ТЕХНИЧЕСКИЙ ОБЗОР

Защита периметра аэропорта с использованием видеоаналитики

Соображения по функциональности и окупаемости

Июль 2021

AXIS COMMUNICATIONS

Содержание

1 **Краткая информация** 3

2 **Введение** 3

3 **Традиционные решения для охраны периметра** 4

3.1 Физические решения 4

3.2 обнаружение вторжения у оград и ворот 4

3.3 Детекторы вторжения снаружи ограды 4

4 **Решение проблем защиты периметра аэропорта** 5

4.1 Новые интеллектуальные решения для видеонаблюдения 5

5 **Затраты и услуги** 5

5.1 Оценка и измерение окупаемости инвестиций 5

5.2 Оценка стоимости 6

6 **Предложение Axis Communications** 6

7 **Информация о продукции** 7

1 Краткая информация

Традиционная защита периметра аэропортов обычно представляет собой ограды или стены, ограничивающие периметр и предотвращающие вторжение. Периметр также должен быть оборудован средствами обнаружения вторжения, передающими сигналы тревоги на диспетчерский пункт. В число доступных решений для обнаружения на периметре и вокруг него входят проводные детекторы, СВЧ датчики, инфракрасные ограждения. Все эти средства полезны, но не лишены недостатков. Одна из проблем - пропуски нарушителей, вторая, не менее неприятная - ложные срабатывания, которые в долгосрочной перспективе могут привести к игнорированию действительно серьезных инцидентов.

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. 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.

В последние годы была значительно усовершенствована и подешевела тепловизионная технология обнаружения. Тепловизионные камеры в сочетании с ПО видеоаналитики обеспечивают круглосуточную защиту вне зависимости от условий освещения. Тепловизионная технология часто является удачным вариантом для аэропортов, поскольку обеспечивает отличную эффективность обнаружения в системах большой протяженности.

Тем, где использование тепловизионной технологии невозможно, отличной альтернативой может быть радарная технология, обладающая схожими преимуществами. Радар Axis способен различать разные виды объектов и может интегрироваться с PTZ-камерами для эффективного отслеживания объектов. Эта технология может работать и днем, и ночью с минимальным количеством ложных срабатываний, экономя средства за счет снижения затрат на расследования и сокращения численности охраны, которая может сосредоточиться на реальных угрозах.

Оценка решения для защиты периметра требует реалистичного и соразмерного подхода. Главной целью всегда является преодоление угроз, но при этом система должна соответствовать всем законодательным требованиям.

Продемонстрировать окупаемость решения для безопасности обычно бывает сложно, поскольку отсутствует доход, который можно было бы сравнить с затратами. Однако замена ручного вмешательства технологиями позволяет получить ощутимый результат. Камеры также могут использоваться для повышения эффективности. Например, можно выводить на экран изображение, показывающее нарушителям, что их идентификационные данные записываются.

Камеры Axis оснащены мощным набором функций для улучшения изображения, лучшего взаимодействия с другим оборудованием и более эффективного сжатия. Они выполнены на фирменных процессорах ARTPEC, разработанных Axis, позволяющих исполнять приложения видеоаналитики для защиты периметра непосредственно в камерах. Такая распределенная архитектура позволяет наращивать число камер по мере необходимости без вложения дополнительных средств в центральные серверы.

2 Введение

Безопасность критического объекта стоит на двух основах: проектирование и защита. Аэропорты часто рассматриваются как элементы особо ответственной инфраструктуры, и к ним предъявляются требования по ограничению рисков вторжения путем реализации соответствующих охранных решений. Такое решение является частью структурированного многоуровневого подхода,

включающего в себя физические барьеры, обнаружение вторжений, контроль доступа и мобильные охранные патрули.

Меры по защите зон ограниченного доступа аэропорта должны, естественно, учитывать имеющиеся угрозы и условия работы, в том числе **авиационные требования**, топографию местности, климатические условия и ограничения, связанные с окружающей средой. Цель этого технического обзора - представить некоторые существующие сегодня подходы к защите аэропортов и применяемые для этого технологии.

3 Традиционные решения для охраны периметра

3.1 Физические решения

Физические решения часто являются одним из основных компонентов "внешнего слоя" многоуровневого подхода к защите объекта. Они обычно представляют собой ограду, часто из проволочной или сварной сетки, сварных секций или бетонных плит. Вблизи радионавигационного и телекоммуникационного оборудования используются ограды из немагнитных материалов. Такие ограды выполняют несколько функций: они четко обозначают границы аэропорта, а также препятствуют проникновению людей и животных. К ограде могут быть добавлены такие элементы, как защита от перелезания, подъездные пути для автомобилей, фундаменты, заслоны.

Для повышения безопасности периметр следует оснастить решениями для автоматического обнаружения, передающими сигнал на диспетчерский пункт в случае вторжения.

3.2 обнаружение вторжения у оград и ворот

Существует несколько типов проводных "детекторов" для охраны протяженных периметров; все они передают сигналы тревоги в реальном времени оператору охранной системы. Некоторые поставщики предлагают ограждения, оснащенные решениями для автоматического обнаружения.

Такие решения, однако, не лишены недостатков и могут давать ложные срабатывания (ложные тревоги). Ложные срабатывания могут быть вызваны животными, движением растений и деревьев, погодными явлениями. В отсутствие видеонаблюдения единственный способ выяснить, что вызвало тревогу, - это направить на место охрану для проверки. Многократные ложные срабатывания могут вызывать усталость у охранников, которые в результате могут начать игнорировать тревоги и в конце концов пропустить реальную угрозу.

3.3 Детекторы вторжения снаружи ограды

В стратегических местах по периметру аэропорта также устанавливаются другие детекторы вторжения, например, СВЧ-датчики, ИК- и лазерные барьеры. Как уже говорилось, они имеют ограничения, включая ложные срабатывания и ограниченные возможности обнаружения по дальности и высоте, если строго не выдерживать правила установки. В авиационных применениях особенно проблематичным может быть использование на периметре радарных (СВЧ) датчиков, поскольку они могут нарушать работу других технических средств, работающих в этом же радиодиапазоне. Уже одного этого достаточно, чтобы от них отказаться. Потенциальные проблемы, создаваемые такими устройствами, можно почти полностью устранить путем тщательного подбора частот и ограничения мощности и тем самым эффективной дальности.

4 Решение проблем защиты периметра аэропорта

4.1 Новые интеллектуальные 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 качестве примера можно привести тепловизионные камеры, которые в сочетании с ПО видеоаналитики позволяют реализовать круглосуточную защиту вне зависимости от условий освещения. Тепловизионная технология часто является удачным выбором для аэропортов, поскольку обеспечивает отличную эффективность обнаружения в системах большого размера.

Тепловизионные камеры формируют изображение на основании инфракрасного излучения объектов, например, автомобилей или людей, и способны обнаруживать их и днем и ночью, на большой дальности и почти при любых погодных условиях. В сочетании с видеоаналитикой современные тепловизионные камеры с достаточной процессорной мощностью способны различать разные типы объектов и могут выдавать оператору предупреждения в соответствии с установленным списком условий, включая направление движения и скорость объекта-нарушителя и его тип (человек/автомобиль). Традиционные камеры тоже способны делать это, но они работают с видимым светом, что накладывает трудноустранимые и очевидные ограничения.

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, использующие видеоаналитику, позволяют подавать сигналы тревоги исходя из заданных правил, например, если кто-либо приближается к ограде на расстояние менее 50 метров. Затем, если то же лицо приближается ближе чем на 10 метров или остается в определенной зоне дольше определенного времени, подается сигнал тревоги более высокого уровня.

В последние годы тепловизионная технология обнаружения была значительно усовершенствована и стала доступнее. Конкурентные цены и возможность эффективного наблюдения на больших расстояниях при любом освещении и в плохую погоду сделали эти тепловизионные камеры одной из наиболее предпочтительных технологий для защиты периметра от вторжений.

5 Затраты и услуги

5.1 Оценка и измерение окупаемости инвестиций

Как и для любой другой меры безопасности, оценку решения для защиты периметра необходимо проводить реалистично и соразмерно. Разумеется, главной целью является преодоление угроз, диапазон которых для современного аэропорта очень широк, от массовых протестов до террористов, но при этом система должна соответствовать всем законодательным требованиям.

Все большую популярность приобретает конвергентный подход к безопасности, учитывающий данные и рекомендации разных подразделений, например, ИТ-службы и отдела эксплуатации. Кроме того, особенно в случае аэропортов с их большими территориями с ограниченным доступом, имеется необходимость подключать на как можно более раннем этапе участников с инженерными требованиями. Традиционно в качестве стартовой точки при построении системы защиты периметра

выбирались традиционные меры защиты, отпугивающие и задерживающие потенциального нарушителя. Только после этого к этим традиционным мерам "прикручивались" технические системы обнаружения. Однако сегодня, в условиях растущего числа интегрированных между собой мер и систем, лучше уже на раннем этапе применять более целостный подход.

Продемонстрировать окупаемость решения для безопасности может быть чрезвычайно сложно. Это связано в первую очередь с отсутствием 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 или повреждением активов, так и косвенные, связанные с ущербом для репутации компании или бренда.

Тем не менее продемонстрировать реальную окупаемость инвестиций возможно, особенно если применение технологий сокращает потребность в ручном вмешательстве или позволяет перенацелить персонал 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, например, звуковые предупреждения или мигающие надписи, указывающие нарушителям, что те обнаружены и должны покинуть территорию.

Если в состав решения входят камеры, повышения эффективности можно достичь, показывая нарушителю, что его идентификационные данные зарегистрированы, например, выводя на экран номер автомобиля или даже изображение самого нарушителя. Только если эти предварительные меры не дают нужного эффекта, на место высылается охрана для принятия более жестких мер. Такой многоуровневый подход к реагированию на тревоги может быть более уместным снаружи периметра, но он позволяет в некоторой степени сократить численность охраны, освободив ресурсы, что представляет собой очевидный выигрыш.

5.2 Оценка стоимости

Оценку стоимости необходимо производить на базе совокупной стоимости владения (TCO) системы, которая 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 нестандартных подходов со стороны отделов финансов и снабжения, поскольку может потребоваться перераспределение средств между операционными и капитальными затратами.

6 Предложение Axis Communications

Открытый подход Axis к интеграции с решениями партнеров означает, что ее тепловизионные сетевые камеры в сочетании с проверенными средствами видеоаналитики позволяют строить высокоэффективные интегрированные решения для защиты периметра аэропортов с высоким уровнем кибербезопасности и хорошими экономическими показателями на протяжении всего срока службы системы.

Там, где тепловизоры могут быть неэффективны, отличной альтернативой может быть радарная (СВЧ)-технология, обладающая во многом схожими преимуществами. Радары Axis способны отличать людей от автомобилей, могут давать информацию о скорости и направлении движения, интегрируются с PTZ-камерами Axis для эффективного наведения на объект и подходят для любой части многоуровневого охранного решения — не только для периметра. Как и тепловизионная технология, радарная работает в любое время суток с минимальным количеством ложных срабатываний, поскольку она нечувствительна к таким типичным помехам, как тени, изменения

освещенности, мелкие животные, капли дождя, насекомые, ветер и плохая погода. Со временем это ведет к растущей экономии за счет снижения затрат на расследования и возможности сокращения численности охраны, которая может сосредоточиться на реальных угрозах.

Камеры оснащены множеством высокотехнологичных функций: Электронная стабилизация изображения (EIS) компенсирует перемещения с большой и малой амплитудой; несколько портов ввода-вывода для сигналов тревоги позволяют подключать внешнее оборудование; высокоэффективная технология сжатия Zipstream уменьшает требования к пропускной способности и ресурсам хранения данных.

Камеры Axis выполнены на фирменных процессорах ARTPEC, разработанных Axis, которые позволяют исполнять встроенные приложения видеоаналитики для защиты периметра непосредственно в камерах. Благодаря этому 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.

Камеры способны обнаруживать четыре разных типа событий, следя за несколькими людьми и автомобилями:

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

Тепловизионные камеры Axis могут работать совместно с IP-громкоговорителями Axis, при обнаружении инициируя воспроизведение автоматических голосовых сообщений в адрес потенциальных нарушителей.

Технологические решения Axis непосредственно интегрируются с традиционными программными платформами для аэропортов (Genetec, Milestone, SeeTec, Prysm и т.д.).

Чтобы выяснить, какое оборудование необходимо для построения усиленного решения для защиты периметра, и определить цену решения, необходим как теоретический анализ, так и посещение места установки. В помощь интеграторам Axis предоставляет инструменты для планирования, проектирования, установки решений и управления ими.

Инструменты проектирования Axis предоставляются бесплатно, плюс на всех этапах проекта интегратор получает поддержку – от выбора нужных продуктов исходя из конкретных критериев до планирования объектов, установки и управления системами. Использование инструментов Axis помогает интегратору легче и эффективнее реализовать свои проекты.

Эти инструменты помогают интегратору выбирать подходящие продукты и оптимально планировать системы, исходя из оценок и рекомендаций, адаптированных к конкретным техническим требованиям, и в результате ускоряют поставку готовых решений. Эти инструменты также облегчают интегратору поддержание безопасности установленных систем, упрощая установку программных обновлений и исправлений.

7 Информация о продукции

Тепловизионные IP-камеры: серия AXIS Q19

www.axis.com/global/fr/products/axis-q19-series

Аналитическое ПО: AXIS Perimeter Defender

www.axis.com/global/fr/products/axis-perimeter-defender

Внешние IP-громкоговорители: AXIS C3003-E Network Horn Speaker

www.axis.com/global/fr/products/axis-c3003-e

IP-радар

www.axis.com/global/fr/products/axis-d2050-ve

О компании Axis Communications

Компания Axis вносит весомый вклад в формирование более разумного и безопасного мира, разрабатывая и внедряя сетевые решения, которые не только способствуют повышению безопасности, но и открывают новые пути ведения бизнеса. Занимая в отрасли ведущие позиции, компания Axis поставляет продукцию и оказывает услуги в сфере сетевого охранного видеонаблюдения и аналитики, контроля доступа, сетевых домофонов и звукового сопровождения. Свыше 3800 специалистов компании Axis трудятся более чем в 50 странах мира, вместе с нашими партнерами разрабатывая и внедряя решения стоящих перед нашими клиентами задач. Компания Axis была основана в 1984 году. Штаб-квартира компании находится в городе Лунд, Швеция.

Более подробную информацию о компании Axis можно найти на нашем веб-сайте *axis.com*.