

# Отечественное решение для защиты сети и фильтрации трафика

Александр Карманов

Presale-инженер «Айдеко»



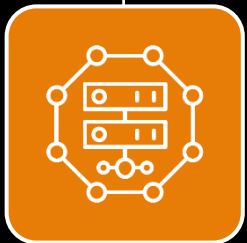
# Айдеко – российский разработчик решений для сетевой безопасности



фильтрация трафика



защита сети



развитие сетевых инфраструктур

## Защищаем сети компаний межсетевым экраном Ideco UTM

с **2005**  
года на рынке ИБ

**4 000**  
компаний используют Ideco UTM

**40 000**  
человек используют VPN-подключения

**2 000**  
бесплатных лицензий для некоммерческого использования

с **2020**  
года сами работаем удаленно



# Ideco UTM

## Задачи:



DPI Фильтрация на 7 уровне модели OSI

15 млн доменов и IP-адресов C&C в нашем BlockList

500 млн URL в обновляемой базе данных

# Соответствие требованиям регулятора

Сертификат ФСТЭК №4503 от 28.12.2021  
г.

Решение входит в реестр  
российского ПО Минцифры РФ

✓ Требования доверия (4)

✓ Требования к МЭ

✓ Требования к СОВ

✓ Профиль защиты МЭ (А четвертого  
класса защиты. ИТ.МЭ.А4.ПЗ)

✓ Профиль защиты МЭ (Б четвертого  
класса защиты. ИТ.МЭ.Б4.ПЗ)

✓ Профили защиты СОВ  
(четвертого класса защиты.  
ИТ.СОВ.С4.ПЗ)

Загрузка интерфейсов, Мбит/с

Локальная сеть ▾ 1 час ▾

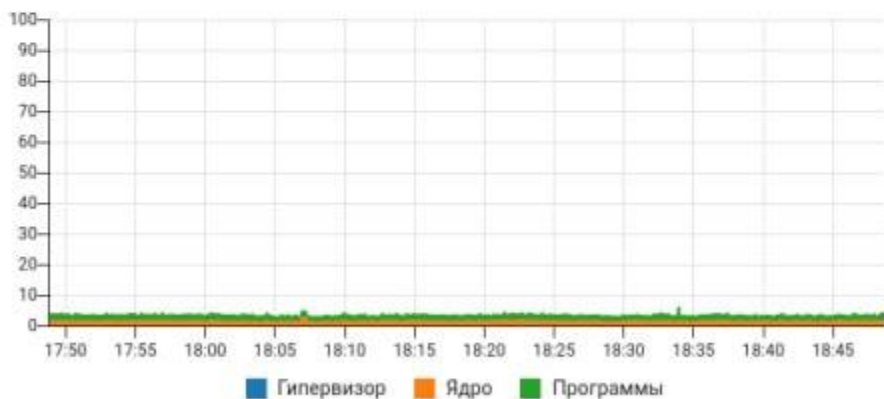


Состояние внешних интерфейсов

Интерфейс	Загруженность (Мбит/с)
К-Телеком	<span style="color: green;">🟢</span> <span style="width: 80%; display: inline-block; border: 1px solid green;"></span> 45,0
Тестовое подключение	<span style="color: grey;">🟡</span>

Загрузка процессора, %

1 час ▾



Время работы сервера 3 дня 7 часов 44 минуты

Топ 5 хостов (входящая скорость), Мбит/с

10.180.100.43	0,97
10.180.108.19	0,15
10.180.180.36	0,13
10.80.100.213	0,09
10.180.100.46	0,06

IPSec (исходящие)

Данные отсутствуют

Занятая оперативная память, ГБ

1 час ▾

























Топ 5 хостов (исходящая скорость), Мбит/с

IPSec (входящие)

Статус	Название
<span style="color: green;">🟢</span>	cloud-da



Поиск

- ▼ Все  
- > Non\_AD   
- > **AD** Servers\_AD 
- ▼ Users\_AD   
- > **AD** Buhgalters 
- ▼ **AD** Developers 
- > **AD** Testing 
-  **AD** Алексей Дегтярев
-  **AD** Анастасия Тураева
-  **AD** Андрей Карелин
-  **AD** Андрей Мокрушин
-  **AD** Артем Щелкунов
-  **AD** Вадим Муравьев
-  **AD** Ваха Ирзаханов
-  **AD** Виктор Гуров
-  **AD** Владимир Ивченко
-  **AD** Владимир Папченко

## Основное

Название

Все

Запретить

Разрешить

Сохранить

# Пользователи

# Авторизация

- ✓ IP, MAC, IP+MAC, подсеть
- ✓ WEB
- ✓ Интеграция с AD: Kerberos, NTLM, security log
- ✓ Агент
- ✓ Обнаружение устройств

The screenshot shows the IDECO UTM web interface. The top left corner displays the IDECO UTM logo and version information: "14.2 сборка 155". The main navigation menu on the left includes: "Панель мониторинга", "Пользователи", "Учётные записи", "Авторизация", "VPN-подключения", "2FA Двухфакторная аутентификация", "Ideco агент", "Active Directory", and "Обнаружение устройств". The "Пользователи" menu item is highlighted.

The main content area is titled "Авторизация" and has a sub-tab "IP и MAC авторизация" selected. Below the tabs, there are control buttons: "+ Добавить", "Столбцы", "Фильтры", and "Высота строки".

The main content displays a table with the following columns: "IP-адрес", "MAC-адрес", and "Пользователь". The table contains the following data rows:

IP-адрес	MAC-адрес	Пользователь
10.180.105.8	—	work01
10.180.108.52	—	Руслан Никифоров
10.180.100.246	—	wifi-500-openspace
10.180.180.173	—	Антон Ковальчук
10.180.100.116	—	TV
10.180.180.174	—	Руслан Ханов

# Файрвол

IDECO UTM  
14.2 сборка 155

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

Файрвол Работает

Счетчик срабатываний

FORWARD DNAT (перенаправление портов) **INPUT** SNAT Логирование

Входящий трафик к службам сервера Ideco UTM

+ Добавить Отображать названия объектов Столбцы Фильтры Высота строки Поиск...

Протокол	Источник	Назначение	Порты назначения	Действие	Счетчик срабатываний	Комментарий	Управление
* Любой	Россия	* Любой	* Любой	Разрешить	0		⏻ ⚙️ ↑ ↓ ✎ 📄 🗑️
* Любой	* Любой	* Любой	* Любой	Запретить			⏻ ⚙️ ↑ ↓ ✎ 📄 🗑️



# Контроль приложений

IDECO UTM  
14.2 сборка 155

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

Контроль приложений Работает

+ Добавить Столбцы Фильтры Высота строки

Поиск...

Название	Применяется для	Протоколы	Действие	Управление
Разрешить тестировщикам торренты	Андрей Карелин Тимур Нураев Дмитрий Юсов Дмитрий Мухаметов Антон Ковальчук Руслан Ханов Андрей Мокрушин Дмитрий Ахметов	Bittorrent Doh_dot	Разрешить	🔌 ⚙️ ↑ ↓ ✎ 🗑️
разрешить TeamView	Андрей Моргунов	Teamviewer	Разрешить	🔌 ⚙️ ↑ ↓ ✎ 🗑️
Даниил	Даниил Овчинников	Rdp	Разрешить	🔌 ⚙️ ↑ ↓ ✎ 🗑️
whatsapp	Все	Whatsapp Whatsappfiles Whatsappcall	Разрешить	🔌 ⚙️ ↑ ↓ ✎ 🗑️
Программы удаленного доступа	Все	Teamviewer Anydesk	Запретить	🔌 ⚙️ ↑ ↓ ✎ 🗑️
TOR и торренты	Все	Bittorrent Tor Edonkey	Запретить	🔌 ⚙️ ↑ ↓ ✎ 🗑️
Запрет шифрованных DNS-запросов	Все	Doh_dot Dnscrypt	Запретить	🔌 ⚙️ ↑ ↓ ✎ 🗑️
Игры	Все	Steam Halflife2 Worldofkungfu World	Запретить	🔌 ⚙️ ↑ ↓ ✎ 🗑️
Криптомайнеры	Все	Mining	Запретить	🔌 ⚙️ ↑ ↓ ✎ 🗑️

# Контент-фильтр

IDECO UTM  
14.2 сборка 155

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

## Контент-фильтр

Правила Пользовательские категории Настройки

URL для категоризации

Отображать названия объектов

Название	Применяется для	Категории	Действие	Управление
Белый список	Все	Белый список (Польз.)	Разрешить	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Блокируем запрещенные сайты	Все	Черный список (Польз.)	Запретить	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
для Марка	Марк Коренберг	Все запросы	Разрешить	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
бухгалтерия и hr	Buhgalters HR Марина Тябина	Анонимайзеры Список Минюста	Разрешить	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
marketing	Дмитрий Юсов Марина Тябина	Маркетинговые услуги Список Минюст	Разрешить	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
whatsapp	Все	Социальные сети Чаты Чаты/Мессе	Разрешить	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Повышаем безопасность сети	Все	Анонимайзеры Ботнеты Высокий ур	Запретить	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Повышаем скорость интернета	Все	Онлайн-реклама и баннеры Торрент-три	Запретить	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Избавляемся от неподобающего контента	Все	Геи, лесбиянки и бисексуалы Казино, л	Запретить	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

# Контент-фильтр

- ✓ Технологический партнер: российская компания SkyDNS
- ✓ Более 100 миллионов доменов и 500 миллионов URL в базе
- ✓ SNI / SSL BUMP
- ✓ Возможность создания своих списков
- ✓ Возможность блокировки приложений (80 и 443)
- ✓ Безопасный поиск
- ✓ Антивирусная проверка WEB трафика
- ✓ Блокировка quic/http3
- ✓ Гибкая настройка политик
- ✓ Обновление сигнатур 2 раза в день с серверов в РФ

# Предотвращение вторжений

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

## Предотвращение вторжений

Работает

Журнал | Правила | Исключения из правил | Настройки

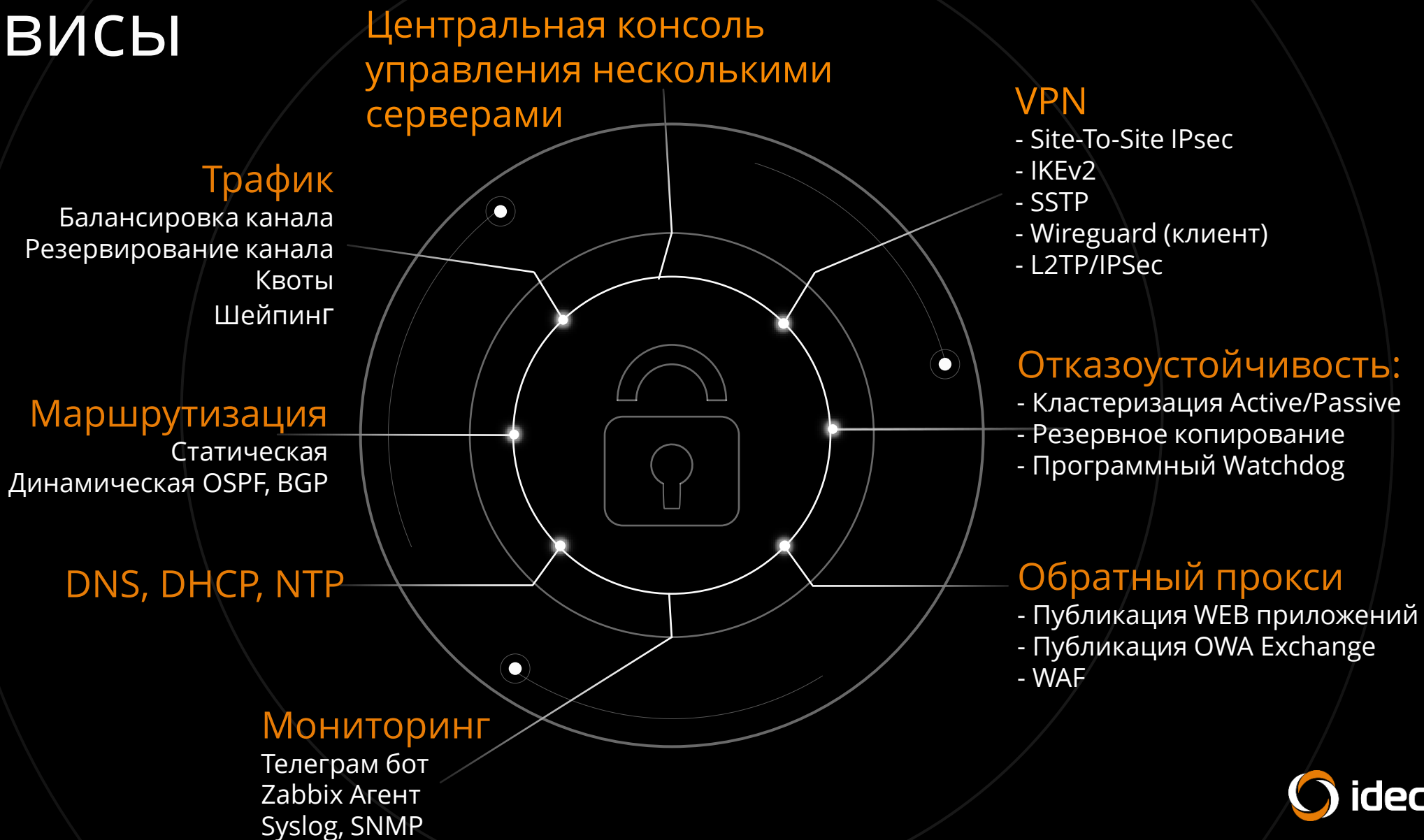
Остановить | Скачать CSV | Столбцы | Фильтры | Высота строки

Дата и время	Результат ...	Уровень угрозы ↑	Наименование правила	Событие безопасности	ID	Про...	Источник	Пользо...	Местоположен...	Назначение	Пользовате
5 мар. 2023 г., 15:22:51	×	Критично	ET POLICY Windows 98 U	Запросы на скомпромет	2007695	TCP	10.180.104.8:58149			42.121.236.55:80	
1 мар. 2023 г., 15:36:48	×	Критично	ET INFO Session Traversa	Попытки получения при	2016150	UDP	139.59.84.212:3478	Индия	10.180.180.36:22000		Андрей Кар
27 фев. 2023 г., 22:40:29	×	Критично	ET INFO Session Traversa	Попытки получения при	2016150	UDP	198.211.120.59:347	Нидерланды	10.180.180.36:22000		Андрей Кар
25 фев. 2023 г., 11:03:16	×	Критично	ET POLICY Windows 98 U	Запросы на скомпромет	2007695	TCP	10.180.104.8:58081			104.21.42.217:80	
24 фев. 2023 г., 23:45:54	×	Критично	ET POLICY Unsupported/f	Запросы на скомпромет	2016870	TCP	10.180.104.8:58059			104.21.42.217:80	
5 мар. 2023 г., 7:11:15	×	Критично	ET POLICY Unsupported/f	Запросы на скомпромет	2016870	TCP	10.180.104.8:58133			42.121.236.55:80	
1 мар. 2023 г., 15:36:48	×	Критично	ET INFO Session Traversa	Попытки получения при	2016150	UDP	139.59.84.212:3478	Индия	10.180.180.36:22000		Андрей Кар
27 фев. 2023 г., 12:52:07	×	Критично	ET INFO Session Traversa	Попытки получения при	2016150	UDP	198.211.120.59:347	Нидерланды	10.180.180.36:22000		Андрей Кар

# Предотвращение вторжений

- ✓ 25 000 сигнатур в 60 категориях правил
- ✓ Обновление раз в 4 часа с серверов в РФ
- ✓ Блокировка по Geo-IP
- ✓ Блокировка обновлений ПО и устаревшего ПО
- ✓ Экспорт журнала в CSV

# Сервисы



# Мониторинг трафика

IDECO UTM  
14.2 сборка 155

new gw.ideco.ru

Панель мониторинга

Пользователи

Мониторинг

Авторизованные пользователи

VPN пользователи

Журналы

Графики загрузки

Монитор трафика

Telegram-бот

SNMP

Syslog

Zabbix агент

Правила трафика

Сервисы

Отчёты

Управление сервером

Почтовый релей

## Монитор трафика

По узлам локальной сети По приложениям

Столбцы Высота строки

Приложение	Сессии	Вх. скорость КБит/с	Исх. скорость КБит/с	Вх. пакеты Kpps	Исх. пакеты Kpps
DNS	574	0,00	0,00	0,00	0,00
IMAPS	149	274,40	32,99	0,02	0,00
Неизвестно	96	4,00	17,68	0,00	0,01
Zabbix	70	0,00	0,00	0,00	0,00
NTP	53	0,00	0,00	0,00	0,00
TLS.GoogleServices	49	0,34	0,31	0,00	0,00
DNS.Steam	34	0,00	0,00	0,00	0,00
LDAP	27	0,00	0,00	0,00	0,00
DNS.Google	23	0,00	0,00	0,00	0,00
SIP	22	4,31	6,20	0,00	0,00
Xiaomi	15	0,00	0,00	0,00	0,00
TLS	12	8,43	3,71	0,00	0,00
DNS.Yandex	11	0,00	0,00	0,00	0,00
QUIC.Google	8	0,19	0,20	0,00	0,00
DNS.GoogleServices	7	0,00	0,00	0,00	0,00
WhatsApp	6	0,00	0,00	0,00	0,00
RTP	5	0,00	0,00	0,00	0,00
DNS.AmazonAWS	4	0,00	0,00	0,00	0,00

Всего ст...



# События безопасности

IDECO UTM  
14.2 сборка 155

new gw.ideco.ru

Панель мониторинга

Пользователи

Мониторинг

Правила трафика

Сервисы

Отчёты

Трафик

События безопасности

Журнал авторизации

Конструктор отчётов

Управление сервером

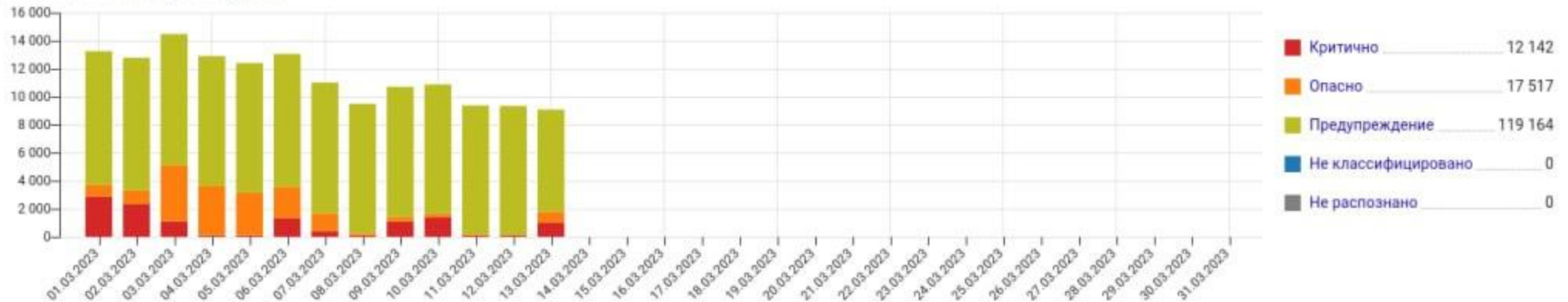
Почтовый релей

## События безопасности

Графики IDS/IPS Журнал IDS/IPS Web Application Firewall

1 мар. 2023 г. - 31 мар. 2023 г.

Количество атак по уровню угрозы



Топ пользователей по заблокированным запросам



Топ атакованных адресов



Топ атакующих адресов



Топ заблокиро





# Отчетность в различных разрезах

IDECO UTM  
14.2 сборка 155

new.gw.ideco.ru

- Панель мониторинга
- Пользователи
- Мониторинг
- Правила трафика
- Сервисы
- Отчёты**
- Трафик
- События безопасности
- Журнал авторизации
- Конструктор отчетов
- Управление сервером
- Почтовый релей

## Трафик

Топ пользователей (МБ)

SRV-MARS	22 024,84
Дмитрий Хомутов	3 959,01
Андрей Моргунов	3 344,89
Арман Дусенов	3 341,08
Олег Пахомов	2 767,97
Остальное	47 880,73

Топ групп (МБ)

SALES	33 724,13
Servers_AD	22 325,92
Developers	4 889,27
Support	4 767,26
Management	3 959,01
Остальное	13 652,93

Топ категорий (МБ)

Категория	Общий (МБ)
Технологии (в целом)	36 168,09
Все некатегоризированные запросы	7 918,44
Прямое обращение по IP	6 217,60
Видео для прослушивания и скачивания	3 503,48
Белый список	3 436,65

Топ сайтов (МБ)

Сайт	Категория	Общий (МБ)
backup-1c-postgres.storage.ya...	Технологии (в целом)	22 018,42
storage.yandexcloud.net	Технологии (в целом)	4 123,67
91.105.192.100	Все некатегоризированные з...	2 962,50
mcs-vm.ideco.ru	Белый список, Технологии (в ...	1 989,56
149.154.167.222	Все некатегоризированные з...	1 045,35

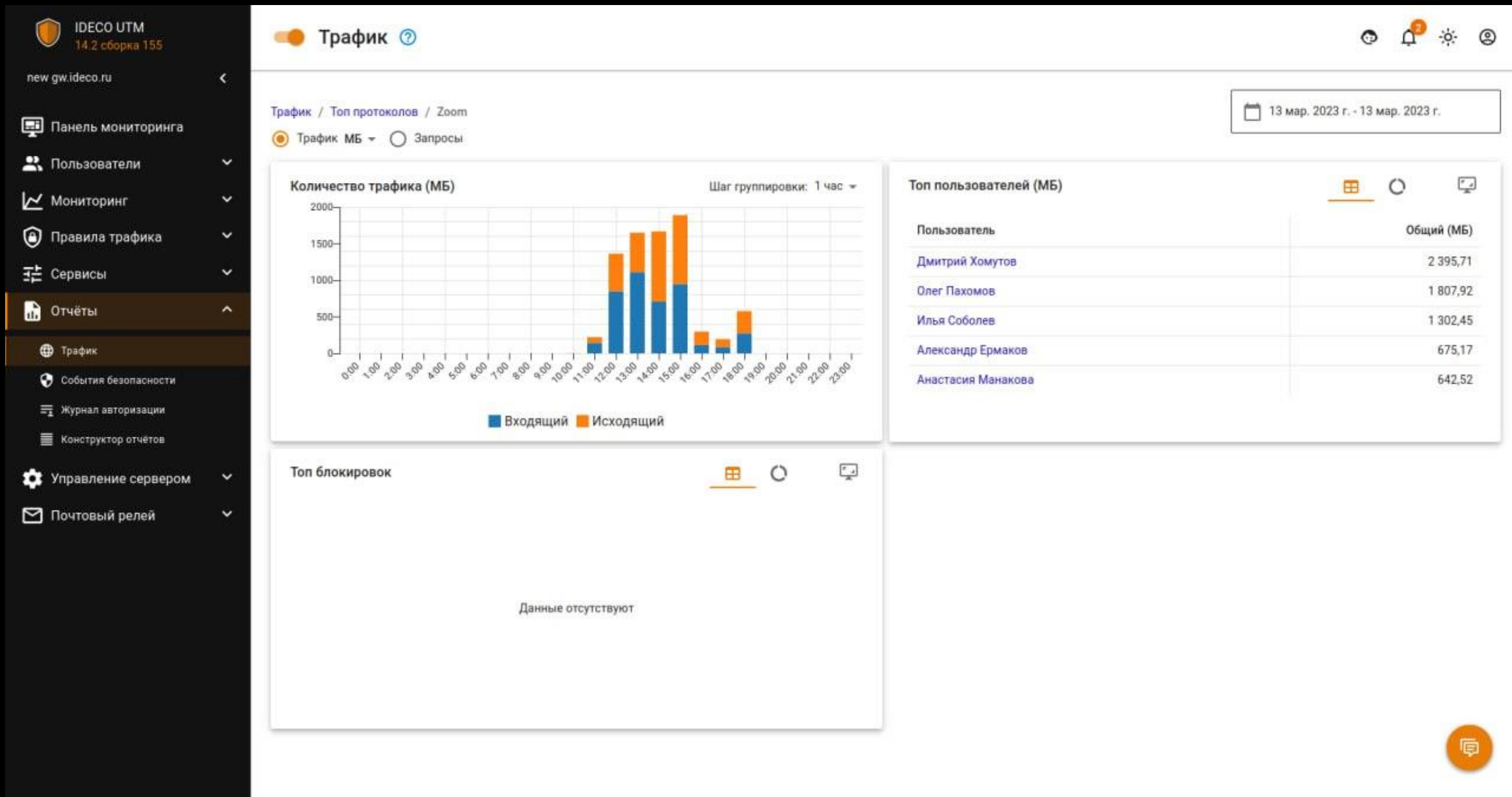
Топ протоколов (МБ)

Протокол	Общий (МБ)
Zoom	7 865,52
IMAPS	3 340,28

Топ заблокированных сайтов

Сайт	Категория	Количество блокировок
www.google-analytics.com	Онлайн-реклама и баннеры	
www.googletagmanager.com	Онлайн-реклама и баннеры	578

# Пример детализации по протоколу



# Почтовый сервер/релей

Основной почтовый домен  
dkim-mx.test.ideco.dev

Имя хоста почтового сервера  
dkim-mx.test.ideco.dev

Используется как HELO почтового сервера

Дополнительные почтовые домены

Добавить домен

Relay-домены  
dkim.test.ideco.dev|10.180.180.229

Почтовые домены в локальной сети, для которых будут пересылаться письма извне. Формат:  
domain.name|192.168.1.1 или domain.name|relay.domain

Добавить Relay-домен

Сохранить

- IMAP(S) (143 STARTT
- POP3(S) (110 STARTT
- Web-почта

Диск для хранения почты

Для хранения почтовых ящи  
отдельный жесткий диск

Подключить

# Переход с конкурентных решений

- ✓ Kerio Control
- ✓ Устаревшие решения под Windows: Microsoft ISA/TMG, UG Proxy and Firewall, Traffic Inspector
- ✓ Различные российские решения
- ✓ L3 FW
- ✓ Cisco ASA/WSA, Checkpoint, Fortinet – здесь сложнее, но активно догоняем
- ✓ Переход с самописных шлюзовых и прокси решений на Linux/FreeBSD

# Customer success

## Гибкая разработка

Моментальная реакция на новые вызовы и угрозы  
Road-map по задачам пользователей

## Защита сети «из коробки»

Преднастроенные правила фильтрации, IPS, FW

## Шай-тек (Shy-tech)

Умные технологии для интуитивно понятных решений



## Многоканальная техподдержка

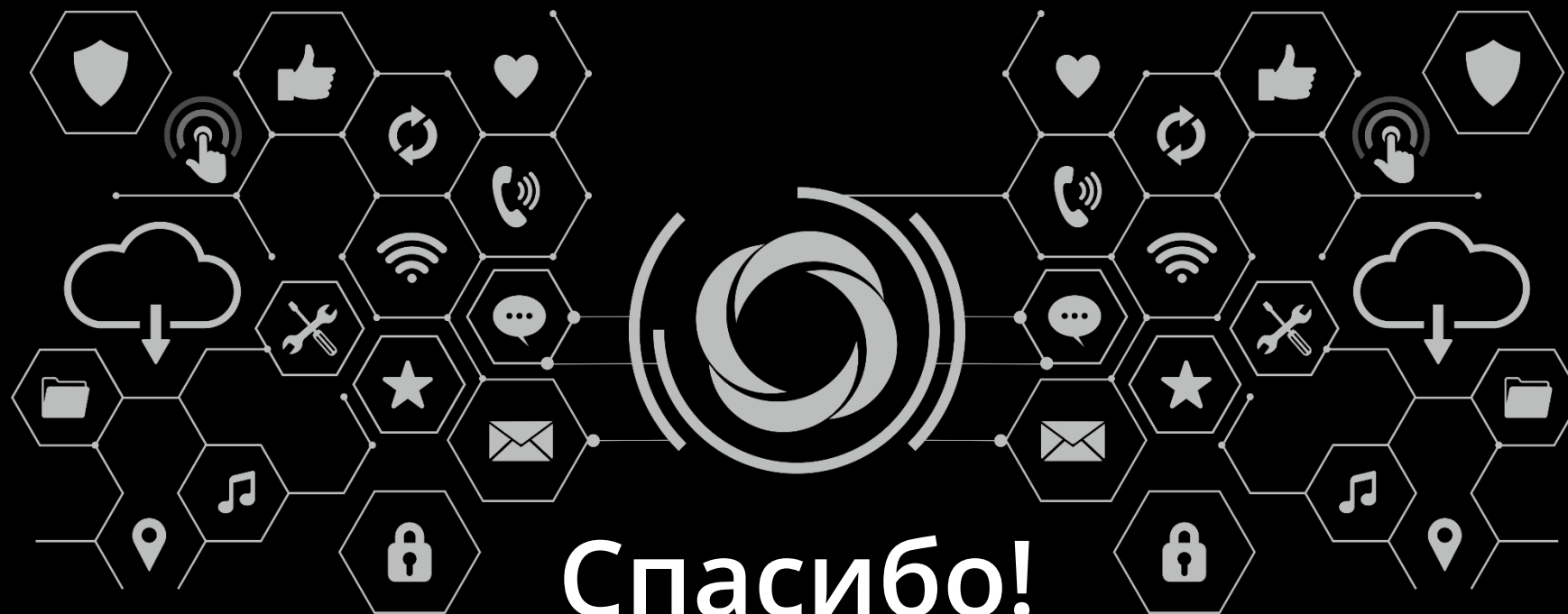
- портал поддержки help.ideco.ru
- электронная почта
- телефон
- Telegram
- чат в продукте

## Customer success


Выделенный менеджер для каждого  
Фокус на долгосрочное партнерство  
CustDev и проблемные интервью  
Близко к community

## Presale


Поддержка и консультации на этапе тестирования и внедрения  
Решения для нестандартных кейсов



 @rasmusowlson

 a.karmanov@ideco.ru



 t.me/idecoutm

 @ideco