

Простые решения в сложных ситуациях

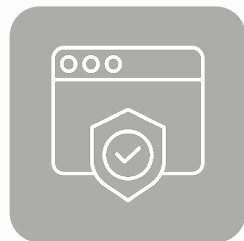
защищаем сеть с Ideco UTM

Руслан Никифоров

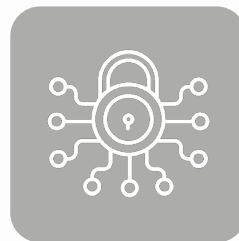
заместитель директора по развитию



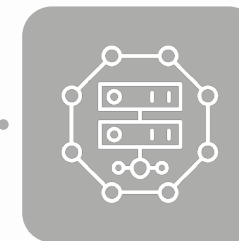
«Айдеко» - российский разработчик программных продуктов, созданных для



фильтрации
трафика



защиты
сети



развития сетевых
инфраструктур

Защищаем сети компаний с помощью межсетевого экрана 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

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 security. Что проверяет?

- ✓ Доступ к вредоносным и потенциально опасным сайтам
- ✓ 15 категорий сайтов, более 120 URL
- ✓ Возможность прохождения вирусного трафика

security.ideco.ru

ideco		8 800 555 33 40 Отдел продаж	
ОТЧЁТ ПО БЕЗОПАСНОСТИ СИСТЕМЫ			
На сайте security.ideco.ru была произведена проверка безопасности вашей системы. С методикой тестирования вы можете ознакомиться в нашем блоге . Результаты проверки содержит данный отчет.			
Название	Результат теста	Средняя доля в трафике*	Модуль Ideco UTM для закрытия уязвимости
Общий уровень защиты	46/76 пропущено	41% **	контент-фильтр, предотвращение вторжений, контроль приложений
Высокий уровень опасности			
Анонимайзеры	4/7 пропущено	0.6%	предотвращение вторжений
Ботнеты	1/1 пропущено	0.3%	предотвращение вторжений
Вирусы (скачивание по http)	2/2 пропущено	0.02%	антивирус веб-трафика
Фишинговые сайты	0/5 пропущено	0.01%	контент-фильтр
Эксплойты в PDF-файлах (скачивание по http)	1/1 пропущено	0.01%	антивирус веб-трафика
Потенциально опасные ресурсы			
Онлайн-казино	3/4 пропущено	0.5%	контент-фильтр
Порнографические сайты	9/11 пропущено	2.7%	контент-фильтр
Сети стран третьего мира	1/5 пропущено	0.1%	контент-фильтр
Федеральный список Минюста	4/4 пропущено	0.19%	контент-фильтр
Пожиратели времени			
Астрология и гороскопы	1/4 пропущено	0.1%	контент-фильтр
Знакомства	6/6 пропущено	2.3%	контент-фильтр
Компьютерные игры	4/5 пропущено	3.6%	контроль приложений
Мультфильмы, аниме и комиксы	3/3 пропущено	0.89%	контент-фильтр
Развлекательные новости и сайты про знаменитостей	3/3 пропущено	4.6%	контент-фильтр
Пожиратели трафика			
Майнинг криптовалют	2/5 пропущено	0.01%	контроль приложений
Рекламные сети	1/5 пропущено	8.33%	контент-фильтр
Торренты и P2P сети	1/5 пропущено	17%	контроль приложений
* На основании исследования 1500 сетей российских компаний			
** Ориентировочная цифра экономии трафика при внедрении Ideco UTM и настройке фильтрации			

Ideco security. Дополнительные проверки

- ✓ Почтовые адреса на компрометацию (по базе из более чем 7 млрд. адресов)
- ✓ Информация о скачанных торрентах
- ✓ Наличие ip-адреса в черных списках
- ✓ Открытые порты и ответы сервисов на внешнем интерфейсе

security.ideco.ru

Проверка почтового адреса на компрометацию:

Адрес	Найденные в базах пароли
ideco@ideco.ru	не найдены

Информация о скачанных торрентах:

Дата (UTC)	Тип	Название	Размер
Jun 21, 2019, 7:48:49 PM	Игры	K3TDM.iso	1.58Гб
Jun 21, 2019, 5:52:48 PM	Игры	The Sims 2 Antology	8.35Гб
Jun 21, 2019, 5:37:06 PM	Игры	Sea Dogs To Each His Own [qoob RePack]	3.42Гб

Наличие IP-адреса в черных списках:

Название сервиса	Результат
Barracuda BBL	Clear
Sorbs.net	Clear
South Korean NBL	Low Risk
Spamcop	Listed
Spamhaus	Clear

Если вы используете статический IP-адрес, то его наличие в чёрных списках — серьёзный симптом участия хостов вашей сети в ботнетах. [Рекомендации](#) по устранению заражения.

Результаты сканирования вашего IP-адреса (178.44.140.63)

Открытые порты:

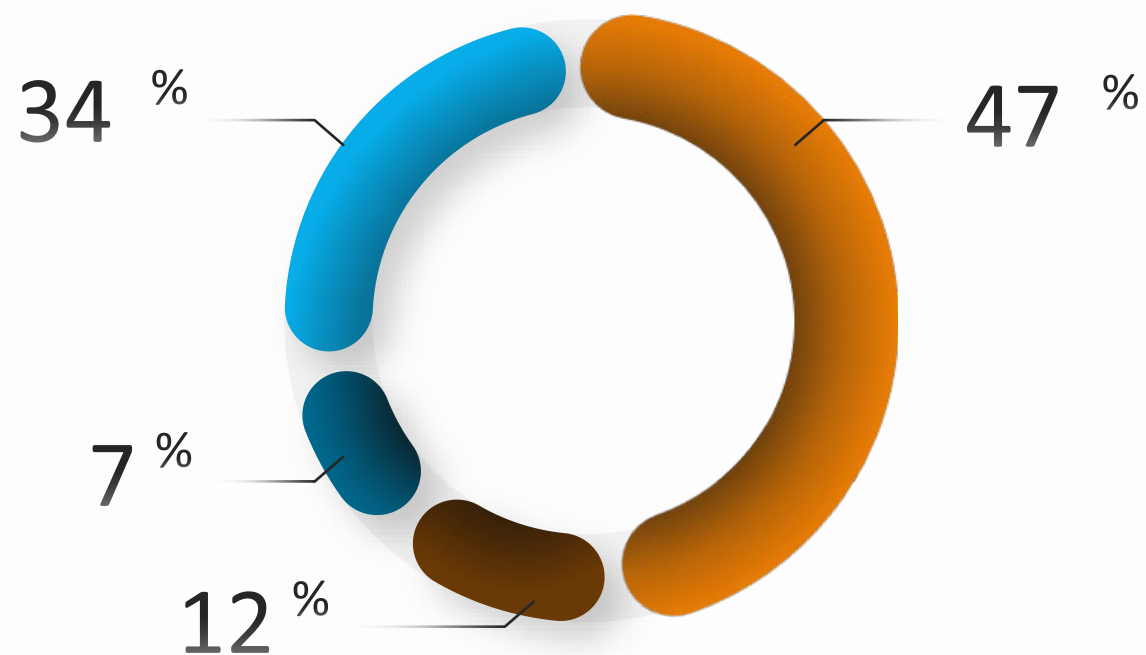
80, 6881





Внимание! Веб-ресурсы рекомендуется публиковать защищая их модулем [Web Application Firewall](#).

Порт	Сервис	Ответ сервиса
80, tcp	http	HTTP/1.1 200 OK Server: Virtual Web 0.9 Set-Cookie: SessionID=; path=/ Content-Type: text/html Content-Length: 151
		DHT Nodes 118.198.73.73 61937 187.233.235.179 42715 60.135.12.62 39204 94.82.177.149 24537 116.141.118.204 41312 199.161.234.168 11992 229.90.194.183 29788 239.134.37.73 48314 224.2.210.103 30581 20.143.11.176 30516 25.229.26.110

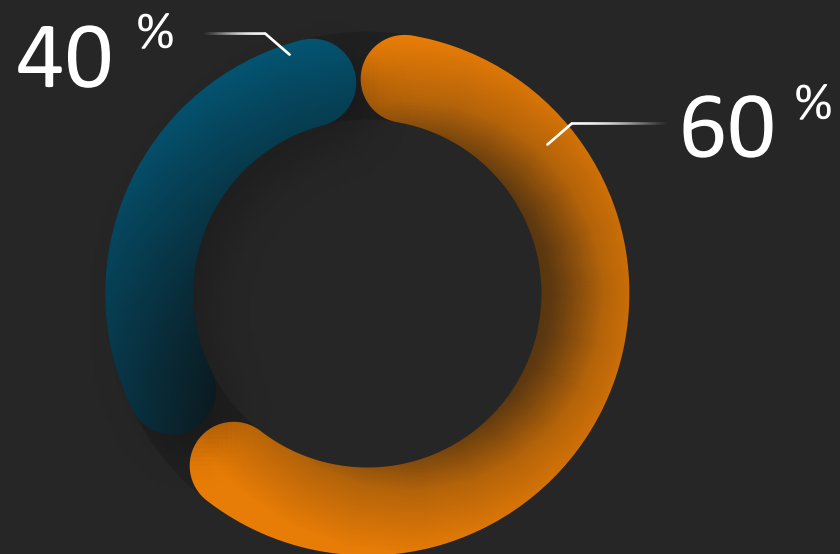
Результат тестирования

Устаревшие, уязвимые решения

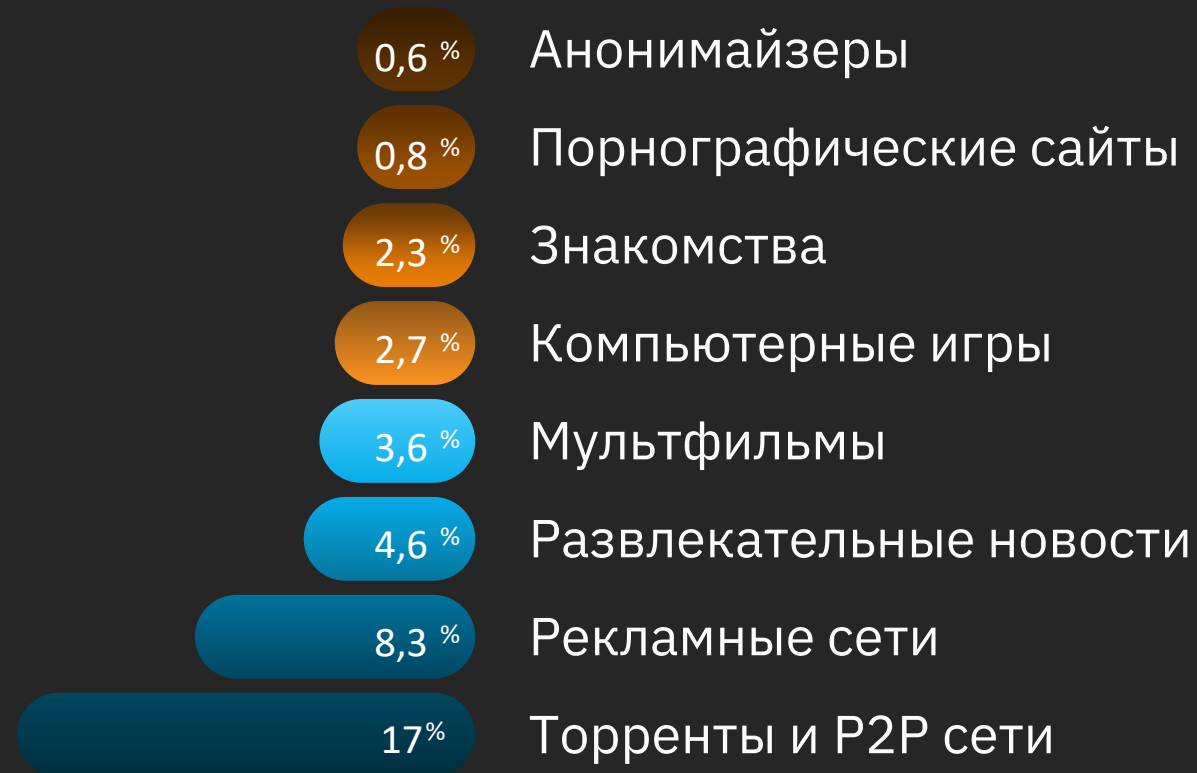


-  L3 фаерволы
-  Устаревшие UTM
-  На ОС Windows
-  Неизвестно

Доля «паразитного трафика»



- Полезный трафик
- Бесплезный трафик



на основе исследования 1500 сетей российских компаний

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

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

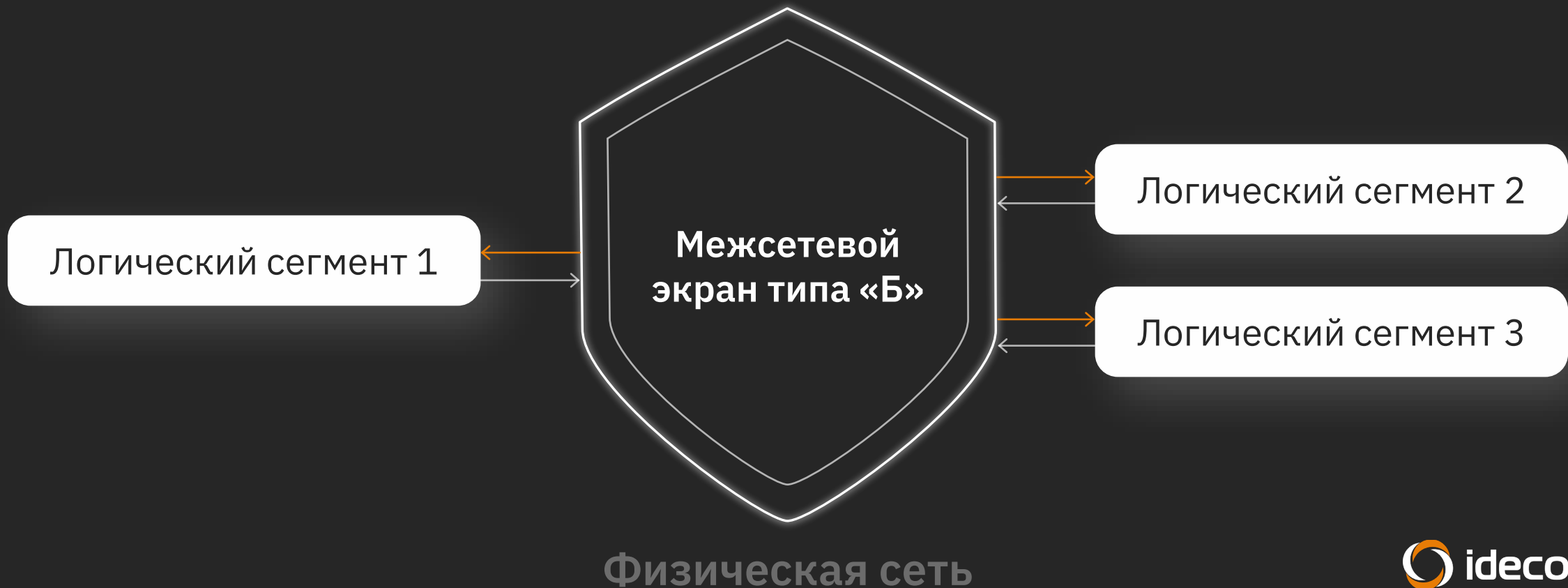
✓ Требования к СОВ

✓ 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)

Установка на виртуальную машину или своё оборудование



Что нового в марте 2022

Idecos UTM 11.8 не обращается к ресурсам за пределами РФ для обновлений, DNS, NTP, проверки связи

Блокировка обновлений Cisco, Microsoft, Adobe

Автоматическое обновление сигнатур по спискам НКЦКИ

Бесплатная редакция SMB: IPS+AC+CF до 31 мая для текущих лицензий, на 90 дней для новых

Бесплатное продление лицензий для возможности обновления всех пользователей до 31.03.2022

Работаем максимально близко к пользователям, без посредников, учитывая пожелания и прописывая roadmap

Держим цены на ПО и продление

Многоканальная техподдержка



Портал технической поддержки



Электронная почта



Телефон



Telegram-бот



JivoSite

ИДЕКО UTM 9.7 сборка 7

- Пользователи
- Учётные записи
- Авторизация
- Active Directory
- Обнаружение устройств
- Мониторинг
- Правила трафика
- Сервисы
 - Сетевые интерфейсы
 - Балансировка и резервирование
 - Маршрутизация
 - Прокси
 - Обратный прокси
 - DNS
 - DHCP-сервер
 - NTP-сервер
 - IPsec
 - Сертификаты
- Отчёты
- Управление сервером
- Почтовый релей

Авторизация

Работает

Основное **VPN-авторизация** Фиксированные IP-адреса VPN

Сеть для VPN-подключений
10.125.0.0/24

Авторизация PPTP

Авторизация PPPoE

Авторизация IKEv2/IPSec

Домен
domain.com

Маршруты
10.0.0.0/8 X

Маршруты
172.16.0.0/12 X

Будут переданы для VPN-подключения в ОС Windows

Добавить маршрут

[PowerShell - скрипт для настройки подключений](#)

Авторизация SSTP

Домен
domain.com

Порт
4443

[PowerShell - скрипт для настройки подключений](#)

Авторизация L2TP/IPSec

PSK
.....

[PowerShell - скрипт для настройки подключений](#)

Сохранить

«Шай-тек» (shy-tech)
или «скромные
ТЕХНОЛОГИИ»:
ЧТО ЭТО ТАКОЕ?

Оптимизируем **время** ваших сотрудников

Минимум времени на внедрение и сопровождение решения

Ресурсы на развитие, оптимизацию и автоматизацию инфраструктуры компании



Спасибо за внимание

Руслан Никифоров
заместитель директора по развитию

@RuslanNikiforov

r.nikiforov@ideco.ru