"Реальное" и "нереальное" видео. Практические задачи СОТ

Тема этой статьи вызвана тем, что вокруг СОТ в последнее время разгорается серьезная дискуссия по различным вопросам применения, характеристик, перспектив развития. Сразу оговорюсь, в данной статье буду касаться только систем противокриминальной защиты

Александр Крахмалев
Заместитель генерального директора
ООО "СИГМА-ИС", к.т.н., проф.,
академик ВАНКБ

Противокриминальная защита – термин, который пока еще не прижился. Он был введен при разработке проекта технического регламента МВД России (разработчик НИЦ "Охрана" МВД России). Термин был введен для краткого определения понятия "системы и средства защиты от угроз несанкционированного проникновения на объект с криминальными целями". Ранее это называлось "охранная сигнализация", но согласитесь, "охранная сигнализация" – это достаточно узкое определение для этой области деятельности. Задача защиты от несанкционированного проникновения не ограничивается только охранной сигнализацией. В современной реальности здесь применяются кроме систем охранной сигнализации, средства инженерной защиты, системы контроля и управления доступом (СКУД) и, наконец, системы охранные телевизионные (СОТ).

Широкое внедрение видеонаблюдения

Тематика СОТ занимает значительную долю в публикациях на страницах различных журналов, имеется масса специализированных изданий, посвященных СОТ, многочисленные сайты и интернет-порталы также занимаются этой тематикой.

Рынок систем видеонаблюдения обширен как по номенклатуре товаров, так и по количеству участников: производителей, разработчиков, поставщиков, продавцов, инсталляторов и других компаний, специализирующихся в этой области.

Идет мощная рекламная кампания по внедрению СОТ в различные сферы применения. И не только реклама, но и реальное внедрение в различные области нашей жизни, касающиеся не только традиционных заказчиков и пользователей систем безопасности, но и широкого круга граждан. Особенно это проявляется в таких проектах, как, например, "Безопасный город", в системах видеонаблюдения на транспорте, системах видеорегистрации на дорогах и др.

Такое широкое применение видеонаблюдения вызывает множество вопросов в областях не только технических и экономических, но и юридических, социальных, этических и др.

Однако вернемся к технике. В этой статье я не собираюсь подвергать критике какие-либо конкретные продукты или решения в области видеонаблюдения, а хочу только выделить некоторые спорные и проблемные моменты, связанные с практическими задачами систем охранного телевидения.

Поговорим о наиболее обсуждаемых вопросах и проблемах, связанных с СОТ.

Качество видеоизображения

Какой уровень качества приемлем для задач СОТ? Понятно, что чем выше качество, тем лучше, но и ясно, что за качество нужно платить, поэтому уровень качества должен определяться по технико-экономическим соображениям. Правда, здесь можно отметить, что технический прогресс в области обработки видео постоянно улучшает технико-экономические показатели оборудования и программных средств систем видеонаблюдения. Однако на каждом конкретном этапе развития техники все равно должны быть определенные минимальные нормы приемлемо допустимого качества. Очевидно также, что эти нормы качества должны различаться для разных задач видеонаблюдения.

Особенно актуален вопрос приемлемости качества видеоизображения в криминалистических задачах и в использовании видеоданных в качестве доказательной базы в суде. Этому вопросу уделяется большое внимание за рубежом и также в России.

Одной из авторитетных организаций, которая профессионально работает в этом направлении, является Европейская сеть судебно-экспертных учреждений – European Network of Forensic Science Institutes (ENFSI). В этой организации состоят более 50 учреждений судебной экспертизы из 32 стран: Австрия, Белоруссия, Бельгия, Болгария, Хорватия, Кипр, Чешская республика, Дания, Эстония, Финляндия, Франция, Германия, Греция, Венгрия, Ирландия, Италия, Латвия, Литва, Нидерланды, Норвегия, Польша, Португалия, Румыния, Россия, Словения, Словакия, Испания, Швеция, Швейцария, Турция, Украина и Великобритания. Россию в ENFSI представляют Российский Федеральный центр судебной экспертизы при Министерстве юстиции РФ, Северо-Западный региональный центр судебной экспертизы Минюста России и Экспертно-криминалистический центр при Министерстве внутренних дел РФ.

Работа ENFSI направлена на решение научных и методических проблем, связанных с производством и оценкой судебных экспертиз. В настоящее время в ENFSI создано 15 рабочих групп экспертов, которые образованы по различным направлениям экспертной деятельности и интересам. Одно из 15 направлений – цифровые изображения в судебной экспертизе.

Рабочая группа по цифровым изображениям в судебной экспертизе объединяет экспертов и научных сотрудников, интересующихся теорией и практикой использования цифровых изображений в судебно-экспертной практике и дока-

зывании по уголовным делам. Большинство членов группы специализируются на фотосъемке мест происшествий, фотограмметрии, компьютерной графике и компьютерном моделировании, анимации, идентификации людей и автомобилей по видеозаписям, сравнении внешнего облика, анализе видеозаписей. В группу входят также специалисты, интересующиеся проблемами исследования изображений в рамках иных видов экспертиз и исследований. Работа в этом направлении осложняется также тем, что в разных странах имеются различия в юридической практике использования доказательной базы в судах. Например, в российской практике, в соответствии со ст.ст. 25.1 и 25.2 КоАП РФ, лицо, в отношении которого ведется производство по делу, и потерпевший вправе представлять суду любые доказательства по делу. По ст. 26.2 КоАП РФ, доказательствами по делу об административном правонарушении являются любые фактические данные, на основании которых судья устанавливает наличие или отсутствие события административного правонарушения, виновность лица, привлекаемого к административной ответственности, а также иные обстоятельства, имеющие значение для правильного разрешения дела. Эти данные устанавливаются в том числе показаниями специальных технических средств. Это достаточно общее определение позволяет произвольно толковать представленные материалы.

Установить более ясные правила в этом вопросе можно созданием специальной нормативно-правовой базы в этой области. Естественно, для этого должна быть научно-техническая проработка этих вопросов: разработка критериев, методов оценки, методик испытаний, апробация, согласование всех заинтересованных сторон и другие действия, которые, как правило, проводятся при создании государственного или международного стандарта. В этом направлении много уже наработано и даже имеются некоторые стандарты и ведомственные методики, но общего подхода пока не выработано, в том числе и за рубежом.

IP-видеотехнологии в СОТ

Широкое внедрение этой технологии, которая, безусловно, перспективна и открывает много новых возможностей для видеонаблюдения, связано с множеством вопросов и новых проблем. Вот только некоторые из них.

Компрессия видеоизображения

Без нее IP-видео нереально. Однако компрессия – это всегда искажение исходного изображения и потери информации. Вопрос в том, что большинство алгоритмов сжатия разрабатывались для других задач, не связанных с системами безопасности. И очевидно, что критерии алгоритмов компрессии для задач СОТ должны быть другие. Работы в этой области проводились по созданию международного и российского стандарта. Наши предложения и наработки вызвали интерес в международных комитетах по стандартизации в области ISO JTC1/SC29 и IEC TC79. Однако стало ясно, что дальнейшие работы в этом направлении требуют серьезного финансирования. И здесь можно еще раз добавить, что стандартизация в России находится не в лучшем состоянии и во многом из-за несовершенства механизма реального финансирования.

Мегапиксельные видеокамеры и HD-качество в СОТ

Высокое разрешение для восприятия оператором, конечно, более информативно и комфортно, однако это требует более мощных вычислительных ресурсов для обработки видеоданных, высокоскоростных каналов передачи информации и больших объемов памяти для хранения видеоданных.

Еще одной проблемой, которую отмечают специалисты, являются трудности реализации видеоаналитики в IP-камерах. Видеоаналитика требует мощных вычислительных ресурсов, а процессоры, которые используются в IP-камерах по технико-экономическим соображениям, не обладают необходимой мощностью.

В ряде публикаций на эту тему также отмечаются недостатки IP-видео:

- Более высокая цена.
- Сложность системы в целом, что требует более квалифицированных специалистов по эксплуатации и обслуживанию.
- Большие потоки и объемы данных в сети, что предъявляет особые требования к сети и сетевому оборудованию.
- Ограничения в длине кабеля (стандартная длина без использования ретрансляторов – 100 м).
- Уязвимость информационной защиты (вынесение за пределы защищенной территории сетевого кабеля, например видеокамеры внешнего наблюдения, дает потенциальную возможность подключения к сети).
- Задержка в отображении (видеоизображение с цифровых видеокамер приходит с некоторой задержкой, что для систем безопасности может быть неприемлемо).
- Совместимость оборудования (отсутствие единых стандартов в настоящее время).

Видеоаналитика

СОТ по своей сущности и способу применения – не автоматизированная система. Решение, в конце концов, принимает человек. И здесь в полной мере проявляется человеческий фактор с худшей своей стороны. Особенно это опасно в системах безопасности. Системы охранной и пожарной сигнализации – это автоматизированные системы. Принятие решения здесь требует максимального быстродействия. Например, практические нормы реагирования в централизованной охране объектов составляют 10 минут для прибытия наряда на охраняемый объект по тревоге автоматической охранной сигнализации и 2 минуты по сигналу о нападении (кнопка тревожной сигнализации). Понятно, что для принятия решения у оператора (дежурного) на ПЦН есть только несколько секунд. Видеонаблюдение здесь в принципе ничего не дает.

Можно, конечно, найти несколько специфических задач, где применение видеонаблюдения будет оправдано. Например, в охране периметра. Датчики охраны периметра по своей специфике всегда имеют высокий уровень ложных тревог (хотя это не совсем ложные тревоги, так как они обусловлены влиянием неизбежных физических факторов, которые трудно разделить от воздействия нарушителя). Кроме того, зона охраны датчика периметра, как правило, составляет несколько десятков метров. Применение СОТ здесь оправдано. При этом оператору не нужно постоянно следить за экраном монитора. Он должен включаться (монитор и оператор) только по сигналу тревоги. Задача оператора – только оценить, ложная тревога или нет, и определить точное место проникновения.

Тем не менее видеоаналитика как автоматизация в системах видеонаблюдения, безусловно, перспективное направление в развитии СОТ. К сожалению, здесь много рекламы и фантазий. Это хорошо для выставок и презентаций, но зачастую вводит в заблуждение потенциальных заказчиков, которые, "клюнув на удочку" рек-

ламных показателей, ставят в реальных технических заданиях явно нереальные задачи.

Здесь может помочь обучение специалистов разного круга. Сейчас достаточно имеется учебных организаций государственного и негосударственного уровня, которые занимаются этими вопросами. Также нужны в этой области нормативно-технические документы-стандарты. К сожалению, в существующих стандартах ГОСТ Р и даже в проектах новых стандартов ИСО/МЭК по СОТ нет ничего конкретного по видеоаналитике. Даже требования к простому видеодетектору движения представлены в общем виде без методов испытания.

Эффективность видеонаблюдения и величина нагрузки на оператора

Это очень важная характеристика СОТ в целом. Ведь именно от действия оператора, его подготовленности, квалификации зависят обоснованность и скорость принятия решения.

СОТ – это человеко-машинная система, оптимальная работа которой в значительной степени зависит от действия человека. Основная задача любой автоматизированной системы – снижение влияния человеческого фактора, который оказывает негативное влияние на работу системы, а именно:

- ограниченные физические возможности человека;
- возможные ошибочные действия;
- недостаточная подготовка и компетентность;
- халатность;
- преднамеренные действия (саботаж, сговор с преступником и т.д.).

Число камер, приходящихся на одного оператора, чаще всего определяется техническими возможностями системы видеонаблюдения. Такой подход к решению проблемы эффективности видеонаблюдения в корне неверен.

Единственный официальный документ, регламентирующий нагрузку на оператора и указывающий на необходимость создания условий для работы оператора видеодисплейного терминала, является СанПиН 2.2.2/2.4.1340-03 "Гигиенические требования к персональным электронно-вычислительным машинам и организации работы". Правда, здесь речь идет об анализе изображения с одного монитора и не для задач видеонаблюдения. Но очевидно, что условия наблюдения изображения с нескольких камер, выведенных на один монитор (или на несколько мониторов), а также требования к работе в системах безопасности только увеличивают нагрузку на оператора и должны быть не хуже требований, указанных в данном документе. Согласно этому документу:

- рекомендуется организация перерывов на 10–15 мин через каждые 45–60 мин работы;
- продолжительность непрерывной работы с видеодисплейным терминалом без регламентированного перерыва не должна превышать 1 час;
- при работе с ПЭВМ в ночную смену с (22 до 6 часов) продолжительность регламентированных перерывов следует увеличить на 30%.

В настоящее время требования по нагрузке на оператора видеонаблюдения с учетом требований СанПиН 2.2.2/2.4.1340-03 вошли в документ Р 78.36.002-2010 "Рекомендации. Выбор и применение систем охранных телевизионных", разработанных ФГУ НИЦ "Охрана" МВД России.

В этих рекомендациях оговаривается, что нагрузка на оператора, занятого непрерывным наблюдением, должна быть не более 4 камер, изображение с которых выведено на один монитор, и при этом должен быть второй монитор для оперативного вывода на него изображения с одной из камер по команде оператора или в автоматизированном режиме, для того чтобы детально рассмотреть ситуацию в поле зрения видеокамеры. Допускается увеличение количества камер из расчета на одного оператора более 4 шт., но тогда с оператора должна сниматься задача непрерывного наблюдения.

Подводя итоги, можно отметить:

1. СОТ играют важнейшую роль в системах безопасности.
2. Проблемы и вопросы, которые связаны с характеристиками, применением, перспективами СОТ, – это естественный процесс развития отрасли. Главное, чтобы они вовремя выявлялись и разрешались.
3. В решении этих задач важнейшую роль должна играть стандартизация на национальном и международном уровне.
4. Ускорению процессов создания необходимых нормативно-технических документов, учитывая, что разработка национальных и международных стандартов достаточно длительная и затратная процедура, должны помочь объединения различных организаций в рамках технических комитетов по стандартизации или ассоциаций (групп) предприятий. В последнем случае могут быть разработаны СТО – стандарты организаций, которые в последующем могут быть приняты в качестве национальных или международных. Пример этому транснациональная промышленная ассоциация ONVIF, которая сейчас активно участвует в создании проектов стандартов ИСО/МЭК на СОТ. По этому примеру надо действовать и в России, главное – участие заинтересованных и квалифицированных специалистов и организация работы по принципу "истина для одного – это то, в чем он уверен, а истина для многих – это то, о чем они договорились". Стандарт – это как раз то, о чем нужно договариваться как можно более широкому кругу участников. ■

Ваше мнение и вопросы по статье направляйте на
ss@groteck.ru