ideco

21.09.2022 11:15 МСК

ВЫБОР ОТЕЧЕСТВЕННОГО NGFW

НА ЧТО ОБРАЩАТЬ ВНИМАНИЕ ПРИ МИГРАЦИИ

Дмитрий Хомутов

Директор «Айдеко»

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.

Более 4 000 компаний используют Ideco UTM

Все сервисы и разработка в РФ

Уход зарубежных ИБ-вендоров

- Cisco
- Trend Micro
- Forcepoint
- Fortinet
- Mikrotik
- Barracuda Networks
- Palo Alto Networks
- GFI (Kerio)

Прекращение действия сертификатов

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 13.05.2022

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

Прекращение действия сертификатов

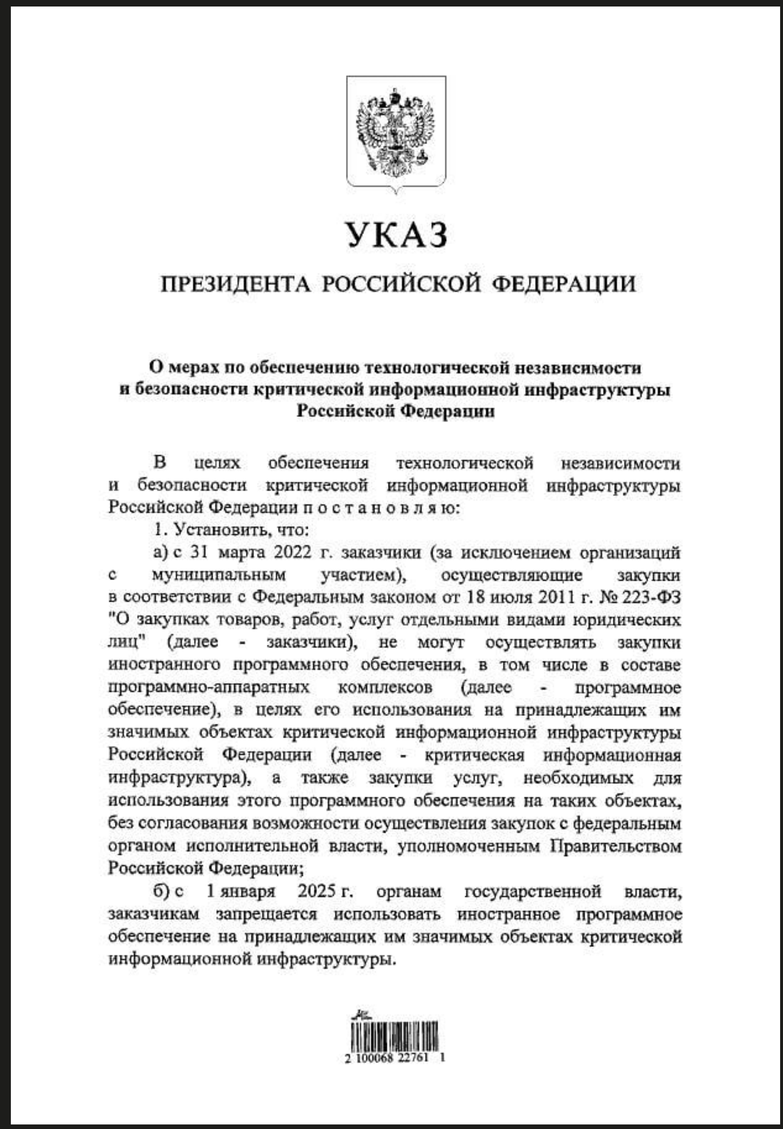
3863	05.11.2019	Действие сертификата соответствия прекращено 14 мая 2022 г.	программно-аппаратный комплекс Коммутатор Huawei серии S5720»	Соответствует требованиям документов: Требования к МЭ, Профиль защиты МЭ(А пятого класса защиты. ИТ.МЭ.А5.ПЗ)	серия
3865	05.11.2019	Действие сертификата соответствия прекращено 14 мая 2022 г.	программно-аппаратный комплекс «Маршрутизатор Huawei серии NE20E»	Соответствует требованиям документов: Требования к МЭ, Профиль защиты МЭ(А пятого класса защиты. ИТ.МЭ.А5.ПЗ)	серия
3909	05.04.2018	05.04.2021	межсетевой экран Huawei Eudemon (модель Eudemon 8000E-X3) версии V500	Соответствует требованиям документов: 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)	серия
3910	06.11.2019	Действие сертификата соответствия прекращено 14 мая 2022 г.	программно-аппаратный комплекс «Коммутатор Huawei серии S12700»	Соответствует требованиям документов: Требования к МЭ, Профиль защиты МЭ(А пятого класса защиты. ИТ.МЭ.А5.ПЗ)	серия
3935	10.05.2018	10.05.2021	маршрутизаторы серии Huawei AR (модели: AR2220E, AR2240, AR161FG-L) версии V200	Соответствует требованиям документов: 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)	серия
3941	06.11.2019	Действие сертификата соответствия прекращено 14 мая 2022 г.	программно-аппаратные комплексы «Маршрутизаторы Huawei серии AR3200, серии AR2200, серии AR1200»	Соответствует требованиям документов: Требования к МЭ, Профиль защиты МЭ(А пятого класса защиты. ИТ.МЭ.А5.ПЗ)	серия
3966	08.11.2019	Действие сертификата соответствия приостановлено 14 февраля 2022 г.	программное обеспечение «Программный комплекс «Huawei Fusion Access» версии 6.X»	Соответствует требованиям документов: ТУ	серия
4023	05.10.2018	05.10.2023	программный комплекс Huawei FusionSphere 6.x	Соответствует требованиям документов: ТУ	серия
4083	04.02.2019	Действие сертификата соответствия приостановлено 14 февраля 2022 г.	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	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)	серия

в 2022 году приостановлено или прекращено действие 56 сертификатов ФСТЭК

Запрет закупки и использования для КИИ

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;

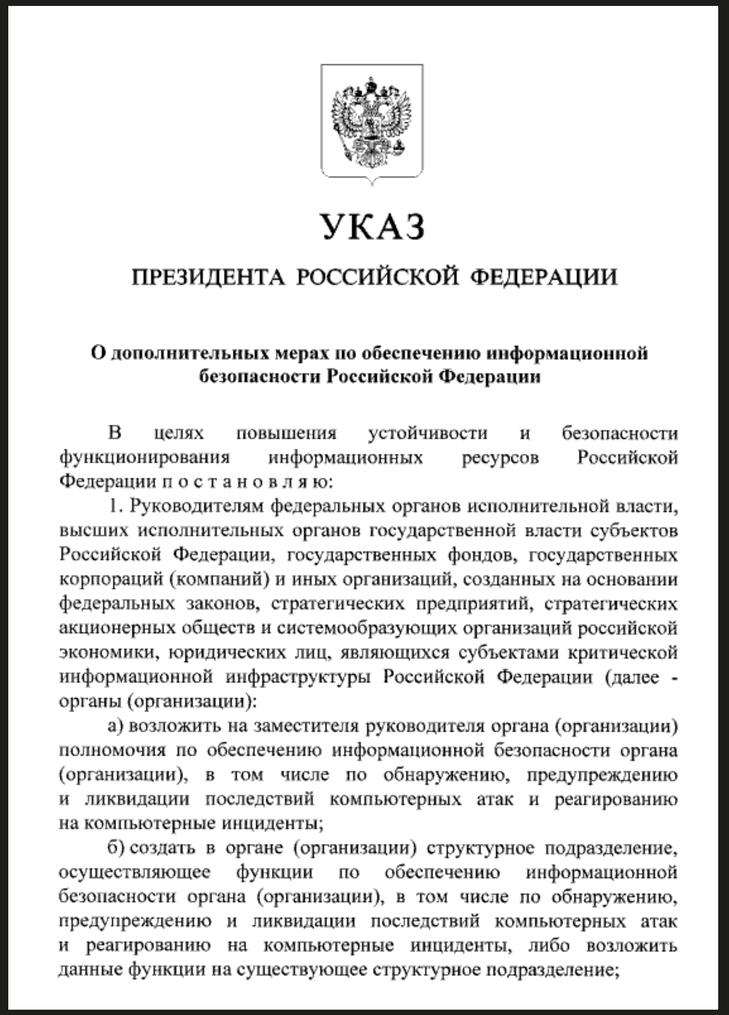
б) с 1 января 2025 г. органам государственной власти, заказчикам запрещается использовать иностранное программное обеспечение на принадлежащих им значимых объектах критической информационной инфраструктуры.

2 100068 22761 1

Запрет использования ПО из недружественных стран

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;

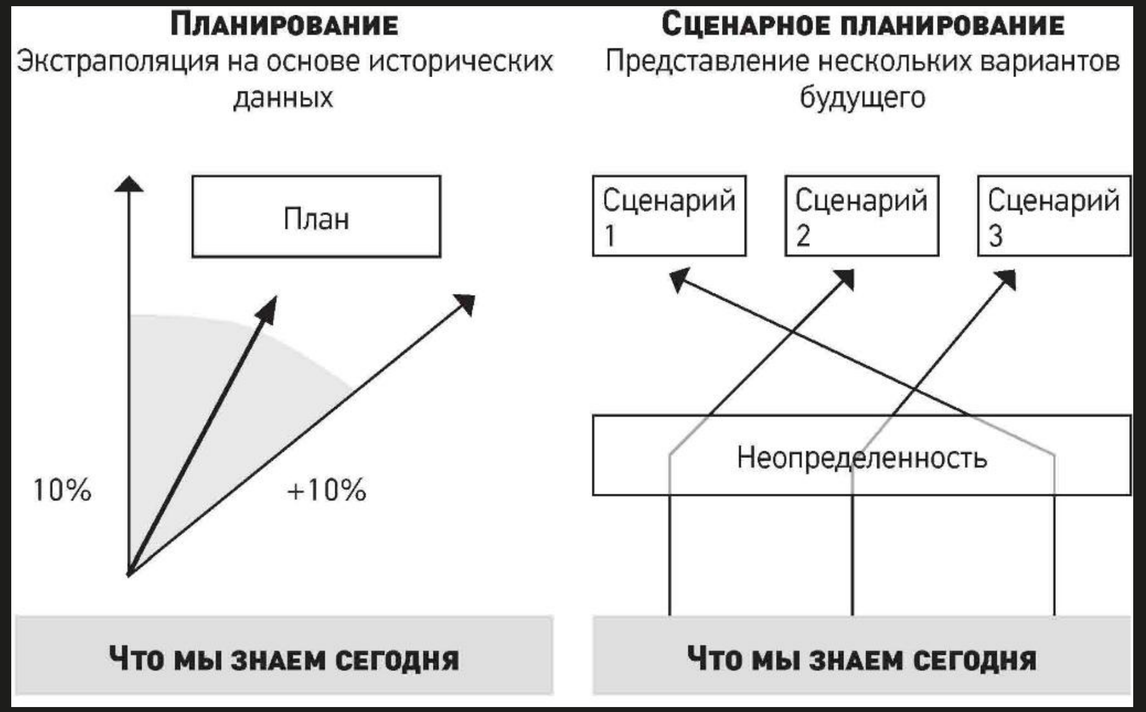
Риски ухода других вендоров

- 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).

Риски планирования

Планируем бюджет на IV квартал 2023 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?



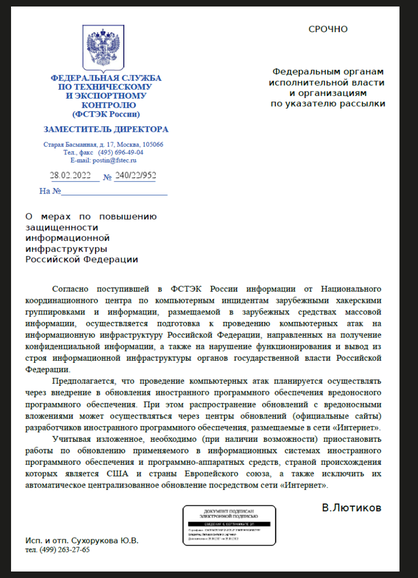
Риски кибаратак

- 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

14 АПР, 18:31 Обновлено 19:37

ЦБ: число крупных кибератак на финорганизации России с конца февраля выросло в 22 раза



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

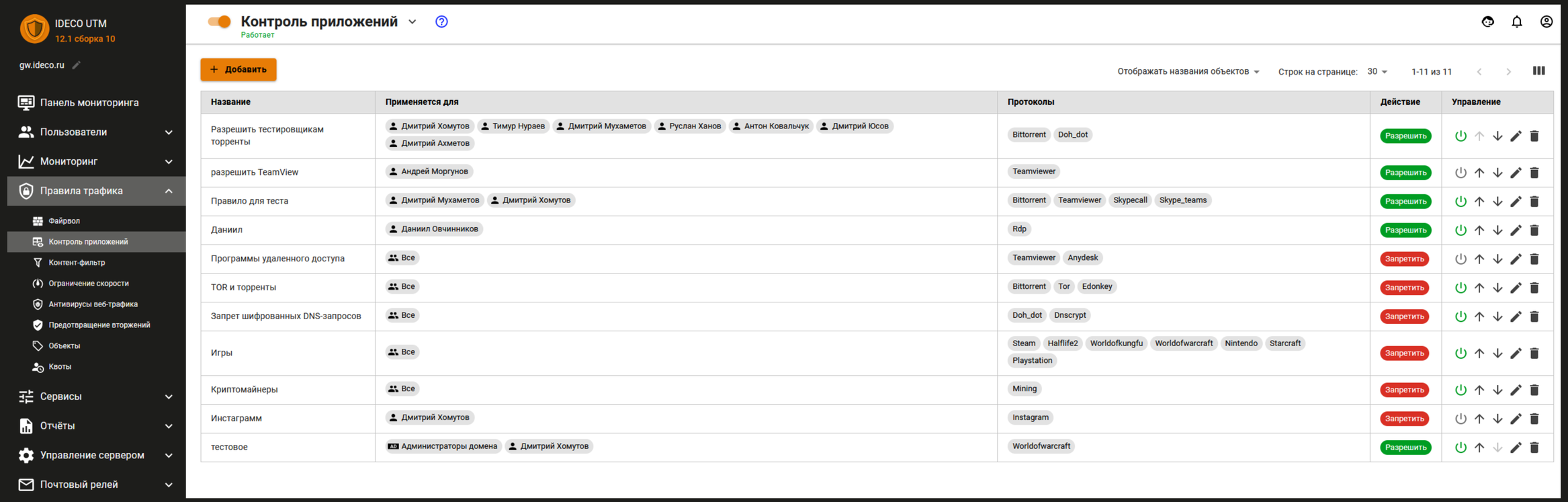
Фантастические (пока) риски

- 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.

Как выбрать замену файрвола?

функциональность NGFW

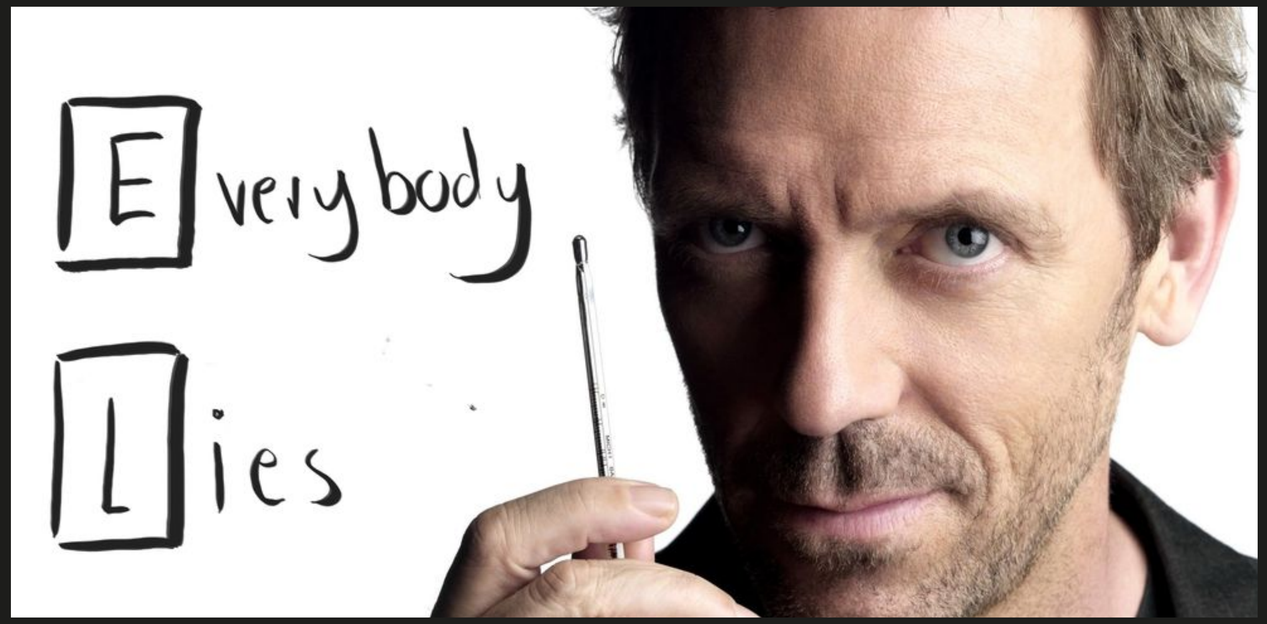
- более 20 модулей фильтрации: FW, CF, AC, IPS, VPN, маршрутизация и др.;
- правила по пользователям, а не IP-адресам;
- сертификация ФСТЭК;
- соответствие требованиям регуляторов (ФСТЭК, ФСБ (НКЦКИ)).



Производительность NGFW

куда смотреть

ideco



Производительность

куда смотреть

ideco

FortiGate® Network Security Platform - *Top Selling Models Matrix

	FG-3960E	FG-3980E	FG-4200F	FG-4400F
Firewall Throughput (1518/512/64 byte UDP)	620 / 610 / 370 Gbps	1.05 Tbps / 1.05 Tbps / 680 Gbps	800 / 788 / 400 Gbps	1.15 / 1.14 / 0.50 Tbps
IPsec VPN Throughput (512 byte) [1]	280 Gbps	400 Gbps	210 Gbps	310 Gbps
IPS Throughput (Enterprise Mix) [2]	30 Gbps	32 Gbps	52 Gbps	94 Gbps
NGFW Throughput (Enterprise Mix) [2, 4]	22 Gbps	28 Gbps	47 Gbps	82 Gbps
Threat Protection Throughput (Ent. Mix) [2, 5]	13.5 Gbps	20 Gbps	45 Gbps [6]	75 Gbps [6]
Firewall Latency	3 µs	3 µs	3.02 µs	2.98 µs
Concurrent Sessions	160 Million	160 Million	210 Million / 450 Million [7]	210 Million / 700 Million [7]
New Sessions/Sec	720,000	800,000	1 Million / 7 Million [7]	1 Million / 10 Million [7]
Firewall Policies	200,000	200,000	200,000	200,000
Max G/W to G/W IPSEC Tunnels	40,000	40,000	40,000	40,000
Max Client to G/W IPSEC Tunnels	200,000	200,000	200,000	200,000
SSL VPN Throughput	9 Gbps	9.5 Gbps	16 Gbps	16 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	30,000	30,000	30,000	30,000
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	23 Gbps	26 Gbps	50 Gbps	86 Gbps
Application Control Throughput (HTTP 64K) [2]	40 Gbps	55 Gbps	135 Gbps	140 Gbps

Производительность

Enterprise mix (EMIX)

Basic Information

Name: Fortinet EMIX

Description: Default. Traffic modeled after Fortinet's Enterprise mix (EMIX).

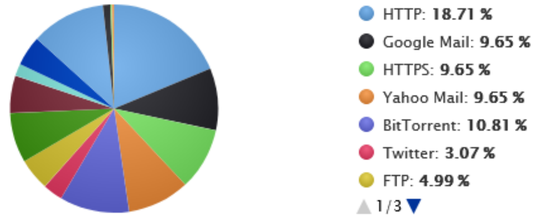
Applications

Weight According To:

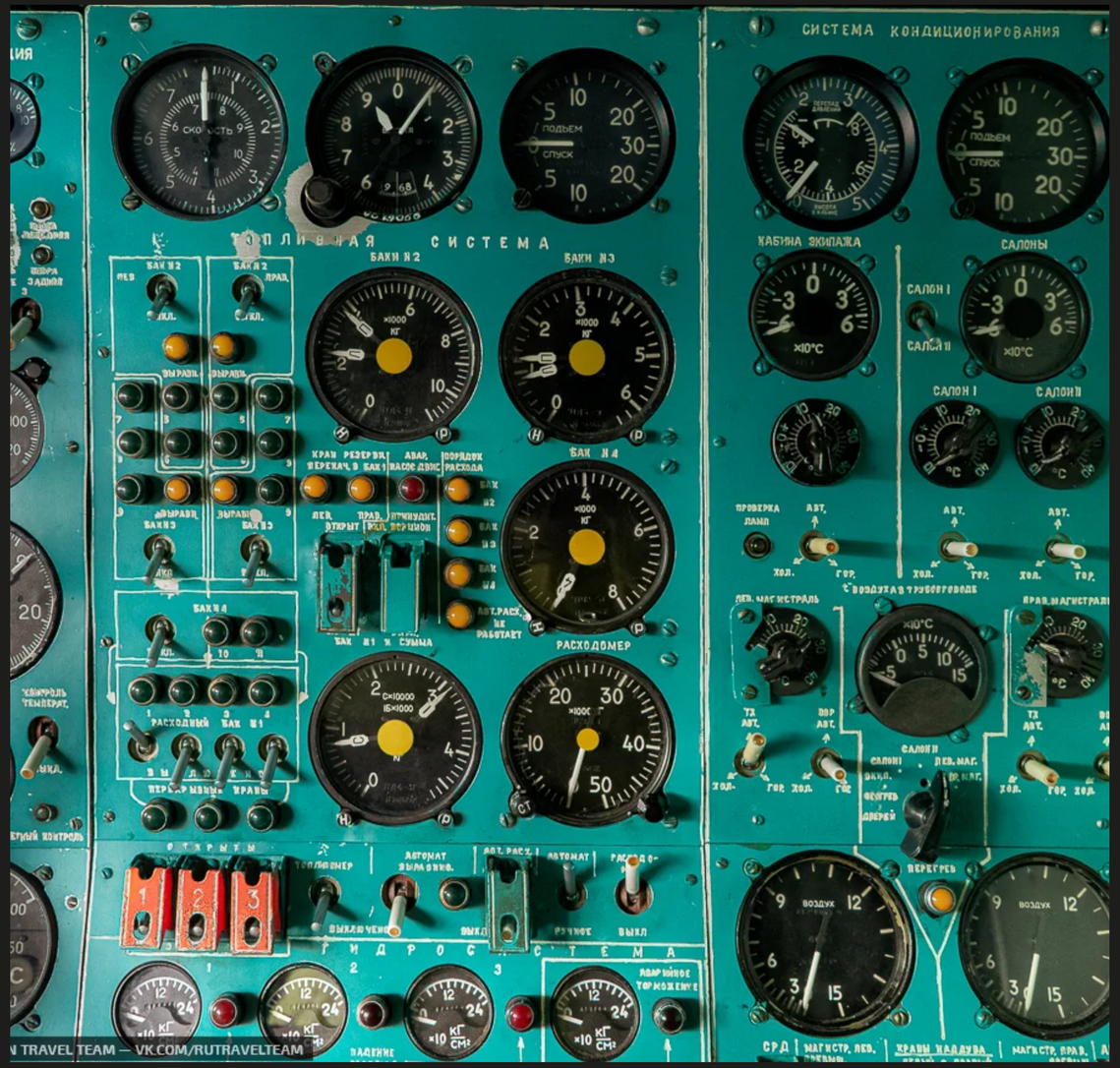
(•) Bandwidth ( ) Flows

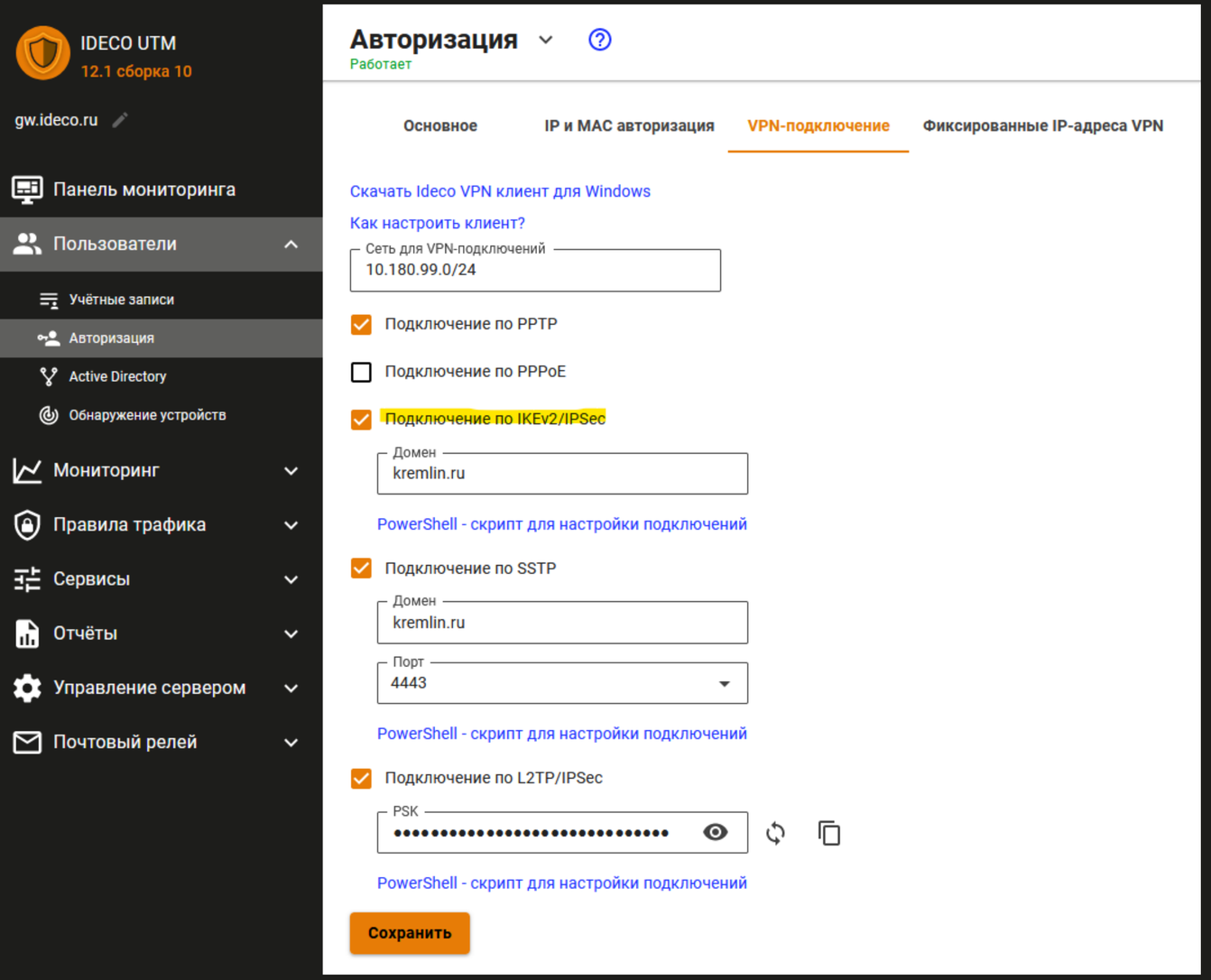
* Weight field is editable, please click the text to edit it.

Name	Weight	Sessions	% Bandwidth	% Flows	# Bytes	Detail
HTTP	225	1	18.71	4.03	138,984	
Google Mail	116	1	9.65	13.59	21,260	
HTTPS	116	1	9.65	2.03	142,292	
Yahoo Mail	116	1	9.65	22.19	13,020	
BitTorrent	130	1	10.81	2.29	141,065	
Twitter	37	1	3.07	2.49	37,009	
FTP	60	2	4.99	2.64	56,591	
AmazonS3	93	1	7.73	1.93	119,741	
Facebook	70	1	5.82	0.82	210,120	
SMTP	23	1	1.91	17.45	3,283	
Google Talk	56	1	4.65	5.08	27,415	
YouTube	139	1	11.56	0.74	466,873	
AOL Chat	14	1	1.16	22.05	1,581	
SSH	3	1	0.24	1.61	4,636	
Oracle DB	4	1	0.33	1	9,946	



UX/UI

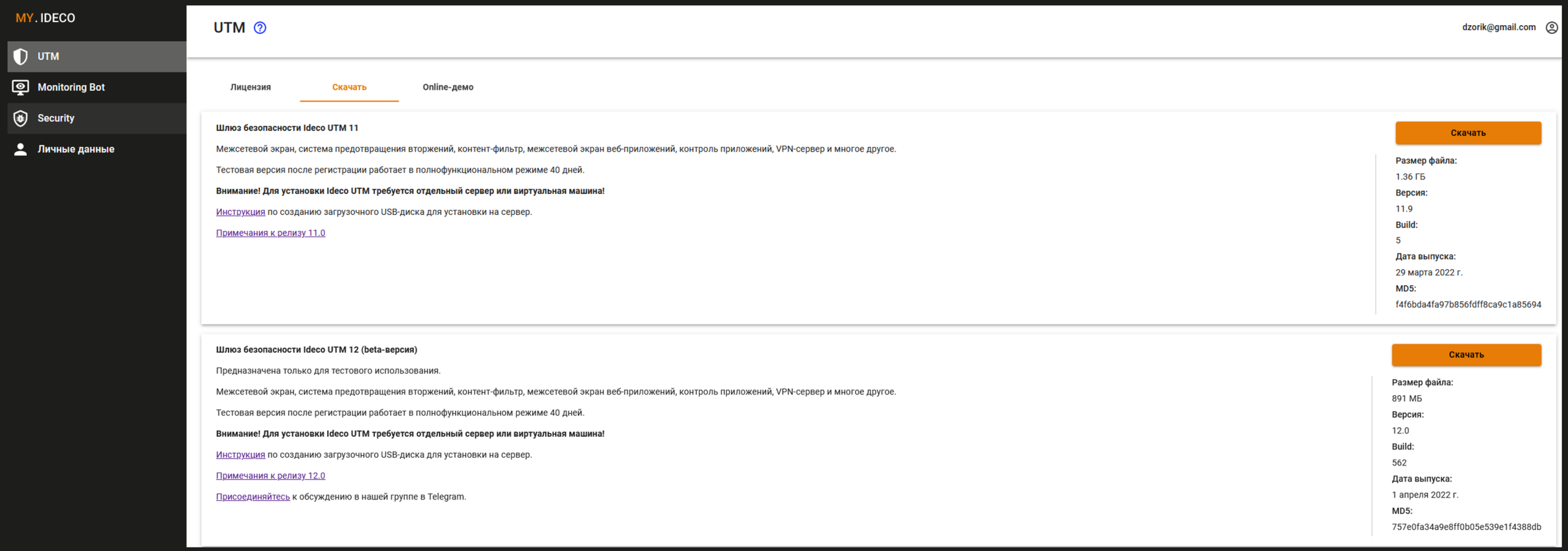

СИСТЕМА КОНДИЦИОНИРОВАНИЯ
ТОПЛИВНАЯ СИСТЕМА
КАБИНА ЭКИПАЖА
САЛОНЫ
ГИДРОСИСТЕМА
TRAVEL TEAM — VK.COM/RUTRAVELTEAM


IDECO UTM
12.1 сборка 10
gw.ideco.ru
Панель мониторинга
Пользователи
Учётные записи
Авторизация
Active Directory
Обнаружение устройств
Мониторинг
Правила трафика
Сервисы
Отчёты
Управление сервером
Почтовый релей
Авторизация
Работает
Основное
IP и MAC авторизация
VPN-подключение
Фиксированные IP-адреса VPN
Скачать Ideco VPN клиент для Windows
Как настроить клиент?
Сеть для VPN-подключений
10.180.99.0/24
Подключение по PPTP
Подключение по PPPoE
Подключение по IKEv2/IPSec
Домен
kremlin.ru
PowerShell - скрипт для настройки подключений
Подключение по SSTP
Домен
kremlin.ru
Порт
4443
PowerShell - скрипт для настройки подключений
Подключение по L2TP/IPSec
PSK
PowerShell - скрипт для настройки подключений
Сохранить

Лучше один раз увидеть

ideco

https://my.ideco.ru



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».

Ideco UTM 13: защита “из коробки”

Преимущества Ideco UTM

ideco

Защита сразу «из коробки»

Готовность к ответу на вызовы 2022

«Шай-тек» (shy-tech) «скромные технологии»

Сервис поддержки on-line

Простой UI/UX

Постоянное развитие

Интересный факт: среднее время ответа технической поддержки в чат - 27 секунд.

ideco

ПОПРОБУЙТЕ САМИ

t.me/idecoutm - группа

my.ideco.ru - скачать

ideco.ru