Кибербезопасность IoT-систем видеонаблюдения

kaspersky

KasperskyOS

По прогнозам экспертов, к 2022 году в мире количество камер видеонаблюдения составит более 45 миллиардов, и большинство из них будут умными. Возможности таких камер делают их привлекательными не только для пользователей, но и для злоумышленников.

Современные камеры видеонаблюдения предлагают различные варианты подключения к проводным и беспроводным сетям передачи данных. А благодаря функциям распознавания лиц, подсчета людей, создания тепловых карт, видеодетектора движения они могут определять поведение и личность человека, «читать» номерные знаки транспортных средств и многое другое.

Исследователи безопасности регулярно находят в умных камерах множество уязвимостей. Злоумышленники могут эксплуатировать их, чтобы шпионить за владельцами, влиять на общую безопасность сетей или даже на корпоративную инфраструктуру.

Важность киберзащиты

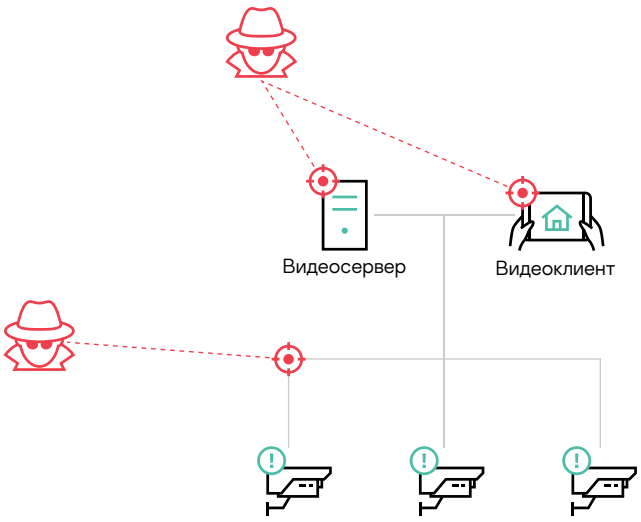
Современные видеокамеры — это достаточно умные и функциональные устройства, так же подверженные хакерским атакам, как другие устройства интернета вещей. Например, в 2019 году исследования показали, что червь Mirai, объединяющий зараженные им устройства в ботнеты, чаще всего атаковал камеры и роутеры. А в 2021 году хакеры скомпрометировали 150 тысяч камер видеонаблюдения в США, Великобритании и Китае, установленные в том числе в школах, больницах, полицейских участках и тюрьмах. Злоумышленникам удалось получить доступ не только к камерам, но и к целым видеоархивам организаций.

Локальные системы видеонаблюдения

В локальных системах видеонаблюдения наибольший риск представляет физическое подключение к системе непосредственно на объекте через камеры.

Камеры видеонаблюдения не предназначены для установки на них средств безопасности. Это значит, что камера не защищена от:

- несанкционированного подключения;
- эксплойтов и другого вредоносного ПО;
- сетевых атак;
- отсутствия видимости происходящего в локальной сети.

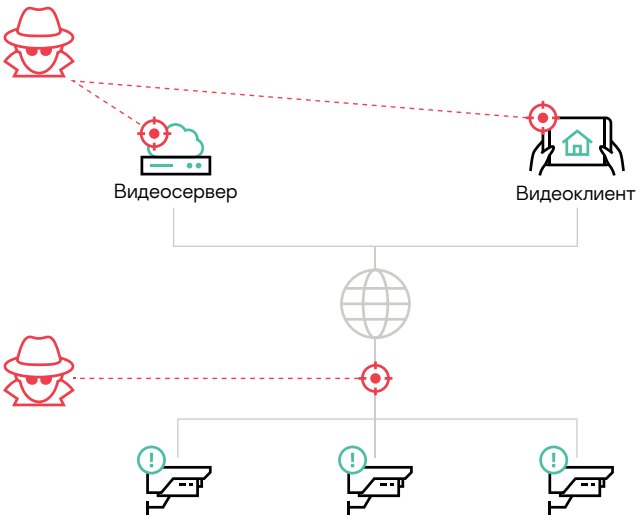


Облачные системы видеонаблюдения

Причиной главных рисков для облачных систем видеонаблюдения является их подключение к интернету. Через него передается на видеосервер видеопоток с камер, и в этот момент эти данные наиболее уязвимы.

Если хакер получит доступ к системе видеонаблюдения через интернет, он сможет:

- эксплуатировать уязвимости;
- проводить сетевые атаки, в том числе DDoS;
- перехватывать видеопоток;
- заражать ее вредоносным ПО.



Для видеосервера и видеоклиента актуальны те же угрозы, что и для любого другого устройства на Windows или Linux

Что и от чего нужно защищать в системах видеонаблюдения?

- Видеоархивы и базы данных:
  - несанкционированный доступ
  - компрометация (взлом, получение доступа, изменение конфигураций, подмена/утечка данных)
- Каналы связи:
  - вывод из строя
  - нестабильная передача данных (не связанная напрямую с вредоносным вмешательством)
  - Man-in-the-middle (получение доступа к данным, их перехват и подмена)
  - DDoS (недоступность канала)
- Камеры:
  - перепрошивка
  - изменение конфигурации
  - смена пароля
  - подделка SSL-сертификата
  - установка вредоносного ПО
  - несанкционированное подключение

Решение

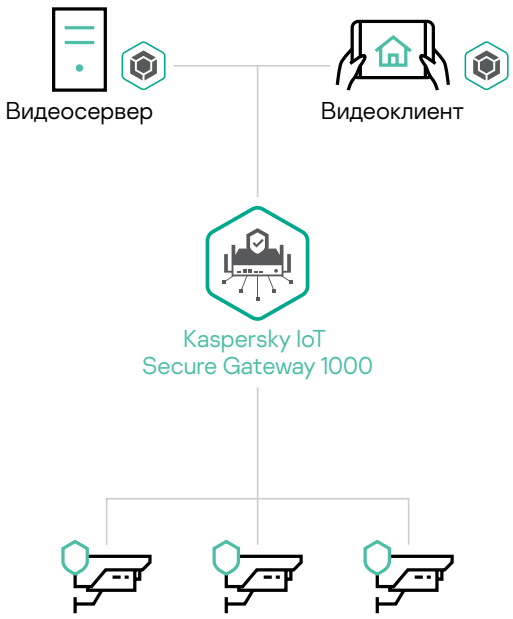
Для безопасности IoT-инфраструктуры систем видеонаблюдения «Лаборатория Касперского» предлагает решение **Kaspersky IoT Infrastructure Security,** ключевой компонент которого — шлюз **Kaspersky IoT Secure Gateway (KISG) 1000** на базе операционной системы KasperskyOS. Устройство обладает **кибериммунитетом** – «врожденной» устойчивостью к подавляющему большинству кибератак, благодаря которой будет выполнять свои критичные функции даже в агрессивной среде. KISG 1000 также обеспечивает возможности мониторинга и защиты всей IoT-инфраструктуры. Шлюз работает на аппаратной платформе Advantech UTX-3117 под управлением **Kaspersky Security Center**. Такое комплексное решение помогает поддерживать безопасность систем, отслеживать их состояние и управлять событиями из единого центра.

Kaspersky IoT Secure Gateway 1000 позволяет разграничить доступ между камерами и видеосервером в локальных системах видеонаблюдения, а в облачных — защитить периметр систем от интернет-угроз.

Функции KISG 1000:

- блокирует все неразрешенные взаимодействия между видеосервером и камерами;
- блокирует попытки атаковать камеры со стороны видеосервера и видеоклиента;
- формирует список камер и сообщает о появлении неавторизованного устройства в локальной сети (что также может свидетельствовать о подмене камеры);
- сообщает, если камера была выведена из строя.

Локальные системы видеонаблюдения



Kaspersky Total Security для бизнеса обеспечивает защиту видеосервера и видеоклиента

Kaspersky IoT Secure Gateway 1000 защищает видеосервер от угроз со стороны камер, а камеры — от угроз со стороны видеосервера и видеоклиента

Облачные системы видеонаблюдения

Kaspersky Total Security для бизнеса обеспечивает защиту видеоклиента

Kaspersky Security для виртуальных и облачных сред обеспечивает защиту видеосервера, размещенного в облаке

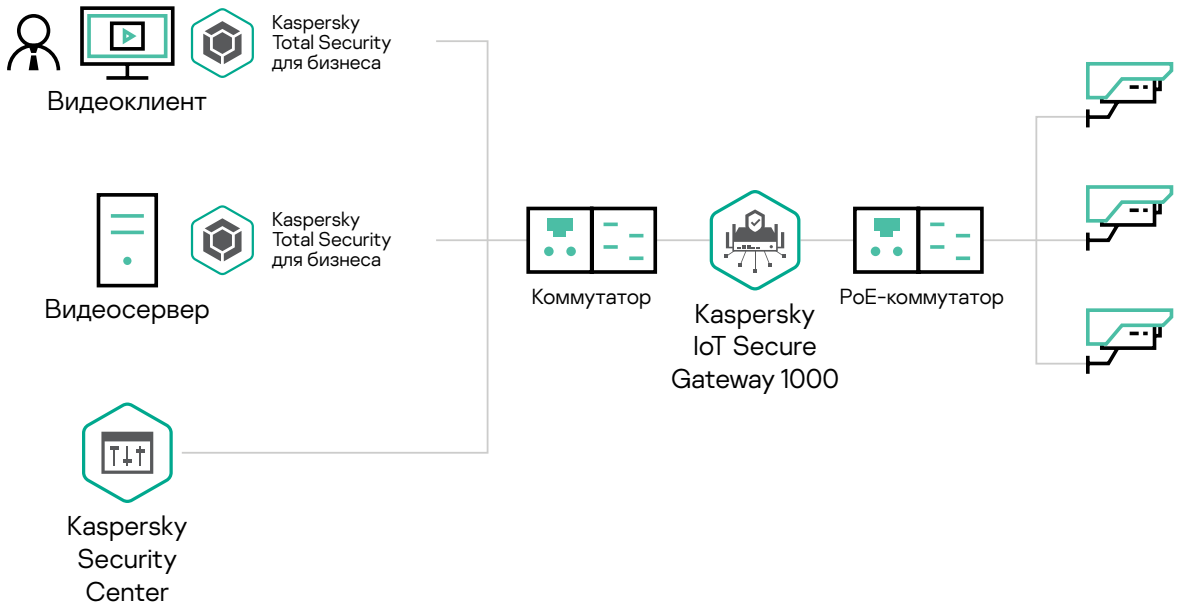
Kaspersky IoT Secure Gateway 1000 защищает видеосервер от угроз со стороны камер, а камеры — от угроз со стороны видеосервера, видеоклиента и интернета

Результат

Кибербезопасность систем видеонаблюдения — задача, требующая комплексного подхода. Защита всех элементов архитектуры системы видеонаблюдения (камер, IoT-шлюзов, видеосервера и видеоклиента) снижает возможность эксплуатации уязвимостей злоумышленниками.

Подход «Лаборатории Касперского» к защите **локальных систем видеонаблюдения** включает в себя:

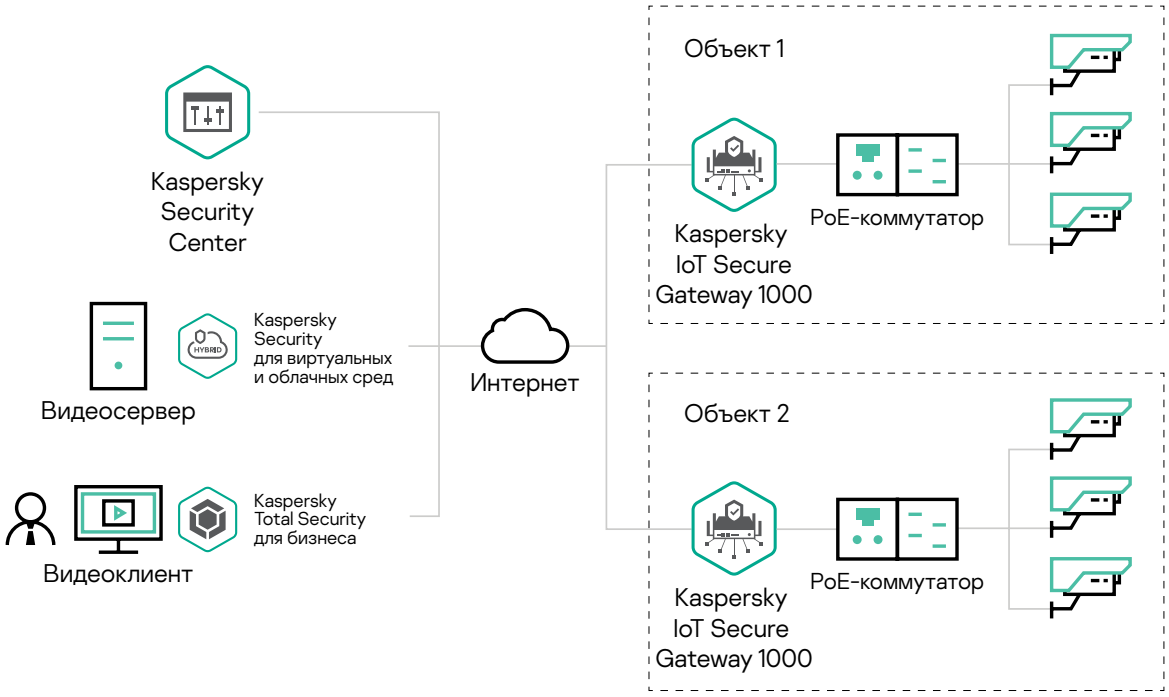
- Kaspersky IoT Infrastructure Security:
  - Kaspersky IoT Secure Gateway 1000
  - Kaspersky Security Center
- Kaspersky Total Security для бизнеса



Уровни	Векторы угроз	Продукты и решения «Лаборатории Касперского»
Управление инфраструктурой системы видеонаблюдения	• Сложность мониторинга безопасности IoT-инфраструктуры (отсутствие полноценной картины в режиме реального времени) • Длительное время реагирования на инциденты ИБ (запоздалое оповещение/обнаружение проблемы)	Kaspersky Security Center
Канал передачи данных	• Man-in-the-middle (получение доступа к данным, их подмена)	Kaspersky IoT Secure Gateway 1000
Шлюз	• Сетевые атаки на опубликованные устройства (устройства с публичным адресом или к которым организован доступ из публичных сетей)	
Камеры	• Сетевые атаки на подключенные устройства (перебор паролей, получение доступа, изменение конфигураций ПО, подмена/утечка данных) • Несанкционированные новые подключения к сети (подключение злоумышленником дополнительных устройств, их включение вместо камер)	

Комплексный подход «Лаборатории Касперского» к защите **облачных систем видеонаблюдения** включает в себя:

- Kaspersky IoT Infrastructure Security:
  - Kaspersky IoT Secure Gateway 1000
  - Kaspersky Security Center
- Kaspersky Total Security для бизнеса
- Kaspersky Security для виртуальных и облачных сред
- Kaspersky DDoS Protection



Уровни	Векторы угроз	Продукты и решения «Лаборатории Касперского»
Управление инфраструктурой системы видеонаблюдения	• Сложность мониторинга безопасности IoT-инфраструктуры (отсутствие полноценной картины в режиме реального времени) • Длительное время реагирования на инциденты ИБ (запоздалое оповещение/обнаружение проблемы)	Kaspersky Security Center
Облако	• DDoS-атаки (недоступность сервиса) • Компрометация платформы видеонаблюдения (взлом, получение доступа, изменение конфигураций, подмена/утечка данных)	Kaspersky DDoS Protection Kaspersky Security для виртуальных и облачных сред
Канал передачи данных	• DDoS-атаки (недоступность канала) • Man-in-the-middle (получение доступа к данным, их подмена)	Kaspersky DDoS Protection Kaspersky IoT Secure Gateway 1000
Шлюз	• Сетевые атаки на опубликованные устройства (устройства с публичным адресом или к которым организован доступ из публичных сетей)	
Камеры	• Сетевые атаки на подключенные устройства (перебор паролей, получение доступа, изменение конфигураций ПО, подмена/утечка данных) • Несанкционированные новые подключения к сети (подключение злоумышленником дополнительных устройств, их включение вместо камер)	

Комплексный подход «Лаборатории Касперского» к защите локальных и облачных систем видеонаблюдения позволяет защитить видеокамеры, облачные платформы и IoT-устройства, а также контролировать их безопасность из единого центра. В частности, кибериммунный Kaspersky IoT Secure Gateway 1000 на базе KasperskyOS служит пограничным сетевым средством безопасности, а платформа Kaspersky Security Center помогает централизованно настраивать шлюзы и управлять их событиями.

KasperskyOS

Kaspersky
IoT Infrastructure
Security

Подробнее на os.kaspersky.ru

www.kaspersky.ru