

**От «лоскутной» к управляемой защите:**  
как выстроить комплексную  
и эшелонированную систему защиты

# Сегодня на вебинаре

NGENIX<sup>7</sup>

01

Что такое эшелонированная защита и почему это эффективный подход к защите в 2027

02

Как разрозненные решения перегружают ИТ- и ИБ-команды и почему они размывают границы ответственности

03

Как связать разные уровни защиты в единую управляемую систему

04

Как NGENIX решает задачи заказчиков: кейсы из реальной практики



Артём Фомичев

Начальник отдела  
технического аккаунтинга,  
NGENIX



## Число многовекторных атак выросло в 2 раза

Злоумышленники комбинируют атаки на сеть и приложения, чтобы обойти защиту, настроенную только на один тип угроз



## 60% атак направлены на уязвимости бизнес-логики

Злоумышленники не стремятся «положить» сайт. Их цель — нарушить ключевые бизнес-процессы (оплата, регистрация)

Атаки нацелены на всю экосистему: сетевая инфраструктура, веб-ресурсы и их бизнес-логика. Фрагментарная защита неэффективна — уязвимость в любом звене может парализовать бизнес



# Злоупотребление бизнес-логикой — скрытая угроза, которую сложно обнаружить

## Заказчик

Крупная компания  
в сегменте e-com

## Проблема

Заказчик заметил циклические всплески активности.росло число регистраций и расходы на SMS-подтверждения, но конверсия и выручка не менялась.

## Что происходило?

Во время анализа мы увидели, что с каждого IP-адреса выполняется несколько регистраций в час. Активность похожа на легитимную, но формы заполняются за сотни миллисекунд. Реальный пользователь так не может.

За счет блокировки нелегитимного бот-трафика мы снизили пиковую нагрузку на сайт на 80% и сократили расходы на SMS



# Концепция эшелонированной защиты

**Эшелонированная защита** — подход к обеспечению безопасности, когда система защиты состоит из нескольких уровней. На каждом — разные средства защиты от киберугроз.

## Способы построения эшелонированной защиты:



### On-Premise (Локальная защита)

Защита разворачивается  
внутри собственной  
инфраструктуры компании



### Мультивендорная (Лоскутная защита)

Система защиты строится  
из отдельных решений  
разных провайдеров



### Комплексная эшелонированная защита

Система защиты строится в едином  
контуре на базе одного ключевого  
провайдера с бесшовной интеграцией  
партнерских решений

# Почему «лоскутная защита» — не самый оптимальный подход?

- 01 Слепые зоны на стыках систем
- 02 Перегрузка ИТ и ИБ-команд
- 03 «Пинг-понг» техподдержек
- 04 Сложность масштабирования и обновления
- 05 Несовместимость отдельных систем



# Преимущества комплексного подхода — на основе решения NGENIX

NGENIX<sup>7</sup>

Удобный и многофункциональный клиентский портал с разделением прав пользователей



Единая техническая поддержка



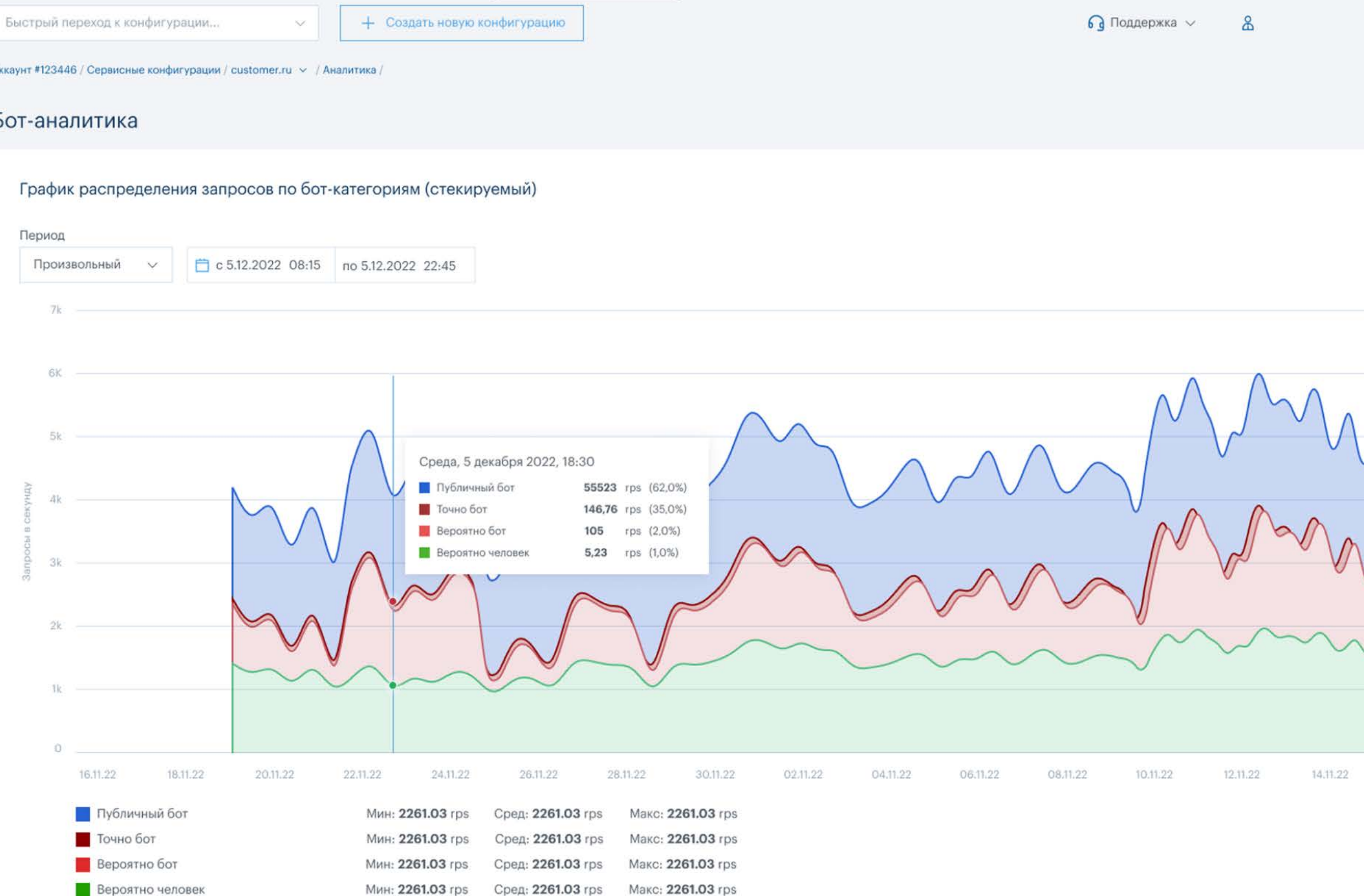
Автоматическое масштабирование при росте нагрузки



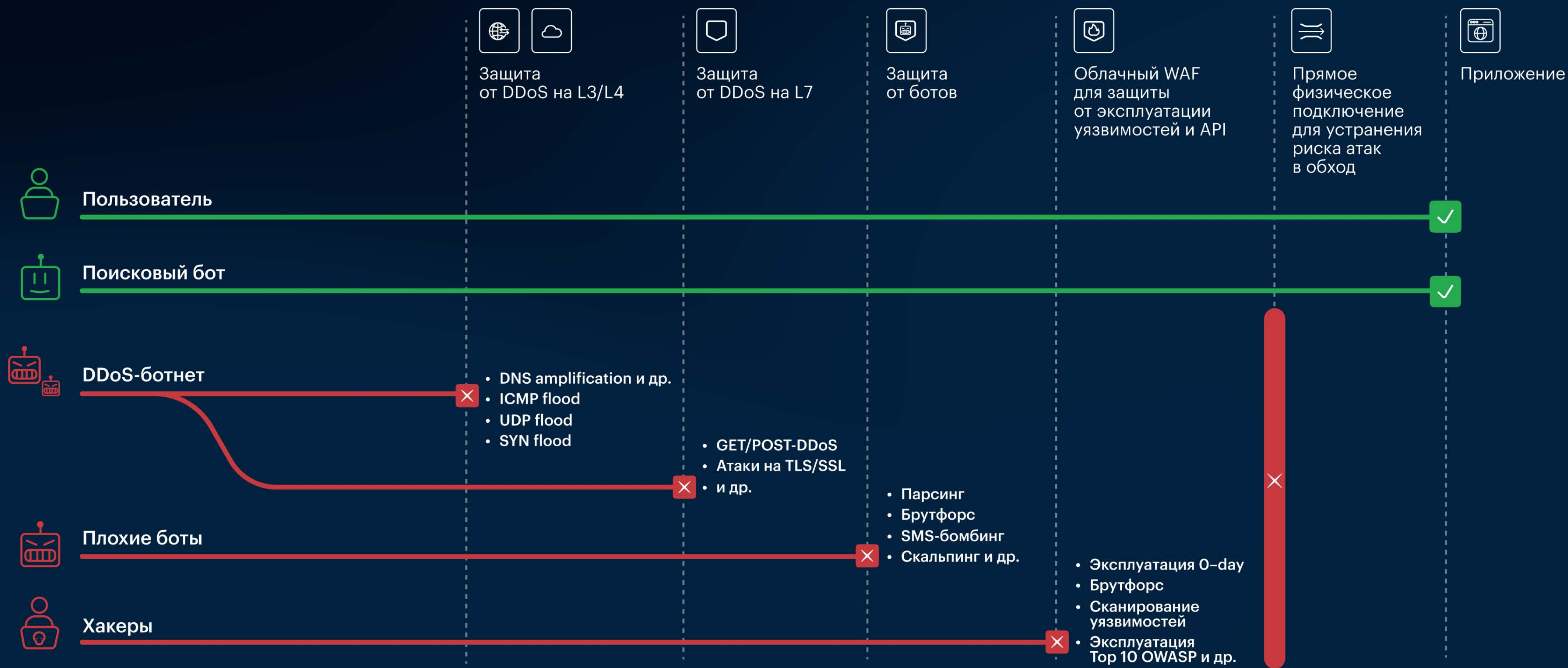
Все эшелоны защиты на своем месте. Работают согласованно и с максимальной выгодой для заказчика



Можно быстро добавить новые эшелоны, которые предусмотрены внутри платформы NGENIX



# Что внутри нашей эшелонированной защиты?



# Как NGENIX решает задачи заказчиков?

Делимся кейсами из реальной практики

Заказчик

## Один из крупнейших российских дистрибьюторов электротехники

Проблема

B2B-портал работает по всей России и в странах СНГ. Раньше могли происходить значительные задержки доставки контента в удалённые регионы.

Задача

Изначально в 2019 году заказчику нужно было ускориться и снизить нагрузку на инфраструктуру, также нужен был WAF.

Позже появилась потребность в построении защиты B2B-портала от DDoS и ботов.

NGENIX<sup>7</sup>

### Какие задачи NGENIX помогает решать заказчику?

-  Обеспечение высокой скорости работы B2B-портала и снижение нагрузки на инфраструктуру.
-  Доступность портала для покупателей во время DDoS-атак или распродаж.
-  Комплексная защита интернет-магазина от актуальных угроз: взломов, эксплуатации уязвимостей, DDoS-атак, а также от ботов (скраперов и брутфорсеров).

« Нам нужно было ускориться и снизить нагрузку на нашу инфраструктуру. Но компания, с которой мы работали на тот момент, не предоставляла услуги CDN. Мы проанализировали большое количество предложений на рынке и в итоге выбрали NGENIX. Привлекло то, что мы можем сразу у одного провайдера комплексно закрыть все потребности: ускорить работу сайта, защититься от DDoS-атак и внедрить облачный WAF.

Начальник по IT-инфраструктуре



Заказчик

## Представитель телекома

Проблема

При резком всплеске  
нелегитимной нагрузки  
ИТ-команда сталкивались  
с критичным ростом  
нагрузки на WAF.

Задача

Снизить нагрузку на WAF  
за счет грамотно построенной  
эшелонированной защиты.

NGENIX<sup>7</sup>

### Как мы помогли заказчику решить эту задачу?



Кэширование статического контента снизило нагрузку на 15% RPS и 8% полосы пропускания.



С помощью правил обработки запросов снизили нагрузку на WAF еще на 10%.



Срезали потребление трафика на 20% и снизили нагрузку на базу данных на 60%.



Заказчик

## Сервис для заказа такси и курьерских доставок

Проблема

Сервис находится под непрерывным давлением атак. Аптайм — критически важная метрика. Но нет большой команды ИТ и ИБ-специалистов.

Задача

Построить эффективную защиту мобильного приложения, сайта-визитки и B2B-порталов при небольшом ИБ-отделе.

NGENIX<sup>7</sup>

### Какие задачи NGENIX помогает решать заказчику?

- ☒ Защита от DDoS-атак на L3, L4 и L7
- ☒ Экономия на CAPEX и OPEX
- ☒ Масштабируемость под объемные атаки
- ☒ Экспертная поддержка 24/7

« Для нас главное преимущество NGENIX — надежная защита без найма огромного штата дорогостоящих ИБ-специалистов. Пользоваться решением NGENIX удобно: многие процессы автоматизированы, всё предоставляется комплексно, а техническая поддержка берёт на себя основную нагрузку. Нет необходимости самостоятельно выстраивать систему мониторинга и реагирования.

Руководитель отдела системной инфраструктуры



# Эшелонированность ≠ набор разрозненных продуктов



## «Лоскутная» эшелонированная защита —

это несколько инструментов, которые не интегрированы друг с другом и даже могут конфликтовать. Несколько техподдержек и консолей управления.



## Комплексная эшелонированная защита —

это продуманная система, где уровни защиты усиливают друг друга. Есть единая техподдержка и удобный веб-интерфейс для управления всеми сервисами защиты.

# С чего начать?

## Шаг 1

определите  
критичные  
бизнес-  
процессы

## Шаг 2

оцените  
риски  
по уровням

## Шаг 3

проведите  
аудит  
текущей  
архитектуры

## Шаг 4

выберите  
оптимальную  
для вас модель  
построения  
эшелонированной  
защиты



Больше об эшелонированной  
защите и новых эшелонах —  
на нашей продуктовой  
онлайн-конференции

Встречаемся 9 декабря в 11:00

NGENIX<sup>7</sup>

**ICEBREAKER**

2026



NGENIX<sup>7</sup>

+7 495 023 63 33  
sales@ngenix.net

[www.ngenix.net](http://www.ngenix.net)



**Бесплатный  
тест 14 дней**