Защита сетевого взаимодействия на базе АПКШ Континент

Лопатин Роман
Заместитель руководителя отдела продаж

КОД БЕЗОПАСНОСТИ

ВНУТРИ И СНАРУЖИ…

Есть чёткое понимание того, что инфраструктура – это всё, что внутри периметра контролируемой зоны.

Но это не так…

Есть чёткое понимание того, что основные угрозы для инфраструктуры и данных исходят изнутри.

Но это не так…

У офицеров по информационной безопасности есть чёткое понимание того, что к угрозам извне они готовы.

Но это не так…

КОД БЕЗОПАСНОСТИ

ЧТО ЕСТЬ ДЛЯ ЗАЩИТЫ ПЕРИМЕТРА…

КОД БЕЗОПАСНОСТИ

РОССИЙСКИЙ ПУТЬ…

ИСТОРИЧЕСКИ СЛОЖИЛОСЬ, ЧТО РОССИЙСКИЕ СРЕДСТВА ЗАЩИТЫ ПЕРИМЕТРА ВЫШЛИ ИЗ КРИПТОГРАФИИ…

НА СЕГОДНЯШНИЙ ДЕНЬ КАЧЕСТВЕННЫХ СРЕДСТВ ЗАЩИТЫ ПЕРИМЕТРА РОССИЙСКОГО ПРОИЗВОДСТВА ПРАКТИЧЕСКИ НЕТ…

МУЛЬТИСЕРВИСНЫХ РЕШЕНИЙ И УСТРОЙСТВ НЕТ В ПРИНЦИПЕ. ДОСТОЙНЫХ НЕТ…

ПЕРСПЕКТИВЫ? ЕСТЬ!
НО НУЖНО ВРЕМЯ…

КОД БЕЗОПАСНОСТИ

ПРЕДМЕТНО ПО НАМ И НЕ ТОЛЬКО…

АПКШ КОНТИНЕНТ 2014

ПАКЕТНАЯ ФИЛЬТРАЦИЯ
VPN-ГОСТ
QOS
BGP
MULTICAST
MULTIWAN
ПОДДЕРЖКА VLAN
ПОДДЕРЖКА NAT/PAT
TRAFFIC SHAPING
ОТКАЗОУСТОЙЧИВОСТЬ

АПКШ КОНТИНЕНТ 2018

SSH
L2 VPN
REMOTE ACCESS VPN
IDS/IPS
DHCP/DHCP RELAY
ПОДДЕРЖКА 3G/4G
АГРЕГАЦИЯ ИНТЕРФЕЙСОВ – LACP
АППАРАТНЫЙ КРИПТОУСКОРИТЕЛЬ

КОД БЕЗОПАСНОСТИ

ЗДЕСЬ И СЕЙЧАС…

ИСТОРИЯ ПЕРВАЯ…

Закончить compliance-сценарий…

Оптимизировать и отладить то, что есть сейчас…

Повысить производительность действующих решений…

Повысить уровень удобства управления и мониторинга…

Добавить дополнительные механизмы защиты без потери производительности

ИСТОРИЯ ВТОРАЯ…

Выпустить продукт, который максимально приближен к требованиям рынка…

Пересмотреть архитектуру решения в сторону мультизадачности…

Удержать производительность на должном уровне…

Постараться сделать безболезненную миграцию действующего решения на новое…

Учесть все требования отечественных регуляторов…

КОД БЕЗОПАСНОСТИ

О РЕГУЛЯТОРАХ...

КОД БЕЗОПАСНОСТИ

ИСТОРИЯ ПЕРВАЯ…

АПКШ КОНТИНЕНТ 2018
Версия 3.9

SSH
L2 VPN
REMOTE ACCESS VPN
IDS/IPS
DHCP/DHCP RELAY
ПОДДЕРЖКА 3G/4G
АГРЕГАЦИЯ ИНТЕРФЕЙСОВ – LACP
АППАРАТНЫЙ КРИПТОУСКОРИТЕЛЬ

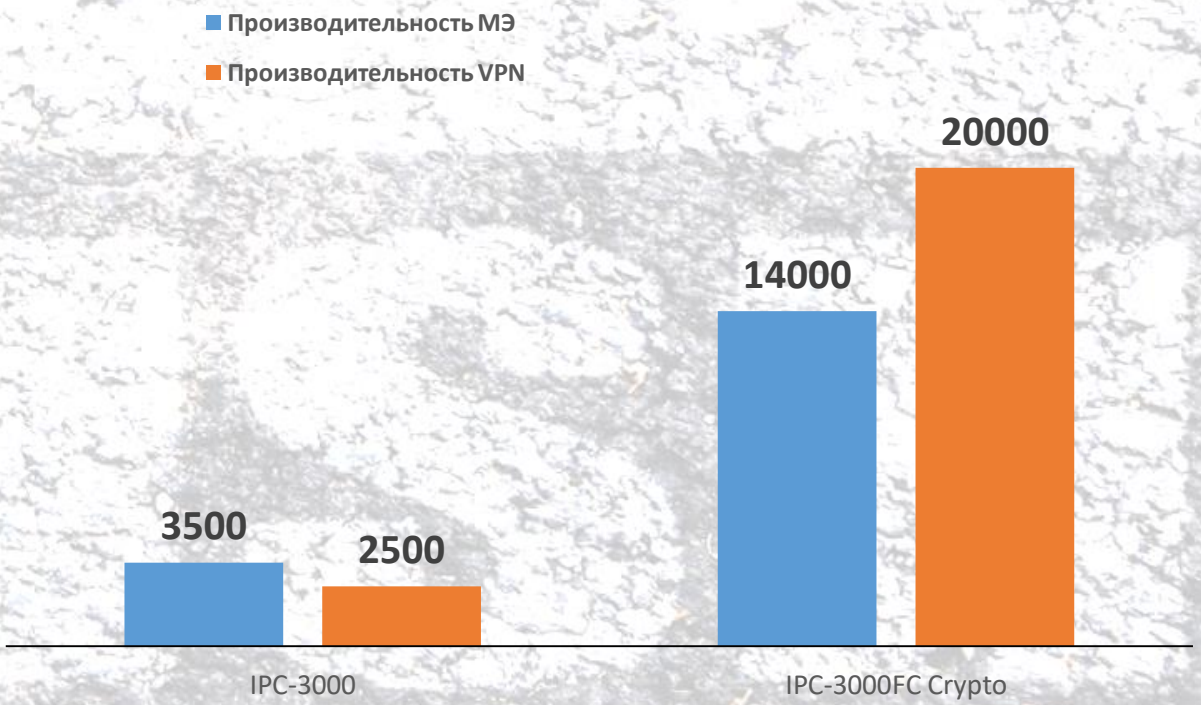
КОД БЕЗОПАСНОСТИ

НОВЫЙ МОДЕЛЬНЫЙ РЯД…

КОД БЕЗОПАСНОСТИ

АППАРАТНЫЙ КРИПТОУСКОРИТЕЛЬ…

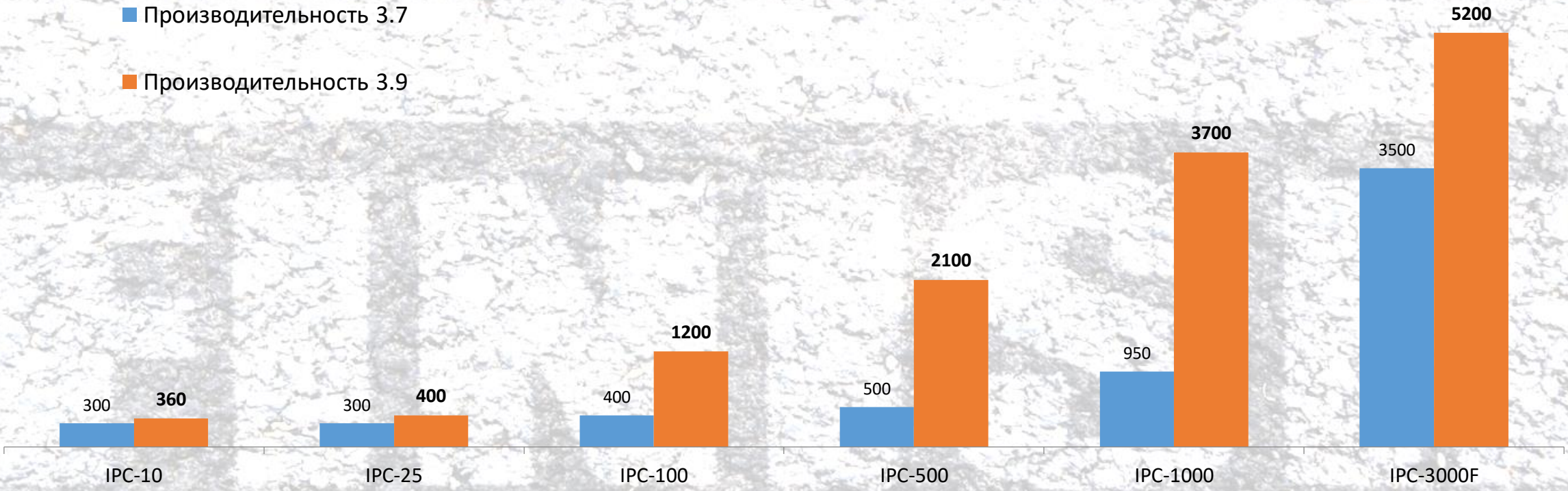
НАКОНЕЦ СДЕЛАН…



КОД БЕЗОПАСНОСТИ

ПРОИЗВОДИТЕЛЬНОСТЬ FW…

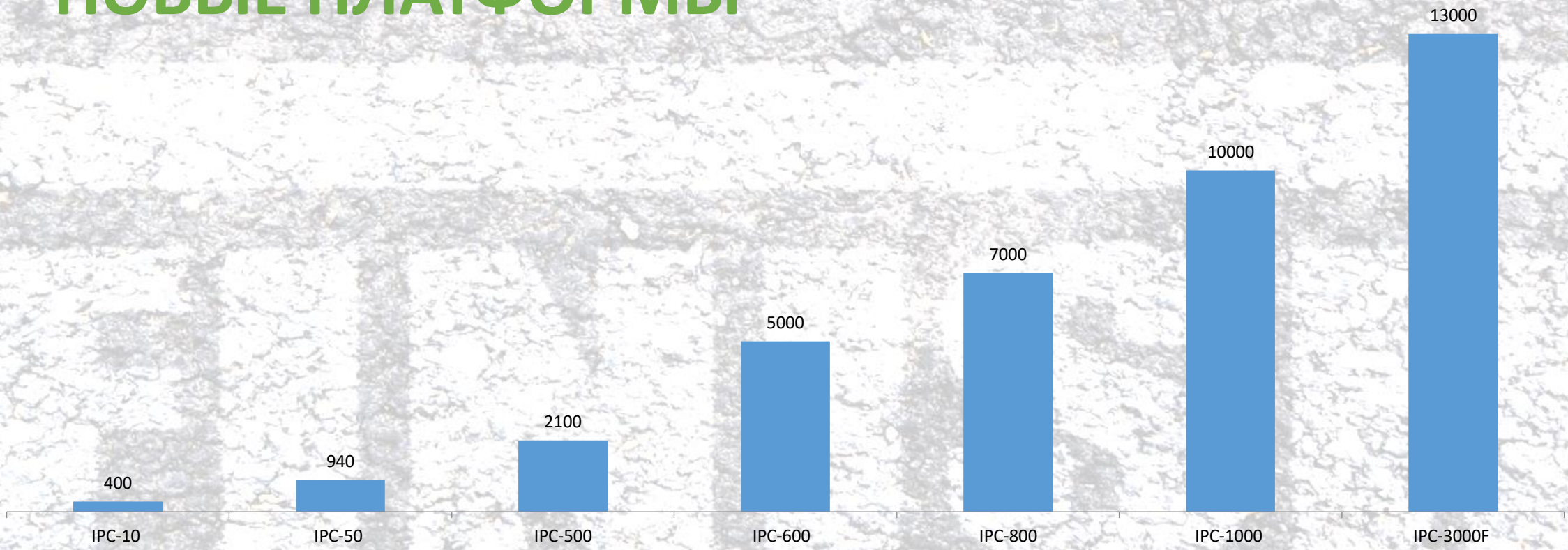
СТАРЫЕ ПЛАТФОРМЫ



КОД БЕЗОПАСНОСТИ

ПРОИЗВОДИТЕЛЬНОСТЬ FW…

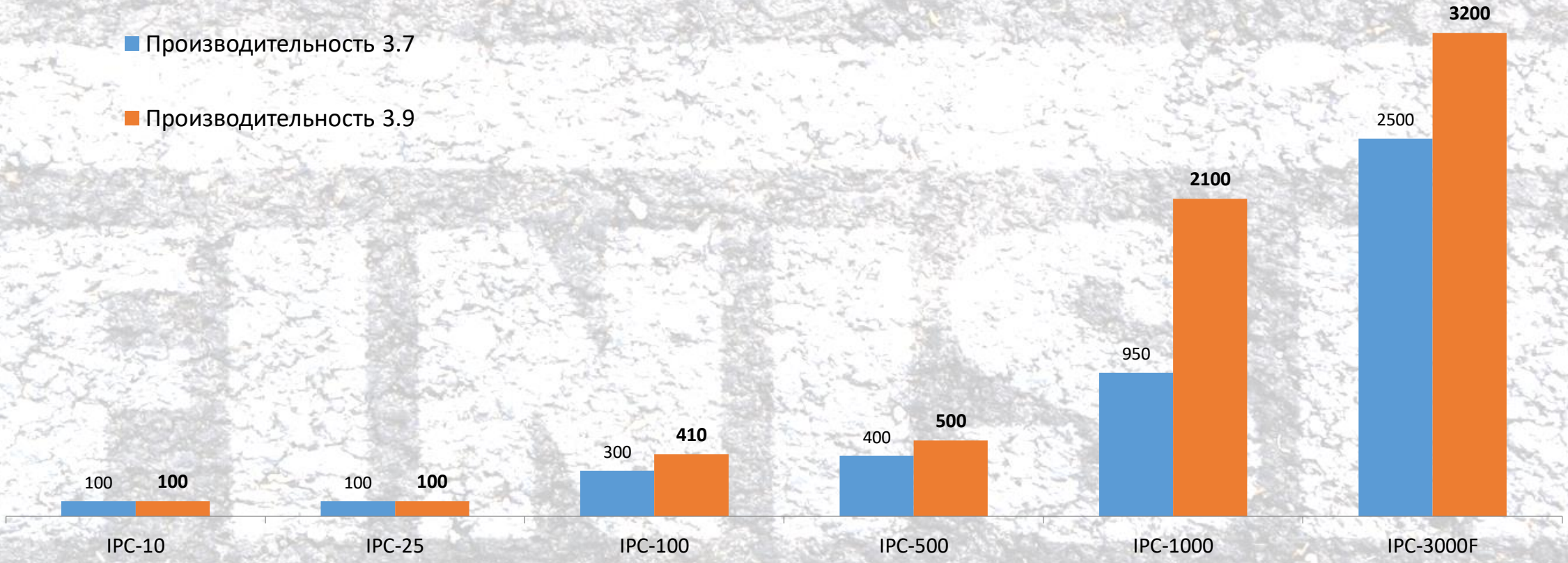
НОВЫЕ ПЛАТФОРМЫ



КОД БЕЗОПАСНОСТИ

ПРОИЗВОДИТЕЛЬНОСТЬ VPN…

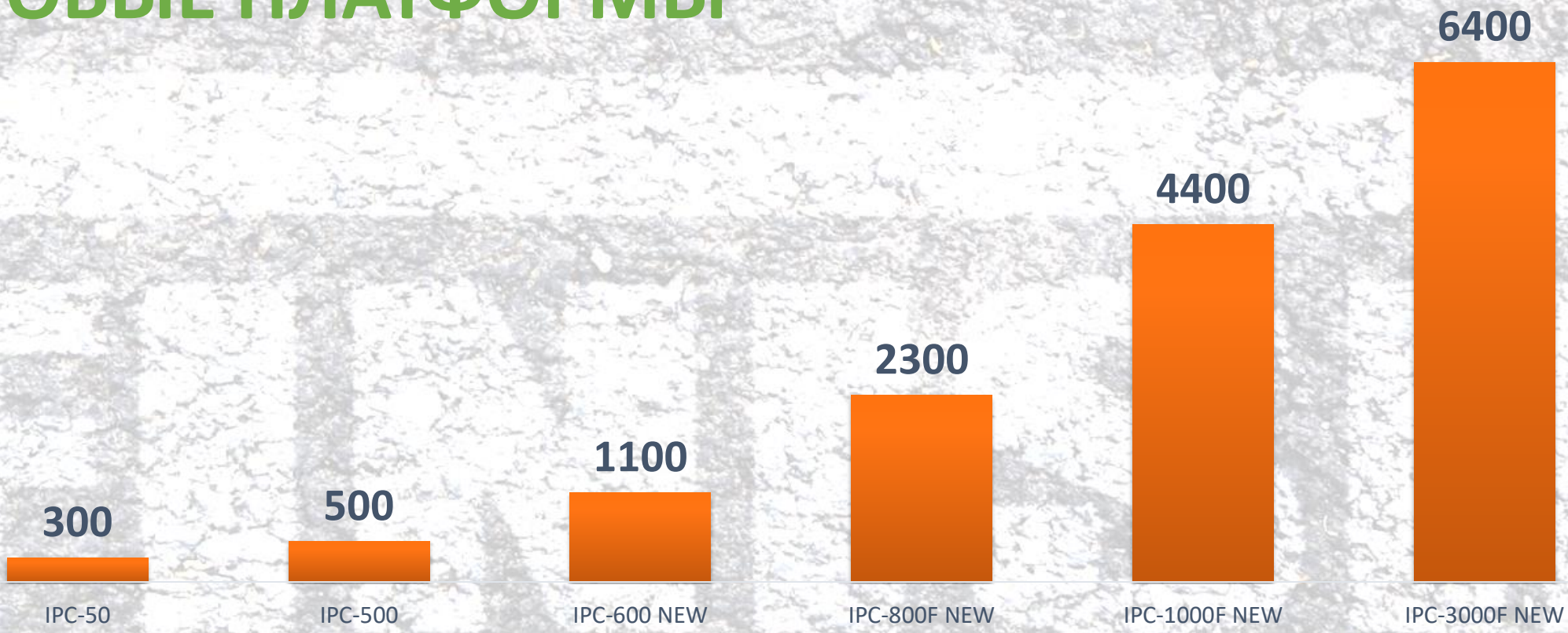
СТАРЫЕ ПЛАТФОРМЫ



КОД БЕЗОПАСНОСТИ

ПРОИЗВОДИТЕЛЬНОСТЬ VPN...

НОВЫЕ ПЛАТФОРМЫ



КОД БЕЗОПАСНОСТИ

ИСТОРИЯ ВТОРАЯ…

АПКШ КОНТИНЕНТ 2019
Версия 4

Архитектура UTM
(FW+VPN+IPS+СД)
DPI
Application & URL Filtering
Высокопроизводительный движок NF2 (~80Гбит/с)
Интеграция с каталогами Active Directory
Возможность настройки L3VPN и L2VPN на одном узле

АВГУСТ 2019…

КОД БЕЗОПАСНОСТИ

REMOTE ACCESS VPN…

КОНТИНЕНТ TLS

Система обеспечения защищенного удаленного доступа к веб-приложениям с использованием алгоритмов шифрования ГОСТ

- **Гибкая система лицензирования**
  (единовременное количество подключений, бесплатный vpn-клиент)
- **Лёгкость масштабирования**
  (увеличения нод с лицензиями на единовременные подключения)
- **Поддержка любых браузеров**
  (не нужен контроль встраивания в браузеры или приложения)
- **Три режима работы**
  (Поддержка работы через прокси, портал приложений, TLS-туннель)

КОД БЕЗОПАСНОСТИ

СОВ/СОА…

КОНТИНЕНТ IPS

Высокопроизводительная система обнаружения и предотвращения вторжений с иерархическим управлением и возможностью контроля сетевых приложений

- Возможность работы в проактивном режиме (оборудование «в разрыв»)
- Лёгкость масштабирования (увеличения нод с балансировщиком)
- Собственная лаборатория по созданию сигнатур (создание новых сигнатур и актуализация имеющихся)
- Функционал DPI на борту (вычистка трафика и контроль приложений)

КОД БЕЗОПАСНОСТИ

WEB APPLICATION FIREWALL…

КОНТИНЕНТ WAF

Система защиты веб-приложений и автоматизированный анализ их бизнес-логики

Обнаружение специфических атак на веб-приложения
(sql-инъекции, OWASP TOP 10, Cross Site Scripting и др.)

Обнаружения аномалий
(bruteforce атаки, запросы/ответы веб-сервера, работа приложений)

Три режима работы
(«в разрыв», зеркалирование, анализ логов активности веб-сервера)

У него есть сертификат ФСТЭК!
☺

БЛАГОДАРЮ ЗА ВНИМАНИЕ!

Роман Лопатин
r.lopatin@securitycode.ru
+7 (495) 982 30 20 (*491)
+7 (926) 567 39 86