Видеонаблюдение на объектах критической инфраструктуры

Рассмотрены типовые задачи, которые необходимо решить, внедряя системы видеонаблюдения на объектах критической инфраструктуры, и возможные варианты решения проблем. Показано, какое оборудование подходит для интеграции такой системы.

ООО «НПО «АвалонЭлектроТех», г. Москва

В статье будут рассмотрены типовые задачи, которые решаются интегратором совместно с заказчиком при реализации проектов по видеонаблюдению на объектах критической инфраструктуры. Также будут обозначены ключевые моменты, на которые стоит обратить внимание при выборе оборудования или комплексного решения.

Прежде всего уточним, о какой части объекта идет речь. Комплекс средств защиты объекта можно разделить на три условных блока: охрану периметра, защиту внутренней территории и защиту непосредственно зданий. Сегодня мы рассмотрим возможные решения для использования в этих подсистемах. В качестве примера возьмем случай, когда злоумышленник или группа проникают через ограждение. Как вариант, оно просто отсутствует, а может быть, не сработал первый периметральный рубеж охраны. Так или иначе, но теперь злоумышленник передвигается по территории объекта.

Существует сценарий, где к реакции системы на вторжение выдвигаются высокие требования:

- необходимо активное реагирование на злоумышленников, даже, возможно, с проактивным воздействием до приезда группы ГНР;
- в пределах огороженного участка находится обширная территория, необходимо информирование о необычной активности в этом районе;
- нужно решение с очень низким уровнем ложных тревог, чтобы не отвлекать сотрудников службы безопасности на объекте, не заставлять их реагировать на частые сработки оборудования или модулей видеоаналитики;
- система должна быть способна работать в условиях большой интенсивности движения в кадре видеокамеры (это мельтешение деревьев и кустов, движущиеся тени в течение дня, изменение погоды – дождь, ветер, снег), а также при сложных условиях освещения (сильный свет или, наоборот, полная темнота).

Вопросы для решения:

- Как обнаружить и проверить наличие движения людей или транспортного средства на территории?
- Как идентифицировать нарушителя?
- Какую платформу выбрать для управления системой видеонаблюдения?
- Как автоматизировать процессы детектирования и реакции?

А теперь проанализируем возможные варианты решения проблем, которые мы обозначили в начале статьи. Рассмотрим один из вариантов детекции нарушителей – аналитические модули, которые работают непосредственно на платформе видеокамеры (рис. 1). Чаще всего это детекторы движения в зоне, пересечения виртуальной линии, реагирующие на присутствие в зоне более положенного времени. Современные аналитические модули, работающие на платформе камер, в большинстве случаев разработаны с использованием алгоритмов глубокого обучения для классификации людей и транспортных средств. В этом случае в интерфейсе камеры присутствует функциональность для калибровки сцены, обеспечивающая ее 3D-представление (автоматическое или ручное) и настройку перспективы.

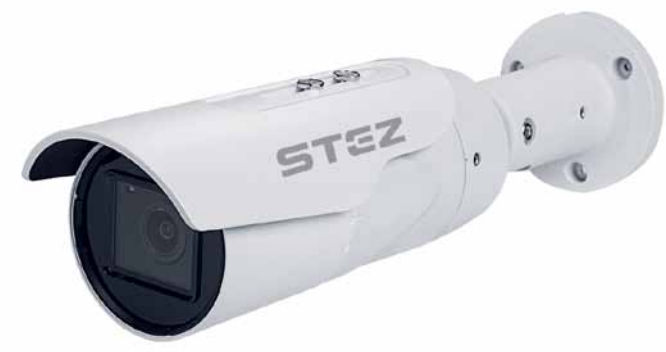

Рис. 1. Сетевая видеокамера STEZ KV-P1015-LVE

Подобный подход позволяет значительно снизить уровень ложных тревог и реагировать на реальные случаи тревоги. Кроме того, решения на базе алгоритмов глубокого обучения позволяют обеспечить визуальное подтверждение обнаруженных объектов в реальном времени и в записанном видео с наложением метаданных в виде ограничительной рамки для транспортных средств и людей, а также траекторий для отслеживания их движения. Важным моментом в этом случае является интеграция подобных модулей видеоанализа и тревог от них в платформу верхнего уровня (систему видеонаблюдения или интеграционную платформу). У каждого такого решения есть собственное API для интеграции, но разработчикам систем верхнего уровня удобнее работать с универсальными интерфейсами, например, через ONVIF и др.

Одним из дополнительных плюсов такого подхода (аналитика на стороне конечного устройства – видеокамеры) является снижение нагрузки на сервер видеозаписи или сервер видеоанализа, которые в этом случае будут обрабатывать только метаданные о произошедшем событии и не будут затрачивать свои ресурсы на обработку видеоизображения. А это уже экономия на конфигурации серверов или их количестве.

В качестве конечных устройств для установки на объекте могут выступать не только камеры визуального спектра. Это могут быть и тепловизоры (рис. 2), которые применимы для условий отсутствия дополнительного освещения и протяженных периметров, а при формировании изображения более устойчивы к плохим погодным условиям (засветка, туман, снег, дождь). Они могут обладать функциональностью встроенных аналитических модулей на основе алгоритмов глубокого обучения. Один из объектов, для которых подходит такое оборудование, – это очистные сооружения, где парение часто делает невозможным наблюдение в видимом спектре, а использование тепловизоров позволяет расширить зону наблюдения. Конечно, ИК-спектр излучения тоже подвержен рассеиванию во влажном воздухе, но в меньшей степени. Если же возникает необходимость контролировать элементы горения при дожигании побочных газов, определить перегрев

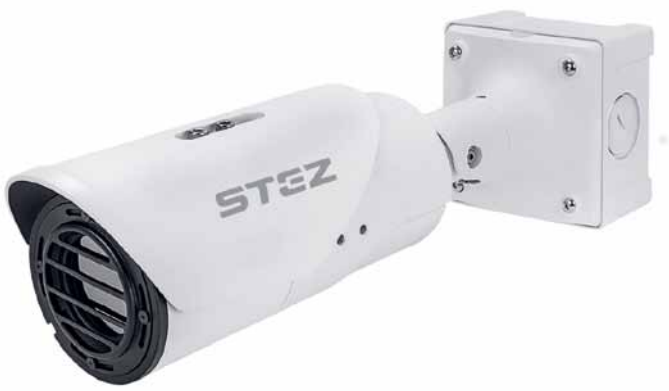

Рис. 2. Сетевая уличная тепловизионная видеокамера KV-P6012-E (19 мм)

оборудования на подстанции и выполнять другие задания такого рода, то можно использовать тепловизионное оборудование с уже откалиброванным сенсором, который способен показать температуру в контролируемой зоне и выдать тревогу при выходе за установленные пределы (опять же, важен процесс интеграции таких устройств и тревог от них в систему верхнего уровня).

При получении тревоги возникает необходимость визуализировать место сработки и рассмотреть его более детально. Для этого в состав решения обязательно добавляют PTZ-камеры (рис. 3), способные по сигналу, поступившему от периметрального оборудования, от модулей видеоанализа на камере или от ПО верхнего уровня, повернуться на тревожный участок и значительно увеличить сцену для большей детализации. За счет использования оптики с кратностью зума 30x и более, а также матриц с большим разрешением оператор получает детализированное изображение для анализа ситуации. Если же необходима проактивная реакция на событие (например, до обследования места тревоги охраной или приезда ГНР), можно добавить в систему прожекторы видимого света, которые будут включаться в ночное время по тревоге, или сетевые динамики (рис. 4), на которые можно заранее записать аудиоконтент и запускать нужный файл по сигналу от охранной системы или напрямую от камеры видеонаблюдения. Подобные решения для реакции на тревогу (сетевые динамики или рупоры) позволяют быстрее реагировать на ситуацию и дают понять нарушителям, что данный объект, внутренняя территория, служебная парковка находятся под постоянным наблюдением и факт нарушения

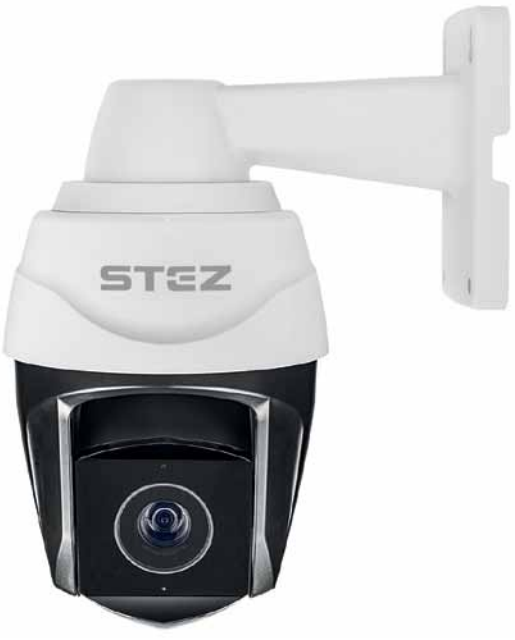

Рис. 3. Сетевая уличная поворотная видеокамера KV-P5015-LE

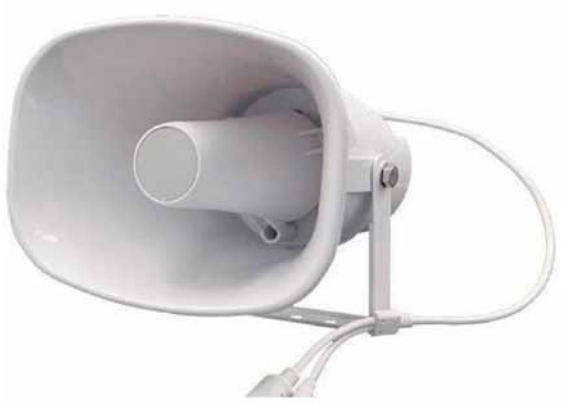

Рис. 4. Сетевой рупор STEZ NS-M2003-E

уже установлен. Для удобства интеграции сетевого аудио в комплексную систему безопасности в данном оборудовании предусмотрены несколько методов взаимодействия между оператором и динамиками. Это может быть SIP-протокол для звонка с телефона оператора, интерфейс ONVIF для интеграции оборудования в ПО верхнего уровня, сетевые микрофоны с возможностью программирования кнопок быстрого вызова для активации на динамике нужного аудиофайла.

При выборе системы верхнего уровня для управления оборудованием видеонаблюдения (и в некоторых случаях сетевым аудио) стоит обратить внимание на несколько моментов. Прежде всего это возможность интеграции в новую систему уже установленных на объекте камер видеонаблюдения или видеорегистраторов с подключенным оборудованием. Какая функциональность конечных устройств интегрирована в платформу (что можно получить от камер, кроме видеопотока)? Есть ли возможность настройки изображения через интерфейс оператора системы, доступны ли тревоги от встроенных в оборудование аналитических модулей, можно ли использовать карты памяти на камерах для резервирования записи в момент пропадания связи с видеосервером?

Также стоит обратить внимание на то, как реализован модуль видеонаблюдения в рамках интеграционной платформы. Будет ли это отдельная видеоподсистема с возможностью настройки конфигурации видеооборудования и видеоаналитики с полной интеграцией функциональности оборудования видеонаблюдения, или мы будем использовать интеграционную платформу для отображения видеопотоков с камер и визуализации тревожных сообщений, а все настройки конечного оборудования производятся из специализированного ПО от вендора камер. Это может сильно повлиять на процесс администрирования системы и ее первичной пусконаладки.

Важная функция современных систем видеонаблюдения – поддержка мультикастинга при работе с видеопотоками. На больших объектах может быть очень много операторов системы, которые пользуются видеоконтентом в реальном времени. В этих случаях либо предусматривается сервер распределения видеопотоков, либо используют мультикастинг при работе с видеокамерами. Это существенно снижает нагрузку на серверы управления видеоподсистемой, и вся нагрузка уходит на сетевое оборудование.

В текущих условиях стоит также обратить более пристальное внимание на производителей оборудования для видеонаблюдения, поскольку многие вендоры ушли с нашего рынка, а среди оставшихся не все настроены на постоянную работу в части поддержания актуальности сертификации оборудования, технической поддержки на стадии его подбора и гарантийных обязательств после реализации продукции.

А. Ю. Новак, менеджер по продукции
«Комплексные системы безопасности»,
ООО «НПО «АвалонЭлектроТех»,
г. Москва,
тел.: +7 (495) 933-8548,
e-mail: info@avalonelectrotech.ru,
сайт: www.avalonelectrotech.ru