



ВЫБОР РОССИЙСКОГО NGFW НА ЧТО ОБРАЦАТЬ ВНИМАНИЕ ПРИ МИГРАЦИИ

Александр Карманов

Presale-инженер «Айдеко»



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

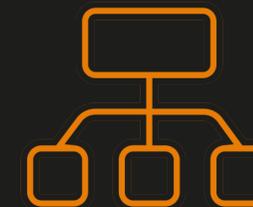
Экономим ваше время на настройке интернет-шлюза и отражения кибератак.



Более 3 000 компаний
используют Ideco UTM



140 человек в команде
S&M / R&D



Лидер по скорости
разработки в отрасли

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

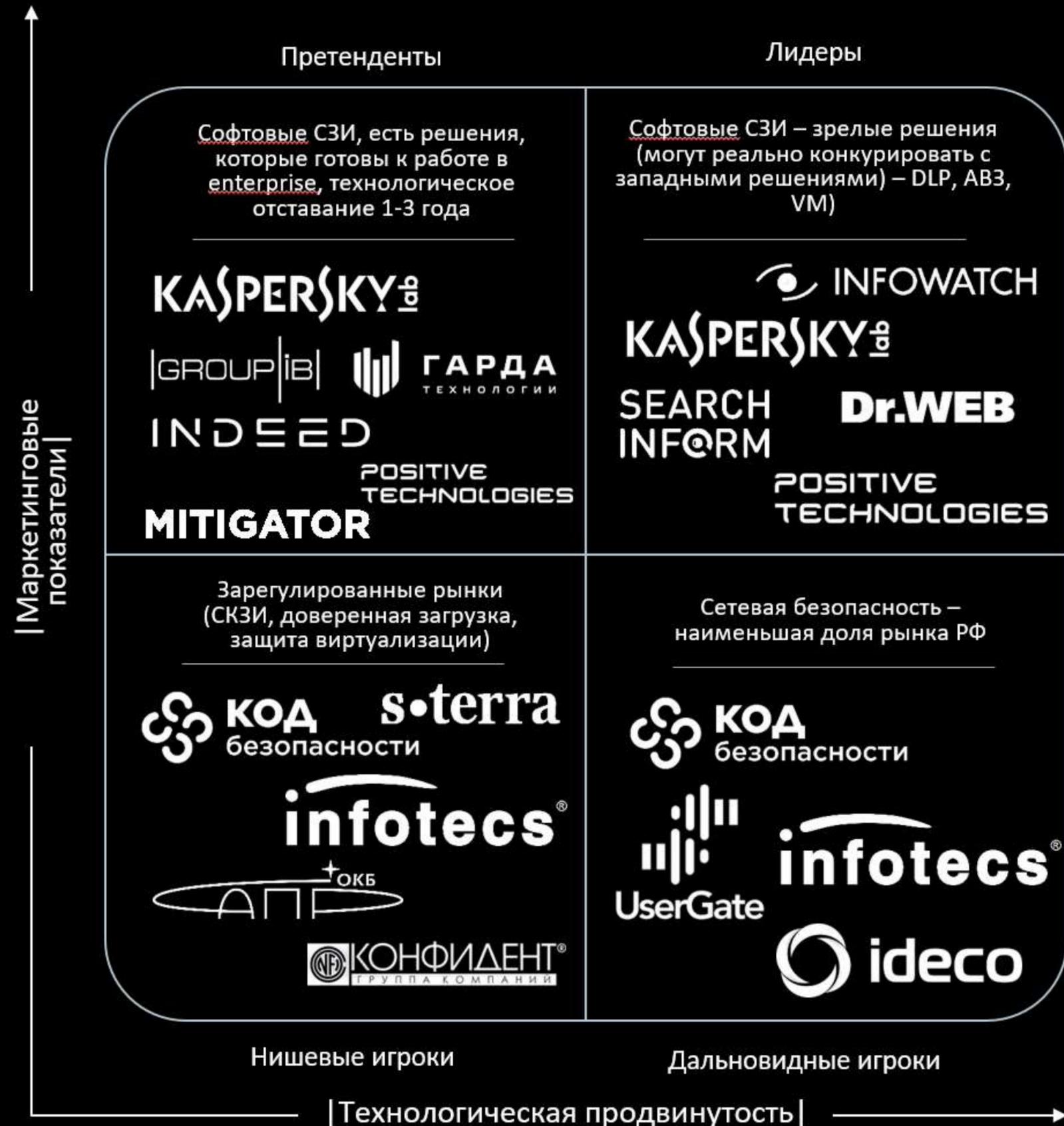
Телеграм бот, Zabbix Агент,
Syslog, SNMP, SIEM
Отчетность по пользователям

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

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"

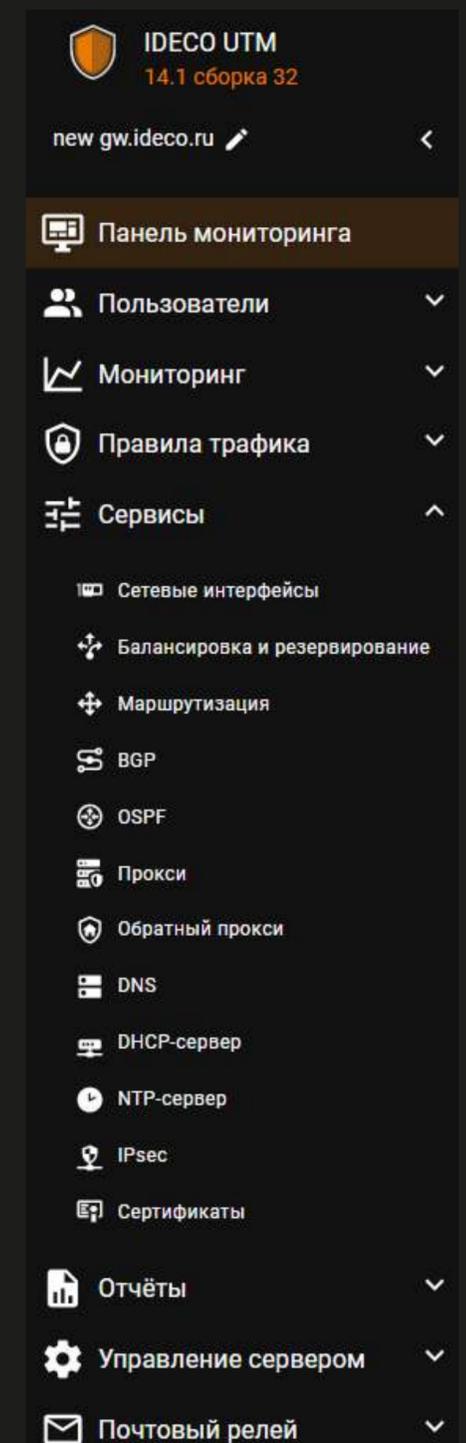
- продукты из реестра соответствуют формальным требованиям к МЭ
- в компании внедрена безопасная разработка (SDL)
- уровень зрелости компании и продукта.

- 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).

The screenshot shows 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.

The screenshot shows the IDECO UTM web interface. On the left is a dark sidebar menu with the following items: IDECO UTM 14.3 сборка 15, UTM01, Панель мониторинга, Пользователи (highlighted), Учётные записи, Авторизация, VPN-подключения (highlighted), Двухфакторная аутентификация, Ideco агент, Active Directory, Обнаружение устройств, Мониторинг, Правила трафика, Сервисы, Отчёты, Управление сервером, and Почтовый релей. The main content area is titled 'VPN-подключения' and shows 'Остановлен' (Stopped) status. It has two tabs: 'Основное' (selected) and 'Фиксированные IP-адреса VPN'. Under 'Основное', there are 'Основные настройки' (Basic settings) with the following fields: 'Сеть для VPN-подключений' (VPN network) set to 10.128.0.0/16, 'Подключение по PPTP' (PPTP connection) unchecked, 'Подключение по PPPoE' (PPPoE connection) unchecked, 'Подключение по IKEv2/IPSec' (IKEv2/IPSec connection) unchecked with 'Домен или IP-адрес' (Domain or IP address) set to lab.rus, 'Подключение по SSTP' (SSTP connection) unchecked with 'Домен' (Domain) set to lab.rus and 'Порт' (Port) set to 1443, and 'Подключение по L2TP/IPSec' (L2TP/IPSec connection) checked with a 'PSK' (Pre-Shared Key) field containing masked characters. There is a 'Сохранить' (Save) button at the bottom.

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.

The screenshot displays the 'Контент-фильтр' (Content Filter) interface in the IDECO UTM management console. The left sidebar shows the navigation menu with 'Правила трафика' (Traffic Rules) selected. The main area shows a table of rules with columns for Name, Applies to, Categories, Action, and Management.

Название	Применяется для	Категории	Действие	Управление
Белый список	Все	Белый список (Польз.)	Разрешить	[Power] [Plus] [Up] [Down] [Edit] [Delete]
Блокируем запрещенные сайты	Все	Черный список (Польз.)	Запретить	[Power] [Plus] [Up] [Down] [Edit] [Delete]
для Марка	Марк Коренберг	Все запросы	Разрешить	[Power] [Plus] [Up] [Down] [Edit] [Delete]
бухгалтерия и hr	Buhgalters, HR, Марина Тябина, Ольга Полуянова	Анонимайзеры, Список Минюста	Разрешить	[Power] [Plus] [Up] [Down] [Edit] [Delete]
marketing	Дмитрий Юсов, Марина Тябина	Маркетинговые услуги, Список Минюста, Социальные сети, Он	Разрешить	[Power] [Plus] [Up] [Down] [Edit] [Delete]
whatsapp	Все	Социальные сети, Чаты, Чаты/Мессенджеры	Разрешить	[Power] [Plus] [Up] [Down] [Edit] [Delete]
Повышаем безопасность сети	Все	Анонимайзеры, Ботнеты, Высокий уровень риска	Запретить	[Power] [Plus] [Up] [Down] [Edit] [Delete]
		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	[Power] [Plus] [Up] [Down] [Edit] [Delete]
		Компьютерные игры, Torrent-файлы		
Избавляемся от неподобающего контента	Все	Геи, лесбиянки и бисексуалы, Казино, лотереи, тотализаторы	Запретить	[Power] [Plus] [Up] [Down] [Edit] [Delete]
		Марихуана, Порнография, Порнография/секс		
		Секс и Зротика		

6. Публикация ресурсов

безопасная публикация



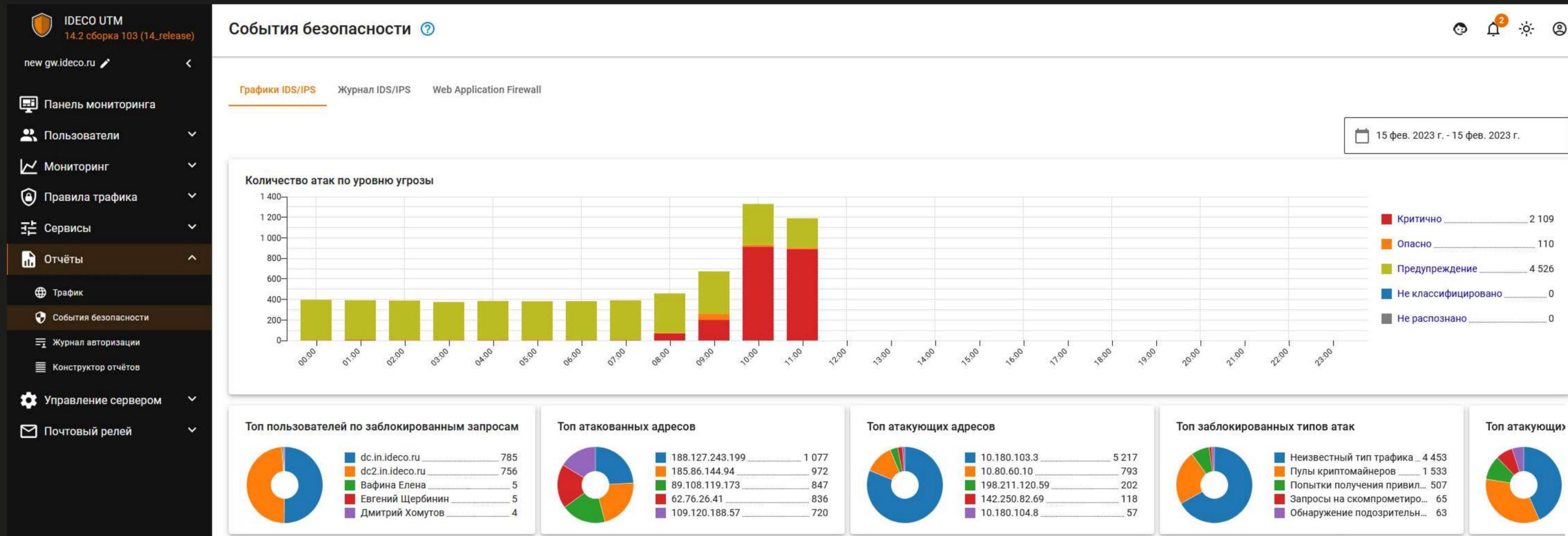
- обратный прокси-сервер с WAF для публикации веб-ресурсов
- почтовый релей для публикации почтового сервера
- защита опубликованных терминальных серверов (RDP).

The screenshot shows the IDECO UTM web interface. The top left header displays 'IDECO UTM 14.2 сборка 103 (14_release)'. Below it is a navigation menu with 'new gw.ideco.ru' and several menu items: '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' menu item is highlighted. The main content area is titled 'Обратный прокси' and contains a 'Создание правила публикации' section. Under 'Основные настройки', there are input fields for 'Запрашиваемый адрес в Интернете', 'Добавить адрес', 'Адрес в локальной сети', and 'URL на который будут перенаправлены запросы'. Under 'Дополнительные настройки', there are two checked checkboxes: 'Перенаправлять HTTP запросы на HTTPS' and 'Web Application Firewall'. There is also a dropdown for 'Тип публикации' set to 'Стандартный' and a text area for 'Комментарий'. At the bottom, there are 'Сохранить' and 'Отмена' buttons.

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



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
 - техподдержка.

The screenshot shows the IDECO UTM management interface. The left sidebar contains a navigation 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 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

А	В	С	Д
Опросник для подбора межсетевого экрана / прокси-сервера			
Характеристика	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	

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
- 3 линии техподдержки.

12. Документация



docs.ideco.dev

- версионирование
- частое обновление
- документирование REST-API.

Ideco UTM v14

Q Search... ^K

Об Ideco UTM

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

Уровень угрозы	Количество
Критично	618
Опасно	3292
Предупреждение	7854
Не классифицировано	0
Не распознано	0

Топ пользователей по заблокированным запросам

Пользователь	Количество
dc2.in.ideco.ru	1495
dc.in.ideco.ru	1172
Антон Ковальчук	1133
Мария Рапу	581
Андрей Карелин	306

Топ атакованных адресов

Адрес	Количество
89.248.236.137	902
89.248.236.16	881
89.248.236.18	866
185.241.193.245	732
89.208.210.197	712

Топ атакующих адресов

Адрес	Количество
10.180.103.3	6279
10.80.60.10	1179
10.180.180.173	1133
10.180.108.9	529
10.180.100.70	306

Топ заблокированных типов атак

Тип атаки	Количество
Неизвестный тип трафика	4780
Телеметрия Windows	2548
Потенциально опасный т...	2123
Определение внешнего IP-а...	574
Попытки получения привил...	559

Топ атакующих стран

Страна	Количество
США	238
Россия	76
Британия	52
Нидерланды	27
Финляндия	10

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 - [Abus	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 - [Abus	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 - [Abus	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 - [Abus	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

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".

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

- 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.

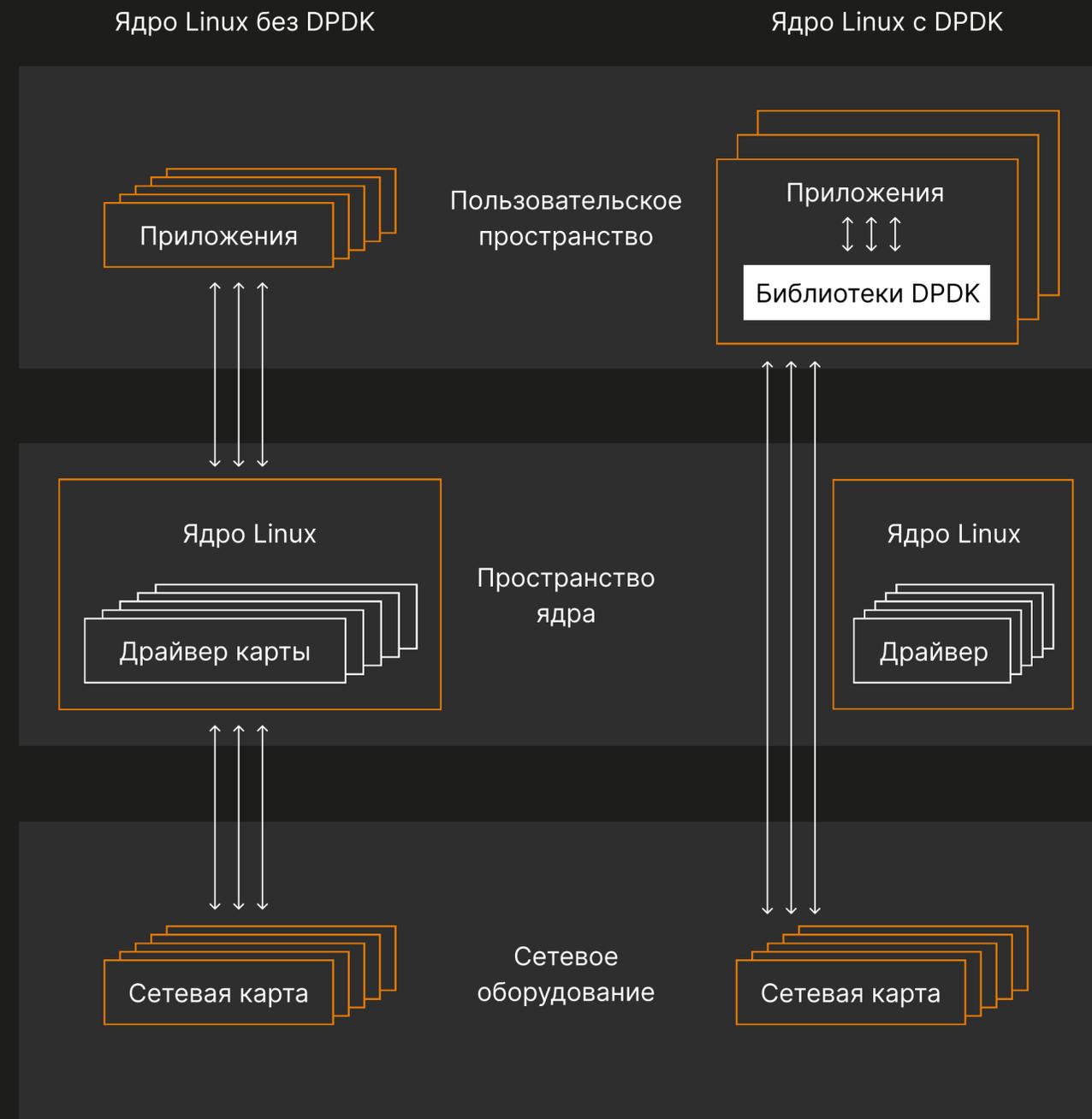
- x10 скорость обработки трафика, полностью «свой» стек обработки трафика, общие правила firewall/DPI/IPS
- x2 скорость обработки веб-трафика, новейший модуль прокси-сервера (от Айдеко)
- высокоскоростной NGFW и технологическое лидерство среди отечественных решений.

Архитектура Ideco UTM



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

Оптимальный фундамент для быстрого развития enterprise-продукта.





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

