устройство
- Гибкие пакеты правил
- Удобный и простой интерфейс
- Отчеты по клику
- Эшелонированная защита
  On-premise + Cloud Signaling + Cloud
- Техническая поддержка 24/7/365. SLA: ответ в течение 5 минут
- **On-premise**
  ПО и ПАК в инфраструктуру
- <1 Менее секунды на Always-on или Ultra-low Time to Mitigate
- В реестре отечественного ПО, аккредитация минцифры
- Сетевая и сессионная защита: до 150 млн правил в системе

servicepipe

Запишитесь на индивидуальную демонстрацию!

Приходите на стенд!

Стенд 11

Напротив зоны кофе-брейка

servicepipe

Москва, Ермолаевский переулок 22-26ст1

+7 (495) 374-6265

welcome@servicepipe.ru