# Ideco ICS

Ideco ICS — современное UTM-решение для защиты сетевого периметра.

#### Простое решение вопросов:

* Защиты от вирусов, шифровальщиков, ботнетов на сетевом уровне.
* Полного контроля доступа к веб-ресурсам для сотрудников с ведением отчетности по всем категориям.
* Безопасное подключение удаленных пользователей по VPN, организация защищенного канала между филиалами.

## Основные угрозы информационной безопасности:

* **Потеря данных** в результате действия компьютерных вирусов, шифровальщиков, шпионского ПО.
* **Фишинг и социальная инженерия**: обход средств антивирусной защиты с помощью легального ПО для удаленного доступа, ссылок на зараженные сайты присланных в электронной почте и в мессенджерах.
* **Целевые атаки** на организации с целью получения информации, шантажа или кражи учетных данных от финансовых инструментов.
* **Открытый шпионаж** (spyware, adware, телеметрия, веб-трекеры) – неконтролируемый сбор информации о пользователях легальным ПО и веб сайтами.
* **Нецелевые атаки** – никто не может чувствовать себя в безопасности, т.к. создатели вредоносного ПО атакуют сервисы и сети, имеющие доступ в Интернет, по результатам сканирования всех IP-адресов.

## Предотвращение угроз

#### Система предотвращения вторжений блокирует:

* Командные центры ботнетов.
* Сканеры уязвимостей.
* Трафик spyware, телеметрию Windows и другого ПО
* Эксплойты, которые используют популярные вирусы-шифровальщики
* Известных злоумышленников по IP Reputation и GeoIP

#### Контроль приложений блокирует:

* TOR (который могут использовать ботнеты для общения).
* Потенциально опасные программы удаленного доступа (TeamView).
* Мессенджеры и другое ПО.

#### Контент-фильтр блокирует:

* Фишинговые сайты.
* Зараженные сайты и сайты, распространяющие вирусы.
* Сайты с нелегальным ПО и хакерскими утилитами.
* Веб-трекеры, рекламу и баннеры, сайты, тайно собирающие информацию о пользователях.

## Самые масштабные вирусные атаки 2017

### Wannacry

Глобальная хакерская атака в настоящее время затронула множество компаний по всему миру. На 12 мая зафиксировали 45 тысяч попыток взлома в 74 странах.

В качестве механизмов проникновения использует электронную почту (этот механизм позволяет ему преодолевать защитные межсетевые экраны). Данная уязвимость позволяет вирусу распространяться внутри зараженной сети и поражать максимальное число уязвимых устройств.

### Petya

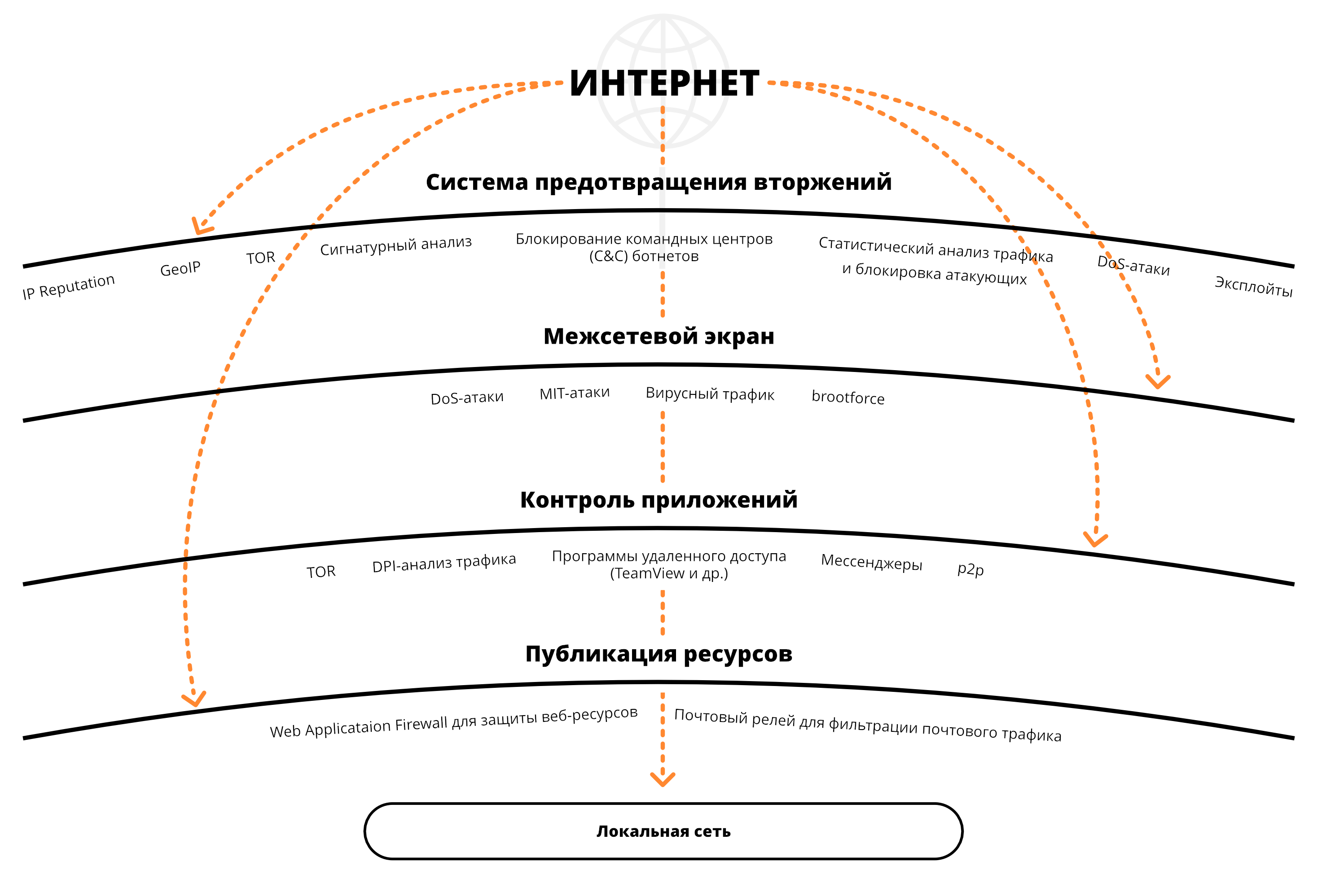
Как и WannaCry, данный шифровальщик сочетает в себе функции вирусного, троянского ПО и сетевых червей. Такое ПО способно проникать внутрь защищенной сети и распространяться далее через уязвимости Windows в NetBIOS или RPC.

В дальнейшем шифровальщик может распространяться в полностью тихом режиме, а в час Х заблокировать компьютер и вывести требования выкупа. При этом даже в случае оплаты пользователь не получает гарантии расшифровки информации. Зачастую шифровальщики не имеют функций расшифровки или в ней содержатся ошибки.

### Bad Rabbit

Rabbit проявляет себя похожим образом c Petya. После неизвестного по длительности «инкубационного периода» распространения в корпоративной сети с помощью брутфорс-атак на компьютеры с ОС Windows происходит активация функций шифрования файлов, и на экран компьютера выводится сообщение вымогателей.

## Средства глубокого анализа трафика

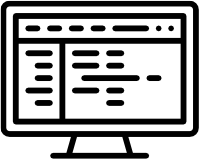
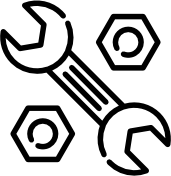
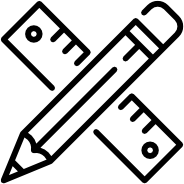


|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Функции** | **Ideco ICS** | **Kerio Control** | **Microsoft TMG** | **Usergate UTM** | **Trafic Inspector  Next Geneeration** | **Интернет Контроль  Сервер** |
| Управление полосой пропускания | + | + | – | + | + | + |
| Фильтрация почтового трафика (антивирус, антиспам) | + | – | + | + | – | + |
| Публикация Outlook Web Access | + | – | + | – | – | – |
| Контроль приложений (DPI) | + | + | – | + | + | – |
| Почтовый сервер | + | – | – | – | – | + |
| Блокировка по IP Reputation | + | – | – | – | – | — |
| Блокировка анонимайзеров | + | – | – | – | – | — |

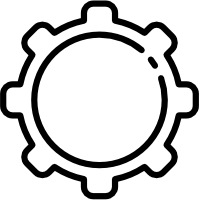
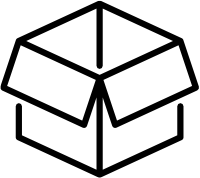
## Сравнение с конкурентами

## Ценность Ideco

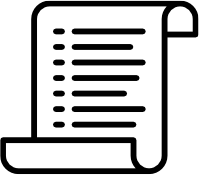
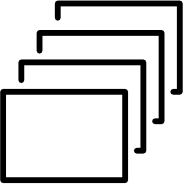
Простой и понятный графический интерфейс



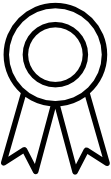
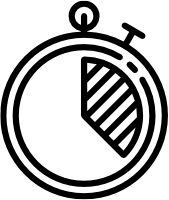
Простое и удобное администрирование



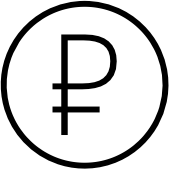
Достаточно невысокие требования к железу



Присутствуем в реестре отечественного ПО



Есть сертификат ФСТЭК



## Есть возможность кастомизации решения под конкретного заказчика

Конкурентоспособное решение по ИБ все в одном

Поддержка всех форматов виртуальных машин

Простота внедрения (1-2 дня)

Гибкая ценовая политика

Все уровни техподдержки от вендора на русском языке с возможностью назначения выделенного инженера.

## Наши клиенты

### Федеральная таможенная служба

* Заместили западное UTM-решение.
* Сложная распределенная сеть.
* На данный момент покрыто 130 подразделений.
* Количество пользователей – 14 500.

### Холдинг «Вертолеты России»

* **Московский Вертолетный Завод им. Миля**

Заместили McAffee Web GateWay (1000 пользователей).

* **Роствертол**Заместили Microsoft TMG (1000 пользователей \* 2 в кластере).

### Министерство Юстиции Российской Федерации

* Интеграция в масштабную ИТ-инфраструктуру.
* Количество пользователей – 700.

### ЦНИИ робототехники и технической кибернетики

* Количество пользователей – 1000.

## Системные требования

|  |  |
| --- | --- |
| Процессор | Intel Pentium G/i3/i5/i7/Xeon E3/Xeon E5 с поддержкой SSE 4.2 |
| Оперативная память | 4 Гб (до 30 пользователей).  8 Гб — для использования системы предотвращения вторжений, антивирусной проверки трафика и большего числа пользователей. |
| Накопитель | Жесткий диск или SSD, объемом 64 Гб или больше, с интерфейсом SATA, SAS или совместимый аппаратный RAID. |
| Сеть | Две сетевые карты (или два сетевых порта) 10/100/1000 Mbps. Рекомендуется использовать карты на чипах Intel, Broadcom. Поддерживаются Realtek, D-Link и другие. |
| Гипервизоры | VMware, Microsoft Hyper-V (1-го поколения), VirtualBox, KVM, Citrix XenServer. |