



# Заккрытие уязвимостей и атак при помощи IPS от Ideco

**Алексей Киселев**  
Presale-инженер

## О компании Ideco



Ideco — российский разработчик решений для защиты корпоративных сетей от кибератак и фильтрации трафика.

2005 год основания

5500+ компаний-заказчиков

250+ сотрудников в команде

3 мажорных релиза каждый год

2025

Российская  
действительность в ИБ

## Актуальные угрозы и вопросы, с которыми столкнулись организации

Увеличение количества атак на российский сегмент

Уязвимости нулевого дня

Уязвимости ПО

Российские решения не могут полностью заменить ушедшие решения по скорости обработки трафика и функциональности

Выполнение рекомендаций регуляторов (гос организации , КИИ)

## Уязвимости вендоров новые каналы подготовки и проведения атак

Вендоры не предоставляют обновлений для закрытия уязвимостей для российских организаций

«Серые» каналы обновлений могут использоваться для подготовки и проведения атак

Техподдержка прекращена

Отозвали сертификаты ФСТЭК

# Решение Ideco NGFW



Защита нулевого дня

Быстрое развитие продукта до 3 релизов в год , минорные обновление версий постоянная проверка кода при выпуске версий, регулярные выпуски сертифицированных версий решений

Сигнатуры Касперского

# Модуль обнаружения и предотвращения атак



The screenshot displays the IDECO NGFW interface for intrusion prevention configuration. The left sidebar shows the navigation menu with 'Правила трафика' (Traffic Rules) selected. The main content area is divided into two panels.

**Top Panel: Предотвращение вторжений (Intrusion Prevention)**

- Status: **Работает** (Working)
- Module 'suricata' is running.
- Module 'suricata-event-syner' is running.
- Database update: **около 13 часов назад** (around 13 hours ago).
- Status: **Обновление не требуется** (Update not required).
- Buttons: **Проверить обновление баз** (Check for database updates), **Добавить** (Add), **Фильтры** (Filters), **Отображение** (Display).

**Bottom Panel: Предотвращение вторжений (Intrusion Prevention)**

- Database update: **около 13 часов назад** (around 13 hours ago).
- Status: **Обновление не требуется** (Update not required).
- Section: **Сети, защищённые от вторжений.** (Networks protected from intrusions.)
- Subnet list:
  - 192.168.0.0/16
  - 10.0.0.0/8

**Signature List Table:**

Название	Тактика	Кол-во сигнатур	Источник правила	Управление
Попытки получения привилегий администратора	Закрепление +4	1617	Стандартные правила	🔗
Попытки проведения DoS-атак	Деструктивное воздействие +1	88	Стандартные правила	🔗
Попытки получения системных файлов	Изучение +4	273	Стандартные правила	🔗
Попытки получения привилегий пользователя	Закрепление +5	794	Стандартные правила	🔗
Потенциально опасный трафик	Деструктивное воздействие +7	5487	Стандартные правила	🔗
Пулы криптомайнеров	Деструктивное воздействие +3	184	Стандартные правила	🔗
Управление вредоносным ПО	Деструктивное воздействие +5	3348	Стандартные правила	🔗
Обнаружение успешных краж учетных данных	Организация управления +3	1473	Стандартные правила	🔗
Попытки авторизации с логином и паролем по-умолчанию	Получение учетных данных	5	Стандартные правила	🔗
Обнаружение DoS-атак	Деструктивное воздействие +1	15	Стандартные правила	🔗
Использование DNS трафика для управления вредоносным ПО	ТА0037 +6	4723	Стандартные правила	🔗
Эксплойты	Выполнение +3	817	Стандартные правила	🔗
Определение внешнего IP-адреса	Первоначальный доступ +1	144	Стандартные правила	🔗
Расширенная база правил (от Лаборатории Касперского)	Выполнение +11	5675	Правила IPS от Лаборатории Касперского	🔗
Анонимайзеры	Предотвращение обнаружения	183	Стандартные правила	🔗
DNS поверх HTTPS	Получение учетных данных	8516	Стандартные правила	🔗
GeoIP Страны Восточной Европы	Предотвращение обнаружения	22	Стандартные правила	🔗
Чёрный список IP-адресов	Организация управления	1888	Стандартные правила	🔗
SSL-сертификаты используемые вредоносным ПО и ботнетами	Организация управления	6265	Стандартные правила	🔗
Телеметрия Windows	Разведка	786	Стандартные правила	🔗
Обнаружение подозрительной сетевой активности	Изучение +6	3488	Стандартные правила	🔗
Блокирование атак	Закрепление +3	976	Стандартные правила	🔗

# Расширенные сигнатуры IPS



Возможность использования расширенной базы правил предотвращения вторжений от Лаборатории Касперского.

Требует дополнительного лицензирования.

The screenshot displays the IDECO NGFW management interface. The top navigation bar shows the device name 'Ngfw18' and the status 'Beta'. The left sidebar contains various configuration categories, with 'Правила трафика' (Traffic Rules) selected. The main content area is titled 'Предотвращение вторжений' (Intrusion Prevention) and shows the status of the 'suricata' and 'suricata-event-syncer' modules. Below this, the 'Список IPS сигнатур' (IPS Signature List) is displayed, showing the 'Расширенная база правил (от Лаборатории Касперского)' (Expanded rule base (from Kaspersky Lab)).

Действие	Тактика	Название	Протокол	Источник	Порт	Назначение	Порт	SID
drop	Изучение	HackTool.ReconScan.TCP...	TCP	any	\$HTTP_PORTS	any	\$HTTP_PORTS	30278764
drop	Изучение	HackTool.ReconScan.TCP...	TCP	any	any	any	\$HTTP_PORTS	30278885
drop	Изучение	HackTool.ReconScan.TCP...	TCP	any	any	any	\$HTTP_PORTS	30278886
drop	Изучение	HackTool.ReconScan.TCP...	TCP	any	any	any	\$HTTP_PORTS	30278887
drop	Изучение	HackTool.ReconScan.TCP...	TCP	any	any	\$HOME_NET	any	30278888
drop	Изучение	HackTool.ReconScan.UID...	UDP	any	any	\$HOME_NET	any	30278889
drop	Изучение	HackTool.ReconScan.TCP...	TCP	any	any	\$HOME_NET	\$HTTP_PORTS	30278890
drop	Изучение	HackTool.ReconScan.TCP...	TCP	any	any	any	\$HTTP_PORTS	30278891
drop	Изучение	HackTool.ReconScan.TCP...	TCP	any	any	\$HOME_NET	\$HTTP_PORTS	30278892
drop	Изучение	HackTool.ReconScan.TF...	UDP	any	any	\$HOME_NET	69	30278895
drop	Изучение	HackTool.ReconScan.TCP...	TCP	any	any	\$HOME_NET	\$HTTP_PORTS	30278896
drop	Изучение	HackTool.Nmap.HTTPSe...	TCP	any	any	any	any	30278899
drop	Изучение	HackTool.ReconScan.TCP...	TCP	any	any	any	\$HTTP_PORTS	30278900
drop	Изучение	HackTool.ReconScan.TCP...	TCP	any	any	any	\$HTTP_PORTS	30278901



**Предотвращение вторжений**

Название: Nfw18

Фильтры: Первоначальный до... +14

- Группа сигнатур - 43
- Действие - 6
- Источник правила - 3
- Протокол - 15
- Тактики по MITRE ATT&CK - 15
- Уровень угрозы - 7
- Цель - 2

Группа сигнатур	Источник правила	SID	Цель	Действие	Уровень угрозы	Последнее обновление	Протокол
Анонимайзеры	Стандартные правила	1003159	-	Блокировать	Незначительный	-	DNS
Анонимайзеры	Стандартные правила	1003160	Сервер	Блокировать	Незначительный	-	HTTP
dostup-rutracker	Предотвращение обнаружения	1003164	Сервер	Блокировать	Незначительный	-	TLS
dostup-rutracker	Предотвращение обнаружения	1003165	Сервер	Блокировать	Незначительный	-	TLS
ZenMate DNS	Предотвращение обнаружения	1003166	-	Блокировать	Незначительный	-	DNS
ZenMate DNS	Предотвращение обнаружения	1003167	-	Блокировать	Незначительный	-	TLS
ZenMate API	Предотвращение обнаружения	1003168	-	Блокировать	Незначительный	-	DNS
ZenMate API	Предотвращение обнаружения	1003169	-	Блокировать	Незначительный	-	TLS
ZenMate proxy	Предотвращение обнаружения	1003170	-	Блокировать	Незначительный	-	DNS
ZenMate proxy	Предотвращение обнаружения	1003171	-	Блокировать	Незначительный	-	TLS
Stealthly	Предотвращение обнаружения	1003172	-	Блокировать	Незначительный	-	DNS
Stealthly	Предотвращение обнаружения	1003173	-	Блокировать	Незначительный	-	HTTP
SetupVPN	Предотвращение обнаружения	1003178	-	Блокировать	Незначительный	-	DNS
SetupVPN	Предотвращение обнаружения	1003179	-	Блокировать	Незначительный	-	TLS
Anonymizer detected	Предотвращение обнаружения	1003180	-	Блокировать	Незначительный	-	DNS

- настройка профилей для организации защиты

- отчеты о выявленных и заблокированных угрозах

IDECO NGFW 19.0.465 Бета  
 Название: Ngfw18  
 Панель мониторинга  
 Пользователи  
 Мониторинг  
 Правила трафика  
 Профили безопасности  
 Сервисы  
 Отчёты и журналы  
 Трафик  
 Системный журнал  
 Журнал веб-трафика  
 Журнал трафика  
 События безопасности  
 Действия администраторов  
 Авторизация администраторов  
 Журнал аутентификации  
 Журнал аутентификации ЛК  
 Конструктор отчётов  
 Syslog  
 Управление сервером  
 Почтовый релей

### События безопасности

ГРАФИКИ IPS | **ЖУРНАЛ IPS** | WEB APPLICATION FIREWALL  
 1 янв. 2025 г., 0:00 – 7 фев. 2025 г., 23:59  
 Фильтры | Отображение | Скачать CSV

Дата и время	Результат	Уровень угрозы	Название правила	Категория правил	ID сигнатуры	Профиль безопасности	IP-адрес	Порт	Состояние	Местоположение (источник)
13 янв. 2025 г., 10:45:09	✗	Критичный	HackTool.Nmap.TCP.ServerRequest	Обнаружение активности тро...	65158634	Профиль IPS рекомендуемый, основной, Профиль IPS блок anydesk	172.16.100.45	59310	—	—
13 янв. 2025 г., 10:45:09	✗	Критичный	HackTool.Nmap.TCP.ServerRequest	Обнаружение активности тро...	41560233					
13 янв. 2025 г., 9:16:39	✗	Критичный	HackTool.Nmap.TCP.ServerRequest	Обнаружение активности тро...	65158634					
13 янв. 2025 г., 9:16:39	✗	Критичный	HackTool.Nmap.TCP.ServerRequest	Обнаружение активности тро...	41560233					
13 янв. 2025 г., 9:15:19	✗	Критичный	HackTool.Nmap.TCP.ServerRequest	Обнаружение активности тро...	65158634					
13 янв. 2025 г., 9:11:24	✗	Критичный	HackTool.Nmap.TCP.ServerRequest	Обнаружение активности тро...	65158634					
13 янв. 2025 г., 9:05:26	✗	Критичный	HackTool.Nmap.TCP.ServerRequest	Обнаружение активности тро...	41560233					
13 янв. 2025 г., 9:05:26	✗	Критичный	HackTool.Nmap.TCP.ServerRequest	Обнаружение активности тро...	65158634					

Содержание сигнатуры

```

drop tcp any any ->
$HOME_NET any
(msg: "HackTool.Nmap.TCP.ServerRequest", fragbits:ID;
dsize:0; flags:S,12; ack:0;
window:1024; threshold:
type both, track_by_dst,
count 1, seconds 60;
reference:url,https://nmap.org/class/type:trojan1;
sid:65158634; rev:1;
metadata:CLASSTAG
hacktool; metadata:IPS
recommend_alert;
metadata:MITRE TA0007

```

Профиль безопасности

Профиль IPS рекомендуемый, основной, Профиль IPS блок anydesk

IDECO NGFW 19.0.465 Бета  
 Название: Ngfw18  
 Панель мониторинга  
 Пользователи  
 Мониторинг  
 Правила трафика  
 Профили безопасности  
 Сервисы  
 Отчёты и журналы  
 Трафик  
 Системный журнал  
 Журнал веб-трафика  
 Журнал трафика  
 События безопасности  
 Действия администраторов  
 Авторизация администраторов  
 Журнал аутентификации  
 Журнал аутентификации ЛК  
 Конструктор отчётов  
 Syslog  
 Управление сервером  
 Почтовый релей

### События безопасности

ГРАФИКИ IPS | ЖУРНАЛ IPS | WEB APPLICATION FIREWALL  
 7 фев. 2025 г., 0:00 – 7 фев. 2025 г., 23:59 **Все**

Количество атак по уровню угрозы

Шаг группировки: 1 день

Топ атакованных адресов

Всего 8

192.168.100.50 8

Топ заблокированных типов атак

Всего 107

Телеметрия Wind... 5-340  
Обнаружение под... 99  
Обнаружение акт... 8

Топ внешних узлов по количеству блокировок

Всего 8

172.16.100.45 8

А что же по скорости..?

# Производительность Ideco NGFW VPP

## Передовые технологии

Собственный сетевой стек технологий на базе DPDK/VPP, обеспечивающий высочайшую скорость фильтрации трафика

## Результаты нагрузочных тестов\*

### Пропускная способность EMIX:

Firewall - до 100 Гбит/с

Firewall и "Инспекция приложений" - до 75 Гбит/с

IPS и "Инспекция приложений" - до 25 Гбит/с

### Пропускная способность HTTP 250 Kb:

Firewall - до 200 Гбит/с

Макс. кол-во парал. сессий TCP -до 25 000 000

Макс. кол-во сессий в секунду TCP -1 000 000

\*Результаты получены на Ideco EX

# Выполнение требований регуляторов



Высокопроизводительные платформы для бизнеса любого масштаба



Ideco SX+ ФСТЭК

до 100 активных  
пользователей интернет



Ideco LX ФСТЭК

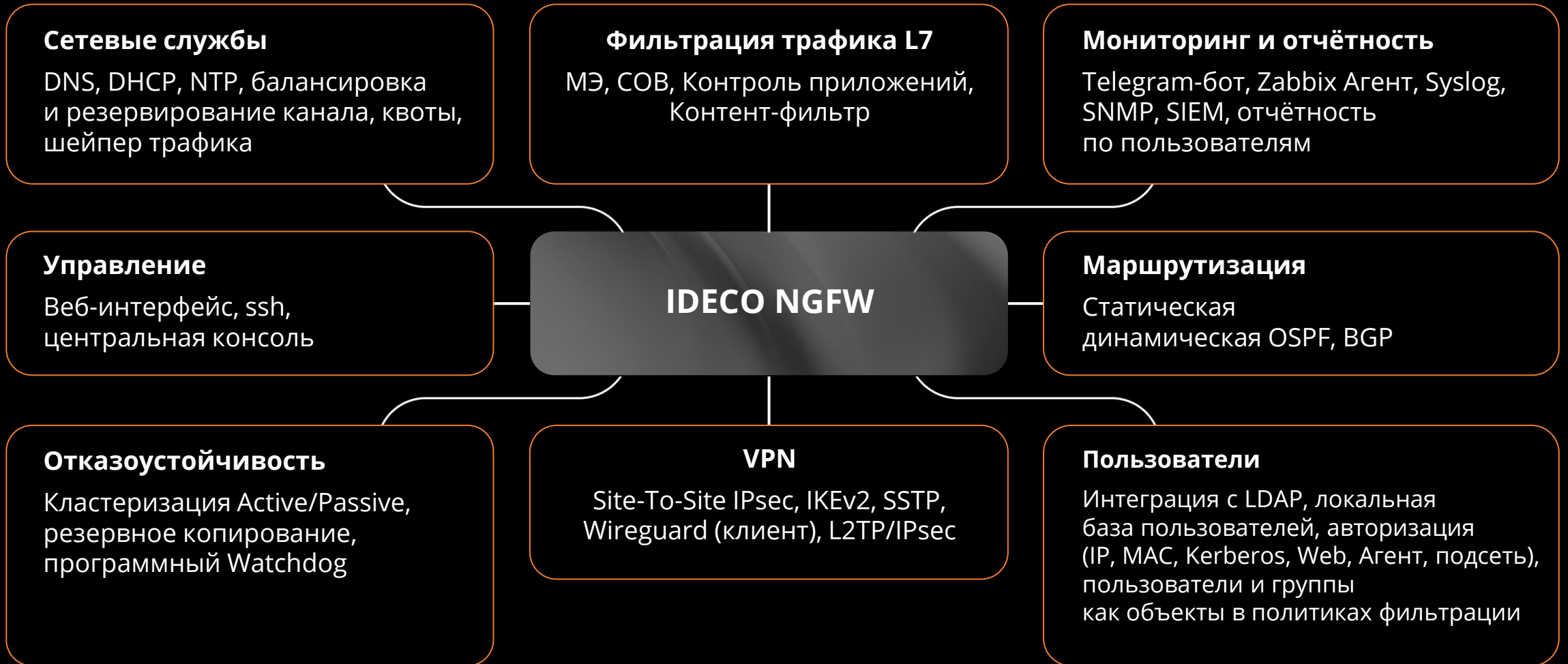
от 300 до 1000 активных  
пользователей интернет



Ideco EX ФСТЭК

для крупных компаний, дата-центров  
и высоконагруженных сетей

# Дополнительные модули в Ideco для обеспечения безопасности периметра организации



# Поддержка заказчиков

1. Зарегистрироваться на [my.ideco.ru](https://my.ideco.ru)
2. Скачать **Ideco NGFW**
3. Установить **Ideco NGFW**

- + 42 дня тестовая лицензия
- + Помощь в тестировании
- + Обратная связь



[my.ideco.ru](https://my.ideco.ru)

# Проектный опыт





Федеральный  
дистрибьютор  
электротехники  
«Русский свет»

### Задачи

- + Решение на 4 000 пользователей для замены Cisco и open source
- + Круглосуточная техническая поддержка с выделенным каналом связи
- + Централизованное управление и мониторинг

### Результат

Осуществлен переход на решение Ideco NGFW.  
Оперативное решение вопросов заказчика в процессе внедрения и эксплуатации.

*«Функционал продукта отвечает всем нашим требованиям!  
Используем Ideco NGFW в нашей компании с июля 2022 года. Все работает без нареканий, рады продолжать наше плодотворное сотрудничество», -  
Алексей Савченко, начальник управления по инфраструктуре ИТ.*



## Задачи

- + Замена решения по защите сети
- + Фильтрация трафика
- + Организация удаленного доступа
- + Контроль выхода в интернет пользователей
- + Отчетность по веб-трафику, публикации сайта

## Результат

Внедрена аппаратная платформа Ideco UTM MX, обеспечивающая безопасность сети университета.

20 июня 2022 года модуль Web Application Firewall помог избежать тяжелых последствий DDoS-атаки, при которой в течение нескольких часов происходило более 20 тысяч запросов к сайту университета.

*«Мы используем аппаратную платформу Ideco UTM MX с сентября 2019 года. В очередной раз убедились, что сделали правильный выбор!», - академик РАН, Заслуженный врач РФ, главный онколог и радиолог УрФО, и.о. ректора ФГБОУ ВО ЮУГМУ Минздрава России Андрей Владимирович Важенин.*

Южно-Уральский  
государственный  
медицинский университет



Департамент  
информационных  
технологий и цифрового  
развития ХМАО

### Задачи

Обеспечить безопасность сети для 2500 пользователей:

- + удобство настройки,
- + интеграция с Active Directory,
- + фильтрация трафика.

Один из ключевых факторов - быстрая и качественная техническая поддержка.

### Результат

Произведена интеграция межсетевого экрана Ideco, закрывающая все потребности заказчика: фильтрация трафика L7, контроль приложений, интеграция с Active Directory. Решение полностью соответствует требованиям заказчика по удобству настройки и интеграции в существующую инфраструктуру. Техническая поддержка по 5 каналам связи. Ответ в веб-интерфейсе продукта в течение 30 секунд.



Алексей Киселев  
presale-инженер

e-mail: [a.kiselev@ideco.ru](mailto:a.kiselev@ideco.ru)  
tg: [@kiselev\\_au](https://www.t.me/kiselev_au)

