



Противодействие DDoS-атакам для непрерывной работы вашего бизнеса



**Kaspersky
DDoS
Protection**

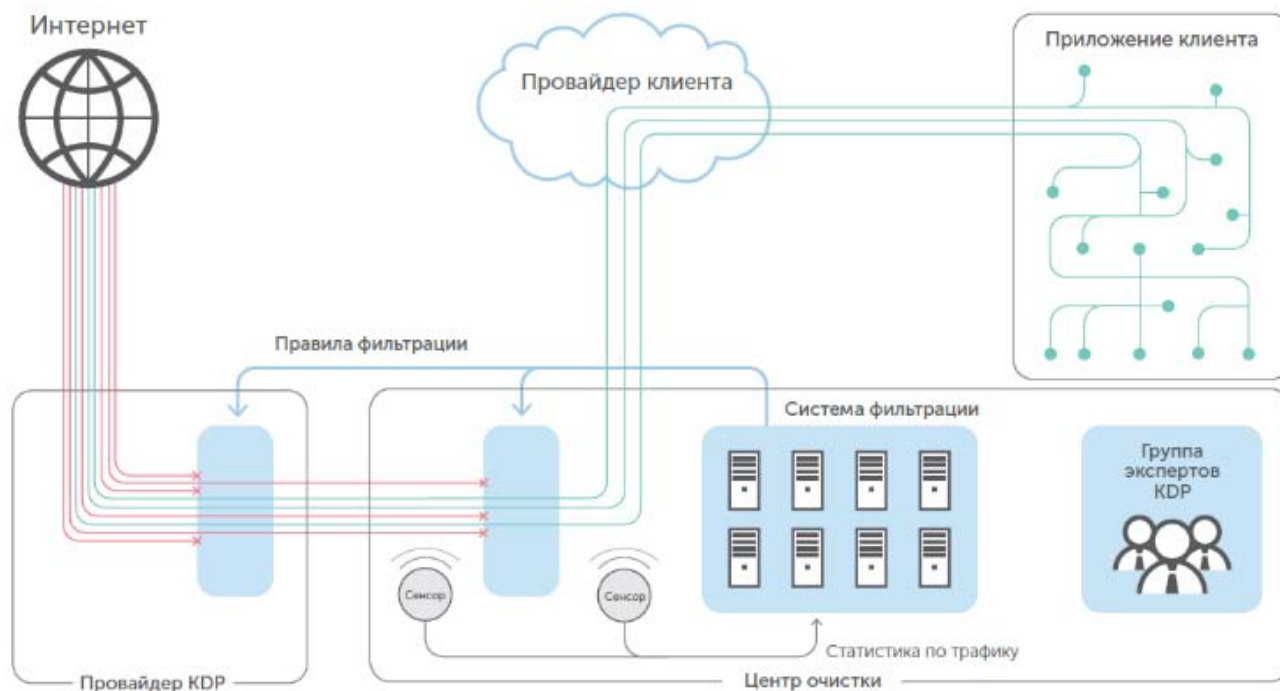


Надежная защита онлайн-ресурсов от DDoS-атак

Варианты противодействия DDoS-атакам

Kaspersky DDoS Protection (KDP) — это специализированное решение для защиты от DDoS-атак, позволяющее обеспечить непрерывность бизнес-процессов и бесперебойную работу ваших критических онлайн-ресурсов и инфраструктуры.

Три версии решения, которые можно выбрать в зависимости от целей, ресурсов и сетевой инфраструктуры:



- **KDP Connect** – перенаправление трафика изменением DNS-записи в режиме Always On, доставка очищенного трафика осуществляется через прокси-сервер, GRE-туннели или через выделенную линию.

- **KDP Connect +** – перенаправление трафика средствами протокола BGP в режиме Always On, доставка очищенного трафика осуществляется через GRE-туннели или выделенную линию.

- **KDP Control** – перенаправление трафика средствами протокола BGP в режиме On Demand, доставка очищенного трафика осуществляется через GRE-туннели или выделенную линию.





Kaspersky Antidrone: защита воздушного пространства от БПЛА

Система противодействия беспилотникам
на объектах любого масштаба



Kaspersky
Antidrone

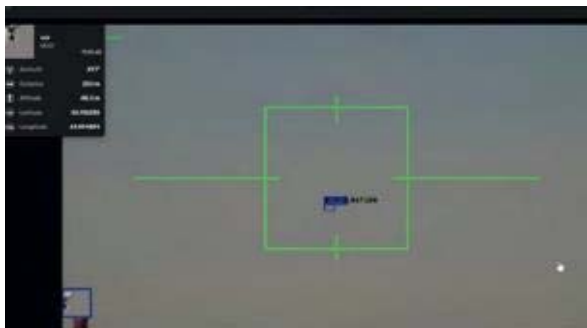


Kaspersky Antidrone: Защита воздушного пространства от БПЛА



Обнаружение

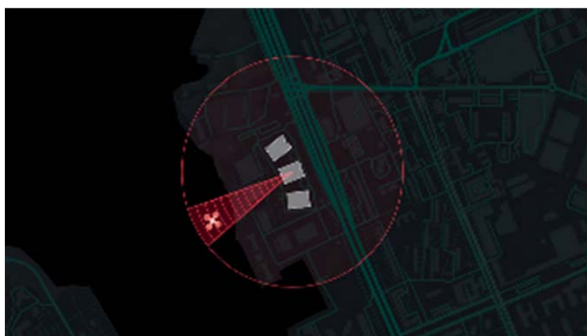
Первичное обнаружение объектов в воздухе происходит за счет применения комбинации сенсоров для аудио-и видеодетектирования, а также лазерного сканирования, радиочастотного и радиолокационного анализа, что позволяет объединить сильные стороны оборудования и обеспечить круглосуточную работу комплекса в различных погодных условиях.



Классификация

Kaspersky Antidrone использует машинное обучение и нейронные сети для классификации обнаруженных целей, определяет тип и модель беспилотника менее чем за 1 секунду.

Данные выводятся в интерфейс, где система сигнализирует о несанкционированном полете и предлагает выбрать стратегию борьбы, основываясь на оценке характеристик и потенциальной опасности каждой цели.



Нейтрализация

В комплексе Kaspersky Antidrone используются несколько дополняющих друг друга методов борьбы с БПЛА.

Система передает управляющий сигнал на аппаратный модуль нейтрализации при возникновении опасности и отображает ситуацию в режиме реального времени в графическом интерфейсе.

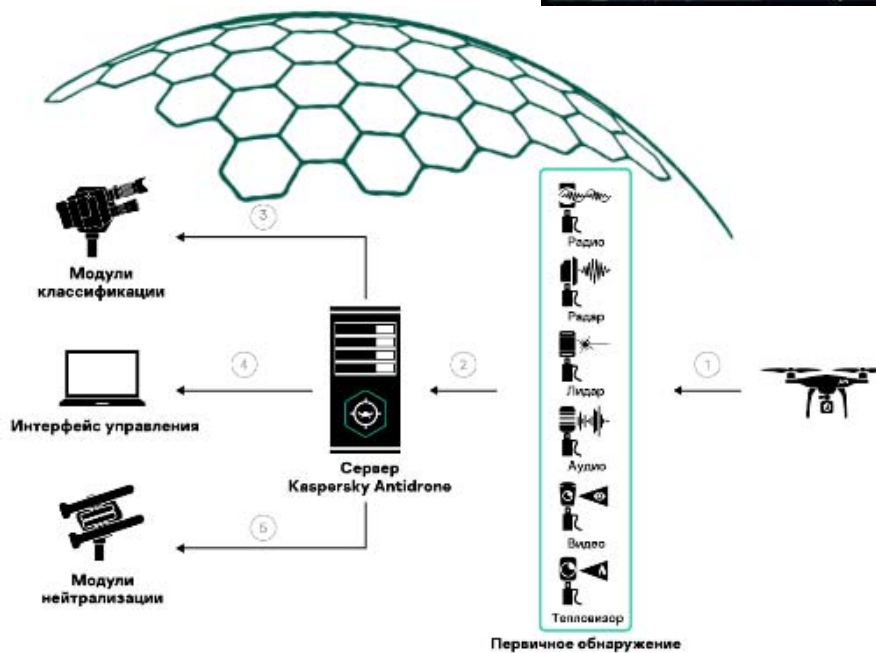
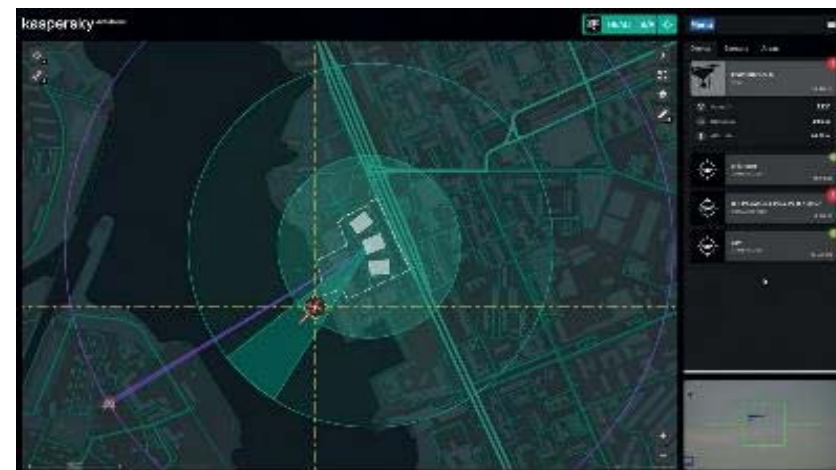


Экосистема комплекса Kaspersky Antidrone

Непрерывный контроль воздушного пространства в режиме реального времени происходит в панели управления, куда приходят оповещения и где собираются данные о прошлых инцидентах.

1. Обнаружение дрона модулями первичного обнаружения
2. Обработка данных в сервере Kaspersky Antidrone для анализа
3. Автоматическое управление модулями классификации
4. Отображение всех этапов в пользовательском интерфейсе
5. Передача управляющего сигнала на модули

- ✓ Интуитивно понятный интерфейс
- ✓ Компоновка и настройка модулей в интерфейсе
- ✓ Точные оповещения об уровне угрозы
- ✓ Отображение объекта любого масштаба
- ✓ Архив происшествий
- ✓ Система самодиагностики
- ✓ Работа без подключения к сети интернет
- ✓ Подключение через API для обогащения SOC
- ✓ Интеграция с SIEM-системами



Альтернативные способы поставки комплекса



Стационарная система

Стационарный вариант используется для защиты статических объектов.

- Модуль первичного обнаружения
- Модули классификации и нейтрализации
- Сервер управления
- Программное обеспечение
- Оборудование по типу объекта



Мобильный комплекс

Мобильная версия подходит для мероприятий и удаленных локаций.

- Мобильная платформа Модуль первичного обнаружения
- Модули классификации и нейтрализации
- Сервер управления



Интеграция ПО

Используется в случае наличия установленного оборудования для наблюдения.

- Оценка оборудования
- Проект комплекса
- Интеграция программного обеспечения



Специальное предложение!

Период действия предложения — до 30.06.2022

Защита уровня **Kaspersky Optimum Security** со скидкой до **30%**

Специальное предложение распространяется на следующие продукты :

Kaspersky EDR для бизнеса Оптимальный

Kaspersky Sandbox

Kaspersky Managed Detection and Response Optimum

Kaspersky Automated Security Awareness Platform

Условия:

Специальное предложение до **30%** распространяется только на новые лицензии (**base**).

Срок действия лицензии — 1-2 года.

Продление лицензий (renewal), а также лицензии Образование, Первая помощь не принимают участия в акции.

Предложение действительно для клиентов SMB.



Анонс вебинаров

webinar





анонс web-семинаров

- | | |
|---------------------------|---|
| 24 мая
начало в 11:00 | Основные составляющие бесперебойной работы ИТ- и ИБ-систем (Red Soft) |
| 26 мая
начало в 11:00 | Шаги по переходу на отечественное программное обеспечение (ПО) |
| 02 июня
начало в 11:00 | Защита персональных данных по №152-ФЗ.
Подготовка к проверке Роскомнадзора |

**Какие темы вам были бы интересны
в следующих наших семинарах?**



The logo consists of a black rectangular box. The top half contains the word "kaspersky" in white lowercase letters. A thin teal horizontal line separates the top half from the bottom half. The bottom half contains the words "Platinum" and "Partner" stacked vertically in white uppercase letters.

kaspersky

Platinum
Partner

Благодарю за внимание!

Руководитель направления решений
«Лаборатории Касперского»

Михаил Усачёв

тел: + 7 (812) 325 84 00

моб: + 7 911 929 60 04

e-mail: Mikhail.Usachev@polikom.ru

ПОЛИКОМ The logo for "ПОЛИКОМ" features the word in a bold, grey, sans-serif font. To its right is a blue square icon containing the word "про" in white lowercase letters.