Министерство связи и массовых коммуникаций Российской Федерации
Федеральное государственное унитарное предприятие «Научно-технический центр «Атлас»
Новосибирский филиал ФГУП «НТЦ «Атлас»

ИМПОРТОЗАМЕЩЕНИЕ
Практика внедрения отечественных СЗИ

Исаев Андрей

Начальник отделения коммерции

Наши заказчики

Проекты

Создание Ситуационного центра Президента Российской Федерации

Реализация плотного проекта «Создание Ситуационного центра ФСИН России»

Внедрение ПАК «Тор» для Федерального агентства по обустройству государственной границы Российской Федерации

Создание и модернизация информационно-телекоммуникационные системы в Государственной Думе и Совете Федераций Российской Федерации

Создание и модернизация информационно-телекоммуникационные системы в Счетной Палате РФ | Верховном Суде РФ | Конституционном Суде РФ Федеральном казначействе РФ | Министерстве финансов РФ

Обслуживание сайта Президента Российской Федерации и Аппарата Правительства Российской Федерации

Актуальность

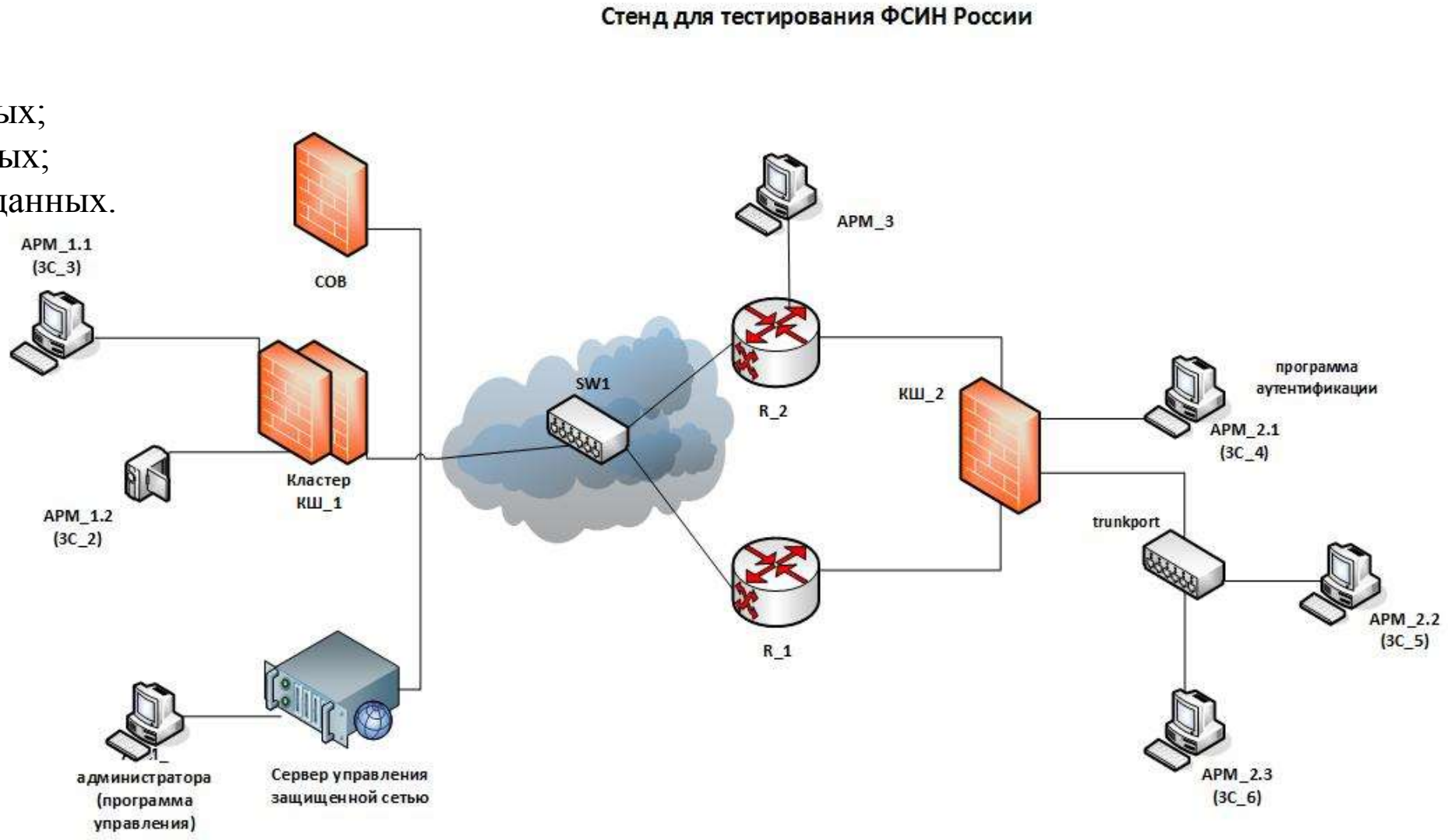
ЗА и ПРОТИВ

+	-
• Независимость от курса валюты • Отсутствие политических влияний • Соблюдение действующего законодательства РФ • Сокращение сроков поставки • Поддержка отечественных производителей • **Обеспечение национальной и государственной безопасности** • **Достижение технологической независимости в критических областях**	• Замена критически важной системы для бизнеса всегда связана с рисками • Отсутствие отечественного ПО, соответствующего функционала • Совместимость отечественных разработок с прикладным ПО • Снижение конкурентоспособности индустрии ИТ

Примеры использование отечественных разработок для построения защищенных систем.

1. Выбор системы защиты каналов связи ведомственной информационной системы ГУФСИН России по НСО

Передача потока аудио данных;
Передача потока видео данных;
Передача потока файловых данных.



Критерии выбора. Результаты испытаний

№ п/п	Наименование критерия	Коэффициент важности	«Код Безопасности»	«Инфотекс»	ФГУП «НТЦ «Атлас»	Примечание
Общая информация						
1	Тип решения (Программно-аппаратный, программный)	1				При отсутствии хотя бы одного показателя средства считается не прошедшим испытания
2	Наличие сертификации ФСТЭК России и ФСБ России	1				
3	СКЗИ решение построено на базе ПО с классом защиты КС3	1				
4	Алгоритм шифрования (ГОСТ 28147 – 89)	1				
5	Поддержка режима закрытой криптографической сети	1				
6	Поддерживаемые схемы организации сети VPN	1				
Обязательные критерии						
7	Возможность централизованного управления через ПО	3				
8	Наличие сертифицированных терминальных решений (тонкий клиент)	5				
…	…	…	…	…	…	..

2. ПАК «Заслон»

Актуальность

Предпосылки трансформаций

- Рост числа пользователей и сервисов
- Рост производительности сетей
- Увеличение числа мобильных пользователей
- Популярность бесплатных CMS

Трансформация целей

- Взлом аккаунтов
- Кража контента
- Репутационные риски
- Информационные вбросы

ВЕБ-порталы

Трансформация методов кибер-атак

- 56% трафика в сети интернет составляют БОТы
- Преобладание атак на уровне приложений
- 95% взломов сайтов осуществляются с помощью автоматизированных средств
- Новые парадигмы взлома с помощью низкочастотных запросов

Результаты трансформаций

- CAPTCHA потеряла свою эффективность
- Блокировки по IP приводят к потерям «здоровой» аудитории
- Стандартные методы и инструменты обнаружения DDoS-атак и Ботов неэффективны

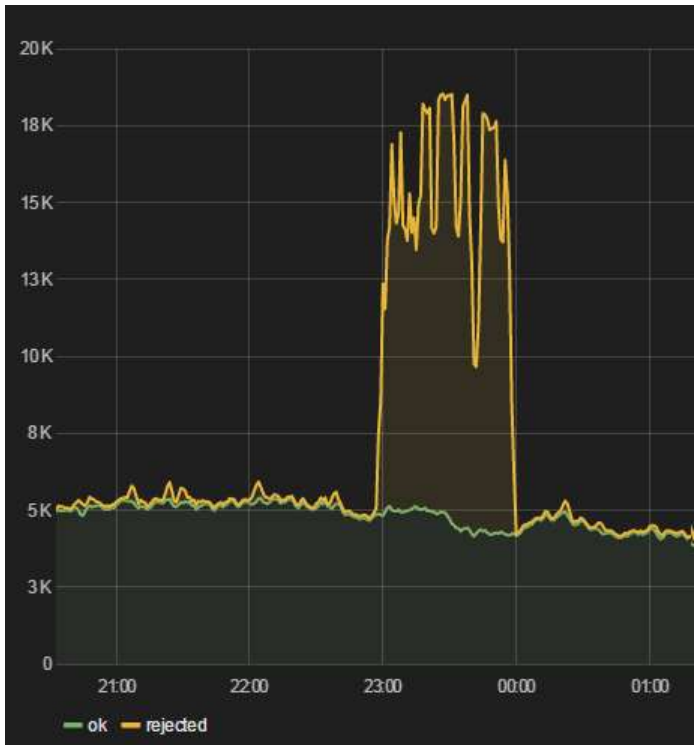
Данные мониторинга сайта за день

Реальная картина мониторинга интернет-ресурса

Соотношение Человек-Бот в количественных показателях

Соотношение Человек-Бот в процентах

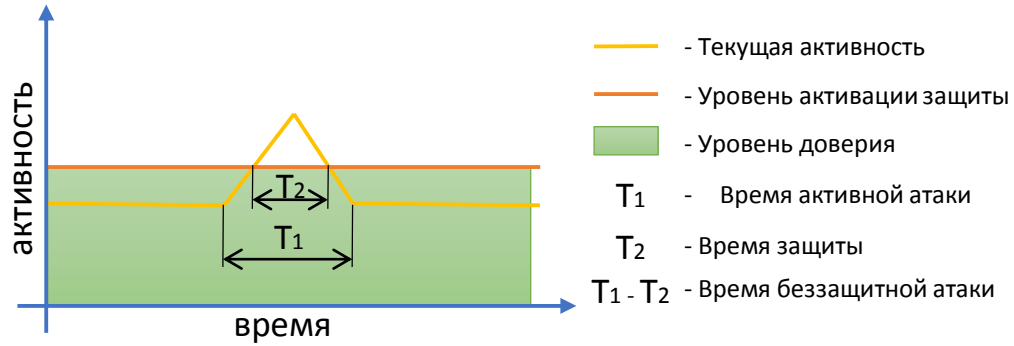
Активная Атака



Боты

Реальные пользователи

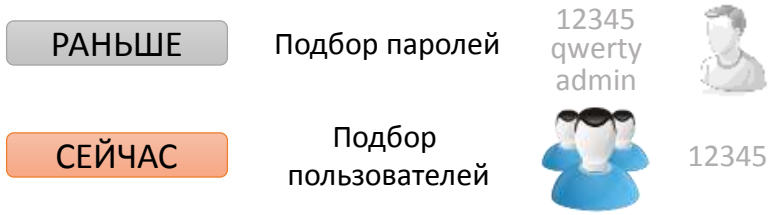
Существующие методы защиты



Большинство сервисов по защите от DDoS используют статистические методы, и включают защиту только при аномалиях.

Сканирования, взломы, подготовки к атаке, кражи контента осуществляются при нормальной активности

Captcha не эффективна. Существует множество сервисов по обходу защиты с помощью «реальных» пользователей сторонних ресурсов



Низкочастотные запросы от БОТ-ов не вызывают подозрений у средств защиты

Ежедневно сайты на основе популярных CMS подвергаются автоматическому сканированию на новые уязвимости

Блокировки по IP-адресам приводят к тому, что блокируются целые сегменты «реальных» пользователей

Сервис очистки от Ботов, DDoS и взлома

Защита от DDoS:

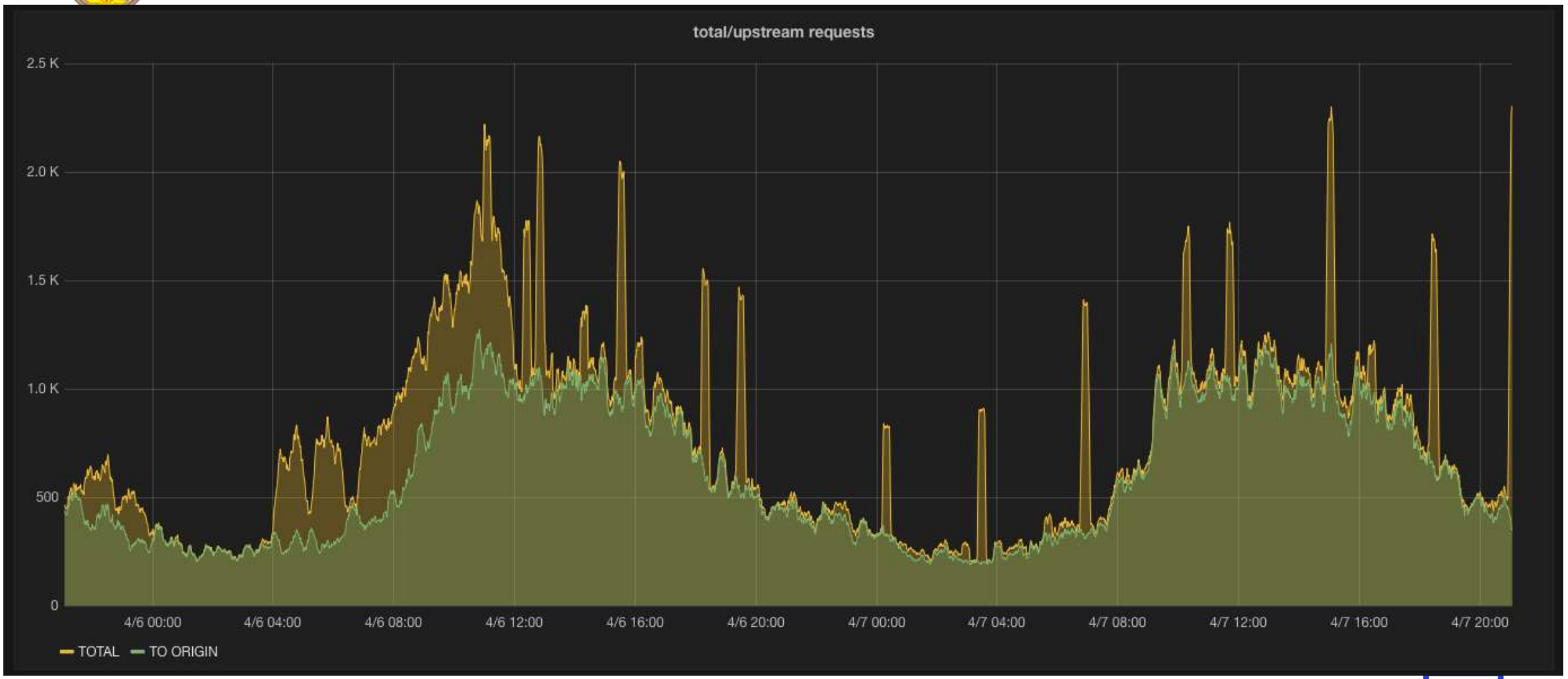
- Защита от DDoS-атак сетевого уровня (L3,4) и уровня приложений (L7)

Защита от Ботов:

- От низкочастотных запросов до массовых атак
- Защита от Ботов на уровне сессии без блокировки по IP-адресам
- Защита от спам-ботов в комментариях и форумах без использования CAPTCHA
- Защита от воровства контента

- **Система активного противодействия ботам и DDoS**
- **Защита сайта от взломов: от сканирований, автоматических реплик.**
- **Защита с первого запроса для HTTPS** как с раскрытием, так и без раскрытия трафика, удовлетворяющая требованиям PCI DSS

Портал федерального ведомства



Спасибо за внимание!

г. Новосибирск, ул. Фрунзе д.5
тел./факс +7 (383) 211-92-76
ac@atlas-nsk.ru
www.atlas-nsk.ru