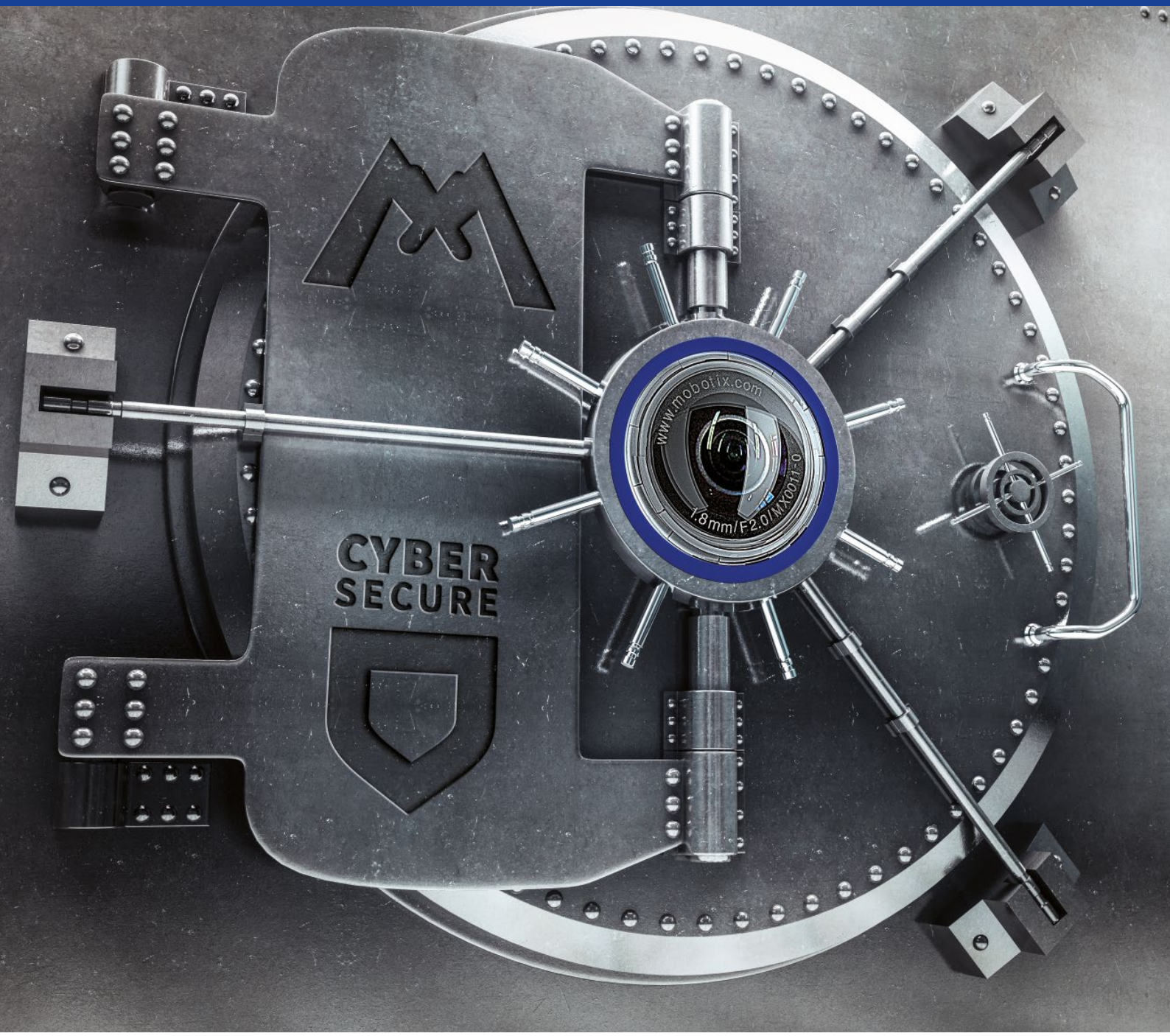
Важность кибербезопасности в охранных видеосистемах

Официальный документ



BeyondHumanVision

MOBOTIX

Вступление

Использование видео для обеспечения безопасности, промышленного контроля и охраны здоровья ежедневно благотворно влияет на жизнь миллиардов людей. Видеонаблюдение касается всех аспектов нашей жизни: от семьи, разгуливающей по безопасному торговому центру под бдительным оком системы видеонаблюдения, до дистанционного видеонаблюдения в целях выявления дефектов на производственной линии или даже наблюдения за ребенком со стороны заботливых родителей.

Каковы основные факторы роста?		
1	Рост озабоченности безопасностью	58 %
2	Улучшение видеоаналитики	51 %
3	Доступность IP-сетей	50 %

Рост использования видео для наблюдения и в других областях ускоряется благодаря расширению информационных, коммуникационных и технологических секторов. Если раньше для оценки видеоизображения и принятия решений требовался оператор, то теперь такие системы взаимодействуют с другими типами входных сигналов от датчиков (например, от систем слежения за температурой, звуком, движением и систем искусственного интеллекта), которые могут автоматически подавать сигналы тревоги или инициировать действия. Системы видеонаблюдения перестали быть пассивными получателями информации и всё больше превращаются в автоматизированный интеллектуальный инструмент, способный выполнять определенные задачи на основе полученных с камер данных.

Простые примеры, такие как распознавание номерных знаков для дорожных сборов и более мощные системы, способные визуально обнаруживать мелкие неисправности в машинах до их поломки, всего лишь верхушка айсберга. Даже в распространенных областях (например, наблюдение в розничных магазинах) последние технологии предлагают новые возможности, такие как подсчет людей или анализ покупок, чтобы помочь в планировании магазина и даже в разработке новых торговых центров.

Спрос постоянно растет. По оценкам компании Cisco, видео для развлекательных и деловых целей к 2020 году составит 79 % интернет-трафика [1]. Помимо этого, процесс создания видео постоянно упрощается благодаря уменьшению размеров, снижению стоимости и энергопотребления камер. С распространением интернет-соединений и более быстрых мобильных сетей передавать видео от источника к месту назначения также становится проще. Видео и особенно видеонаблюдение в значительной степени воспринимаются как социальное благо за счет уменьшения количества преступлений и укрепления личной свободы в более безопасной среде. Кроме того, по мере роста популярности видео все чаще подвергается нападениям со стороны преступников, террористов и других групп, которые хотят нарушить работу платформ видеонаблюдения или использовать их в преступных целях.

Риски небезопасного видеонаблюдения и устройств «Интернета вещей»

В прежние времена атаки на сети видеонаблюдения были редки в силу замкнутого характера таких систем, которые часто подключались к местным диспетчерским помещениям с помощью прямых кабельных соединений. Кроме того, старые видеокамеры, как правило, имели простейшую прошивку, которая лишь отправляла видео по коаксиальному кабелю, что давало очень небольшие возможности для атаки. Однако времена меняются, и современные видеокамеры фактически представляют собой компьютеры, подключенные к цифровому датчику изображения. С развитием Интернета и дешевых камер системы видеонаблюдения становятся всё более доступными по любой IP-сети.

Как и в случае атак на системы безопасности розничных магазинов и поставщиков услуг, часто направленных на сбор данных о кредитных картах и другой ценной информации, сложность и изменчивый характер процессов, программных протоколов и механизмов аутентификации означают, что будут возникать уязвимости. Эта проблема не нова. Более чем за десять лет исследователи безопасности [2] обнаружили в камерах уязвимости, которые затронули и крупных международных поставщиков, и более мелкие региональные бренды. Список проблем растет. Вот лишь некоторые из них:

- атаки, направленные на получение пароля администратора устройства путем взлома системы безопасности из учетной записи пользователя по умолчанию;
- эксплойты, которые обходят аутентификацию пользователя, используя учетные данные, жестко запрограммированные в устройстве его производителем в качестве backdoor;
- выполнение произвольного кода на устройстве без аутентификации за счет использования уязвимостей в обработчике пакетов протокола RTSP;
- уязвимость системы безопасности, которая позволяет злоумышленнику обойти аутентификацию оператора камеры и получить прямой доступ к файлам конфигурации;
- эксплойты, которые позволяют злоумышленнику сбросить пароль устройства, а затем разрешить несанкционированную модификацию файлов конфигурации и предоставить злоумышленнику доступ к основным функциям камеры;
- атака на камеры, позволяющие третьим сторонам перехватывать трансляцию видеопотоков, отправленных по частной сети или интернет-соединению.

Многие из этих проблем, которые влияют на множество брендов, лицензирующих технологии от крупных поставщиков, привели к появлению «слабых мест» у миллионов устройств. Хотя крупные поставщики с хорошей репутацией часто выпускают исправления для устранения проблем, многие небольшие компании их попросту игнорируют. Даже при наличии исправлений обновления выполняются вручную, и многие владельцы платформ видеонаблюдения не знают об этих проблемах. Проблемы затрагивают и домашних пользователей, поскольку во многих охранных видеосистемах потребительского класса, приобретенных в розницу, исправления до сих пор не установлены.

Целевые атаки и ботнеты

Хотя это похоже на сюжет голливудского блокбастера, способность систематически выводить из строя всю охранную видеосистему, защищающую ценные объекты, участки и даже города, не выходит за рамки возможного. Многие поставщики систем видеонаблюдения постоянно используют одни и те же программные библиотеки, которые управляют потоковой передачей, аутентификацией пользователей и переносом видео на носители, поэтому опытные преступники рассматривают атаки на такие системы не только как способ совершения преступления, но и как возможность вызвать страх и панику.

Еще одна проблема — обход сети: злоумышленники получают плацдарм в подключенном устройстве, например камере, а затем, используя такую позицию с аутентификацией, и в других подключенных ресурсах. Хотя хорошо спроектированные средства защиты сети способны блокировать большинство атак, по мере распространения камер и других устройств «Интернета вещей», а также их внедрения в основные процессы риск может расти. Однако атаки на камеры не единственная проблема. Недавно камеры сами захватывались и использовались в качестве оружия посредством распределенных DDoS-атак.

Массовая DDoS-атака в октябре 2016 года, затронувшая Twitter, Amazon, Tumblr, Reddit, Spotify и Netflix, была, в частности, порождена ботнетом на основе червя Mirai. Как сообщила эксперт по безопасности Эллисон Никсон (Allison Nixon), директор по исследованиям компании Flashpoint, ботнет в основном подверг риску цифровые видеомагнитофоны (DVR) и IP-камеры, произведенные китайской компанией XiongMai Technologies. Компания XiongMai изготавливает и продает компоненты производителям оборудования, которые используют их в своих собственных продуктах, в результате чего десятки тысяч устройств превращаются в опасное кибероружие [3].

Правительство, регулирующие органы и законодательство

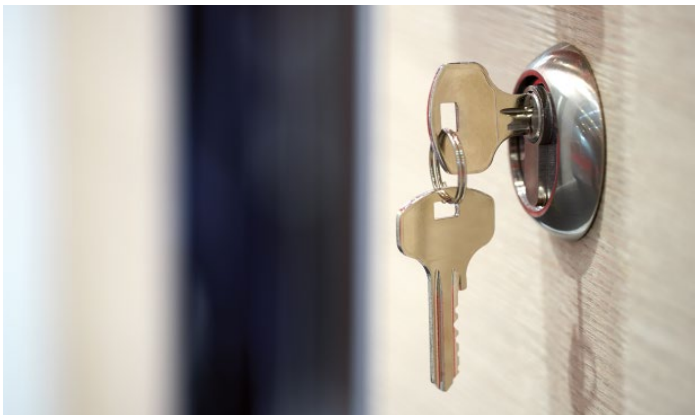
По оценкам Gartner, Cisco и других компаний, взрывной рост подключенных к Интернету устройств (в пределах 25–50 млрд [4] штук к 2020 году) вызывает у национальных правительств и международных регулирующих органов ряд «головных болей». В отличие от радиопередатчиков, телевизионных станций или автотранспортных средств законодательство практически не регулирует устройства, которые можно подключать к Интернету. Не существует никаких утвержденных стандартов, определяющих степень безопасности тех или иных устройств. Что происходит, если такое устройство взломано или используется для атаки третьей стороны? Уголовное право в большинстве стран может иметь дело с киберпреступлениями, в которых есть преступник и жертва. Однако по мере роста автономности технологии и риска того, что незащищенные устройства будут привлекать вирусы, от эпидемий которых страдали пользователи настольных ПК, эти вирусы могут появиться вновь, например, в сетях камер видеонаблюдения, а для таких случаев существует немного способов обнаружения и быстрого устранения проблемы.

Потенциальная финансовая и уголовная ответственность

Проблема ответственности стоит весьма остро. Установка систем видеонаблюдения может привести к снижению расходов на страхование и увеличению вероятности поимки преступников. Однако если система видеонаблюдения оказывается неработоспособной из-за эксплойта и преступление совершено, но не зафиксировано камерой, страховые компании могут отменить все выплаты из-за несоблюдения условий покрытия. На кого подавать в суд жертве в этом случае? На производителя камеры? На поставщика контрактов на обслуживание систем видеонаблюдения? А в случае инцидента с общественной безопасностью возьмут ли на себя ответственность местные органы власти? Так много вопросов относительно последствий нарушения безопасности систем и так мало прецедентов. Поэтому на рынке существует большая неопределенность.

Проблемы конфиденциальности

Хотя вопросы финансовой и уголовной ответственности, связанные со взломом устройств видеонаблюдения, всё еще открыты для обсуждения, в большинстве развитых стран сформировались законы, касающиеся



неприкосновенности частной жизни граждан. Их детали могут незначительно отличаться, но в целом все конфиденциальные личные данные, связанные со здоровьем, финансами, сексуальной ориентацией, политической принадлежностью и многим другим, должны собираться и храниться безопасным образом. Это распространяется и на видеоданные. Например, пациенты, которые посещают психолога, или лица, участвующие в политических митингах, рассчитывают на то, что материалы видеонаблюдения будут храниться в безопасности и не станут всеобщим достоянием. В случае кибератаки на устройство или сеть видеонаблюдения очень высок риск того, что личная информация, такая как изображения и другие данные, позволяющие идентифицировать конкретных лиц, может быть украдена и без разрешения передана третьим лицам. Это нарушило бы права на неприкосновенность частной жизни пользователей, отслеживаемых системой, и могло бы иметь правовые последствия для лица, назначенного ответственным за обработку персональных данных.

Государственное регулирование

Правительства во всем мире стремятся лучше понять, как обезопасить новую волну устройств «Интернета вещей». Высокопоставленные члены Европейской комиссии открыто обсудили разработку процесса сертификации устройств «Интернета вещей», который обеспечивал бы защиту пользователей. Комиссия также приняла участие в создании группы под названием Alliance for Internet of Things Innovation, которая включает несколько крупных поставщиков технологий, лидеров отраслей в области энергетики, автомобильной промышленности и здравоохранения. Цель этой группы — начать процесс разработки комплекса рекомендаций. В США Министерство внутренней безопасности опубликовало руководство по стратегическим принципам защиты «Интернета вещей» [5], в числе которых такие ключевые идеи, как внедрение защиты на этапе проектирования, поддержка обновлений для систем безопасности и управление уязвимостями с особым вниманием к определению приоритетов мер безопасности в зависимости от потенциального воздействия. Однако глобального или отраслевого консенсуса, такого как стандарты PCI-DSS в кредитных отраслях, пока нет. В результате безопасность устройств «Интернета вещей» сейчас основана на руководствах, разрабатывающихся разными странами по отдельности, и слабом регулировании, которое заметно различается по области применения и эффективности.

Как компания MOBOTIX решает эти проблемы?

MOBOTIX — лидер в области цифрового видеонаблюдения. В отличие от многих других компаний она разрабатывает все свое программное обеспечение самостоятельно. Это не только позволяет предлагать высокотехнологичные продукты, но и является существенным преимуществом, когда речь идет о безопасности. Контролируя разработку программного обеспечения, компания MOBOTIX становится менее уязвимой для таких ситуаций, когда недостаточно хорошо разработанные сторонние программные и аппаратные средства могут привести к проблеме безопасности. Там, где мы используем широко поддерживаемые отраслевые стандарты, такие как ONVIF, в нашей компании действуют политики немедленного выпуска всех исправлений по мере их появления. Благодаря использованию единого программного обеспечения для всех моделей камер MOBOTIX этот процесс постоянного обеспечения актуальности и безопасности встроенного ПО камеры значительно упрощается для наших международных клиентов.

Безопасность в компании с самого начала занимала особое место, и это проявляется в нескольких областях.

Безопасная операционная система и обновления

Подход MOBOTIX к обеспечению безопасности начинается с разработки операционной системы камеры и стека приложений. Все устройства MOBOTIX созданы на основе модифицированной защищенной ОС Linux, из которой удалены стандартные службы и модули. Критически важные модули Linux, такие как аутентификация, полностью переработаны инженерами MOBOTIX, чтобы исключить уязвимость этих модулей к стандартным эксплойтам или методам инъекции кода. Это системное программное обеспечение не является открытым. В нем применены дополнительные технологии защиты программного обеспечения. Кроме того, каждое обновление прошивки и элементов программного обеспечения устройства зашифровано и снабжено цифровой подписью, чтобы избежать фальсификации.

Безопасная конфигурация камеры

Доступ к интерфейсу конфигурации камеры предоставляется только авторизованным пользователям, а для обеспечения внутренней безопасности каждая система позволяет создавать и применять различные права для разных групп пользователей. На практике это означает, что камеры MOBOTIX никогда не сохраняют пароли пользователей в текстовом виде. Вместо этого пароли хешируются с применением надежного алгоритма одностороннего хеширования (SHA-512). Поэтому, даже если файл конфигурации окажется не в тех руках, получить пароль в текстовом виде будет чрезвычайно сложно. Не самые важные службы ОС Linux отключены, чтобы ограничить возможности потенциальных эксплойтов и предотвратить атаки. Также отсутствует недокументированный пароль для Telnet или мастер-пароль. Доступ к камере MOBOTIX и ее настройка осуществляются через собственный веб-интерфейс (графический пользовательский интерфейс). Пароли можно хранить в системах управления привилегированным доступом, таких как BeyondTrust и CyberArk, которые могут дополнительно защищаться с помощью систем двухфакторной аутентификации.

Безопасная сеть и связь между устройствами

Все данные, которыми камеры MOBOTIX обмениваются с другими узлами сети, можно зашифровать и обеспечить таким образом их конфиденциальность и целостность при передаче. В качестве стандарта поддерживаются HTTPS (SSL/TLS) и сертификаты, которые обеспечивают соответствие рекомендациям, применяемым в основных структурах безопасности таких экспертных центров, как институт SANS. MOBOTIX также включает в себя встроенную поддержку управления уникальными сертификатами X.509 на каждой камере и корневыми центрами сертификации, чтобы организации могли расширять безопасность устройств, охватывая камеры и дверные коммуникаторы, для аутентификации которых используются системы типа OpenVPN. Это означает, что если камера физически украдена или взломана, злоумышленник не сможет атаковать остальную сеть камер, используя учетные данные уязвимой камеры.

Безопасная внутренняя запись и защита от фальсификации

Все созданные камерой записи перед сохранением могут быть зашифрованы, начиная с циклического буфера, который использует встроенную SD-карту в каждой камере. Компания MOBOTIX создала безопасную файловую систему. Это означает, что если камера физически взломана или украдена, ранее записанное видео, которое все еще находится в камере, невозможно извлечь, не получив предварительно права администратора, защита которых обеспечивается описанными выше процессами безопасной конфигурации. Чтобы предотвратить несанкционированный доступ, каждое созданное камерой MOBOTIX изображение можно подписать цифровой подписью с использованием

настраиваемых сертификатов. Поэтому такие записи принимаются в качестве доказательств в суде.

Функции безопасности	Стандартные IP-камеры	MOBOTIX
HTTPS (SSL/TLS) и сертификаты	✓	✓
Дайджест-аутентификация для HTTP	✓	✓
Списки контроля доступа	✓	✓
Пользователи и группы с настраиваемыми правами	⚠	✓
Обнаружение несанкционированного доступа	✗	✓
Защита от ботов	✗	✓
Шифрование записи	✗	✓
Шифрование видео и сообщений	✗	✓
VPN-клиент	✗	✓

Обнаружение несанкционированного доступа

Даже имея отлаженные системы и процессы обеспечения безопасности, было бы безрассудно предположить, что злоумышленники не будут пытаться взломать камеры MOBOTIX, поэтому компания MOBOTIX вложила средства в дополнительные меры по обнаружению таких попыток. Используя ряд элементов обнаружения несанкционированного доступа, все камеры и дверные коммуникаторы по зашифрованному каналу сообщают о любых случаях неавторизованного входа в систему и атаках методом «грубой силы». Кроме того, уведомления могут отправляться в случае нескольких неудачных попыток входа в систему, а IP-адрес «нарушителя» при этом будет автоматически блокироваться.

Обзор

Популярность видеонаблюдения в здравоохранении, обеспечении безопасности и промышленности постоянно растет. С повышением важности таких элементов кибератаки всё чаще будут направляться на дополнительные (контроль доступа, мониторинг состояния окружающей среды и т. п.) и аналитические процессы (например, распознавание лиц).

Составители спецификаций на охранные видеосистемы, поставщики услуг и даже регулирующие органы должны будут усилить контроль безопасности как в рамках заботы об общественных интересах, так и для выполнения будущих юридических обязательств. Осознав эти проблемы, отраслевые лидеры, такие как компания MOBOTIX, и другие участники рынка активно работают над защитой аппаратного и программного обеспечения устройств на самых ранних этапах проектирования.

Однако защита всей среды должна быть не хуже, чем у защищенных устройств. Бессмысленно запирать двери, если окно осталось открытым. Поэтому составителям спецификаций и операторам систем видеонаблюдения и более широких сетей «Интернета вещей» необходимо оценивать и другие элементы: базовую сеть, инфраструктуру хранения данных и критически важный человеческий фактор, который зачастую оказывается слабым звеном. Несколько отраслевых групп, включая институт SANS, разработали руководства (например, The Centre for Internet Security (CIS) Critical Security Controls), которые рекомендуют определенный набор действий по кибербезопасности, обеспечивающий конкретные и действенные способы блокировки самых распространенных и опасных атак [6].

Уже сейчас ясно, что безопасность устройств и платформ станет ключевым фактором в крупных видеопроектах, а поскольку информация о проблемах «Интернета вещей» распространяется все шире, компания MOBOTIX готовится к совместной с партнерами по отрасли, заказчиками и органами власти работе по защите всех технологий и систем, чтобы сделать общество более безопасным для всех.

Дополнительная информация

https://www.coresecurity.com/system/files/publications/2016/05/corelabs-ipcams-research-falcon-riva.pdf
https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/
https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Источники

[1] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.
[2] html https://www.coresecurity.com/advisories/hikvision-ip-cameras-multiple-vulnerabilities
[3] https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/
[4] http://www.telecomtv.com/articles/iot/internet-of-things-to-reach-25-billion-devices-within-five-years-11931/
[5] https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf
[6] https://uk.sans.org/critical-security-controls

Немецкая компания MOBOTIX разрабатывает и производит системы на базе IP-видеокамер, программное обеспечение для управления видео и анализа видеоданных с 2000 года.

Системы MOBOTIX известны своим **высоким уровнем надежности**. Все наружные камеры проходят экстремальные испытания при температурах от –30 до +60 °C. Они не имеют дополнительных элементов, систем подогрева и охлаждения, а также движущихся частей, поэтому практически не требуют технического обслуживания.

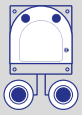
MOBOTIX предлагает **единое, комплексное решение**, включающее карту microSD для сохранения видеоданных, аудиопакет HD (с микрофоном и динамиком) с функциями интернет-телефонии и анализа видеоизображения, а также профессиональную систему управления видео и программное обеспечение для распознавания движения, которое сводит ложные срабатывания к минимуму.

Системе с **децентрализованной архитектурой** не требуется центральный компьютер, что значительно снижает нагрузку на сеть. Интеллектуальные камеры MOBOTIX самостоятельно обрабатывают и сохраняют изображения, запускают события, а в случае удаленного доступа регулируют частоту кадров и разрешение в зависимости от пропускной способности канала передачи данных.

Видеосенсоры 6MP Moonlight и предлагаемая дополнительно **тепловизионная технология** позволяют достоверно обнаруживать движущиеся объекты даже в самых неблагоприятных условиях освещенности и на большом расстоянии. Благодаря этому всего несколько камер способны охватить значительные площади. Они требуют меньшего количества кабелей, объектов ИТ-инфраструктуры и дополнительных источников освещения. Питание камер MOBOTIX обеспечивается по сети Ethernet мощностью не более 4–5 Вт.

Интеллектуальная система на базе IP-видеокамер MOBOTIX **снижает совокупные расходы**. Вложенные средства окупаются за короткий срок, а бесплатное программное обеспечение и обновления гарантируют работоспособность в течение многих лет.

Наружные камеры с двойным объективом

M16 AllroundDual	S16 FlexMount	D16 DualDome
		
Надежность в экстремальных условиях	Универсальная камера с двумя объективами	Модульная камера с двумя объективами

Тепловизионные

M16 Thermal	S16 DualThermal
	
Тепловизионная камера с двумя объективами	Тепловизионная камера с двумя объективами

Наружные камеры с одним объективом

M26 Allround	S26 FlexMount	Q26 Hemispheric	D26 Dome
			
Надежность в экстремальных условиях	Незаметная камера, анализ видеоданных	Незаметная камера, анализ видеоданных	Модульная, фиксированная, купольная

Для помещений

i26 Panorama	c26 Hemispheric	p26 Allround	v26 MiniDome
			
180° полусферическая	Незаметная камера, анализ видеоданных	Модульная потолочная камера	Антивандальная камера

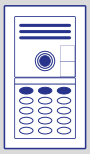
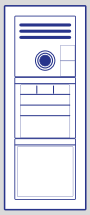
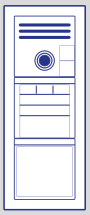
Дверные модули

Камера	BellRFID	Клавиатура
		

MxDisplay+

Абонентская станция


Дверные комплекты

Двухместная рамка		Трехместная рамка	
			

RU_11/17

MOBOTIX AG
Kaiserstrasse
D-67722 Langmeil
Тел.: +49 6302 9816-103
Факс: +49 6302 9816-190
sales@mobotix.com
www.mobotix.com

MOBOTIX