ideco

ВЫБОР РОССИЙСКОГО NGFW
НА ЧТО ОБРАЩАТЬ ВНИМАНИЕ ПРИ МИГРАЦИИ

Александр Карманов

Presale-инженер «Айдеко»

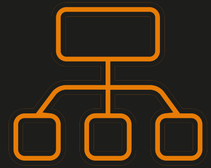
Айдеко

Помогаем клиентам защититься от современных угроз безопасности, средствами удобного межсетевого экрана Ideco UTM.

Экономим ваше время на настройке интернет-шлюза и отражения кибератак.

Более 3 000 компаний
используют Ideco UTM

140 человек в команде
S&M / R&D



Лидер по скорости
разработки в отрасли

* сертификат ФСТЭК А4/Б4, СОВ 4, УД 4, в реестре Минцифры

Ideco UTM

Фильтрация трафика L7
МЭ, СОВ, Контроль приложений,
Контент-фильтр

Сетевые службы
DNS, DHCP, NTP, балансировка и
резервирование канала, квоты,
шейпер трафика

Маршрутизация
Статическая
Динамическая OSPF, BGP

Управление
Веб-интерфейс, ssh,
центральная консоль

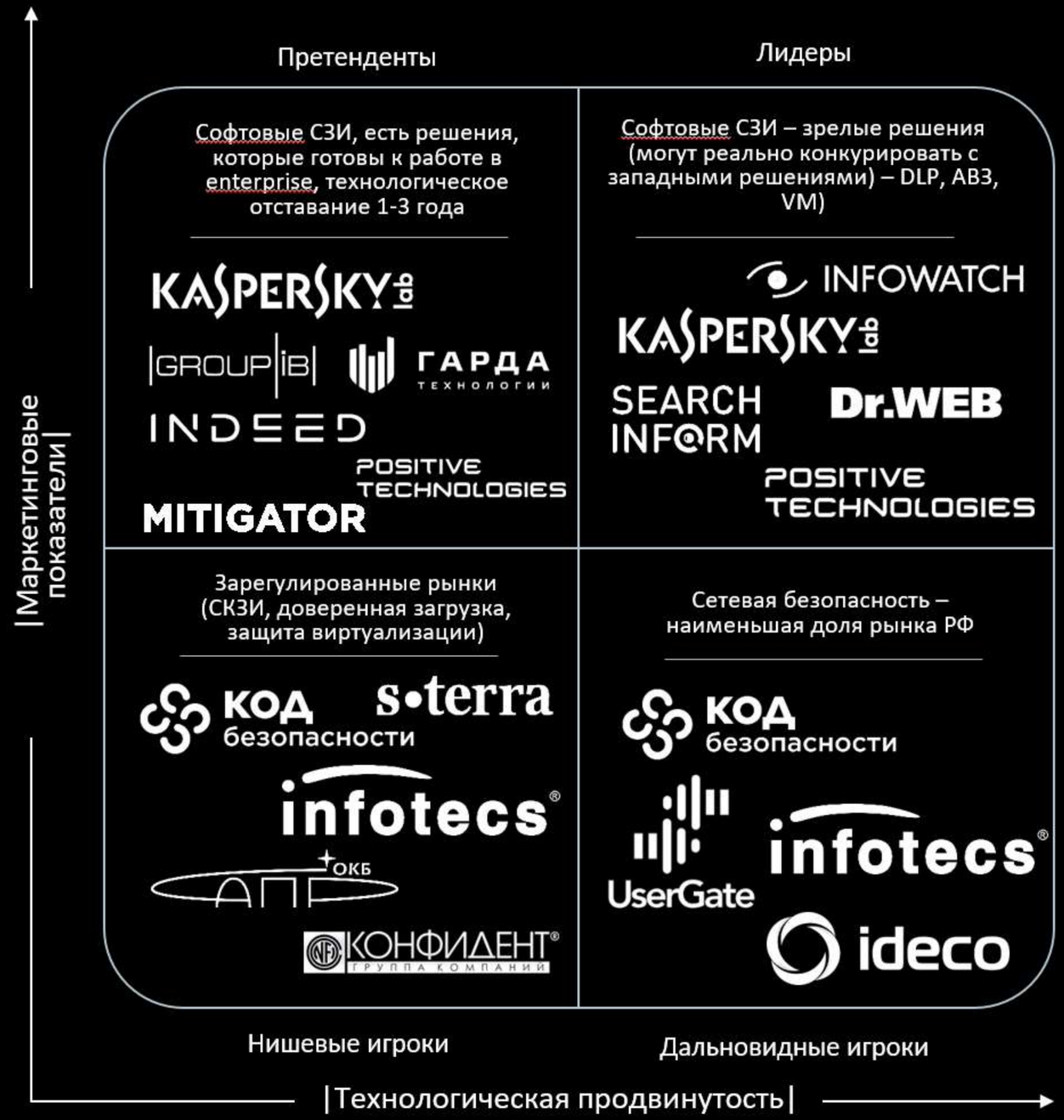
Мониторинг и отчетность
Телеграм бот, Zabbix Агент,
Syslog, SNMP, SIEM
Отчетность по пользователям

Пользователи
- Интеграция с LDAP
- Локальная база пользователей
- Авторизация (IP, MAC, Kerberos, Web, Агент, подсеть)
- Пользователи и группы как объекты в политиках фильтрации

Отказоустойчивость:
- Кластеризация Active/Passive
- Резервное копирование
- Программный Watchdog

VPN
- Site-To-Site Ipsec
- IKEv2
- SSTP
- Wireguard (клиент)
- L2TP/IPSec

ideco



IBS Platformix

Структура рынка. Гартнер по-русски

Сетевая безопасность

Наиболее проблемный, но в то же время наиболее востребованный сегмент СЗИ

Решение с «отсутствием» аналогов

NAC, безопасный Wi-Fi, MDM, безопасность в облаках, но есть рынки Латинской Америки, Индии, Китая

Главный тренд - резкое повышение спроса на ресурсы и компетенции интеграторов

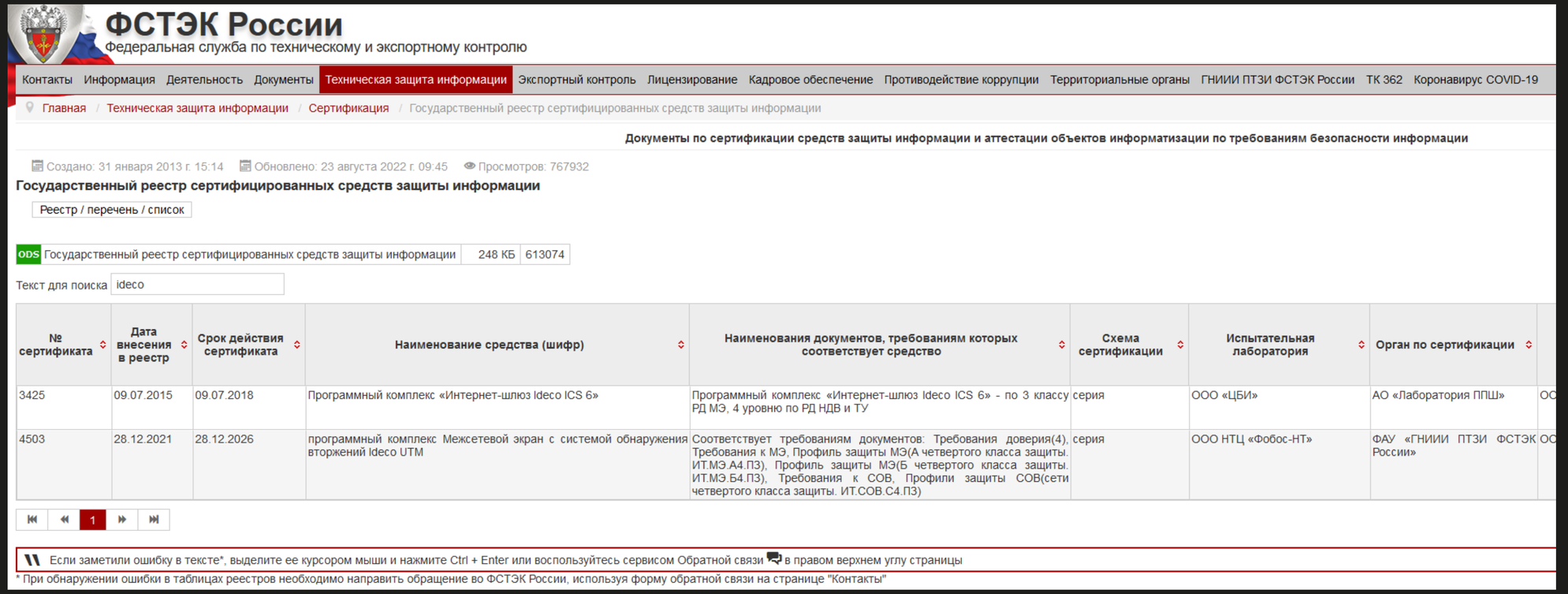
Критерии выбора NGFW

16 критериев выбора отечественных межсетевых экранов.

Все, что есть в Ideco UTM.

синяя или оранжевая таблетка?

1. Комплаенс



ФСТЭК России
Федеральная служба по техническому и экспортному контролю

Контакты | Информация | Деятельность | Документы | Техническая защита информации | Экспортный контроль | Лицензирование | Кадровое обеспечение | Противодействие коррупции | Территориальные органы | ГНИИИ ПТЗИ ФСТЭК России | ТК 362 | Коронавирус COVID-19

Главная / Техническая защита информации / Сертификация / Государственный реестр сертифицированных средств защиты информации

Документы по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации

Создано: 31 января 2013 г. 15:14 Обновлено: 23 августа 2022 г. 09:45 Просмотров: 767932

Государственный реестр сертифицированных средств защиты информации

Реестр / перечень / список

ODS Государственный реестр сертифицированных средств защиты информации 248 КБ 613074

Текст для поиска ideco

№ сертификата	Дата внесения в реестр	Срок действия сертификата	Наименование средства (шифр)	Наименования документов, требованиям которых соответствует средство	Схема сертификации	Испытательная лаборатория	Орган по сертификации	
3425	09.07.2015	09.07.2018	Программный комплекс «Интернет-шлюз Ideco ICS 6»	Программный комплекс «Интернет-шлюз Ideco ICS 6» - по 3 классу РД МЭ, 4 уровню по РД НДВ и ТУ	серия	ООО «ЦБИ»	АО «Лаборатория ППШ»	ОС
4503	28.12.2021	28.12.2026	программный комплекс Межсетевой экран с системой обнаружения вторжений Ideco UTM	Соответствует требованиям документов: Требования доверия(4), 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)	серия	ООО НТЦ «Фобос-НТ»	ФАУ «ГНИИИ ПТЗИ ФСТЭК России»	ОС

1

Если заметили ошибку в тексте*, выделите ее курсором мыши и нажмите Ctrl + Enter или воспользуйтесь сервисом Обратной связи в правом верхнем углу страницы

* При обнаружении ошибки в таблицах реестров необходимо направить обращение во ФСТЭК России, используя форму обратной связи на странице "Контакты"

- продукты из реестра соотвествуют формальным требованиям к МЭ
- в компании внедрена безопасная разработка (SDL)
- уровень зрелости компании и продукта.

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:

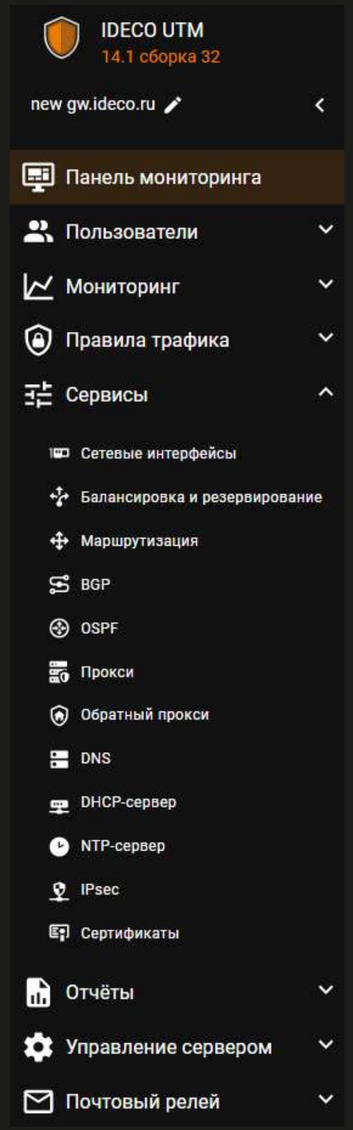
  187-ФЗ «О безопасности КИИ РФ»

  152-ФЗ «О персональных данных»

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

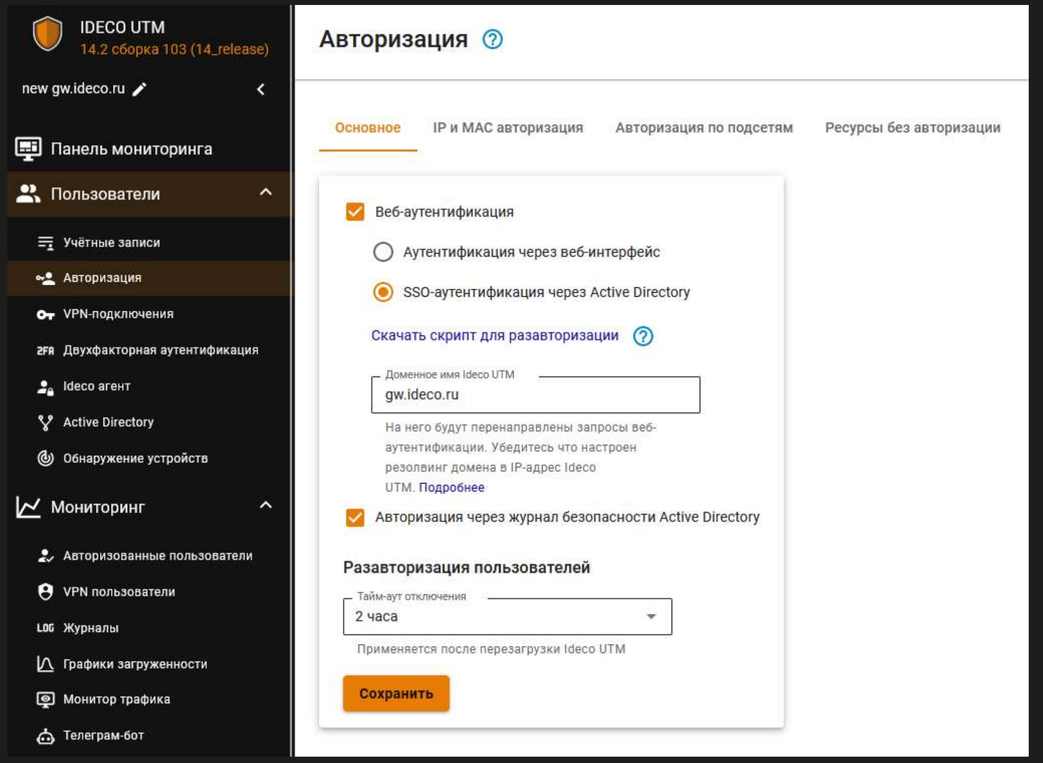
2. Сетевая и общая функциональность

- маршрутизация трафика (статическая, OSPF, BGP)
- сетевые сервисы (DNS, DDNS, NTP, DHCP, публикация ресурсов)
- балансировка, резервирование и агрегирование (LACP) каналов
- кластеризация
- централизованное управление.



3. Аутентификация пользователей

- интеграция с Microsoft Active Directory (несколькими доменами, Kerberos/NTLM, аутентификация по логам безопасности)
- интеграция с ALD PRO (июнь 2023)
- веб-авторизация
- IP, IP+MAC для аутентификации устройств
- авторизация подсетей (SIP-телефонов, камеры, Wi-Fi сети)
- автоматическая авторизация устройств и создание пользователей
- VPN: PPTP, PPPoE, IKEv2/IPSec, L2TP/IPSec, SSTP
- двухфакторная аутентификация (звонок, SMS, OTP-токен).



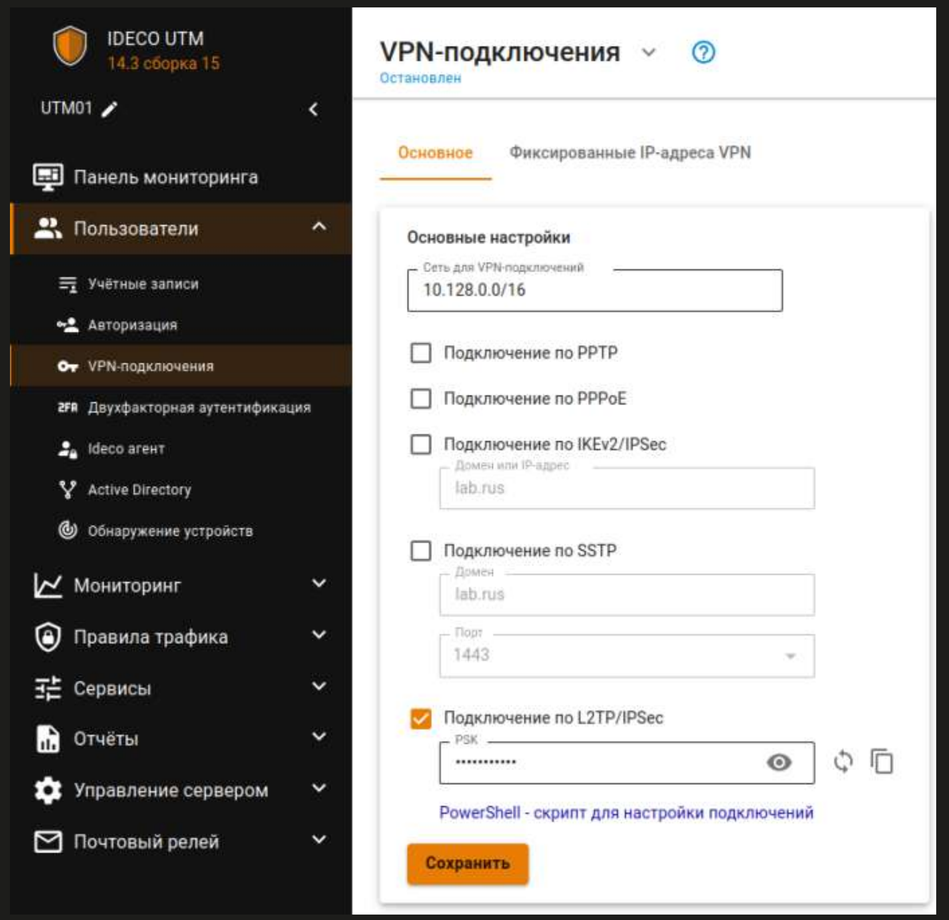
4. VPN-сервер

client-to-site

- IKEv2/IPSec
- L2TP/IPSec
- SSTP (SSL-VPN)
- Ideco agent (Wireguard).

site-to-site

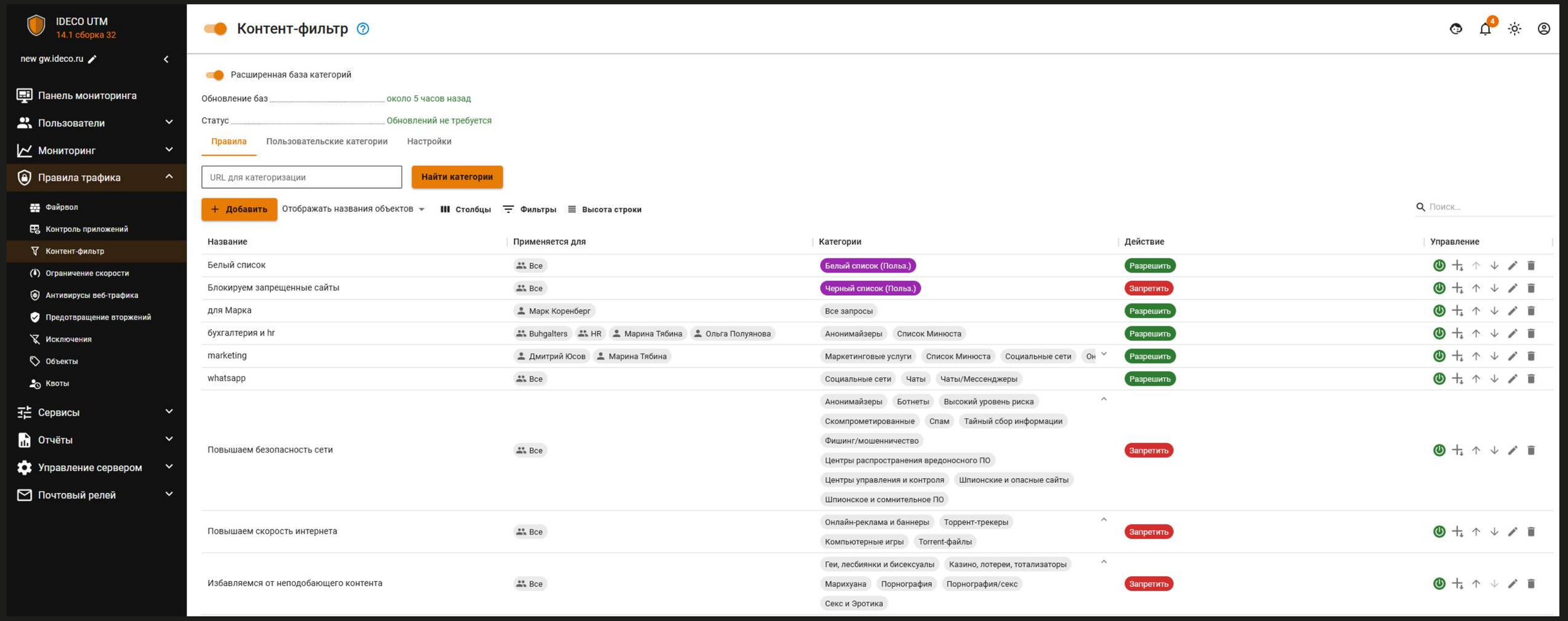
- IKEv2/IPSec.



5. Фильтрация трафика

функциональность NGFW/UTM

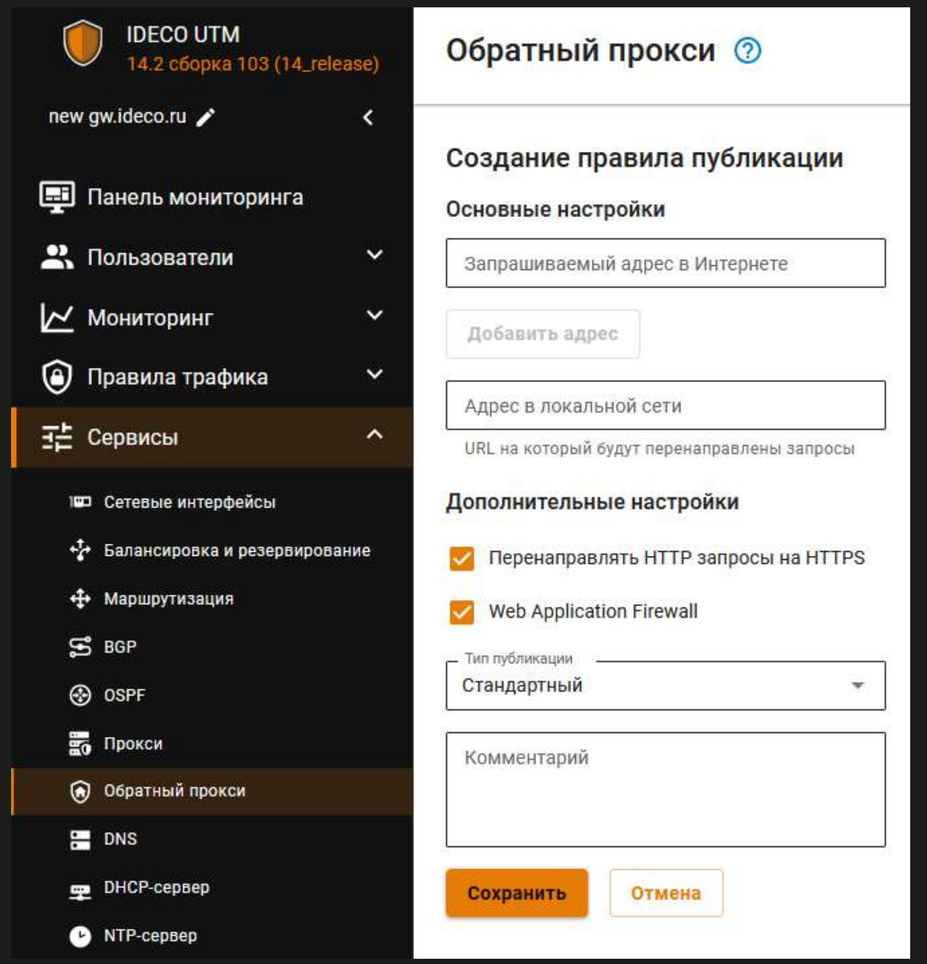
- модули анализа трафика до L7: FW, CF, AC, IPS, AV
- правила по пользователям и группам, а не IP-адресам.



6. Публикация ресурсов

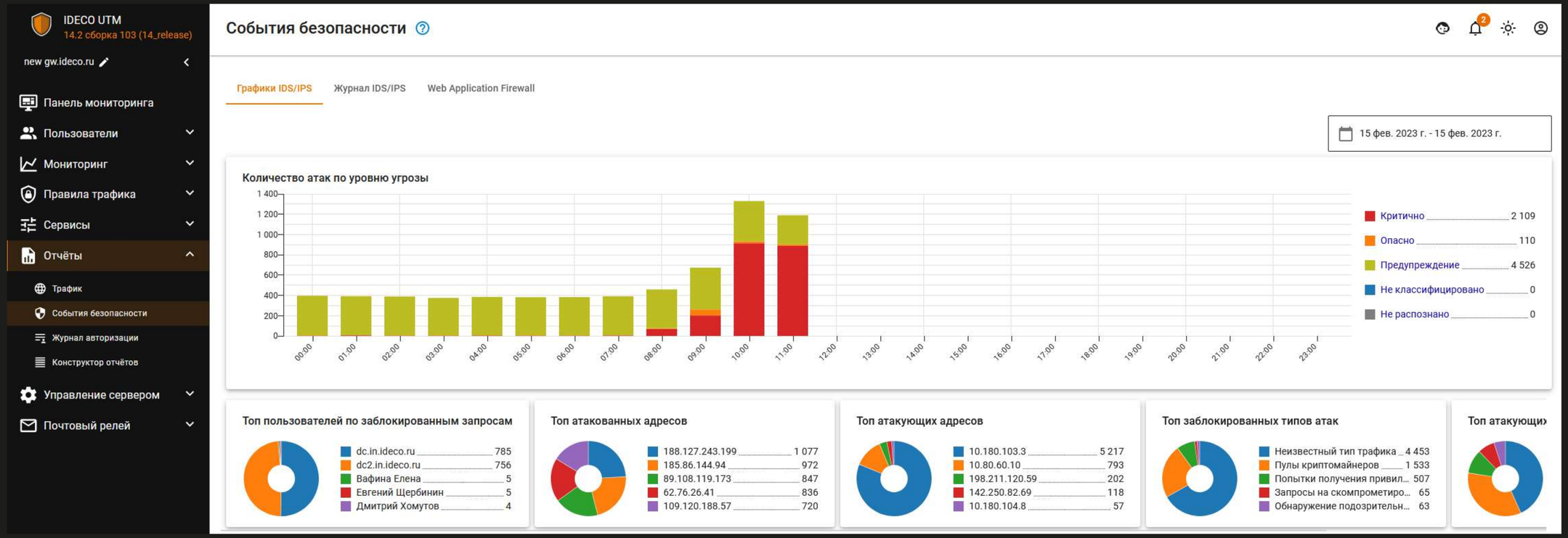
безопасная публикация

- обратный прокси-сервер с WAF для публикации веб-ресурсов
- почтовый релей для публикации почтового сервера
- защита опубликованных терминальных серверов (RDP).

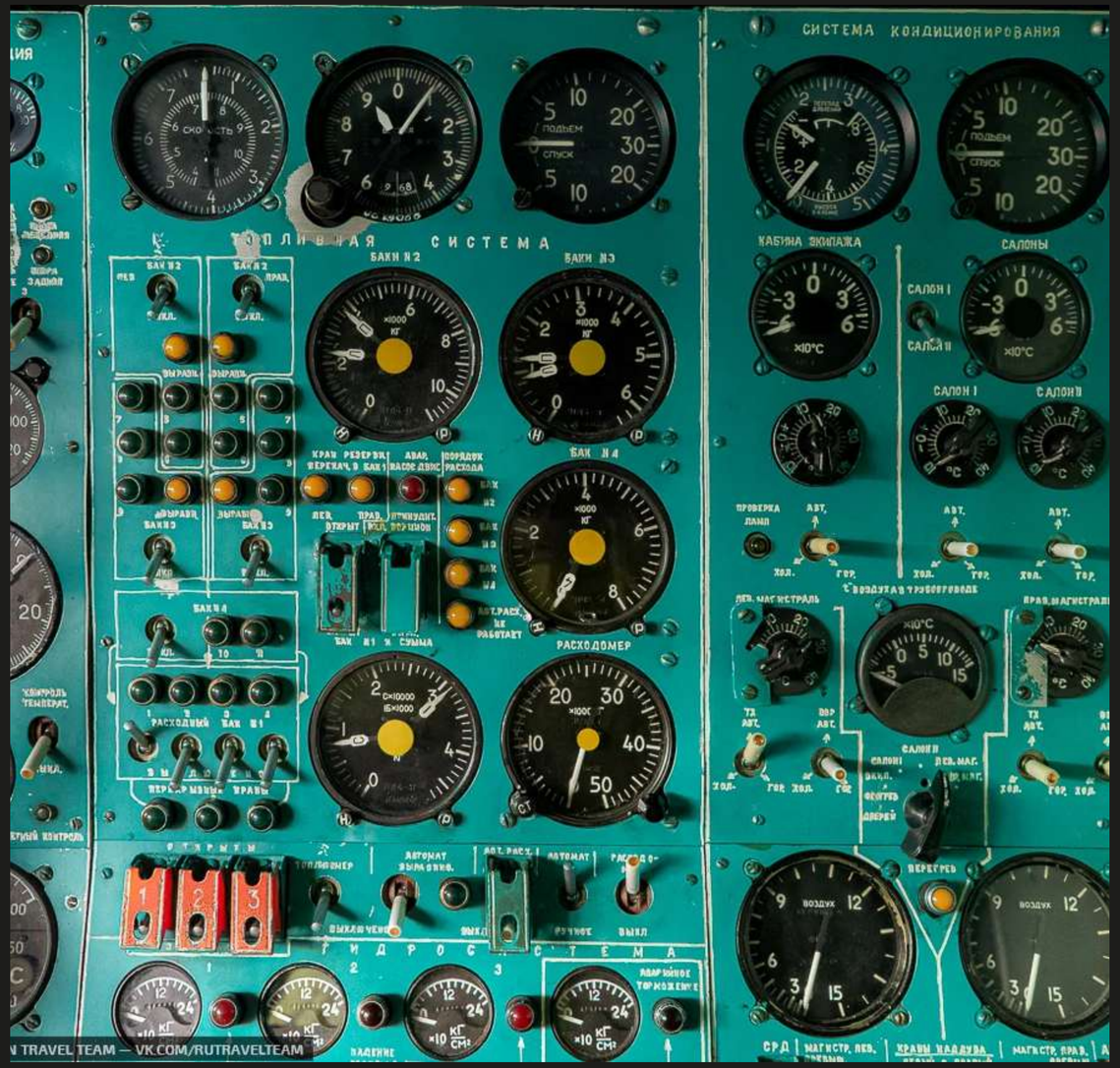


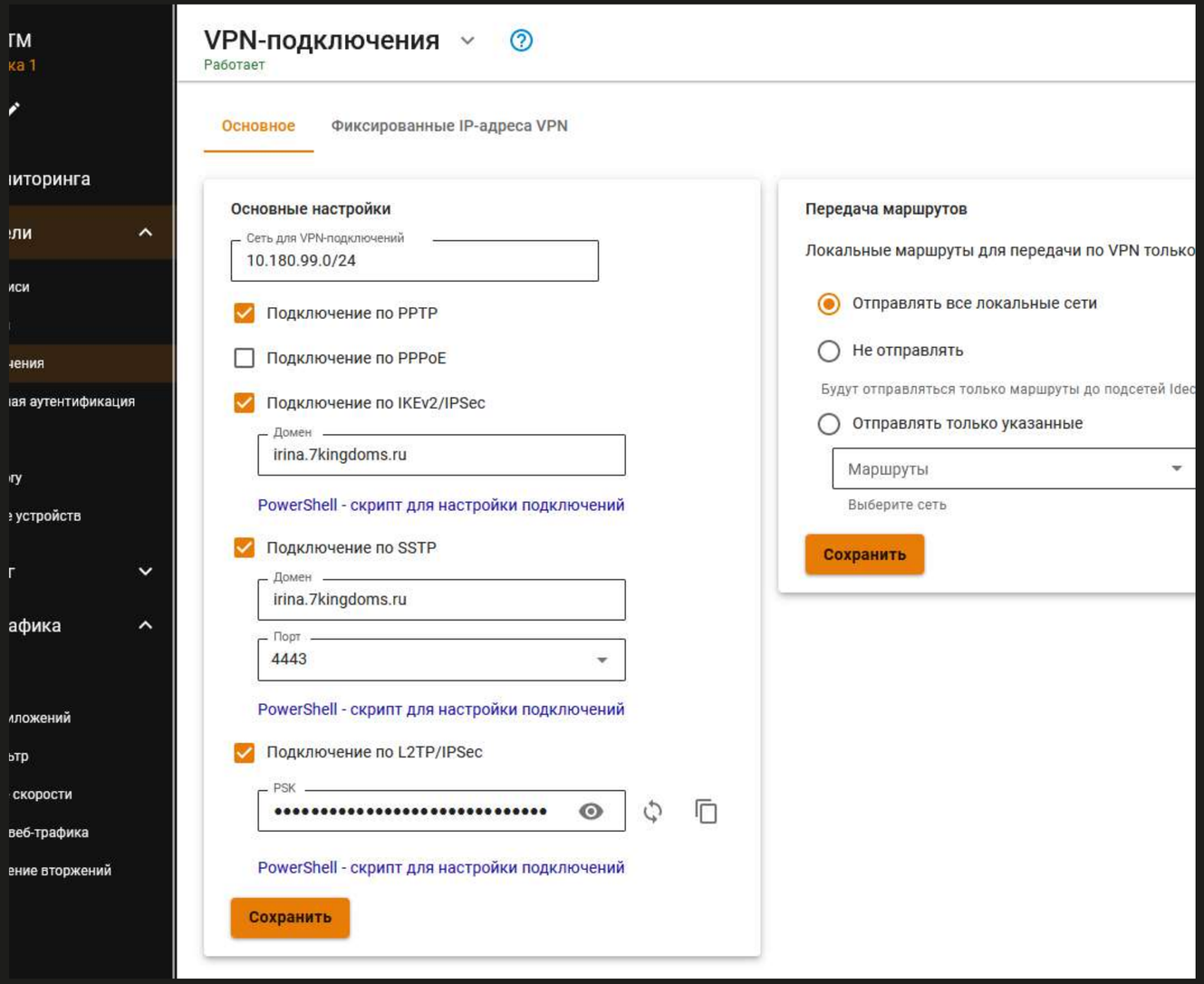
7. Мониторинг, отчёты, журналирование

- интеграции с внешними системами: syslog (с SIEM), SNMP, Zabbix-агент, ICAP (DLP)
- отчеты по трафику (общий трафик, приложения, веб-трафик по категориям)
- мониторинг (пользователи, трафик, трафик приложений)
- нагрузка на сервер (процессор, память, LA), сетевые интерфейсы, диск
- события безопасности
- журналы системы (в веб-интерфейсе с версии 14.2).



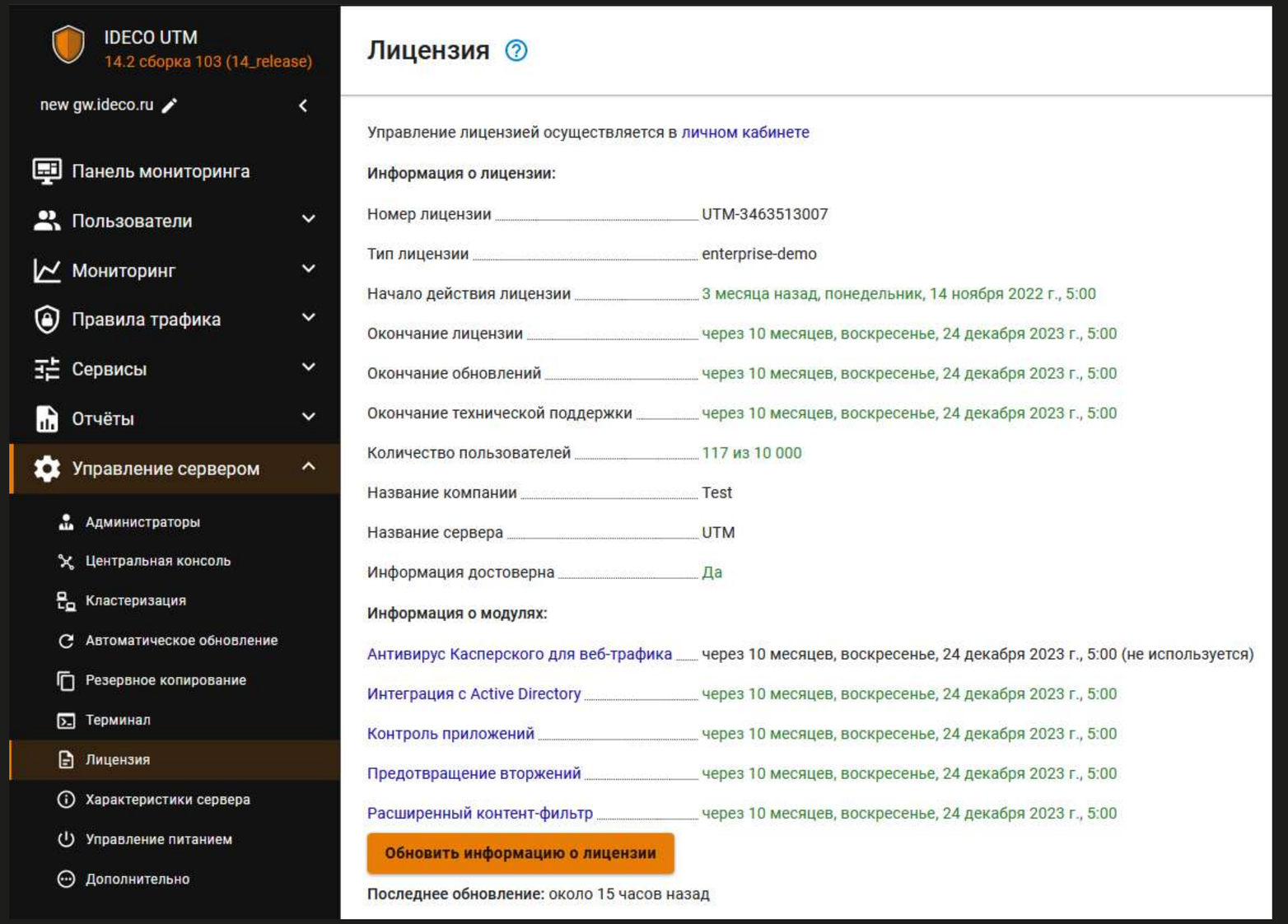
8. Простой и удобный UX/UI





9. Лицензирование

- количество пользователей одновременно выходящих в интернет (каждый пользователь может авторизовать до 5 устройств)
- безлимитные по количеству пользователей лицензии возможны для ПАК-ов
- лицензия бессрочная
- в Security Update входит:
  - переход на новые версии
  - расширенные базы КФ
  - работа и базы IPS
  - работа и базы АС
  - антивирус/антиспам Касперского
  - техподдержка.



10. Производительность и сайзинг

как подобрать ПАК или мощность гипервизора

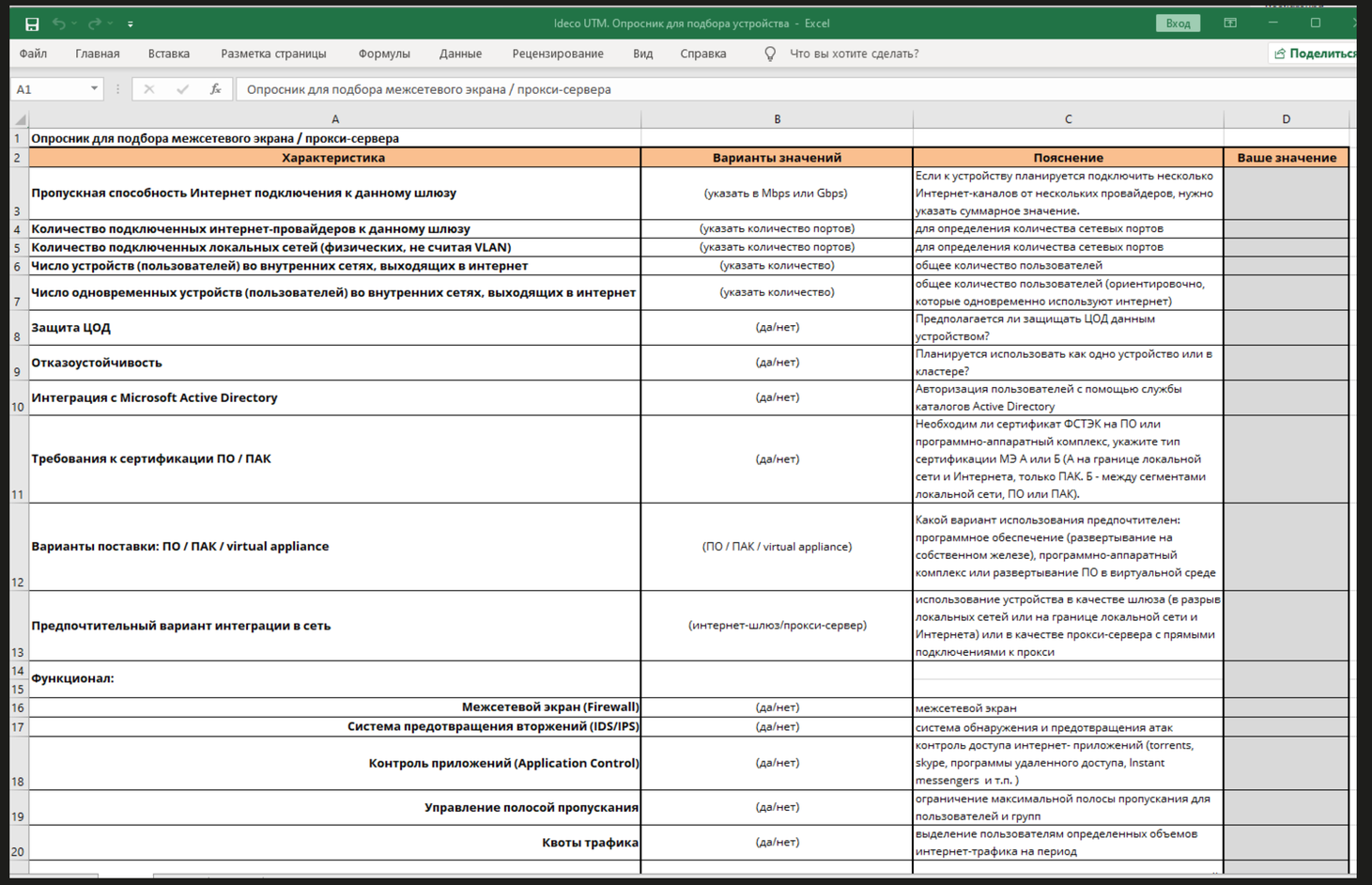
Основные параметры:

- ФСТЭК/НЕ ФСТЭК
- ПАК/ПО
- количество пользователей
- скорость трафика (для внешних интерфейсов).

Наибольшее влияние
на производительность:

- IPS
- антивирус веб-трафика.

Обращайтесь на sales@ideco.ru



Ideco UTM. Опросник для подбора устройства - Excel

Файл Главная Вставка Разметка страницы Формулы Данные Рецензирование Вид Справка Что вы хотите сделать?

A1: Опросник для подбора межсетевого экрана / прокси-сервера

	A	B	C	D
1	**Опросник для подбора межсетевого экрана / прокси-сервера**			
2	**Характеристика**	**Варианты значений**	**Пояснение**	**Ваше значение**
3	**Пропускная способность Интернет подключения к данному шлюзу**	(указать в Mbps или Gbps)	Если к устройству планируется подключить несколько Интернет-каналов от нескольких провайдеров, нужно указать суммарное значение.	
4	**Количество подключенных интернет-провайдеров к данному шлюзу**	(указать количество портов)	для определения количества сетевых портов	
5	**Количество подключенных локальных сетей (физических, не считая VLAN)**	(указать количество портов)	для определения количества сетевых портов	
6	**Число устройств (пользователей) во внутренних сетях, выходящих в интернет**	(указать количество)	общее количество пользователей	
7	**Число одновременных устройств (пользователей) во внутренних сетях, выходящих в интернет**	(указать количество)	общее количество пользователей (ориентировочно, которые одновременно используют интернет)	
8	**Защита ЦОД**	(да/нет)	Предполагается ли защищать ЦОД данным устройством?	
9	**Отказоустойчивость**	(да/нет)	Планируется использовать как одно устройство или в кластере?	
10	**Интеграция с Microsoft Active Directory**	(да/нет)	Авторизация пользователей с помощью службы каталогов Active Directory	
11	**Требования к сертификации ПО / ПАК**	(да/нет)	Необходим ли сертификат ФСТЭК на ПО или программно-аппаратный комплекс, укажите тип сертификации МЭ А или Б (А на границе локальной сети и Интернета, только ПАК. Б - между сегментами локальной сети, ПО или ПАК).	
12	**Варианты поставки: ПО / ПАК / virtual appliance**	(ПО / ПАК / virtual appliance)	Какой вариант использования предпочтителен: программное обеспечение (развертывание на собственном железе), программно-аппаратный комплекс или развертывание ПО в виртуальной среде	
13	**Предпочтительный вариант интеграции в сеть**	(интернет-шлюз/прокси-сервер)	использование устройства в качестве шлюза (в разрыв локальных сетей или на границе локальной сети и Интернета) или в качестве прокси-сервера с прямыми подключениями к прокси	
14	**Функционал:**			
15				
16	**Межсетевой экран (Firewall)**	(да/нет)	межсетевой экран	
17	**Система предотвращения вторжений (IDS/IPS)**	(да/нет)	система обнаружения и предотвращения атак	
18	**Контроль приложений (Application Control)**	(да/нет)	контроль доступа интернет- приложений (torrents, skype, программы удаленного доступа, Instant messengers и т.п.)	
19	**Управление полосой пропускания**	(да/нет)	ограничение максимальной полосы пропускания для пользователей и групп	
20	**Квоты трафика**	(да/нет)	выделение пользователям определенных объемов интернет-трафика на период	

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.

11. Техническая поддержка

На этапе тестирования

- подключение presale-инженера для презентации по ВКС
- подключение presale-инженера в сделках более 150 пользователей для проведения пилотного проекта
- чат в TG для быстрых ответов в пилотном проекте.

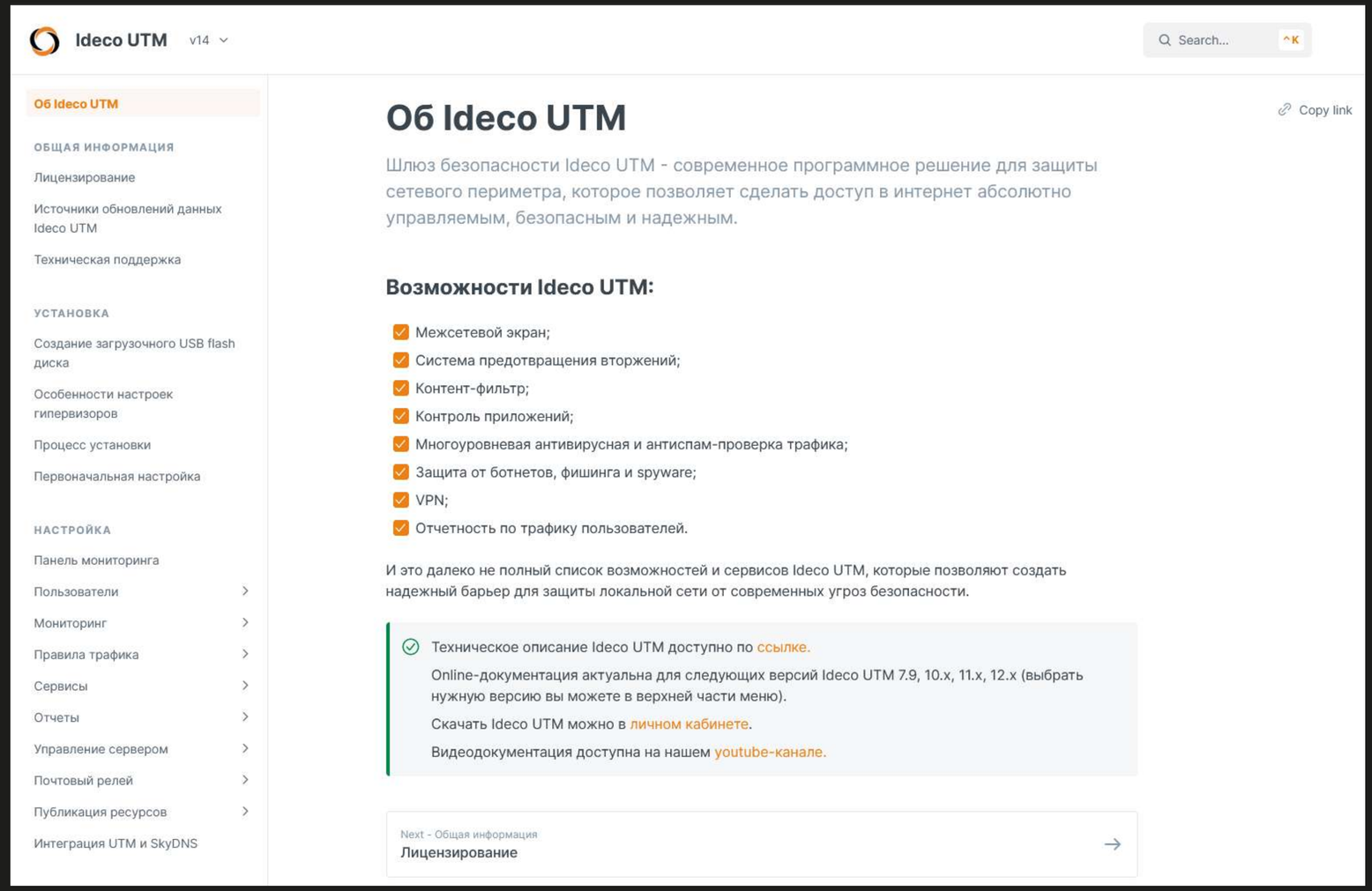
Техническая поддержка

- каналы обращения: телефон, емейл, tg-бот, портал поддержки, чат в интерфейсе
- стандартная поддержка 12x5+8 часов суббота
- расширенная поддержка 24x7×365
- 3 линии техподдержки.

12. Документация

docs.ideco.dev

- версионирование
- частое обновление
- документирование REST-API.

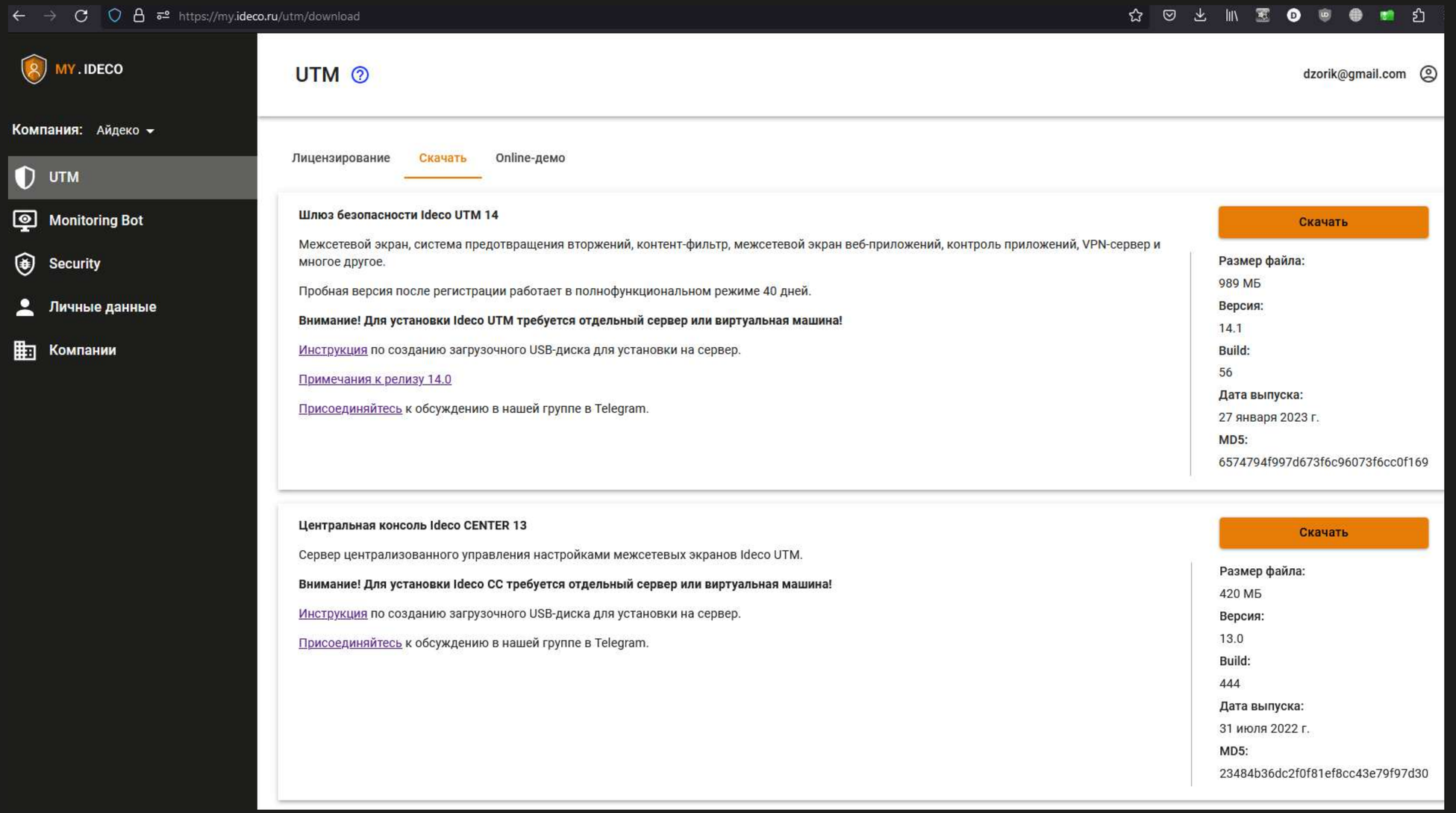


13. Сообщество и обратная связь

Ideco UTM: создаём вместе
1 054 участника

t.me/idecoutm

14. Тестирование



15. Преимущества Ideco UTM

ideco

Защита сразу «из коробки»

Готовность к ответу на вызовы 2023

Реактивные технологии

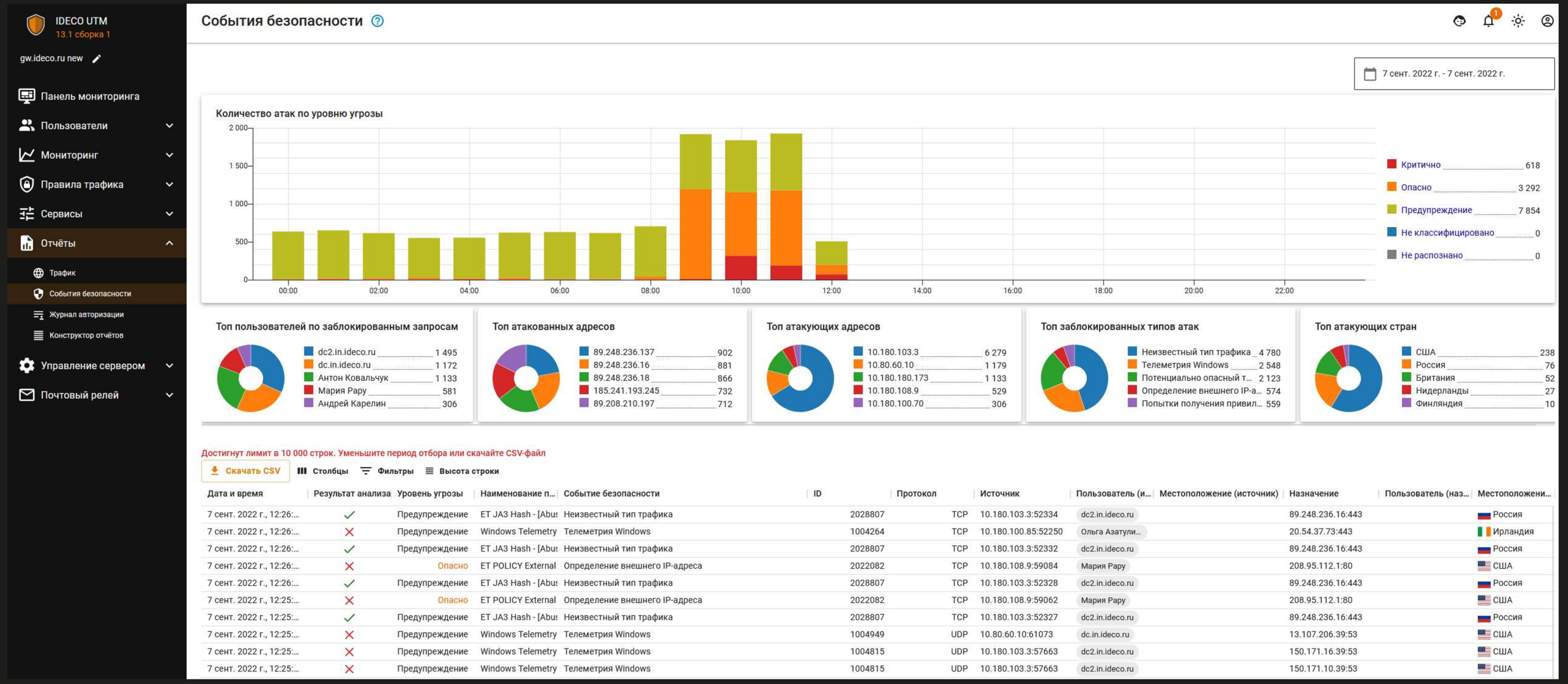
Сервис поддержки on-line

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

Чемпион по скорости разработки

Интересный факт: среднее время ответа технической поддержки в чат - 45 секунд.

Ideco UTM 14: защита “из коробки”



Killer Feature

ideco

Продукт

- VPN-агент/агент аутентификации
- аутентификация по логам безопасности контроллеров домена Active Directory
- нативные VPN-протоколы IKEv2 и SSTP
- полный доступ к системе через терминал.

Поддержка

- чат в веб-интерфейсе, среднее время ответа - 45 секунд
- общение с разработчиками в сообществе в tg-группе
- быстрое развитие продукта.

Коммерческие условия

- цена ниже многих конкурентов
- кластер отказоустойчивости входит в базовую лицензию
- центральная консоль управления входит в базовую лицензию
- нет привязки лицензии к “железу”.

16. RoadMap

ideco

Муравей на ходу делает больше, чем дремлющий бык.

R&D

- dataplane
- frontend
- backend
- devops
- ручное тестирование
- автоматизированное тестирование
- документация
- ФСТЭК.

8 development teams

2023 год

Ideco UTM 15

- пропуск мультикаст-трафика
- адаптивность веб-интерфейса под мобильные устройства
- балансировка трафика обратным прокси-сервером
- интеграция с ALD PRO
- аудит действий администраторов
- авторизация пользователей терминальных серверов.

Будущее: Ideco ~~UTM~~ NGFW 16

- x10 скорость обработки трафика,
  полностью «свой» стек обработки трафика,
  общие правила firewall/DPI/IPS

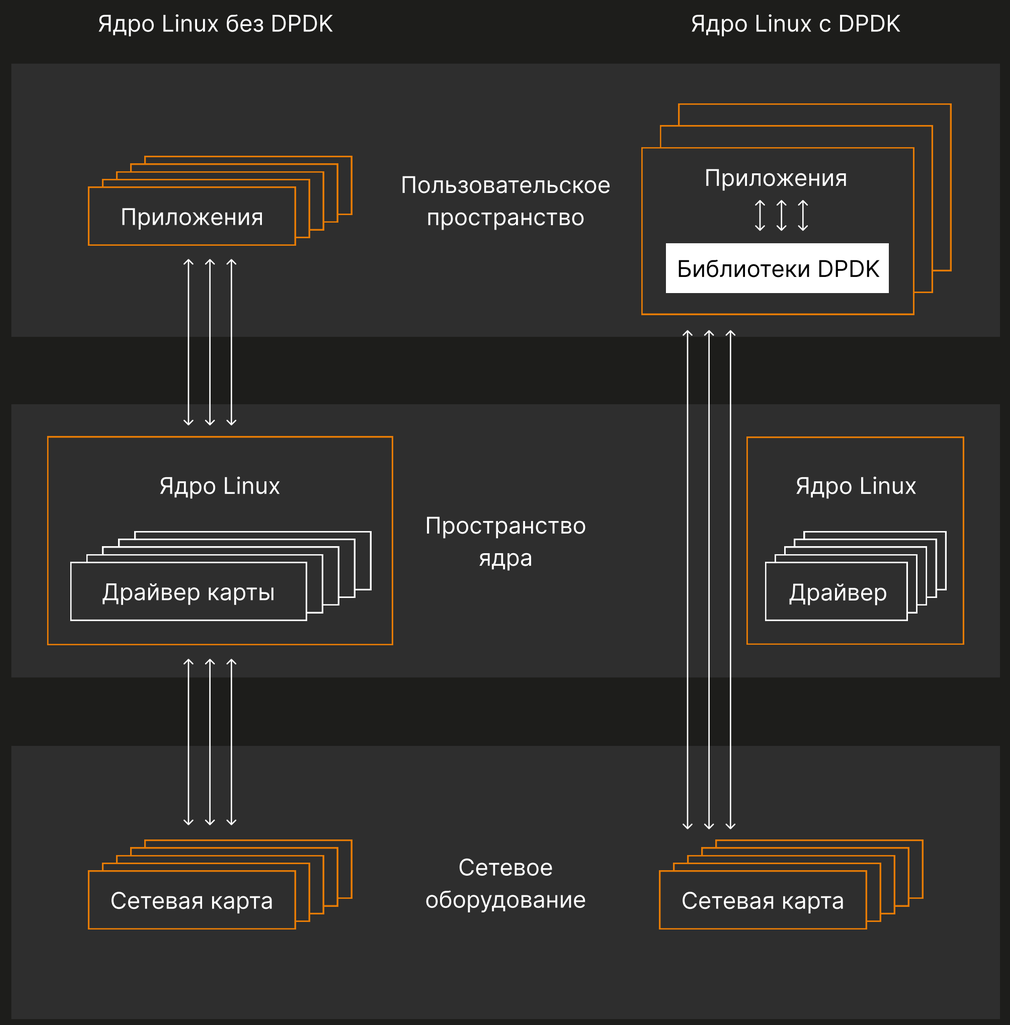
- x2 скорость обработки веб-трафика,
  новейший модуль прокси-сервера (от
  Айдеко)

- высокоскоростной NGFW и технологическое
  лидерство среди отечественных решений.

Архитектура Ideco UTM

- Linux 5.18
- сила opensource-модулей
- микросервисы vs монолит
- kernel vs userspace (DPDK).

Оптимальный фундамент для быстрого развития enterprise-продукта.



ideco

СОЗДАЕМ ВМЕСТЕ

t.me/idecoutm - группа
t.me/ideco - канал
my.ideco.ru - скачать