

ВЫБОР РОССИЙСКОГО NGFW

НА ЧТО ОБРАЩАТЬ ВНИМАНИЕ ПРИ МИГРАЦИИ

Дмитрий Хомутов
Директор «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



120 человек в команде
S&M / R&D



Лидер по скорости
разработки в отрасли



Ideco UTM

Фильтрация трафика L7

МЭ, COB, Контроль приложений,
Контент-фильтр

Пользователи

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

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

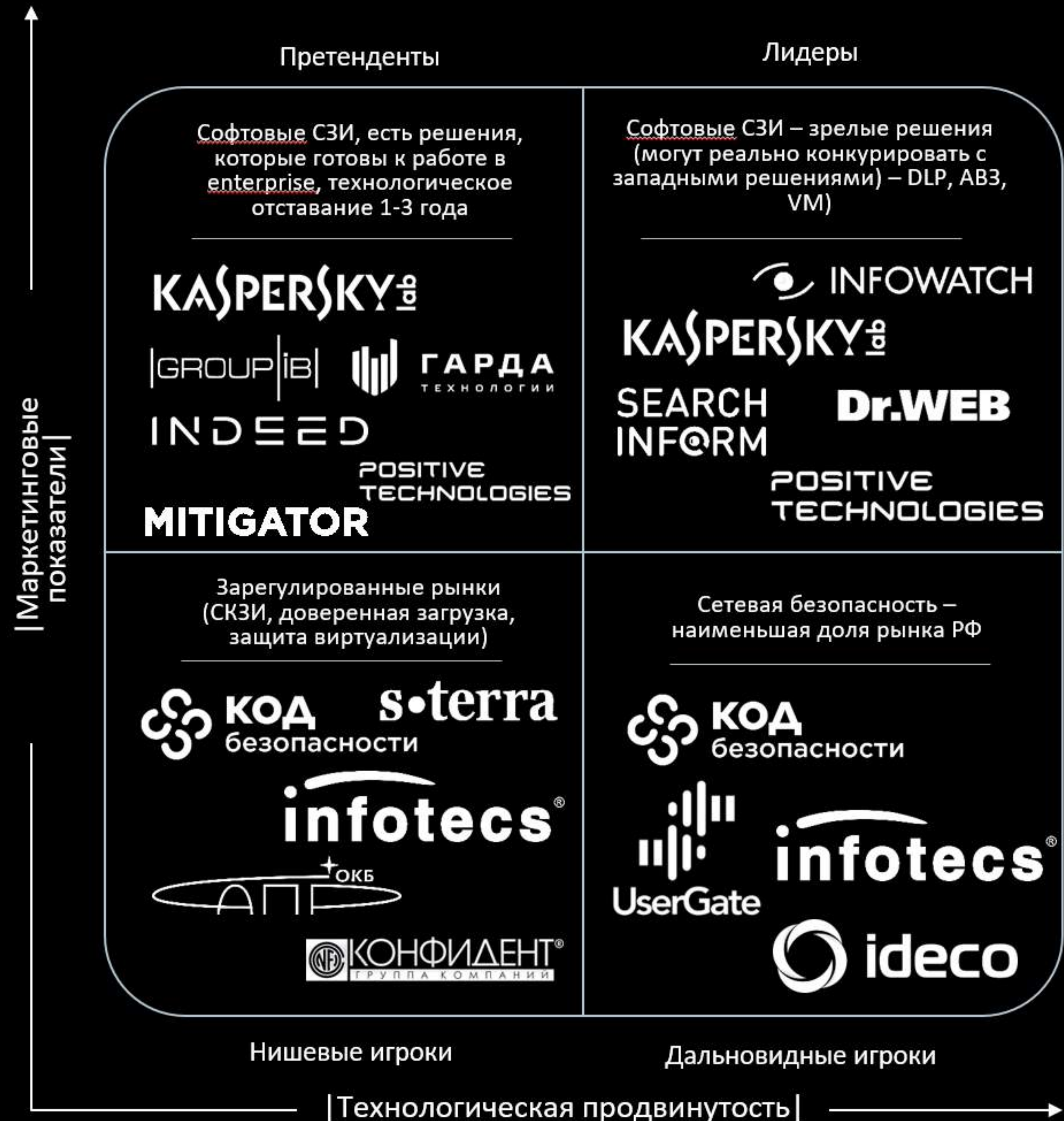
Телеграм бот, Zabbix Агент,
Syslog, SNMP, SIEM
Отчетность по пользователям

Отказоустойчивость:

- Кластеризация Active/Passive
- Резервное копирование
- Программный Watchdog

VPN

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



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:

№ 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»
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»

« 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 соответствуют формальным требованиям к МЭ;
- в компании внедрена безопасная разработка (SDL);
- уровень зрелости компании и продукта.

Idecso UTM: сертификация ФСТЭК и Минцифры

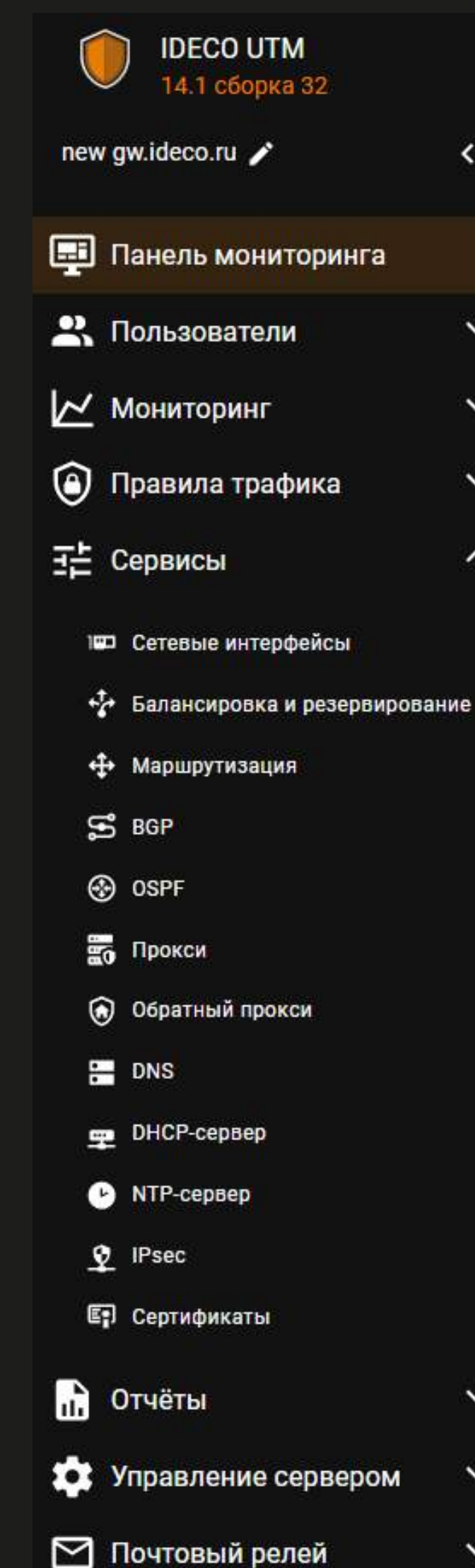


- Сертификат ФСТЭК МЭ А4/Б4, СОВ 4, УД4;
- реестр программного обеспечения Минцифры: запись в реестре №329 от 08.04.2016;
- для защиты:
 - ГИС: до 1 К3 (включительно),
 - ИСПДн: до 1 У3 (включительно),
 - АСУ: до К1 (включительно),
 - Значимые объекты КИИ: до 1 класса (включительно),
 - ИС ОП: II класс;
- 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».



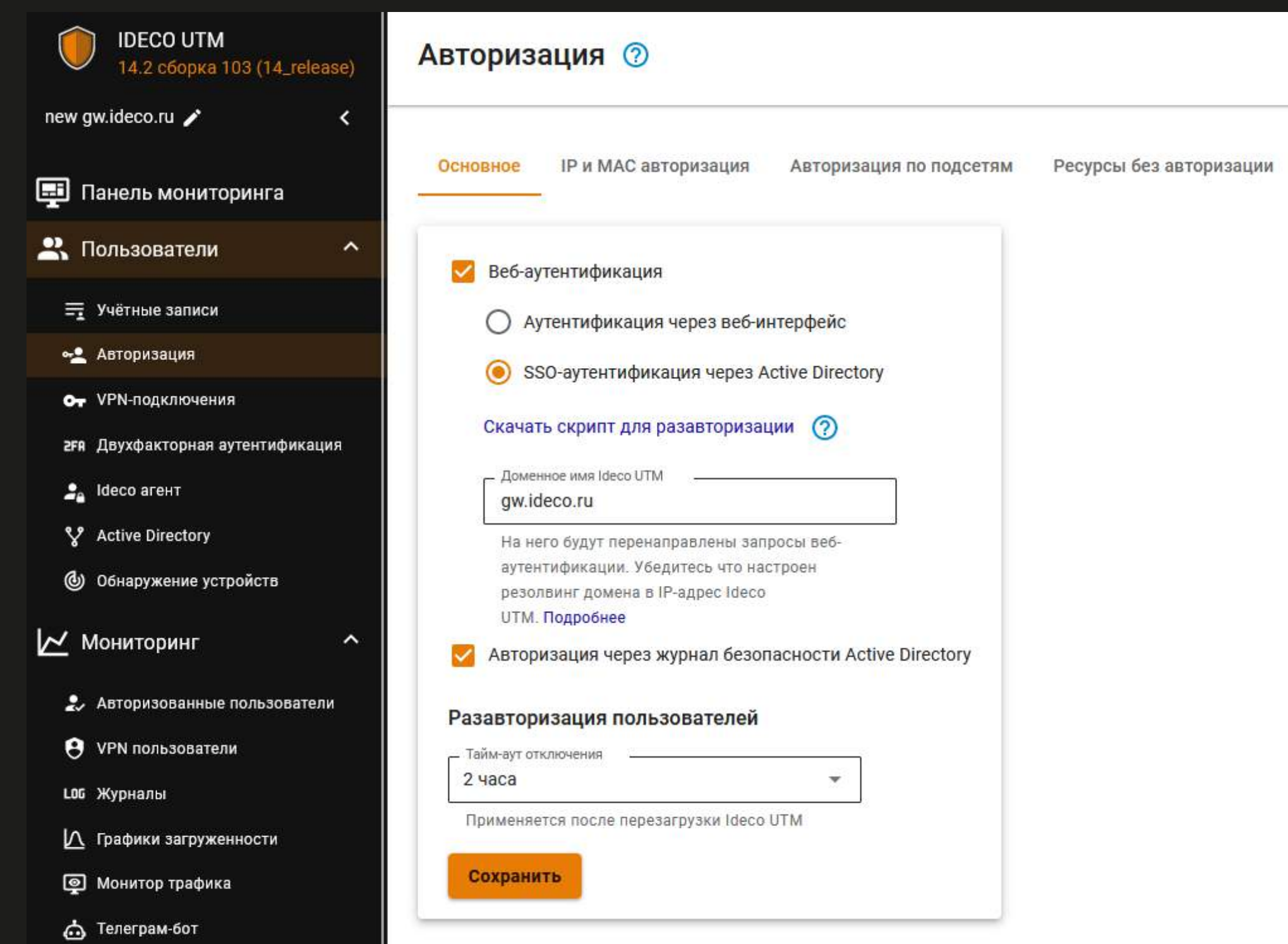
2. Сетевая и общая функциональность

- 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 (апрель 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).



The screenshot displays the IDECO UTM web interface. On the left is a dark sidebar menu with the following items: 'Панель мониторинга', 'Пользователи', 'Учётные записи', 'Авторизация', 'VPN-подключения', 'Двухфакторная аутентификация', 'Ideco агент', 'Active Directory', 'Обнаружение устройств', 'Мониторинг', 'Авторизованные пользователи', 'VPN пользователи', 'Журналы', 'Графики загруженности', 'Монитор трафика', and 'Телеграм-бот'. The main content area is titled 'Авторизация' and has several tabs: 'Основное', 'IP и MAC авторизация', 'Авторизация по подсетям', and 'Ресурсы без авторизации'. The 'Основное' tab is active. It contains the following settings:

- Веб-аутентификация
 - Аутентификация через веб-интерфейс
 - SSO-аутентификация через Active Directory
- [Скачать скрипт для разавторизации](#)
- Доменное имя Ideco UTM:
- На него будут перенаправлены запросы веб-аутентификации. Убедитесь что настроен резолвинг домена в IP-адрес Ideco UTM. Подробнее
- Авторизация через журнал безопасности Active Directory
- Разавторизация пользователей
 - Тайм-аут отключения:
 - Применяется после перезагрузки Ideco UTM
-

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.

IDECO UTM 14.1 сборка 32
new.gw.ideco.ru

Панель мониторинга
Пользователи
Мониторинг
Правила трафика
Файрвол
Контроль приложений
Контент-фильтр
Ограничение скорости
Антивирусы веб-трафика
Предотвращение вторжений
Исключения
Объекты
Квоты
Сервисы
Отчёты
Управление сервером
Почтовый релей

Контент-фильтр

Расширенная база категорий
Обновление баз около 5 часов назад
Статус Обновлений не требуется

Правила Пользовательские категории Настройки

URL для категоризации

Отображать названия объектов Столбцы Фильтры Высота строки

Название	Применяется для	Категории	Действие	Управление
Белый список	Все	Белый список (Польз.)	Разрешить	
Блокируем запрещенные сайты	Все	Черный список (Польз.)	Запретить	
для Марка	Марк Коренберг	Все запросы	Разрешить	
бухгалтерия и hr	Buhgalters HR Марина Тябина Ольга Полуянова	Анонимайзеры Список Минюста	Разрешить	
marketing	Дмитрий Юсов Марина Тябина	Маркетинговые услуги Список Минюста Социальные сети Он	Разрешить	
whatsapp	Все	Социальные сети Чаты Чаты/Мессенджеры	Разрешить	
Повышаем безопасность сети	Все	Анонимайзеры Ботнеты Высокий уровень риска	Запретить	
		Скомпрометированные Спам Тайный сбор информации		
		Фишинг/мошенничество		
		Центры распространения вредоносного ПО		
		Центры управления и контроля Шпионские и опасные сайты		
Шпионское и сомнительное ПО				
Повышаем скорость интернета	Все	Онлайн-реклама и баннеры Торрент-трекеры	Запретить	
		Компьютерные игры Торрент-файлы		
Избавляемся от неподобающего контента	Все	Геи, лесбиянки и бисексуалы Казино, лотереи, тотализаторы	Запретить	
		Марихуана Порнография Порнография/секс		
		Секс и Зротика		

6. Публикация ресурсов

безопасная публикация



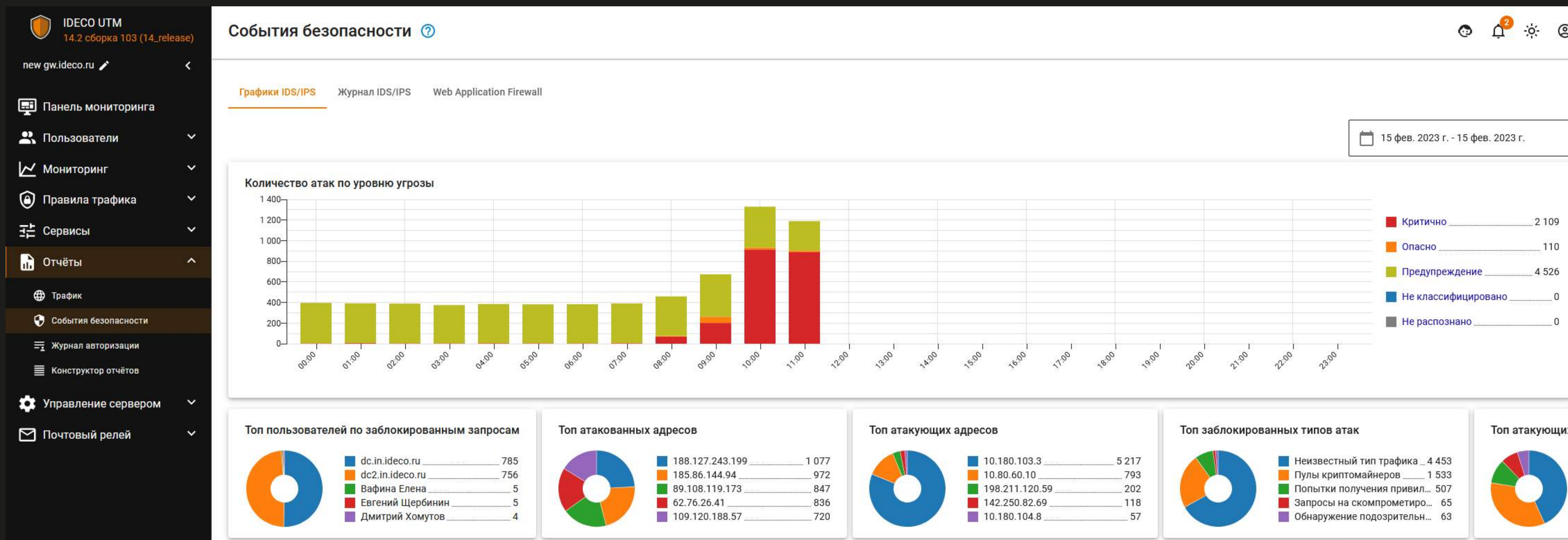
- обратный прокси-сервер с WAF для публикации веб-ресурсов;
- почтовый релей для публикации почтового сервера;
- защита опубликованных терминальных серверов (RDP).

The screenshot shows the IDECO UTM web interface. The top left corner displays the IDECO UTM logo and version information: "14.2 сборка 103 (14_release)". Below this, the current gateway is identified as "new gw.ideco.ru". A sidebar menu on the left lists various system functions: "Панель мониторинга", "Пользователи", "Мониторинг", "Правила трафика", "Сервисы", "Сетевые интерфейсы", "Балансировка и резервирование", "Маршрутизация", "BGP", "OSPF", "Прокси", "Обратный прокси", "DNS", "DHCP-сервер", and "NTP-сервер". The "Обратный прокси" (Reverse Proxy) option is selected and highlighted. The main content area is titled "Обратный прокси" and contains a "Создание правила публикации" (Create publication rule) section. Under "Основные настройки" (Basic settings), there are input fields for "Запрашиваемый адрес в Интернете" (Requested address in Internet) and "Адрес в локальной сети" (Address in local network), with a "Добавить адрес" (Add address) button. A note indicates that the URL will be redirected to the local address. Under "Дополнительные настройки" (Additional settings), there are two checked checkboxes: "Перенаправлять HTTP запросы на HTTPS" (Redirect HTTP requests to HTTPS) and "Web Application Firewall". A dropdown menu for "Тип публикации" (Publication type) is set to "Стандартный" (Standard). A "Комментарий" (Comment) field is also present. At the bottom, there are "Сохранить" (Save) and "Отмена" (Cancel) buttons.

7. Мониторинг, отчеты, 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



VPN-подключения Работает

Основное Фиксированные IP-адреса VPN

Основные настройки

Сеть для VPN-подключений
10.180.99.0/24

Подключение по PPTP

Подключение по PPPoE

Подключение по IKEv2/IPSec

Домен
irina.7kingdoms.ru

PowerShell - скрипт для настройки подключений

Подключение по SSTP

Домен
irina.7kingdoms.ru

Порт
4443

PowerShell - скрипт для настройки подключений

Подключение по L2TP/IPSec

PSK
.....

PowerShell - скрипт для настройки подключений

Сохранить

Передача маршрутов

Локальные маршруты для передачи по VPN только

Отправлять все локальные сети

Не отправлять

Будут отправляться только маршруты до подсетей Idec

Отправлять только указанные

Маршруты

Выберите сеть

Сохранить

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 AC;
 - антивирус/антиспам Касперского;
 - тех. поддержка.

The screenshot shows the IDECO UTM management interface. The left sidebar contains a menu with the following items: Панель мониторинга, Пользователи, Мониторинг, Правила трафика, Сервисы, Отчёты, Управление сервером (highlighted), Администраторы, Центральная консоль, Кластеризация, Автоматическое обновление, Резервное копирование, Терминал, Лицензия (highlighted), Характеристики сервера, Управление питанием, and Дополнительно. The main content area is titled 'Лицензия' and displays the following information:

Управление лицензией осуществляется в личном кабинете

Информация о лицензии:

Номер лицензии	UTM-3463513007
Тип лицензии	enterprise-demo
Начало действия лицензии	3 месяца назад, понедельник, 14 ноября 2022 г., 5:00
Окончание лицензии	через 10 месяцев, воскресенье, 24 декабря 2023 г., 5:00
Окончание обновлений	через 10 месяцев, воскресенье, 24 декабря 2023 г., 5:00
Окончание технической поддержки	через 10 месяцев, воскресенье, 24 декабря 2023 г., 5:00
Количество пользователей	117 из 10 000
Название компании	Test
Название сервера	UTM
Информация достоверна	Да

Информация о модулях:

Антивирус Касперского для веб-трафика	через 10 месяцев, воскресенье, 24 декабря 2023 г., 5:00 (не используется)
Интеграция с Active Directory	через 10 месяцев, воскресенье, 24 декабря 2023 г., 5:00
Контроль приложений	через 10 месяцев, воскресенье, 24 декабря 2023 г., 5:00
Предотвращение вторжений	через 10 месяцев, воскресенье, 24 декабря 2023 г., 5:00
Расширенный контент-фильтр	через 10 месяцев, воскресенье, 24 декабря 2023 г., 5:00

Обновить информацию о лицензии

Последнее обновление: около 15 часов назад

10. Производительность и сайзинг



как подобрать ПАК или мощность гиперизора

Основные параметры

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

Наибольшее влияние на производительность:

- IPS;
- антивирус веб-трафика.

Обращайтесь к нашим партнерам или на sales@ideco.ru

А	В	С	Д
Опросник для подбора межсетевого экрана / прокси-сервера	Варианты значений	Пояснение	Ваше значение
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.	
Количество подключенных интернет-провайдеров к данному шлюзу	(указать количество портов)	для определения количества сетевых портов	
Количество подключенных локальных сетей (физических, не считая VLAN)	(указать количество портов)	для определения количества сетевых портов	
Число устройств (пользователей) во внутренних сетях, выходящих в интернет	(указать количество)	общее количество пользователей	
Число одновременных устройств (пользователей) во внутренних сетях, выходящих в интернет	(указать количество)	общее количество пользователей (ориентировочно, которые одновременно используют интернет)	
Защита ЦОД	(да/нет)	Предполагается ли защищать ЦОД данным устройством?	
Отказоустойчивость	(да/нет)	Планируется использовать как одно устройство или в кластере?	
Интеграция с Microsoft Active Directory	(да/нет)	Авторизация пользователей с помощью службы каталогов Active Directory	
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).	
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	
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	
Функционал:			
Межсетевой экран (Firewall)	(да/нет)	межсетевой экран	
Система предотвращения вторжений (IDS/IPS)	(да/нет)	система обнаружения и предотвращения атак	
Контроль приложений (Application Control)	(да/нет)	контроль доступа интернет- приложений (torrents, skype, программы удаленного доступа, Instant messengers и т.п.)	
Управление полосой пропускания	(да/нет)	ограничение максимальной полосы пропускания для пользователей и групп	
Квоты трафика	(да/нет)	выделение пользователям определенных объемов интернет-трафика на период	

Ideco SX+

до 75 пользователей



Ideco SX+

Решения для малого бизнеса

Предназначен для небольших организаций, численностью до 75 активных пользователей интернет. Позволяет ввести ограничения по трафику для каждого из сотрудников или отдельных групп, защитить периметр сети, сегментировать сеть и использовать несколько интернет-провайдеров (благодаря 6 сетевым интерфейсам), а также предоставить возможность удаленной работы сотрудников по VPN.



Характеристики

Процессор	Intel Core i5-10210U (1.6GHz, 6M, 4-Cores)
Память	16GB SO-DIMM DDR4
Хранилище	mSATA 256GB.
Сетевой адаптер	6 x i210/i211

Производительность (трафик EMIX)

Межсетевой экран	до 5 Гб/сек
Контентная фильтрация	до 2 Гб/сек
Контроль приложений	до 1 Гб/сек
Предотвращение вторжений	до 0,4 Гб/сек
Режим NGFW	до 0,4 Гб/сек

Ideco MX и LX



1U-сервера. MX 50-350 пользователей, LX до 1000

Ideco MX и LX

Решения для малого и среднего бизнеса

Серверы этой линейки обладают повышенным уровнем надёжности, производительности и управляемости в сочетании с возможностью наращивания ресурсов вычислительной системы. Всё это обеспечивает непрерывность бизнес-процессов как малых, так и средних предприятий.

Позволяют защищать локальную сеть предприятия от внешних угроз, контролировать потоки трафика и решать все основные потребности сетевой инфраструктуры.



Производительность (трафик EMIX)

	MX	LX
Межсетевой экран	до 8 Гб/сек	до 11,5 Гб/сек
Контентная фильтрация	до 5 Гб/сек	до 8,1 Гб/сек
Контроль приложений	до 2,2 Гб/сек	до 3,5 Гб/сек
Предотвращение вторжений	до 1,2 Гб/сек	до 1,8 Гб/сек
Режим NGFW *	до 1,2 Гб/сек	до 1,8 Гб/сек

Характеристики

	MX	LX
Процессор	Intel Xeon E-2234 (3.6GHz, 8M, 4-Cores)	Intel® Xeon® E-22xx (8 ядер, 16Mb, 8 GT/s)
Память	16Gb DDR4-2133 ECC	32Gb DDR4-2133 ECC
Хранилище	240Gb SATA SSD	240Gb SATA SSD
Сетевой адаптер	4x Gigabit LAN ports	4x Gigabit LAN ports

Ideco LX+ и EX



2U сервера. LX+ до 3000 пользователей, EX до 10000

Ideco LX+ и EX

Решения для среднего и крупного бизнеса

Серверы этой линейки обладают повышенным уровнем надёжности, производительности и управляемости в сочетании с возможностью наращивания ресурсов вычислительной системы. Всё это обеспечивает непрерывность бизнес-процессов предприятий любого размера.

Позволяют защищать локальную сеть предприятия от внешних угроз, контролировать потоки трафика и решать все основные потребности сетевой инфраструктуры.



Характеристики

	LX+	EX
Процессор	Intel Xeon Silver 4214R 12 ядер, 24 потока	Intel Xeon Gold 6238R 28 ядер, 56 потока
Память	64Gb DDR4 ECC REG	64Gb DDR4-2133 ECC
Хранилище	480Gb SATA SSD	480Gb SATA SSD
Сетевой адаптер	4x Gigabit LAN ports, 4x10 Gb SFP+	4x Gigabit LAN ports, 4x10 Gb SFP+
Источник питания	2x Блока питания 800 Вт (2*800 Вт)	2x Блока питания 800 Вт (2*800 Вт)

Производительность (трафик EMIX)

	LX+	EX
Межсетевой экран	до 19,6 Гб/сек	до 42 Гб/сек
Контентная фильтрация	до 10,2 Гб/сек	до 25 Гб/сек
Контроль приложений	до 4 Гб/сек	до 8,8 Гб/сек
Предотвращение вторжений	до 2 Гб/сек	до 5 Гб/сек
Режим NGFW *	до 2 Гб/сек	до 5 Гб/сек

Ideco MX и MX+ Cert



сертифицированные ФСТЭК, в апреле 2023 будет в наличии новая модель на Xeon

Ideco MX и MX+ Cert

Сертифицировано ФСТЭК

Сертифицирован по требованиям к межсетевым экранам типа А, Б 4-го класса и системам обнаружения вторжений. Сертификат №4503 от 28.12.2021.

Сертифицированная аппаратная платформа MX для организаций от 100 до 350 пользователей, MX+ от 300 до 700. Позволяет защищать локальную сеть предприятия от внешних угроз, контролировать потоки трафика и решать все потребности сетевой инфраструктуры. Соответствие требованиям ФСТЭК, решение широкого круга задач и возможность интеграции с AD/LDAP позволяет линейке Ideco MX обеспечить потребности компаний малого и среднего бизнеса.



Характеристики

	MX Cert	MX + Cert
Процессор	Intel Atom C-3758 (8 ядер, 2,2 ГГц)	Intel® Atom C-3958 (16 ядер, 2,0 ГГц)
Память	16GB DDR4	32Gb DDR4
Хранилище	240Gb SATA SSD	240Gb SATA SSD
Сетевой адаптер	8×1Gb Lan	8×1Gb Lan

Производительность (трафик EMIX)

	MX Cert	MX + Cert
Межсетевой экран	до 3 Гб/сек	до 6 Гб/сек
Контентная фильтрация	до 1,7 Гб/сек	до 3,2 Гб/сек
Контроль приложений	до 0,7 Гб/сек	до 1,3 Гб/сек
Предотвращение вторжений	до 0,3 Гб/сек	до 0,6 Гб/сек
Режим NGFW *	до 0,3 Гб/сек	до 0,6 Гб/сек

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 24x7x365;
- SLA первого ответа 4 часа;
- 3 линии тех. поддержки.

12. Документация



docs.ideco.dev

- версионирование;
- частое обновление;
- документирование REST-API.

Ideco UTM v14

Q Search... ^K

Об Ideco UTM Copy link

Шлюз безопасности Ideco UTM - современное программное решение для защиты сетевого периметра, которое позволяет сделать доступ в интернет абсолютно управляемым, безопасным и надежным.

Возможности Ideco UTM:

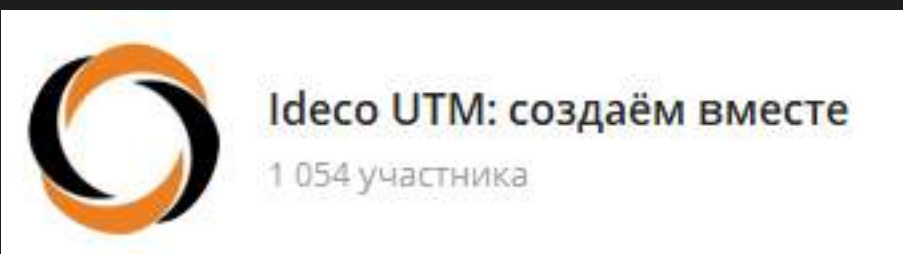
- ✓ Межсетевой экран;
- ✓ Система предотвращения вторжений;
- ✓ Контент-фильтр;
- ✓ Контроль приложений;
- ✓ Многоуровневая антивирусная и антиспам-проверка трафика;
- ✓ Защита от ботнетов, фишинга и spyware;
- ✓ VPN;
- ✓ Отчетность по трафику пользователей.

И это далеко не полный список возможностей и сервисов Ideco UTM, которые позволяют создать надежный барьер для защиты локальной сети от современных угроз безопасности.

✓ Техническое описание Ideco UTM доступно по [ссылке](#).
Online-документация актуальна для следующих версий Ideco UTM 7.9, 10.x, 11.x, 12.x (выбрать нужную версию вы можете в верхней части меню).
Скачать Ideco UTM можно в [личном кабинете](#).
Видеодокументация доступна на нашем [youtube-канале](#).

Next - [Общая информация](#)
[Лицензирование](#) →

13. Сообщество и обратная связь



t.me/idecoutm



15. Преимущества Ideco UTM



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”

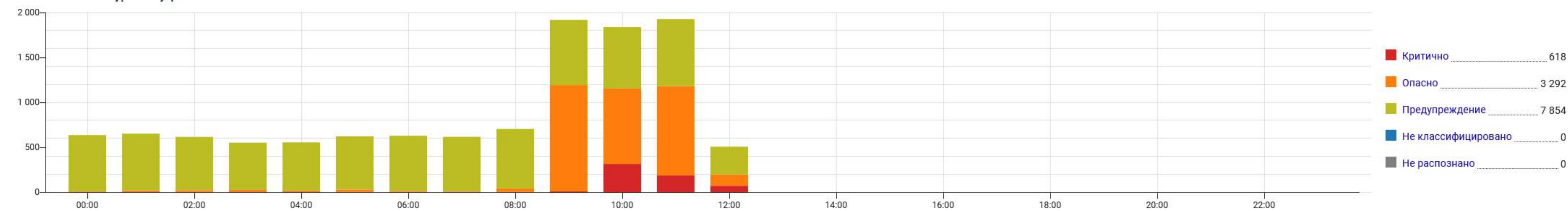


- IDECO UTM 13.1 сборка 1
- gw.ideco.ru new
- Панель мониторинга
- Пользователи
- Мониторинг
- Правила трафика
- Сервисы
- Отчёты
- Трафик
- События безопасности
- Журнал авторизации
- Конструктор отчётов
- Управление сервером
- Почтовый релей

События безопасности

7 сент. 2022 г. - 7 сент. 2022 г.

Количество атак по уровню угрозы



Топ пользователей по заблокированным запросам



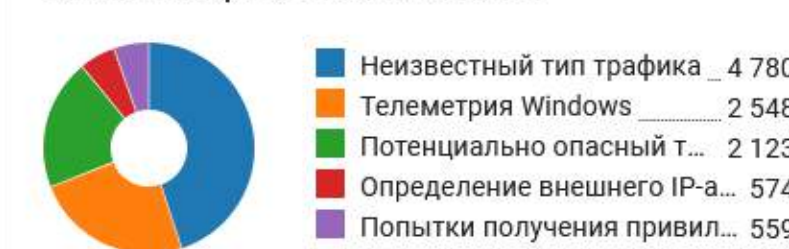
Топ атакованных адресов



Топ атакующих адресов



Топ заблокированных типов атак



Топ атакующих стран



Достигнут лимит в 10 000 строк. Уменьшите период отбора или скачайте CSV-файл

[Скачать CSV](#) Столбцы Фильтры Высота строки

Дата и время	Результат анализа	Уровень угрозы	Наименование п...	Событие безопасности	ID	Протокол	Источник	Пользователь (и...	Местоположение (источник)	Назначение	Пользователь (наз...	Местоположени...
7 сент. 2022 г., 12:26:...	✓	Предупреждение	ET JA3 Hash - [Abu...	Неизвестный тип трафика	2028807	TCP	10.180.103.3:52334	dc2.in.ideco.ru	89.248.236.16:443		Россия	
7 сент. 2022 г., 12:26:...	✗	Предупреждение	Windows Telemetry	Телеметрия Windows	1004264	TCP	10.180.100.85:52250	Ольга Азатули...	20.54.37.73:443		Ирландия	
7 сент. 2022 г., 12:26:...	✓	Предупреждение	ET JA3 Hash - [Abu...	Неизвестный тип трафика	2028807	TCP	10.180.103.3:52332	dc2.in.ideco.ru	89.248.236.16:443		Россия	
7 сент. 2022 г., 12:26:...	✗	Опасно	ET POLICY External	Определение внешнего IP-адреса	2022082	TCP	10.180.108.9:59084	Мария Рапу	208.95.112.1:80		США	
7 сент. 2022 г., 12:26:...	✓	Предупреждение	ET JA3 Hash - [Abu...	Неизвестный тип трафика	2028807	TCP	10.180.103.3:52328	dc2.in.ideco.ru	89.248.236.16:443		Россия	
7 сент. 2022 г., 12:25:...	✗	Опасно	ET POLICY External	Определение внешнего IP-адреса	2022082	TCP	10.180.108.9:59062	Мария Рапу	208.95.112.1:80		США	
7 сент. 2022 г., 12:25:...	✓	Предупреждение	ET JA3 Hash - [Abu...	Неизвестный тип трафика	2028807	TCP	10.180.103.3:52327	dc2.in.ideco.ru	89.248.236.16:443		Россия	
7 сент. 2022 г., 12:25:...	✗	Предупреждение	Windows Telemetry	Телеметрия Windows	1004949	UDP	10.80.60.10:61073	dc.in.ideco.ru	13.107.206.39:53		США	
7 сент. 2022 г., 12:25:...	✗	Предупреждение	Windows Telemetry	Телеметрия Windows	1004815	UDP	10.180.103.3:57663	dc2.in.ideco.ru	150.171.16.39:53		США	
7 сент. 2022 г., 12:25:...	✗	Предупреждение	Windows Telemetry	Телеметрия Windows	1004815	UDP	10.180.103.3:57663	dc2.in.ideco.ru	150.171.10.39:53		США	

Killer Feature



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

Муравей на ходу делает больше, чем дремлющий бык.



R&D

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

8 development teams

Ideco UTM 15. Апрель 2023 года

- 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

Релиз август 2023 года.



- 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.

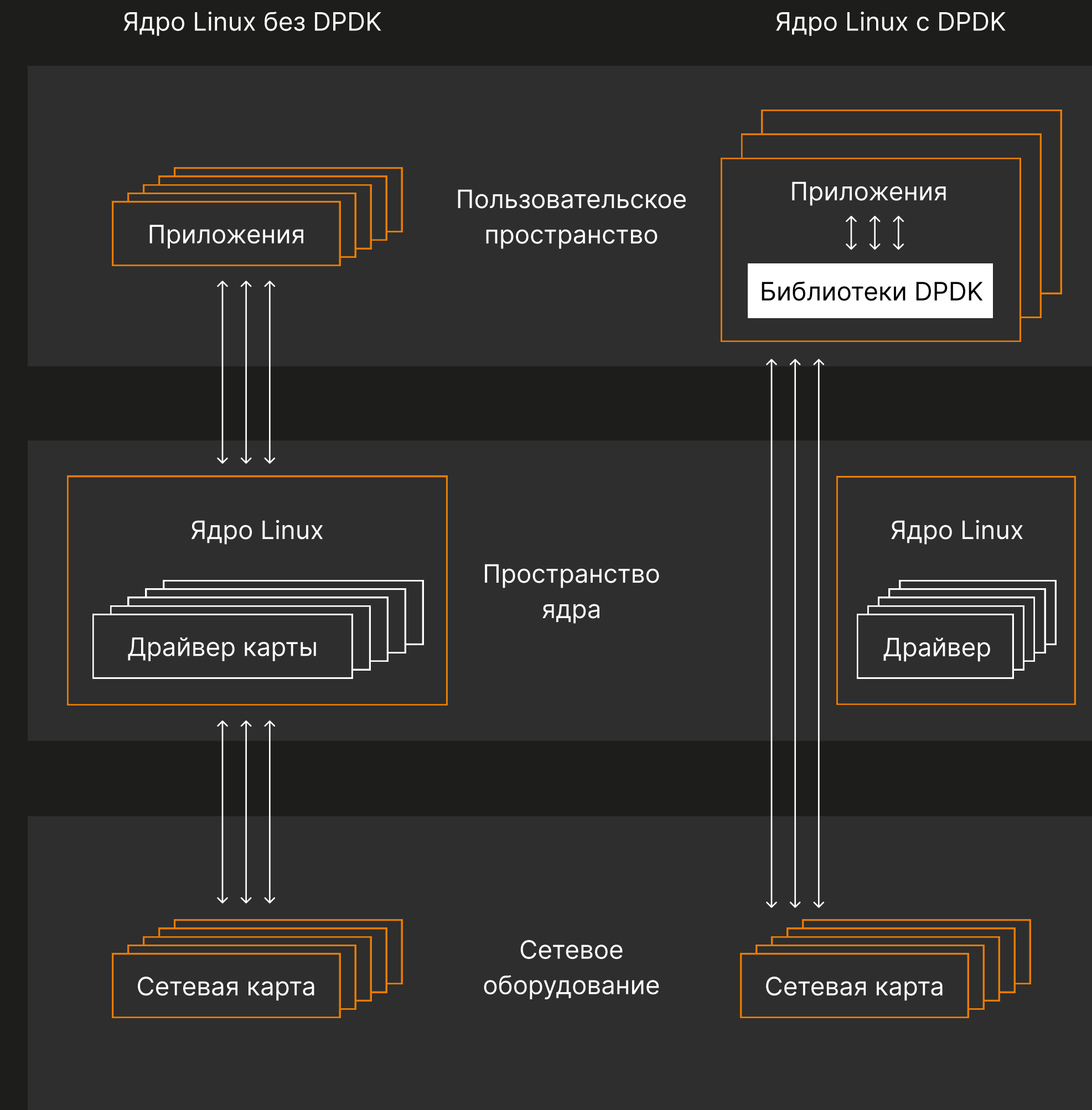


Архитектура Ideco UTM

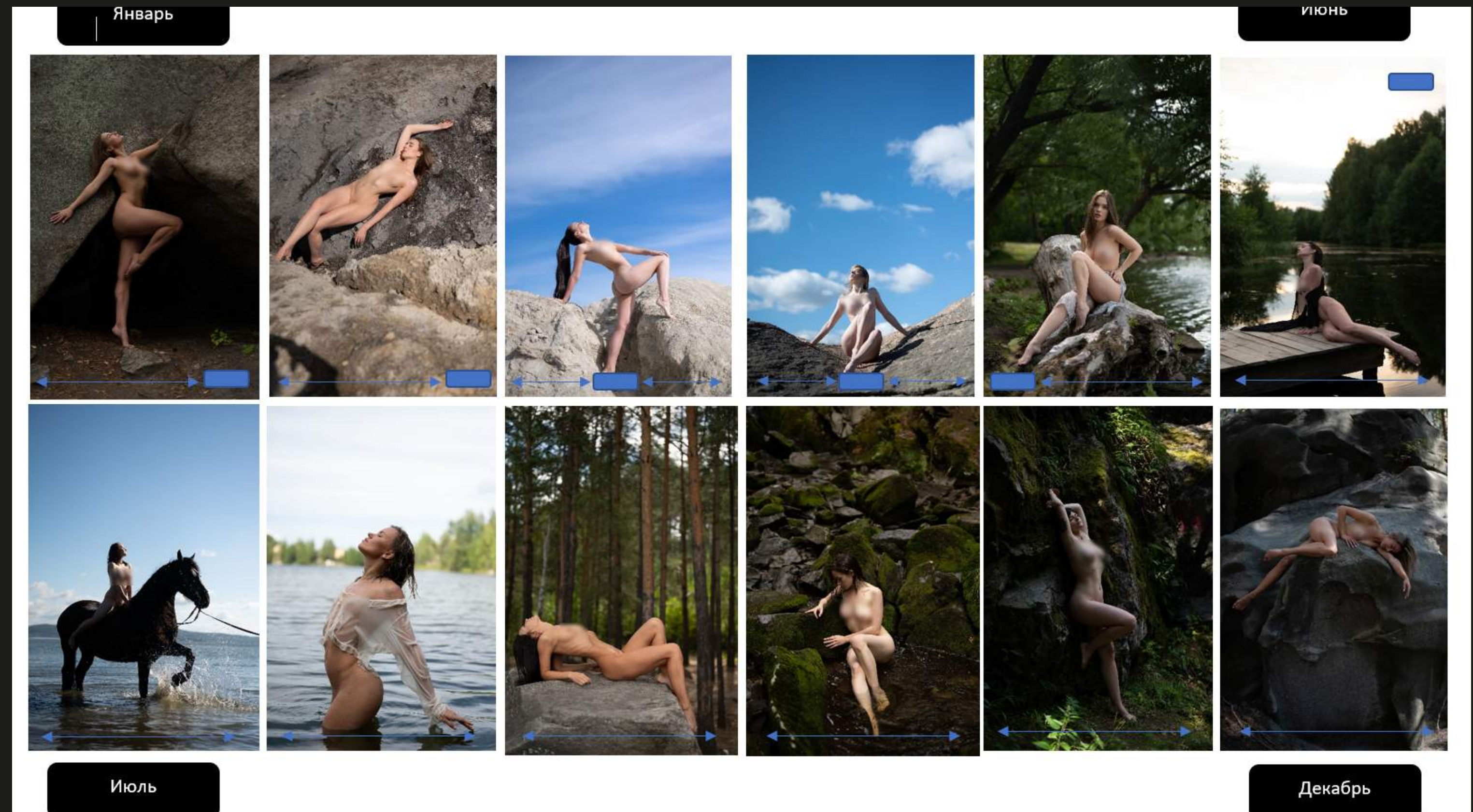


- Linux 5.18;
- сила opensource-модулей;
- микросервисы vs монолит;
- kernel vs userspace (DPDK).

Оптимальный фундамент для быстрого развития enterprise-продукта.



Уникальный календарь Айдеко



Интересный факт: это уже 12-ый календарь от компании Айдеко.



СОЗДАЕМ ВМЕСТЕ

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

t.me/idecoutm - группа

t.me/ideco - канал

my.ideco.ru - скачать

