7 причин перейти на отечественный NGFW сегодня

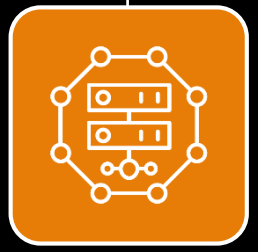
Анна Исакова

Руководитель отдела маркетинга

Айдеко – российский разработчик решений для сетевой безопасности

фильтрация трафика

защита сети



развитие сетевых инфраструктур

Защищаем сети компаний межсетевым экраном Ideco UTM

с 2005 года на рынке ИБ

4 000 компаний используют Ideco UTM

40 000 человек используют VPN-подключения

2 000 бесплатных лицензий для некоммерческого использования

с 2020 года сами работаем удаленно

ideco

1

2022
Количество кибератак выросло на 14,8%

16% Государственные учреждения

11% Медицинские учреждения

8% Промышленные предприятия

5% СМИ

ideco

1

2022
Количество кибератак выросло на 14,8%

16% Государственные учреждения

11% Медицинские учреждения

8% Промышленные предприятия

5% СМИ

Лучшая защита – кибератака, которая не случилась!

- Акцент на предупреждение угроз
- Проводить анализ уязвимостей
- Защита всех рубежей
- Своевременная установка обновлений
- Внедрение передовых технологий

ideco

2

С чем сталкиваются организации сегодня?

Уход с рынка зарубежных производителей

Рост рисков киберугроз

Бюджеты на ИБ и внутренняя борьба за них

Необходимость защиты сети в соответствии с требованиями регуляторов

Дефицит новых кадров, загруженность текущих

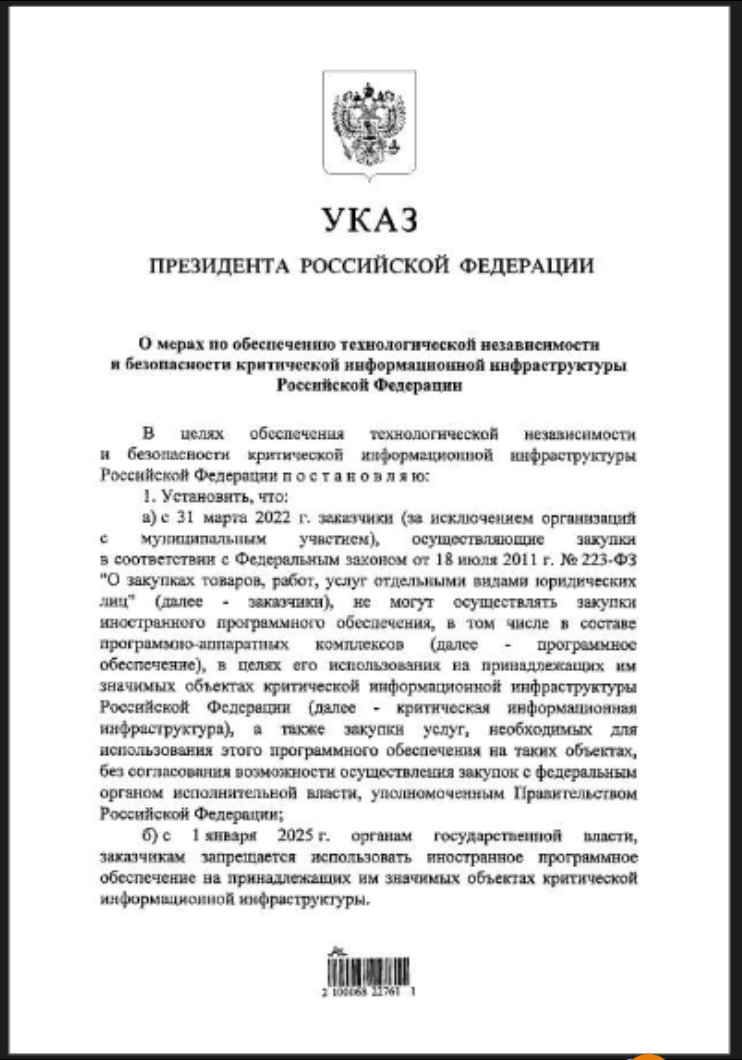
ideco

3

На уровне государства

Указ Президента от 30.03.2022 № 166 "О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации":

- **запрет покупки зарубежного ПО и ПАК для значимых объектов КИИ по 223-ФЗ с 31 марта 2022;**
- **запрет использования зарубежного ПО и ПАК для значимых объектов КИИ с 1.01.2025.**



УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации

В целях обеспечения технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации п о с т а н о в л я ю:

1. Установить, что:

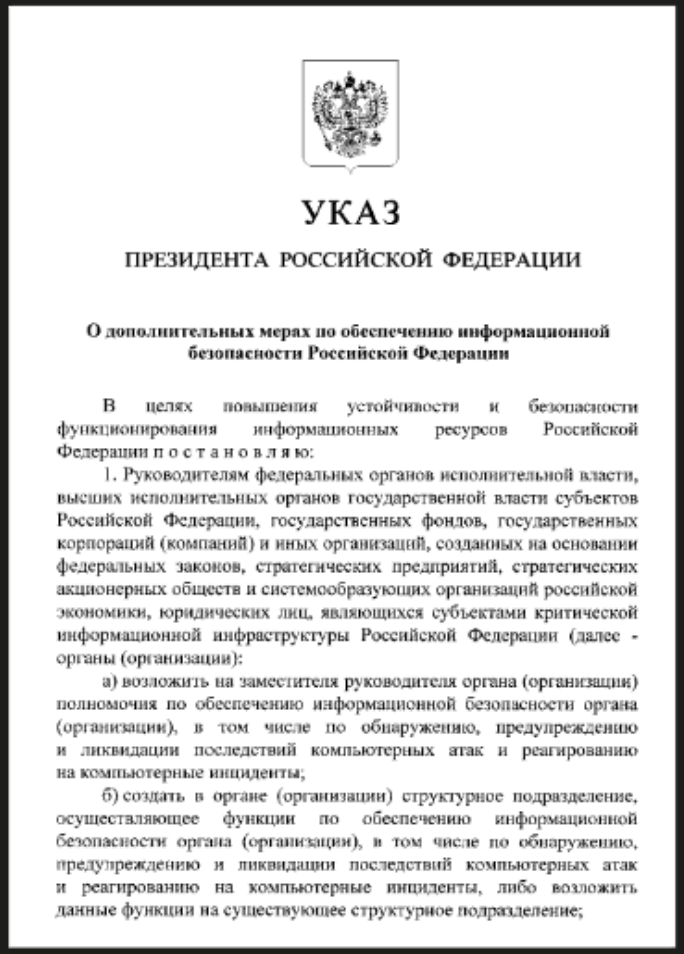
а) с 31 марта 2022 г. заказчики (за исключением организаций с муниципальным участием), осуществляющие закупки в соответствии с Федеральным законом от 18 июля 2011 г. № 223-ФЗ "О закупках товаров, работ, услуг отдельными видами юридических лиц" (далее - заказчики), не могут осуществлять закупки иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов (далее - программное обеспечение), в целях его использования на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура), а также закупки услуг, необходимых для использования этого программного обеспечения на таких объектах, без согласования возможности осуществления закупок с федеральным органом исполнительной власти, уполномоченным Правительством Российской Федерации;

б) с 1 января 2025 г. органам государственной власти, заказчикам запрещается использовать иностранное программное обеспечение на принадлежащих им значимых объектах критической информационной инфраструктуры.

3

Указ Президента от 01.05.2022 № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации":

- **распространяется на органы госвласти, высшие исполнительные органы госвласти, государственные фонды, госкорпорации, иные предприятия, созданные на основании ФЗ, стратегические предприятия, стратегические акционерные общества, системообразующие организации экономики и субъекты КИИ (без привязки к владению значимыми или незначимыми объектами);**
- **с 1-го января 2025 все попавшие под Указ организации не смогут использовать средства защиты из недружественных государств, а также от иных организаций, которые прямо или косвенно подконтрольны таким государствам.**



УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О дополнительных мерах по обеспечению информационной безопасности Российской Федерации

В целях повышения устойчивости и безопасности функционирования информационных ресурсов Российской Федерации п о с т а н о в л я ю:

1. Руководителям федеральных органов исполнительной власти, высших исполнительных органов государственной власти субъектов Российской Федерации, государственных фондов, государственных корпораций (компаний) и иных организаций, созданных на основании федеральных законов, стратегических предприятий, стратегических акционерных обществ и системообразующих организаций российской экономики, юридических лиц, являющихся субъектами критической информационной инфраструктуры Российской Федерации (далее - органы (организации):

а) возложить на заместителя руководителя органа (организации) полномочия по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты;

б) создать в органе (организации) структурное подразделение, осуществляющее функции по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, либо возложить данные функции на существующее структурное подразделение;

ideco

4

Ideco UTM

Задачи:

- Защита сети, фильтрация трафика
- Учет, авторизация пользователей и устройств
- Организация удаленного защищенного доступа
- Отчетность и мониторинг
- Соблюдение требований регулятора
- Оптимизация использования интернет-канала

DPI-фильтрация на 7 уровне модели OSI

15 млн доменов и IP-адресов C&C в нашем BlockList

500 млн URL в обновляемой базе данных

ideco

Межсетевой экран нового поколения

Модули Ideco UTM:

- DPI-фильтрация на 7 уровне модели OSI
- 15 млн доменов и IP-адресов C&C в нашем BlockList
- 500 млн URL в обновляемой базе данных

ideco

Центральная консоль

для централизованного управления настройками межсетевых экранов Ideco UTM

Общие политики безопасности
Добавятся для модулей контент-фильтр, контроль приложений, а также для ограничения скорости.

Мониторинг серверов
Добавится мониторинг за состоянием серверов (загрузка канала, нагрузка ЦП и т.д.) и атаками на них.

Отчётность по трафику
Позволит в одном месте следить за активностью пользователей на всех серверах Ideco UTM.

ideco

5 Сервисы

Центральная консоль управления несколькими серверами

VPN
- Site-To-Site IPsec
- IKEv2
- SSTP
- Wireguard (клиент)
- L2TP/IPSec

Трафик
Балансировка канала
Резервирование канала
Квоты
Шейпинг

Отказоустойчивость:
- Кластеризация Active/Passive
- Резервное копирование
- Программный Watchdog

Маршрутизация
Статическая
Динамическая OSPF, BGP

DNS, DHCP, NTP

Обратный прокси
- Публикация WEB-приложений
- Публикация OWA Exchange
- WAF

Мониторинг
Телеграм-бот
Zabbix Агент
Syslog, SNMP

ideco

5 Соответствие требованиям регулятора

Сертификат ФСТЭК №4503 от 28.12.2021 г.

Решение входит в реестр российского ПО Минцифры РФ

- Требования доверия (4)
- Требования к МЭ
- Требования к СОВ
- Профиль защиты МЭ (А четвертого класса защиты. ИТ.МЭ.А4.ПЗ)
- Профиль защиты МЭ (Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ)
- Профили защиты СОВ (четвертого класса защиты. ИТ.СОВ.С4.ПЗ)

ideco

Переход с конкурентных решений

- Kerio Control
- Устаревшие решения под Windows: Microsoft ISA/TMG, UG Proxy and Firewall, Traffic Inspector
- Различные российские решения
- L3 FW
- Cisco ASA/WSA, Checkpoint, Fortinet – здесь сложнее, но активно догоняем
- Переход с самописных шлюзовых и прокси-решений на Linux/FreeBSD

ideco

6 Больше, чем продукт

Гибкая разработка

Моментальная реакция на новые вызовы и угрозы
Road-map по задачам пользователей

Защита сети «из коробки»

Преднастроенные правила фильтрации, **IPS, FW**

Шай-тек (Shy-tech)

Умные технологии
для интуитивно-понятных решений

Многоканальная техподдержка

-портал поддержки **help.ideco.ru**
-электронная почта
-телефон
-**Telegram**
-чат в продукте

Presale

Поддержка и консультации на этапе тестирования и внедрения
Решения для нестандартных кейсов

ideco

7 Будущее

Рост кибератак на 20% по сравнению с 2022 годом

Фишинг –звонки и письма через непривычные нам сейчас каналы распространения (мессенджеры, QR-коды со ссылками, бумажные почтовые рассылки и т.д.)

Развитие законодательной базы - методологические документы
и практика применения мер воздействия

Импортозамещение в растущем тренде

ideco

7 Будущее

x10 скорость обработки трафика, полностью «свой» стек обработки трафика,общие правила firewall/DPI/IPS

x2 скорость обработки веб-трафика, новейший модуль прокси-сервера (от Айдеко)

Переход на новую систему обработки трафика – DPDK, VPP, eBPF.
Переход с последовательной обработки пакетов к параллельной.

Высокоскоростной NGFW и технологическое лидерство среди отечественных решений

ideco

ideco

Спасибо!

@IsAnna

a.isakova@ideco.ru

t.me/idecoutm

@ideco