Как российский межсетевой экран помогает идти по пути импортозамещения

Дмитрий Хомутов

Исполнительный директор Айдеко

О компании

Находимся в Екатеринбурге. Работаем с 2005 года. Помогаем клиентам защититься от современных угроз безопасности, средствами удобного и «умного» межсетевого экрана Ideco UTM.

Более 4 000 компаний
используют Ideco UTM

Более 40 000 человек
используют
VPN-подключения

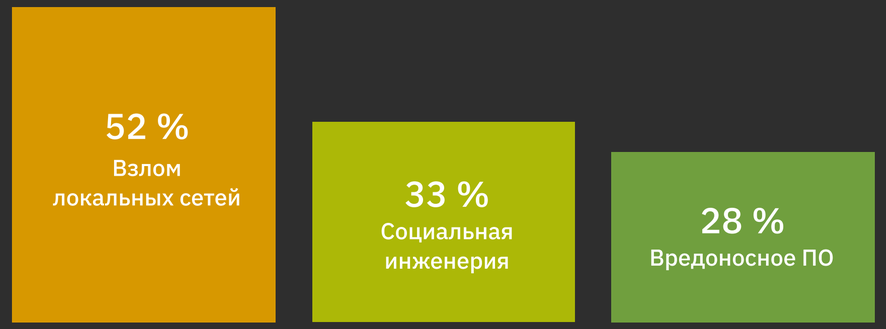
Год сами
работаем удаленно

Проблема №1. Рост рисков киберугроз

По данным Cybersecurity Ventures:

68% крупных компаний считают, что риски в области кибербезопасности возрастают в связи с удаленным доступом сотрудников.

Кибер - атаки в 2020



Интересный факт: С 7 мая 2021 года в результате атаки шифровальщика на трубопроводного оператора Colonial Pipeline на Восточном побережье США возник дефицит 45% горючего.

Текущие решения: Network Firewalls/UTM/NGFW

ideco

- Требуют высокой квалификации специалистов для настройки и поддержки.
- В 95% случаев представляют собой программно-аппаратные комплексы (которые устаревают за 3-4 года).

Check Point SOFTWARE TECHNOLOGIES LTD.

FORTINET

paloalto NETWORKS

Source: Gartner (November 2020)

Интересный факт: термин UTM ввела IDC в 2004 году,

термин NGFW ввели PaloAlto и Gartner в 2008 году,

с 2018 года Gartner объединил квадраты и назвал их Network Firewalls.

Все равно: рост ущерба от киберпреступлений

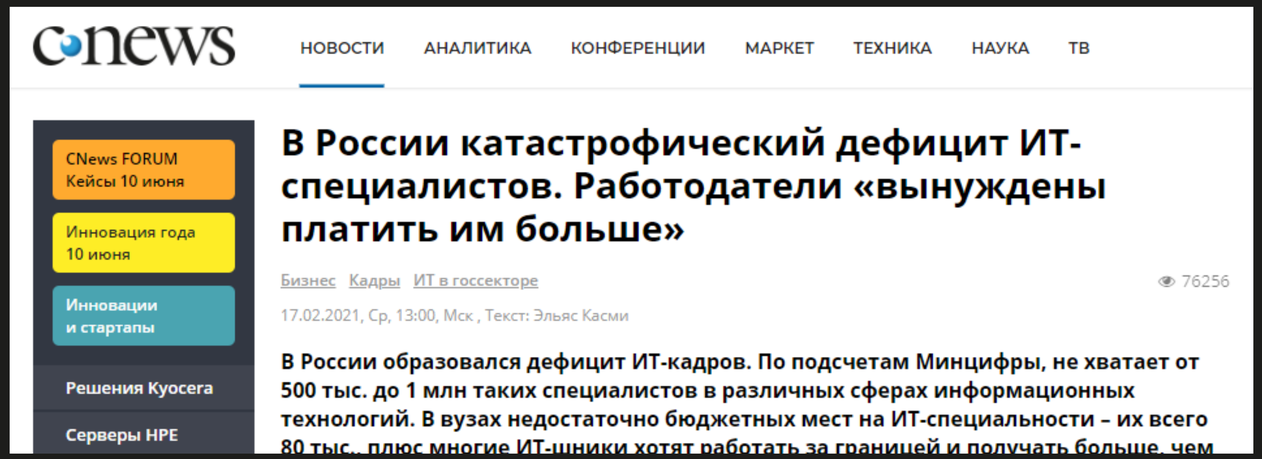
ideco

- 8 промышленных предприятий России из 10 имеют проблемы с обслуживанием ИТ-инфраструктуры (Group-IB, июнь 2021)
- В первой половине 2021 года, в России было зафиксировано почти в 3 раза больше атак на объекты критической инфраструктуры, чем за весь 2019 год (Group-IB, июнь 2021).
- Каждая десятая ИТ-инфраструктура госорганов, банков, ТЭК, транспортных и оборонных учреждений заражена вирусом («Ростелеком-Солар», июнь 2021).

Интересный факт: Shodan.io проиндексировал 6300 уязвимых камер видеонаблюдения, расположенных на объектах критической инфраструктуры РФ.

Проблема №2. ИТ-кадры

- отсутствие или нехватка компетентных специалистов по ИТ/ИБ;
- нет времени или опыта для работы с новыми решениями;
- работает - и ладно, не будем трогать, лишь бы не сломать.



Проблема №3. Мусорный трафик

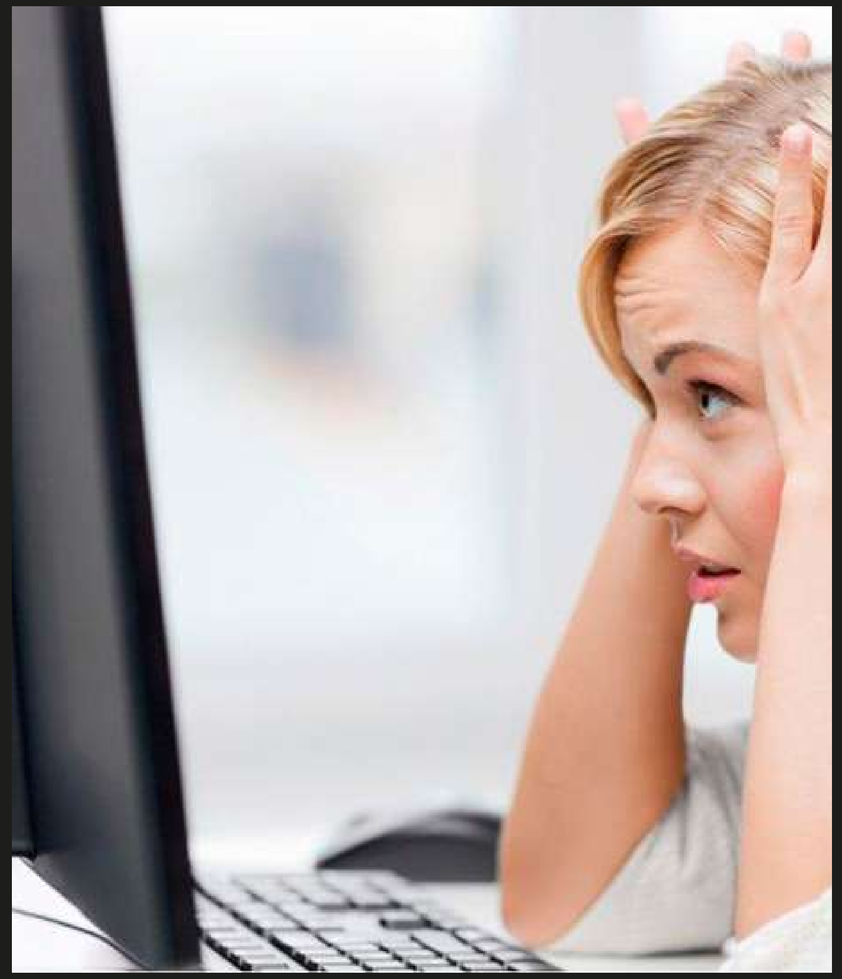
ideco

ограниченная ширина интернет-канала
и безграничные потребности в трафике;

медленный и нестабильный интернет
для требуемых по работе ресурсов.

кража времени: развлекательные
и фейковые новости, соц. сети, форумы;

кража внимания: кликбейт, ремаркетинг,
баннеры, всплывающие окна;



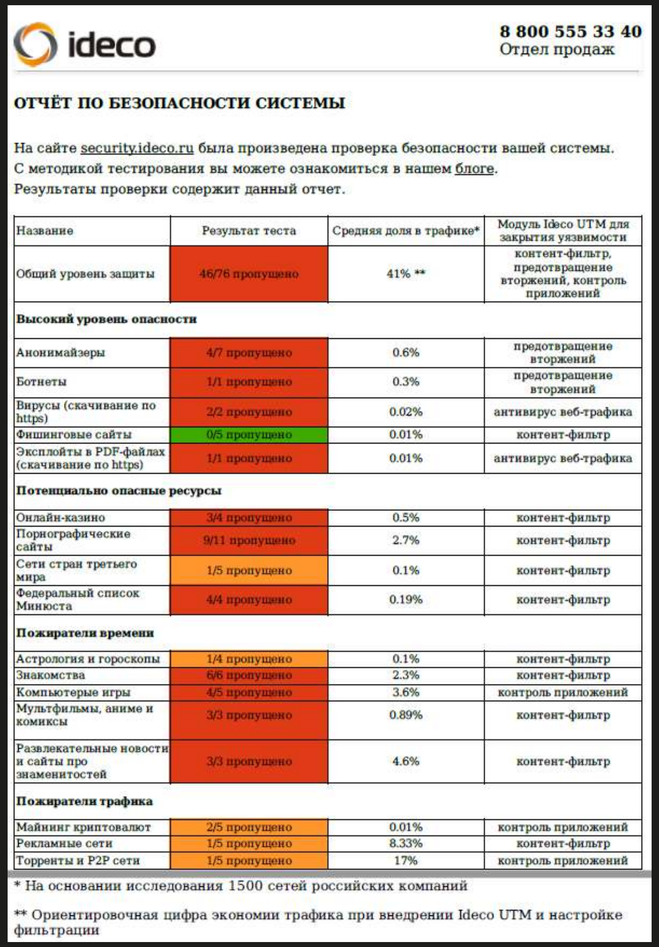
Боли рынка

А ещё: ФСТЭК, КИИ, импортозамещение, бюджеты.

Ideco Security. Как проверить вашу защиту ?

- проверит 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 https)	2/2 пропущено	0.02%	антивирус веб-трафика
Фишинговые сайты	0/5 пропущено	0.01%	контент-фильтр
Эксплойты в PDF-файлах (скачивание по https)	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

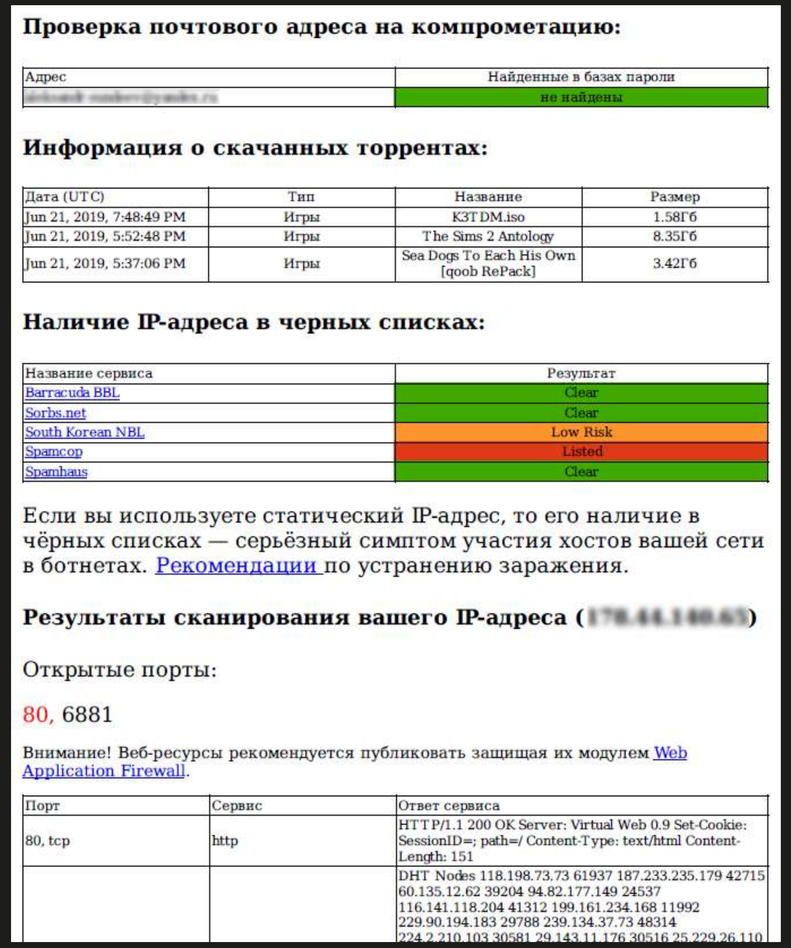
* На основании исследования 1500 сетей российских компаний

** 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);
- информацию 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
[redacted]	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 ([redacted])

Открытые порты:

80, 6881

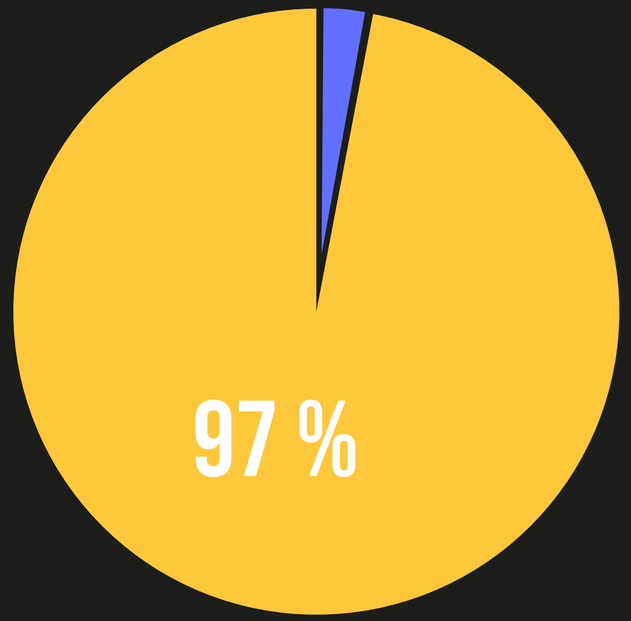
Внимание! Веб-ресурсы рекомендуется публиковать защищая их модулем Web Application Firewall.

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 29.143.11.176 30516 25.229.26.110

Результат тестирования

ideco

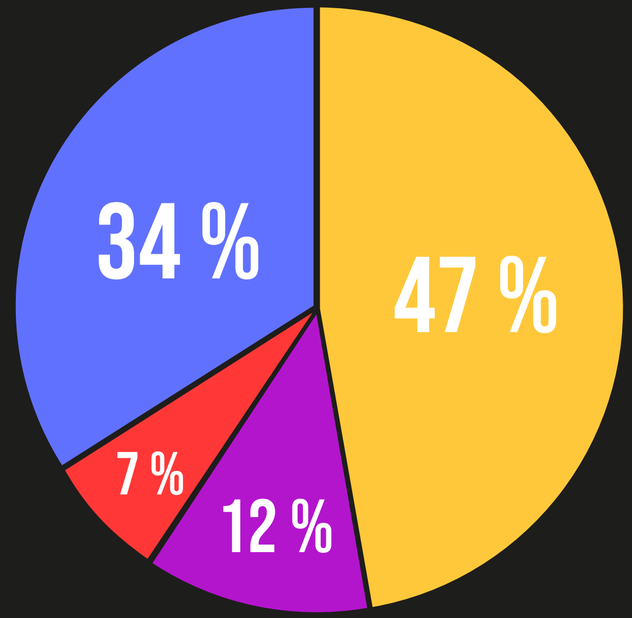
Потенциально опасные ресурсы



Блокируют

Не блокирует

Устаревшие, уязвимые решения



L3 файрволы

На ОС Windows

Устаревшие UTM

Неизвестно

Доля «паразитного трафика»

Анонимайзеры	0.6 %
Порнографические сайты	2.7 %
Знакомства	2.3 %
Компьютерные игры	3.6 %
Мультфильмы	0.8 %
Развлекательные новости	4.6 %
Рекламные сети	8.3 %
Торренты и P2P сети	17 %

* на основе исследования 1500 сетей российских компаний

Использование интернет-канала

Решаем проблемы безопасности за вас

ideco

Защита сразу «из коробки»

Легкая интеграция

Понятные настройки

Техподдержка on-line

Легкая миграция

Быстрое развертывание

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

Контентная фильтрация

Блокировка анонимайзеров

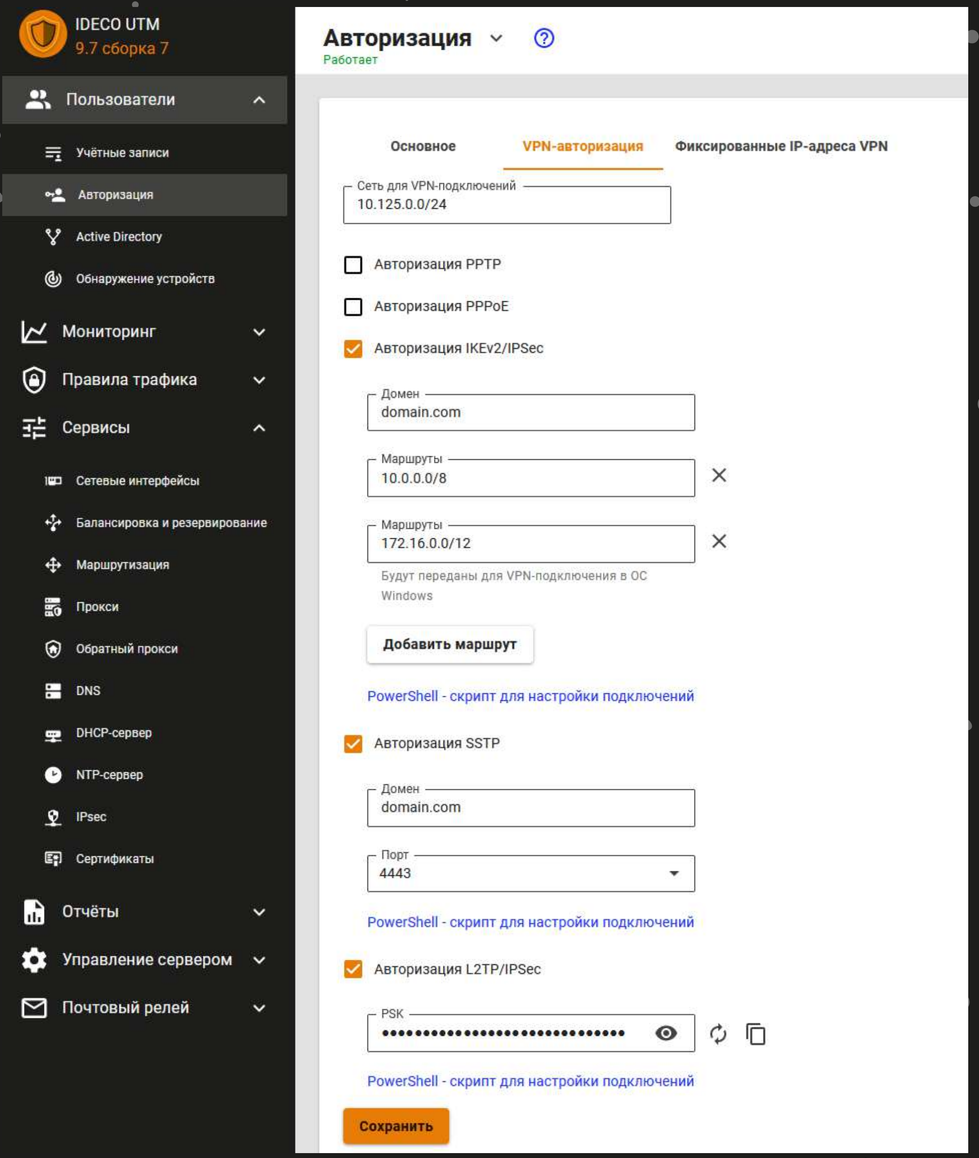
Предотвращение вторжений

Контроль приложений (DPI)

Публикация ресурсов

Антивирусная проверка

«Шай-тек» (shy-tech) «скромные технологии» что это такое?



Преимущества Ideco UTM

ideco

Программное решение

Бесплатное тестирование

Техническая поддержка

Быстрое развитие продукта

Обратная связь без посредников

Гибкая ценовая политика

Сертификат ФСТЭК МЭ А4/Б4, СОВ 4, УД4

сроки получения - сентябрь/октябрь 2021 года

ideco

СПАСИБО ЗА ВНИМАНИЕ

d.homutov@ideco.ru

t.me/idecoutm

ideco.ru