ТЕХНИЧЕСКИЙ ОБЗОР

Защита периметра средствами интеллектуального видеонаблюдения

Выбор датчиков, приложения и ключевые рекомендации по построению готового к будущему развитию решения по обеспечению безопасности в различных отраслях

Июль 2021

AXIS COMMUNICATIONS

Содержание

1 Краткая информация

Ограда является важнейшей составляющей "наружного слоя" системы защиты объекта, выступая в качестве барьера, заслона и средства отпугивания людей и животных. Для повышения эффективности ограда может быть дополнена другими защитными средствами, поскольку любой физический барьер может лишь на время задержать или осложнить вторжение.

Вдоль ограды располагают разного рода детекторы. По всему периметру ограды могут следовать проводные детекторы, а в стратегических точках периметра могут быть установлены радарные датчики, инфракрасные барьеры и лазеры.

Любые детекторы могут выдавать ложные тревоги, реагируя, например, на животных, движение растений и деревьев, погодные явления. Могут существовать и другие ограничения, например, конфликты частот при использовании радарных датчиков, или физические ограничения среды установки оборудования.

Камеры обладают очевидным преимуществом, когда нужно контролировать большие территории или несколько объектов. Современные сетевые решения для видеонаблюдения позволяют сочетать обработку данных в камерах и технологии искусственного интеллекта. Присущие этой технологии масштабируемость, эффективность и способность отпугивать нарушителей делают видеокамеры экономически высокоэффективным дополнением к любой системе безопасности.

Хотя появление камер и детекторов движения расширило диапазон и возможности решений для защиты периметра, они все еще могут сталкиваться с трудностями при обнаружении объектов в плохую погоду. Правильно откалиброванные и дополненные видеоаналитикой тепловизионные камеры могут обеспечить эффективное наблюдение и мониторинг при любых условиях освещения и практически в любую погоду.

Средства видеоаналитики прошли значительный путь развития и сегодня широко распространились даже в камерах для рынка домашней безопасности. Аналитические приложения позволяют сократить потребность в емкости хранения данных, записывая только фрагменты видео, содержащие представляющие интерес события. Когда записываемое видео обрабатывается непосредственно в камерах, существенно снижается нагрузка на сеть, поскольку с камер передаются только действительно важные видеоданные. Это дает очевидные преимущества в сценарии наблюдения из централизованной диспетчерской.

Как и для любой другой меры безопасности, оценку решения для защиты периметра необходимо проводить реалистично и соразмерно. Разумеется, главной целью является преодоление угроз.

Все большую популярность приобретает конвергентный подход к безопасности, учитывающий мнения и рекомендации разных подразделений, например, ИТ-службы и отдела эксплуатации. Сюда входит необходимость привлечения специалистов инженерного направления на как можно более раннем этапе.

Продемонстрировать окупаемость решения для безопасности, предотвращающего инциденты, может быть чрезвычайно сложно. Это связано главным образом с отсутствием потенциального дохода, который можно было бы сопоставить с затратами. Демонстрация ощутимой окупаемости возможна; примером могут быть решения, которые не только предупреждают персонал о подозрительном поведении или проникновении на территорию, но и инициируют автоматические меры реагирования.

2 Введение

Электронные решения для защиты периметра традиционно были уделом высокозащищенных государственных и коммерческих объектов и очень богатых людей. Однако с развитием технологий,

ростом конкуренции на рынке и последовавшим в результате снижением цен относительно высокотехнологичные решения стали доступны гораздо большему кругу пользователей.

Из чего состоит современное решение для защиты периметра? Какие технологии в нем применяются и как они могут обеспечить надежную и действенную защиту?

В этом техническом обзоре рассматриваются некоторые существующие сегодня подходы к защите периметра и применяемые для этого технологии.

3 Решения для защиты периметра

3.1 Физические решения

Физические решения часто являются одним из основных компонентов "внешнего слоя" многоуровневого подхода к защите объекта. Обычно они представляют собой ограду, часто из проволочной или сварной сетки, сварных секций или бетонных плит. Ограда периметра выполняет сразу множество функций, в том числе служит физическим барьером, который задерживает или предотвращает вторжение. Ограда также может препятствовать наблюдению извне, закрывая собой объекты; наконец, она является средством отпугивания и предотвращает проникновение животных. Для повышения эффективности ограда может быть дополнена такими элементами, как защита от перелезания, выделенные подъездные пути для автомобилей, заслоны.

Однако любой физический барьер лишь задерживает вторжение. Поэтому периметр необходимо также оснастить средствами автоматического обнаружения вторжений, способными подавать проверяемые сигналы тревоги в режиме реального времени, предоставлять сведения о местоположении, отслеживать объекты и обеспечивать возможность сбора доказательной базы и данных для расследования инцидентов.

3.2 Обнаружение вторжений на физическом периметре

Для защиты протяженных периметров часто применяют разного рода проводные "детекторы". они обычно представляют собой заглубленные в землю или проложенные по ограде провода, следующие по периметру ограды, и не обязательно прокладываются по прямой. Они также обеспечивают обнаружение за углами и **за перегибами рельефа**. Некоторые поставщики предлагают ограждения, оснащенные решениями для автоматического обнаружения.

Как и другие типы охранных датчиков, проводные детекторы могут давать ложные срабатывания (ложные тревоги). Ложные срабатывания часто бывают вызваны животными, движущимися растениями и деревьями, а также погодными явлениями. Проводные охранные датчики лучше всего работают вместе с системами видеонаблюдения. Видео позволяет не только подтвердить факт вторжения, но и выяснить причину тревоги. Само по себе проводное решение способно лишь выдать сигнал тревоги; оно не может дать информации о количестве нарушителей и других сведений, необходимых для реагирования.

3.3 Другие датчики вторжения

В стратегических местах периметра также могут устанавливаться другие детекторы вторжения, в том числе радары, ИК- и лазерные барьеры. Как уже говорилось, эти технологии имеют ограничения, включая ложные срабатывания и ограниченные возможности обнаружения по дальности и высоте, если не соблюдать правила установки.

Использование радаров на периметре может быть особенно проблематичным в присутствии других электронных устройств. Эти устройства могут работать в той же части радиочастотного спектра, и хотя тщательный подбор частот и уменьшение мощности могут уменьшить помехи, они также снижают эффективную дальность радара.

4 Решения на базе видео

4.1 Применение видеокамер

Современные сетевые видеокамеры совсем не похожи на автономные камеры старых аналоговых систем видеонаблюдения. Современные сетевые решения позволяют сочетать обработку данных в камерах и технологии искусственного интеллекта. Однако технологии достигли этого уровня лишь недавно и находятся еще в младенческом возрасте.

Камеры обладают очевидным преимуществом, когда нужно контролировать большие территории или несколько объектов. Присущие этой технологии масштабируемость, эффективность и способность отпугивать нарушителей делают видеокамеры экономически высокоэффективным дополнением к любой системе безопасности.

Если позволяет местное законодательство, камеры можно использовать для наблюдения и за физическим периметром, создавая дополнительную буферную зону наблюдения и потенциально предоставляя оператору больше времени на реагирование. Решения с использованием видеоаналитики позволяют инициировать сигналы тревоги в соответствии с заданным набором правил. Например, звуковой сигнал тревоги может включаться при приближении человека ближе 50 метров к ограде; если то же лицо входит в 10-метровую зону или задерживается в контролируемом пространстве дольше определенного времени, подается сигнал тревоги более высокого уровня.

4.2 Тепловизионные решения для видеонаблюдения

Сочетание камер видеонаблюдения и программных детекторов движения позволяет расширить зону действия и возможности решений для защиты периметра, перейдя от простого обнаружения к сложному анализу вторжений. В то же время эффективность видеонаблюдения может сильно снижаться при неблагоприятных погодных условиях.

Растущая доступность тепловизионных камер ведет к их все более широкому применению для охраны периметра. Правильно откалиброванные и дополненные видеоаналитикой тепловизионные камеры могут обеспечить эффективное наблюдение и мониторинг при любых условиях освещения и практически в любую погоду. Тепловизионные матрицы значительно превосходят по контрастности матрицы обычных камер и поэтому очень хорошо подходят для защиты периметра за счет лучшей чувствительности обнаружения.

Изображение на тепловизионной матрице формируется инфракрасным излучением самих объектов - например, автомобилей или людей. В сочетании с видеоаналитикой современные тепловизионные камеры с достаточной процессорной мощностью способны различать разные типы объектов-нарушителей и могут выдавать оператору предупреждения в соответствии с установленным списком условий, включая направление движения и скорость человека или автомобиля. Традиционные камеры тоже способны делать это, но только при наличии видимого света. Такие камеры рассматриваются в следующем разделе.

4.3 Камеры видимого диапазона

Все стандартные камеры видеонаблюдения видимого диапазона нуждаются для своей работы в естественном или искусственном освещении. Освещение для видеонаблюдения - это отдельная важная область знания, которой посвящено множество статей. Мы лишь повторим очевидный, но ключевой момент: стандартным видеокамерам нужен видимый свет. Освещение может создавать сложности в любой обстановке, с очевидными эффектами при изменении характеристик света. Один из факторов, которые часто упускают из вида или недостаточно понимают — это влияние погоды.

Тепловизионные камеры имеют свои преимущества, но это не означает, что они могут или должны быть прямой заменой камерам видимого диапазона — вовсе нет. Эти две технологии лучше всего работают вместе в составе единого интегрированного решения. Традиционные камеры не могут обнаруживать объекты на таких дальностях, как тепловизионные; с другой стороны, тепловизионные камеры не могут дать изображение с детализацией, достаточной для расследования, в противоположность камерам видимого диапазона. Эти две технологии часто используют совместно; при этом тепловизионная камера отвечает за обнаружение и подачу сигналов тревоги, а камера видимого диапазона дает доказательный материал и обеспечивает слежение.

4.4 Аналитика видеоконтента

Сетевое видеонаблюдение радикально расширило возможности систем безопасности. Эффективная иерархия разрешений позволяет организовать контролируемый доступ к видео, распространение и хранение записей для теоретически неограниченного круга заинтересованных лиц. Одно из технологических достижений, обеспечивающих еще большую масштабируемость - это видеоаналитика.

Видеоаналитика прошла большой путь развития, в немалой степени благодаря прогрессу технологий IP-камер. Свидетельство этому - камеры для домашних охранных систем, многие из которых теперь оснащены некоторым количеством аналитических функций, позволяющих, например, обнаруживать движение в зоне наблюдения. С камерой могут поставляться дополнительные функции, такие как детектор пересечения линий, обнаружение перемещенных объектов и даже подсчет людей.

Видеоаналитика позволяет сократить требования к ресурсам для хранения видео за счет того, что записываются только фрагменты, в которых что-то происходит. Кроме того, если записываемое видео обрабатывается непосредственно в камерах ("аналитика на периферии системы"), существенно снижается нагрузка на сеть, поскольку с камер передаются только действительно важные видеоданные. Это дает очевидные преимущества в сценарии централизованной диспетчерской, когда оператору необходимо проверять видео только когда поступает сигнал тревоги, значительно облегчая работу оператора и повышая эффективность деятельности в целом.

Существуют две обширные категории архитектур систем видеоаналитики: централизованные и распределенные. Централизованная архитектура подразумевает сбор информации с видеокамер и датчиков и направление ее на центральный сервер для анализа. В распределенных архитектурах периферийные устройства (сетевые камеры и видеокодеры) сами способны обрабатывать видео и извлекать содержательную информацию. Аналитические приложения, работающие на периферии системы, избавляют от необходимости иметь выделенные серверы для аналитики, а поскольку сжатие применяется только при передаче видеоданных на центральный сервер, анализ можно производить на несжатом видеопотоке. То есть мы имеем гораздо более экономически эффективную и гибкую архитектуру. На практике серверы, которые в обычной ситуации могли бы обработать лишь несколько видеопотоков из-за ограниченной процессорной мощности, справляются с сотнями видеопотоков, если большая часть обработки производится в камерах.

4.4.1 Скорость обработки и графические процессоры

Хотя многие аналитики прогнозируют замедление предсказанного Гордоном Муром экспоненциального роста производительности со временем уже в ближайшем будущем, сегодняшний рост вычислительной мощности в сочетании с уменьшением размеров позволяет производителям и разработчикам камер по-новому подходить к использованию процессорных ресурсов.

До недавнего времени вся дополнительная процессорная мощность использовалась для улучшения качества изображения, увеличения разрешения и более эффективного сжатия видео. Однако сейчас, по-видимому, рынок достиг некоторого плато спроса на разрешение. Соответственно производители теперь используют процессорные мощности для поддержки нового беспрецедентного уровня аналитических возможностей. Во многих случаях это означает, что вместо того, чтобы анализировать видео на мощных серверах, это можно делать в камере.

Уменьшение размеров и рост производительности современных процессоров позволяет встраивать в камеры графические процессоры с возможностями параллельной обработки, что открывает новые возможности для аналитики. Эти новые возможности привели к тому, что внимание разработчиков программного обеспечения переключилось на создание новых версий существующих проверенных серверных аналитических приложений, адаптированных для работы на периферии системы. Это, в свою очередь, способствует росту спроса на более интеллектуальные камеры с возможностями, не ограниченными только безопасностью и видеонаблюдением.

4.4.2 Глубокое обучение и искусственный интеллект

Значительный шаг в производительности аналитических приложений на периферии системы стал возможен благодаря графическим процессорам, но растет спрос и на другие виды технологий для задач видеонаблюдения, позволяющие реализовать такие функции, как подсчет людей и управление заполненностью. Развитие ИИ и машинного обучения привело к появлению встроенных в камеру специализированных процессоров глубокого (DLPU), которые радикально изменили ситуацию.

DLPU - это специализированный процессор для широкого применения алгоритмов глубокого обучения. Аналитика на базе глубокого обучения позволяет достигать высокой точности обнаружения и классификации, поскольку обучение алгоритма происходит на реальных объектах. Это означает, что решение для обнаружения вторжений, защищающее периметр, можно настроить так, чтобы оно реагировало только на строго определенные объекты и сценарии, реализуя сложные цепочки условий.

Система может распознавать и идентифицировать даже объекты, видимые лишь частично, например, автомобиль по заднему бамперу. На момент написания этой статьи, несмотря на некоторые смелые заявления, большинство представленных на рынке проверенных решений способны различать лишь людей и автомобили разных типов. Однако модели камер со средствами аналитики, способными к более детальному различению, например, к определению цвета одежды человека, уже находятся на продвинутых стадиях испытаний.

Такие успехи технологии могут привести к появлению высокоспециализированных систем обнаружения, способных идентифицировать и различать сотрудников, клиентов, случайных прохожих и потенциальные угрозы. С точки зрения безопасности углубленная аналитика в сочетании с продуманной системой физической безопасности позволяет построить решение для обнаружения и предотвращения правонарушений с более высокой эффективностью и точностью. Следующий этап развития возможностей может быть не так уж и далек.

5 Затраты

5.1 Оценка и измерение окупаемости инвестиций

Как и для любой другой меры безопасности, оценку решения для защиты периметра с точки зрения уязвимости и устойчивости необходимо проводить реалистично и соразмерно. Разумеется, главной целью является преодоление угроз, диапазон которых для почти всех крупных корпоративных или государственных объектов в современных условиях очень широк, от случайных нарушителей до массовых протестов и даже террористов.

Все большую популярность приобретает конвергентный подход к безопасности, учитывающий мнения и рекомендации разных подразделений, например, ИТ-службы и отдела эксплуатации. Сюда входит необходимость привлечения специалистов со знаниями инженерных требований на как можно более раннем этапе. Традиционно в качестве стартовой точки при выборе мер защиты периметра использовались традиционные меры защиты, отпугивающие и задерживающие потенциального нарушителя. Только после этого проектировщик системы безопасности "прикручивал" к ним технические системы обнаружения. Однако сегодня, в условиях растущего числа интегрированных между собой мер и систем, требуется более взвешенный и целостный подход.

Продемонстрировать окупаемость решения для безопасности, предотвращающего инциденты, может быть чрезвычайно сложно. Это связано в первую очередь с отсутствием потенциального дохода, который можно было бы сравнить с затратами. Обычно сотрудникам службы безопасности приходится объяснять коллегам из финансового отдела стоимость разного рода инцидентов в сфере безопасности; это могут быть как прямые затраты, связанные с потерей и уничтожением активов, так и косвенные, связанные с ущербом для репутации.

Тем не менее продемонстрировать реальную окупаемость инвестиций возможно, особенно если применение технологий сокращает потребность в определенных ручных вмешательствах или позволяет перенацелить персонал службы безопасности на другие задачи. Примером могут быть решения, которые не только предупреждают персонал о подозрительном поведении или проникновении на территорию, но и способны реализовать автоматические "мягкие" меры реагирования. Это могут быть IP-аудиосистемы, транслирующие записанные звуковые предупреждения, или мигающие надписи, информирующие потенциального нарушителя, что он обнаружен, и предписывающие ему покинуть территорию.

Если в состав решения входят камеры видеонаблюдения, можно повысить эффективность реагирования, демонстрируя нарушителю, что он идентифицирован, например, выводя на экран номер автомобиля или даже изображение самого нарушителя. Только если эти меры не дают нужного эффекта, на место высылается охрана для расследования и принятия более жестких мер. Такой многоуровневый подход к реагированию на тревоги может быть более уместным снаружи периметра. Он сокращает необходимость вмешательства персонала на ранних этапах, освобождая человеческие ресурсы, что представляет собой очевидный выигрыш.

5.2 Оценка стоимости

Оценку стоимости необходимо производить на базе совокупной стоимости владения (TCO) системы. TCO включает в себя все затраты на решение на протяжении всего жизненного цикла; затраты на материалы и рабочую силу, на исследования, на установку системы и ее эксплуатацию, на техобслуживание, вывод из эксплуатации и утилизацию. Это может потребовать изменения подходов со стороны отделов финансов и снабжения, поскольку может потребоваться перераспределение средств между операционными и капитальными затратами.

Как и для любого другого материального актива, организации необходимо знать срок службы решения для защиты периметра. Сотрудники службы безопасности и ИТ-отдела могут помочь своим коллегам из финансового отдела, объяснив и показав, как приобретение правильной технологической платформы для будущих решений может сэкономить средства. Особенность интеллектуальных устройств охранного наблюдения в том, что они имеют определенный запас ресурсов на будущее. А именно, устройства с достаточной процессорной мощностью позволяют неоднократно воспользоваться преимуществами новых этапов технологического развития, в первую очередь благодаря аналитической обработке на базе ИИ и машинного обучения.

6 Предложение Axis Communications

Открытый подход Axis к интеграции с решениями партнеров означает, что ее сетевые датчики в сочетании с проверенными средствами видеоаналитики и искусственным интеллектом позволяют реализовать высокоэффективные интегрированные решения для защиты периметра с высоким уровнем кибербезопасности и хорошими экономическими показателями в масштабах всего предприятия и на протяжении всего срока службы системы.

Там, где тепловизионные датчики могут быть неэффективны, отличной альтернативой может быть радарная (СВЧ) технология, обладающая во многом схожими преимуществами при потенциально еще меньшем уровне ложноположительных срабатываний. В радарах Axis используются такие же технологии машинного обучения и глубокого обучения, что и в старших моделях камер видеонаблюдения. Радары Axis способны точно обнаруживать, классифицировать и отслеживать людей и автомобили с практически нулевым уровнем ложных тревог.

Радарная технология работоспособна и днем и ночью и практически нечувствительна к таким распространенным помехам, как движущиеся тени и световые блики, мелкие животные и насекомые, а также погодные явления. Это обеспечивает очень высокие экономические показатели решения, позволяя охране сосредоточиться на реальных подтвержденных угрозах. Радар способен определять скорость объекта, что позволяет точно рассчитывать место контакта или даже применять ограничения скорости.

Эффективность решения обычно стоит первым пунктом в любом запросе информации или опроснике по анализу рынка. Камеры Axis выполнены на высокопроизводительных фирменных процессорах ARTPEC, разработанных Axis, которые позволяют исполнять в камере самые сложные приложения видеоаналитики. Важно, что это решение базируется на собственных разработках, а не на компонентах стороннего поставщика.

Благодаря такому размещению "интеллекта" на периферии системы несколько камер могут параллельно отслеживать несколько событий, происходящих одновременно в разных местах. Такая распределенная архитектура позволяет по мере потребности расширять решение до необходимого числа камер без вложения дополнительных средств в центральные серверы.

Сертифицированное британскими правительственными ведомствами решение AXIS Perimeter Defender (APD) позволяет обнаруживать четыре разных типа событий для одного или нескольких людей и автомобилей:

- • несанкционированное проникновение в заданную зону;
- • движение по контролируемой зоне в определенном порядке и направлении;
- • движение по контролируемой зоне при определенных условиях;
- присутствие посторонних

Возможности APD не ограничиваются сигнализацией о вторжении и съемкой соответствующего видео. Это ПО также предоставляет метаданные, которые можно отображать поверх видеоизображения для указания границ и траекторий движения людей и автомобилей. В рамках более интегрированного подхода камеры Axis (видимого диапазона или тепловизионные) можно сочетать с IP-громкоговорителями Axis, транслирующими автоматические сообщения при обнаружении нарушителя, возможно, в автономном режиме. Такие автоматические уведомления позволяют постепенно наращивать уровень ответных мер и противодействия им, что помогает оценить намерения нарушителя и требуемый уровень ответа.

APD может интегрироваться непосредственно с программным обеспечением, традиционно применяемым в корпоративных платформах (например, Genetec, Milestone, Seetec, Prysm, Qognify и т.д.).

Axis предоставляет бесплатные инструменты для проектирования после обследования объекта и поддержку на всех этапах проекта – от выбора нужных продуктов исходя из конкретных критериев до точного расчета требований к хранению данных, установки технического решения и управления системами. Инструменты Axis помогают консультантам планировать и оценивать систему, а интеграторам - проще и эффективнее управлять проектами. Эти инструменты также облегчают поддержание безопасности установленных систем, упрощая установку обновлений и исправлений системы безопасности.

Несмотря на меняющиеся угрозы и меры противодействия, один критически важный аспект остается неизменным: целостность и безопасность периметра. Периметр - важнейший объект для тех, кто отвечает в организации за создание безопасной и защищенной среды для персонала, посетителей и публики. В этой статье рассказывается о преимуществах интегрированного технологического подхода к планированию безопасности периметра. Также подчеркивается, что инвестиции в технологии безопасности требуют обоснования окупаемости. В любом случае понимание возможностей современных технологий и тенденций развития - это то, что необходимо любому практику для разумного подхода к операционной безопасности и закупкам новых технологий, независимо от его места работы, должности и отрасли.

Информация о продукции

Тепловизионные IP-камеры:

AXIS Q19 и другие www.axis.com/en-gb/products/thermal-cameras

Аналитическое ПО:

Приложение для охраны периметра AXIS Perimeter Defender

www.axis.com/en-gb/products/axis-perimeter-defender

Внешние IP-громкоговорители:

AXIS C1310-E www.axis.com/en-gb/products/axis-c1310-e

Охранный IP-радар:

D2110-VE www.axis.com/en-gb/products/axis-d2110-ve

T10169467/RU/M1.3/2107

О компании Axis Communications

Компания Axis вносит весомый вклад в формирование более разумного и безопасного мира, разрабатывая решения, которые повышают безопасность и эффективность бизнеса. Занимая в отрасли технологий сетевого видео ведущие позиции, компания Axis поставляет решения для видеонаблюдения, контроля доступа, сетевых домофонов и звукового сопровождения. Эффективность наших решений повышается благодаря приложениям интеллектуальной аналитики и высококачественному обучению.

Около 4000 специалистов компании Axis трудятся более чем в 50 странах мира, вместе с нашими партнерами по технологиям и по системной интеграции разрабатывая и внедряя решения задач, стоящих перед клиентами по всему миру. Компания Axis была основана в 1984 году. Штаб-квартира компании находится в городе Лунд, Швеция