ideco

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.

Экономим ваше время на настройке интернет-шлюза.

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 программного обеспечения 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»,

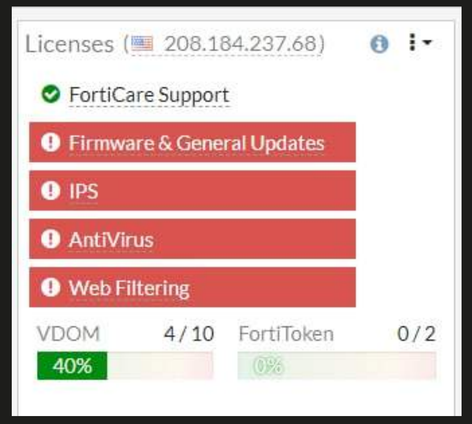
  152-ФЗ «О персональных данных»,

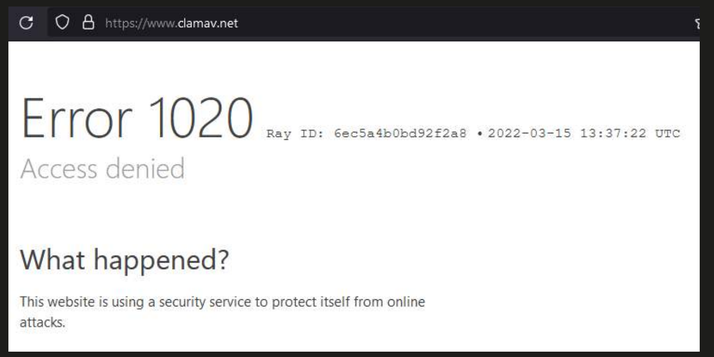
  139-ФЗ и 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

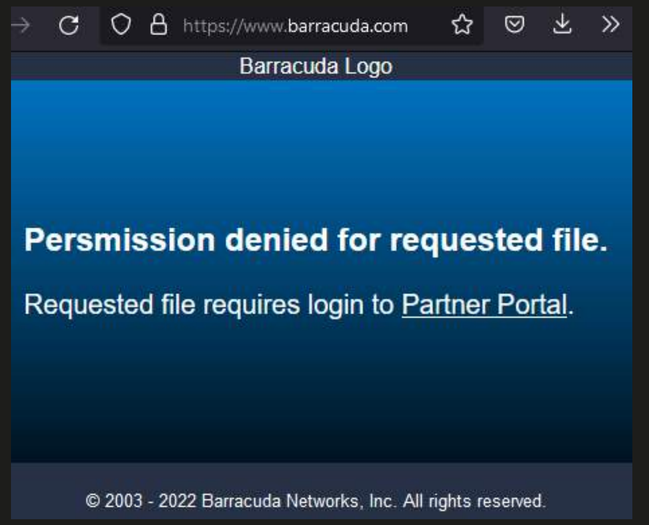
Санкционные риски с иностранными вендорами

ideco

- 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
- Elastic
- ESET
- Forcepoint
- Skybox (Израиль)
- EY
- Fortinet
- Google Cloud
- HPE (+Aruba)
- IBM
- Juniper
- KPMG
- Microsoft
- Mikrotik
- NortonLifeLock
- Oracle
- PWC
- Sectigo
- Panda Security
- Veeam
- VMWare
- Imperva
- MicroFocus (+ ArcSight и Fortify)
- One Identity
- RSA NetWintess
- Symantec
- Supermicro
- Tenable
- Barracuda Networks
- Palo Alto Networks
- GFI (Kerio)
- Lenovo
- Qualys

- 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 18.04.2022

Регуляторные риски

Действие сертификатов ФСТЭК прекращено для вендоров, не оказывающих тех. поддержку.

4222	11.02.2020	Действие сертификата соответствия прекращено 31 марта 2022 г.	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 прекращено 31 марта 2022 г.	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 прекращено 31 марта 2022 г.	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 прекращено 31 марта 2022 г.	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)
4323	10.11.2020	Действие сертификата соответствия прекращено 31 марта 2022 г.	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)

информация из реестра ФСТЭК от 11.04.2022

https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00

Регуляторные риски

Действие сертификата соответствия ФСТЭК приостановлено в 2022 году:

- программно-аппаратный комплекс Коммутатор Huawei серии S5720» (приостановлено 14 февраля 2022 года)

- 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

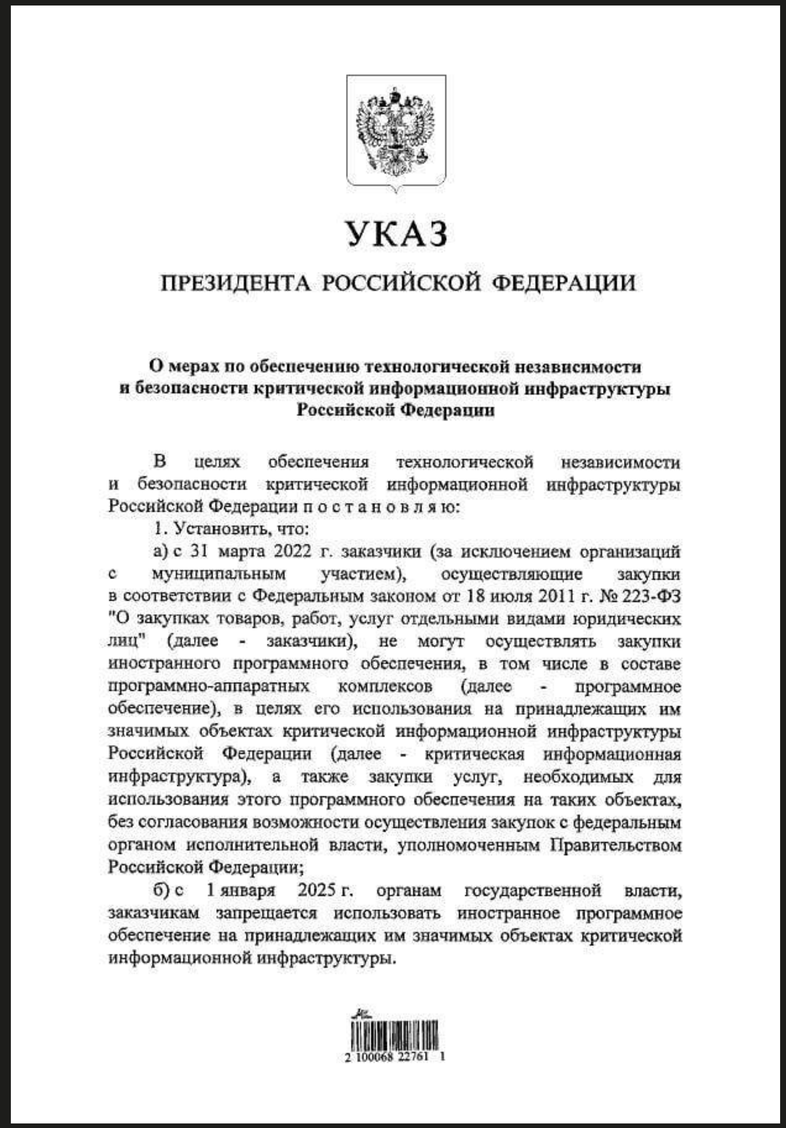
- программное обеспечение «Trend Micro Deep Security 10»

информация из реестра ФСТЭК от 11.04.2022

https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00

Регуляторные риски

- 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.

2 100068 22761 1

Курсовые риски

Пример:

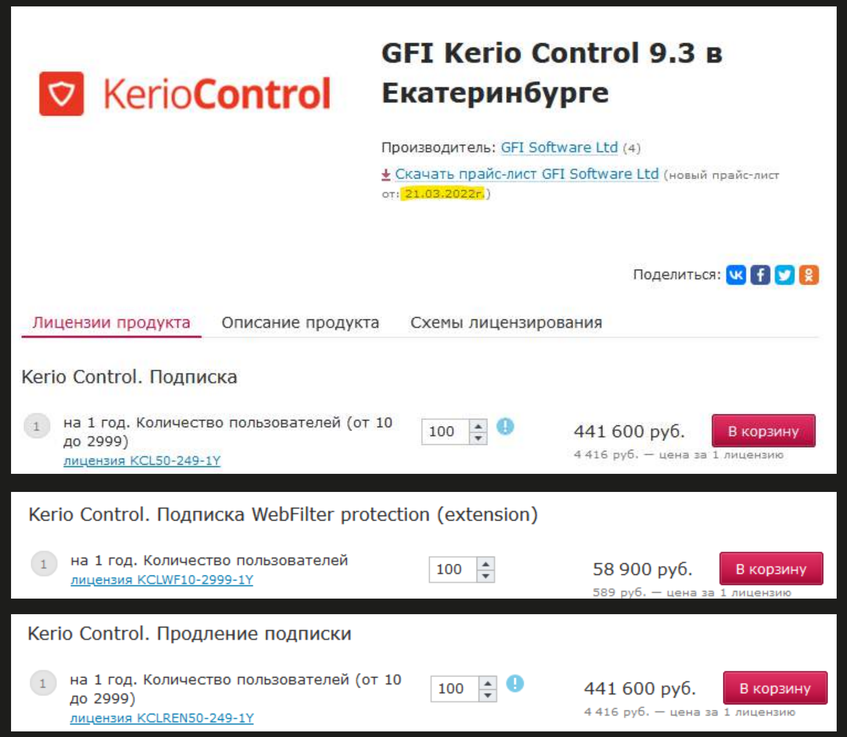
GFI Software — мальтийская компания, производитель средств антивирусной защиты, фильтрации веб-контента. Основана в 1992 году. Имеет представительства в США, Великобритании, Германии, Кипре, Австралии и Мальте. В начале 2017 года приобрела компанию Kerio Technologies Inc.

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:

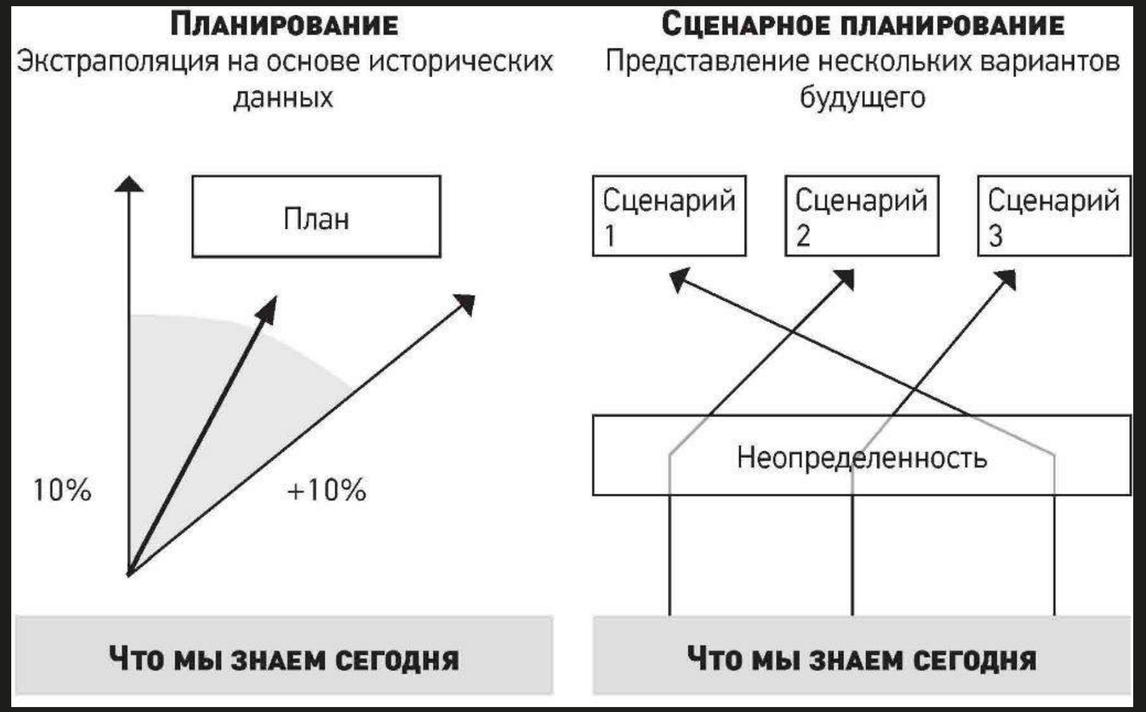
— Новая покупка 135 000 р. (дешевле в 3,7 раза);

— 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?

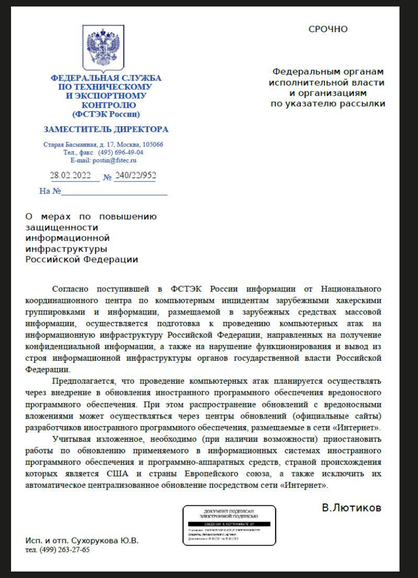


Риски кибаратак

- 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



СРОЧНО

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 №

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

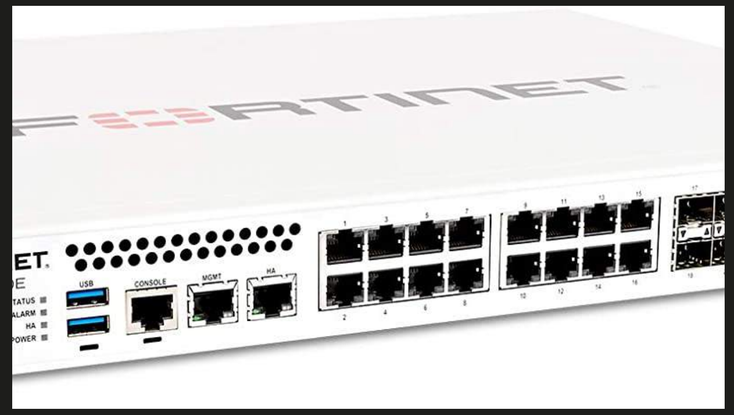
Может ли быть еще страшнее?

- 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.

Импортозамещение: NGFW

ideco

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



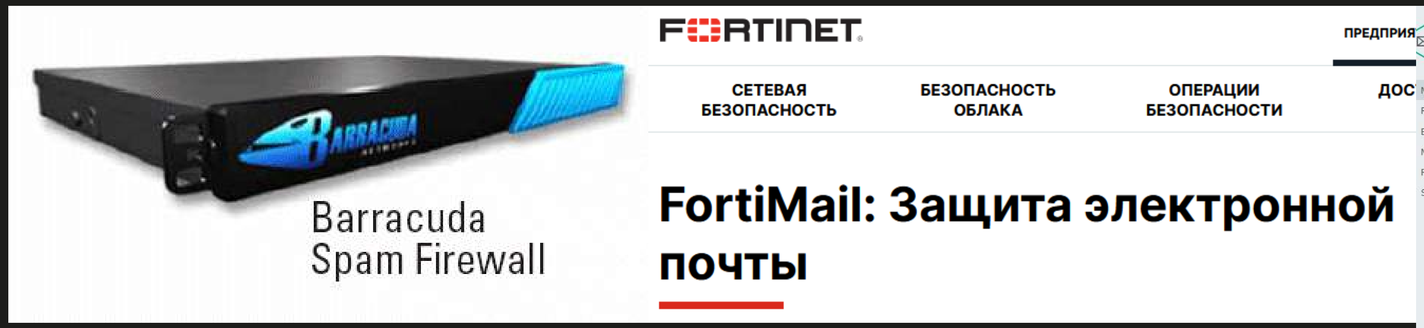
Преимущества Ideco UTM:

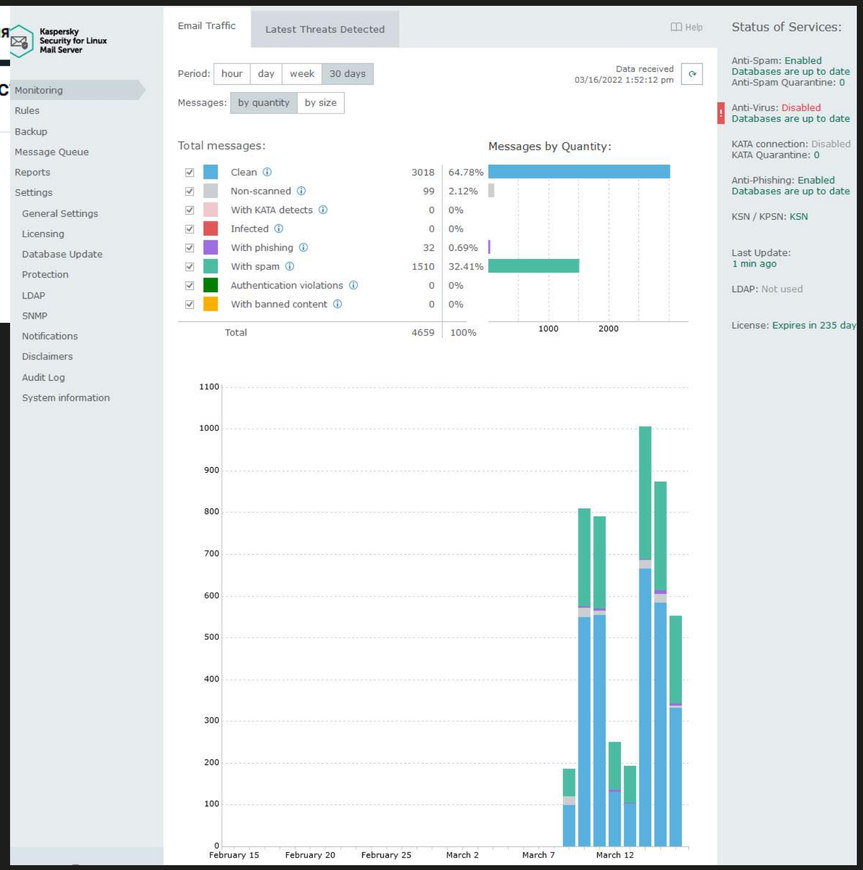
- программное решение, можно использовать свое железо и гипервизоры;
- простой интерфейс и техподдержка онлайн - быстрое внедрение и минимум трудозатрат;
- быстрый ответ на меняющуюся обстановку.

Импортозамещение: защита почты

ideco

Ideco UTM — антиспам и фильтрация почтового трафика заменяет:





Преимущества Ideco UTM & KLMS:

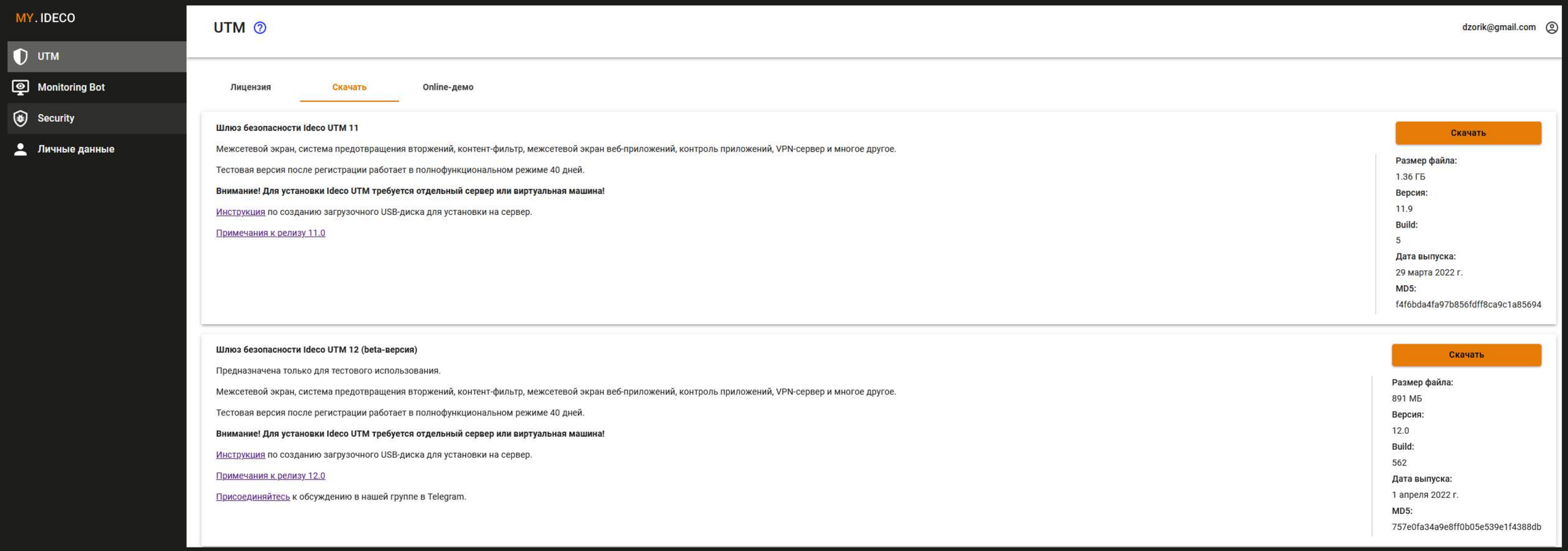
- Мощное решение на основе технологий Касперского.
- Не нужно ставить и поддерживать ОС.
- Веб-интерфейс администрирования.
- Защита от атак по SMTP-протоколу с помощью IPS.
- Отличная ценовая политика.

Минимальные аппаратные требования актуальной версии

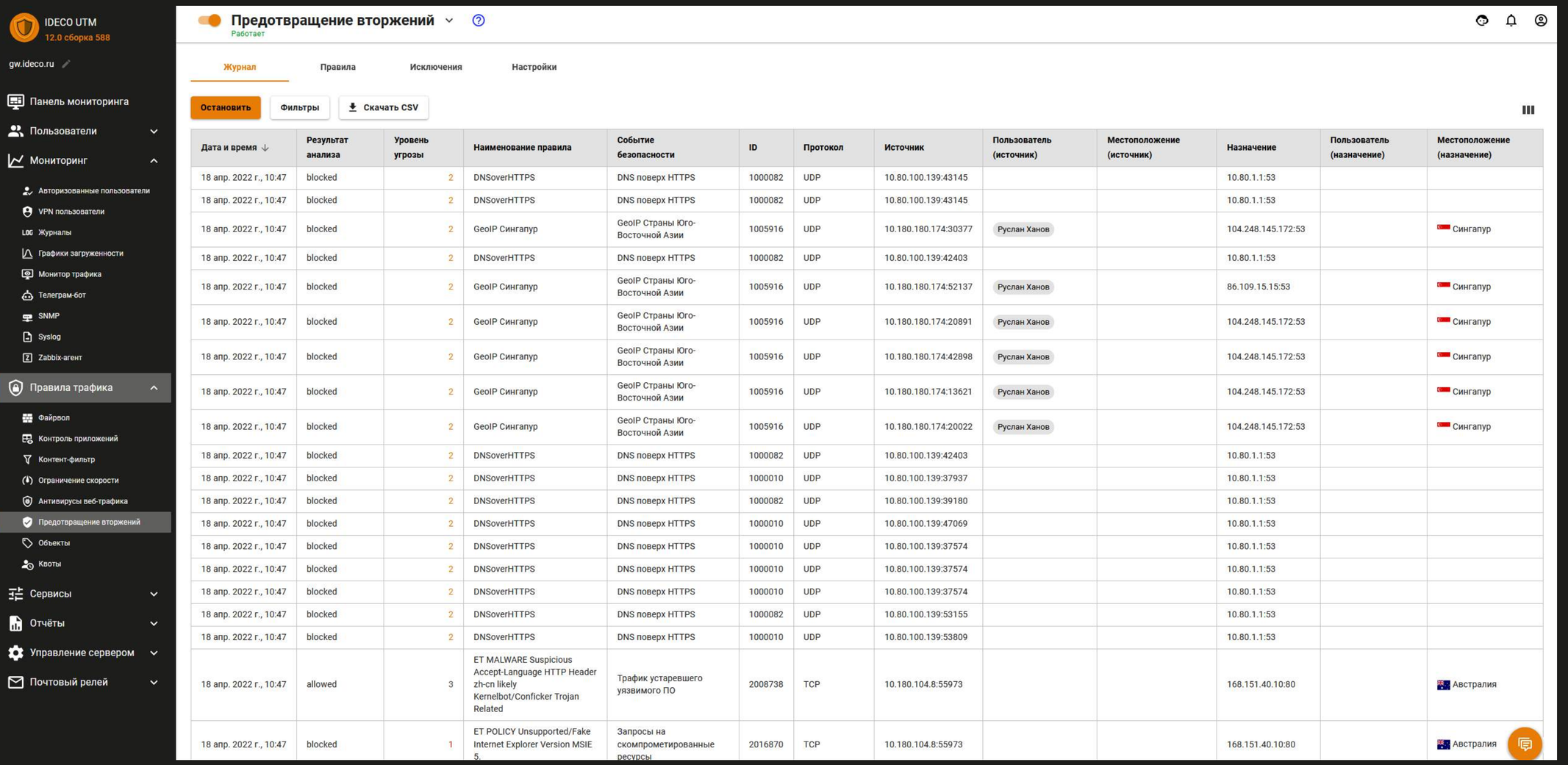
Платформа	Обязательная поддержка UEFI
Процессор*	Intel Pentium G/i3/i5/i7/Xeon E3/Xeon E5 с поддержкой SSE 4.2
Оперативная память*	8 Гб (16 Гб при количестве пользователей более 75)
Накопитель	Жесткий диск или SSD, объемом 64 Гб или больше, с интерфейсом SATA, mSATA, SAS, NVMe или совместимый аппаратный RAID. Дополнительный жесткий диск или SSD при использовании почтового сервера.
Сеть	Две сетевые карты (или два сетевых порта) 100/1000 Mbps. Рекомендуется использовать карты на чипах Intel, Broadcom. Поддерживаются Realtek, D-Link и другие.
Гипервизоры	VMware, Microsoft Hyper-V (2-го поколения), VirtualBox, KVM, Citrix XenServer.
Дополнительно	Монитор и клавиатура
Замечания	Обязательная поддержка UEFI. Не поддерживаются программные RAID-контроллеры (интегрированные в чипсет). Для виртуальных машин необходимо использовать фиксированный, а не динамический размер жесткого диска.

Ideco UTM 12: скачать

https://my.ideco.ru



Ideco UTM 12: защита “из коробки”



Дата и время	Результат анализа	Уровень угрозы	Наименование правила	Событие безопасности	ID	Протокол	Источник	Пользователь (источник)	Местоположение (источник)	Назначение	Пользователь (назначение)	Местоположение (назначение)
18 апр. 2022 г., 10:47	blocked	2	DNSoverHTTPS	DNS поверх HTTPS	1000082	UDP	10.80.100.139:43145			10.80.1.1:53		
18 апр. 2022 г., 10:47	blocked	2	DNSoverHTTPS	DNS поверх HTTPS	1000082	UDP	10.80.100.139:43145			10.80.1.1:53		
18 апр. 2022 г., 10:47	blocked	2	GeoIP Сингапур	GeoIP Страны Юго-Восточной Азии	1005916	UDP	10.180.180.174:30377	Руслан Ханов		104.248.145.172:53		Сингапур
18 апр. 2022 г., 10:47	blocked	2	DNSoverHTTPS	DNS поверх HTTPS	1000082	UDP	10.80.100.139:42403			10.80.1.1:53		
18 апр. 2022 г., 10:47	blocked	2	GeoIP Сингапур	GeoIP Страны Юго-Восточной Азии	1005916	UDP	10.180.180.174:52137	Руслан Ханов		86.109.15.15:53		Сингапур
18 апр. 2022 г., 10:47	blocked	2	GeoIP Сингапур	GeoIP Страны Юго-Восточной Азии	1005916	UDP	10.180.180.174:20891	Руслан Ханов		104.248.145.172:53		Сингапур
18 апр. 2022 г., 10:47	blocked	2	GeoIP Сингапур	GeoIP Страны Юго-Восточной Азии	1005916	UDP	10.180.180.174:42898	Руслан Ханов		104.248.145.172:53		Сингапур
18 апр. 2022 г., 10:47	blocked	2	GeoIP Сингапур	GeoIP Страны Юго-Восточной Азии	1005916	UDP	10.180.180.174:13621	Руслан Ханов		104.248.145.172:53		Сингапур
18 апр. 2022 г., 10:47	blocked	2	GeoIP Сингапур	GeoIP Страны Юго-Восточной Азии	1005916	UDP	10.180.180.174:20022	Руслан Ханов		104.248.145.172:53		Сингапур
18 апр. 2022 г., 10:47	blocked	2	DNSoverHTTPS	DNS поверх HTTPS	1000082	UDP	10.80.100.139:42403			10.80.1.1:53		
18 апр. 2022 г., 10:47	blocked	2	DNSoverHTTPS	DNS поверх HTTPS	1000010	UDP	10.80.100.139:37937			10.80.1.1:53		
18 апр. 2022 г., 10:47	blocked	2	DNSoverHTTPS	DNS поверх HTTPS	1000082	UDP	10.80.100.139:39180			10.80.1.1:53		
18 апр. 2022 г., 10:47	blocked	2	DNSoverHTTPS	DNS поверх HTTPS	1000010	UDP	10.80.100.139:47069			10.80.1.1:53		
18 апр. 2022 г., 10:47	blocked	2	DNSoverHTTPS	DNS поверх HTTPS	1000010	UDP	10.80.100.139:37574			10.80.1.1:53		
18 апр. 2022 г., 10:47	blocked	2	DNSoverHTTPS	DNS поверх HTTPS	1000010	UDP	10.80.100.139:37574			10.80.1.1:53		
18 апр. 2022 г., 10:47	blocked	2	DNSoverHTTPS	DNS поверх HTTPS	1000010	UDP	10.80.100.139:37574			10.80.1.1:53		
18 апр. 2022 г., 10:47	blocked	2	DNSoverHTTPS	DNS поверх HTTPS	1000082	UDP	10.80.100.139:53155			10.80.1.1:53		
18 апр. 2022 г., 10:47	blocked	2	DNSoverHTTPS	DNS поверх HTTPS	1000010	UDP	10.80.100.139:53809			10.80.1.1:53		
18 апр. 2022 г., 10:47	allowed	3	ET MALWARE Suspicious Accept-Language HTTP Header zh-cn likely Kernelbot/Conficker Trojan Related	Трафик устаревшего уязвимого ПО	2008738	TCP	10.180.104.8:55973			168.151.40.10:80		Австралия
18 апр. 2022 г., 10:47	blocked	1	ET POLICY Unsupported/Fake Internet Explorer Version MSIE 5	Запросы на скомпрометированные ресурсы	2016870	TCP	10.180.104.8:55973			168.151.40.10:80		Австралия

Ideco UTM: наши преимущества

- программное решение (гипервизоры, собственные 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

t.me/idecoutm - группа

t.me/ideco - канал

my.ideco.ru - скачать

ideco.ru