

Сергей ЛЁВИН,
главный конструктор СИГМА-ИС

Верификация тревог

в охранной сигнализации

Ложные срабатывания извещателей в охранной сигнализации — это постоянная головная боль для всех, кто так или иначе сталкивается с системами безопасности (охранники, владельцы объектов охраны, инженеры техобслуживания). С каждым годом охранные извещатели становятся все умнее, производительность встроенных в датчики процессоров растет в полном соответствии с законом Мура, но проблемы все равно остаются. На пост охраны «ложняки» как приходили, так и приходят.

В этом случае на объектах с постоянным присутствием персонала службы безопасности решается все достаточно просто — охранник просто встает со своего насиженного кресла и проверяет факт срабатывания. В случае реальной опасности вызывает подмогу, в противном же случае это будет для него просто разминкой, для здоровья полезно. Если, конечно, это не происходит каждые пять минут. Когда же речь идет о централизованной охране, каждое ложное срабатывание обходится гораздо дороже. После прихода сигнала тревоги на пульт охраны дежурный оператор обязан вызвать ближайшую группу быстрого реагирования. Далее вызывается собственник или ответственное лицо, дверь торжественно вскрывается, выясняется, что никакого злоумышленника не было, и все, не очень довольные друг другом, разъезжаются до следующего «ложняка». Все это очень неудобно и накладно. Поэтому, чтобы исключить лишние телодвижения по любому поводу, разработаны различные методики верификации тревог. Данные процедуры позволяют в значительной степени повысить достоверность информации, приходящей с охраняемого объекта. Рассмотрим две, на мой взгляд, наиболее эффективные из них: последовательная верификация и видеоверификация.

ПОСЛЕДОВАТЕЛЬНАЯ ВЕРИФИКАЦИЯ

Вообще, этот способ защиты от ложных срабатываний и повышения надежности обнаружения проникновений уже давно используется в системах охраны периметра. Там это называется многорубежная охрана. На одном участке периметра устанавливается сразу несколько охранных извещателей, обязательно различного физического принципа действия. Каждый извещатель составляет один рубеж охраны. Таким образом, для трех рубежей охраны, что является нормой для хорошей системы безопасности, нам нужно применить датчики трех разных типов. Напомню, что в периметральных системах используются линейные извещатели, которые защищают от преодоления участок определенной длины. Обычно это 100–200 м. Один извещатель может реагировать на вибрацию, которая передается на чувствительный элемент от колебаний ограждения при попытке кого-либо перелезть через него. Второй извещатель может быть емкостного типа и будет реагировать на изменения емкости контура при появлении внутри него человека. И наконец, третий тип — это, допустим, радиоволновый линейный извещатель, срабатывающий при пересечении некой невидимой границы, создаваемой вдоль ограждения. Еще раз оговорюсь, что важно, чтобы все датчики на

одном участке были разного принципа обнаружения. Тогда возможные помехи, которые могут вызвать ложное срабатывание одного извещателя, с высокой долей вероятности не окажут такого же воздействия на другие. Например, сильные порывы ветра могут ввести в заблуждение вибрационный датчик, хотя, конечно, отстройка от естественных помех должна быть заложена в каждом извещателе, но сами понимаете, на практике может случиться всякое. Так вот, на радиоволновый извещатель тот же ветер не должен оказать никакого влияния. При использовании такой тактики охраны, которая иногда называется мажоритарной логикой, в случае срабатывания одного датчика на участке система молчит или охраннику выдается предупреждение. Если же в течение заданного интервала времени на этом же участке периметра срабатывает второй извещатель, тогда выдается полноценная тревога. Такой подход радикально повышает качество работы системы безопасности, ведь когда в течение короткого промежутка времени в одном месте срабатывают два или даже три совершенно разных по принципу действия датчика, вероятность, что это действительно попытка проникновения, значительно повышается. Безусловно, платой за это оказывается более высокая стоимость подобного решения. Но ведь мы знаем, что на безопасности нельзя экономить. Хочу отметить, что в данном случае целесообразно применять именно отдельные извещатели, а не комбинированные, когда в одном устройстве реализовано

несколько принципов обнаружения. Ведь иногда источником ложных срабатываний является неисправность или некорректность настройки самого устройства, причем это может быть какой-то общий узел, который будет провоцировать ложные тревоги сразу по всем каналам обнаружения такого совмещенного извещателя.

Если говорить про централизованную охрану таких объектов, как квартиры, дома или офисы, то реализация тактики применения нескольких типов извещателей здесь также возможна. Например, в помещении устанавливаются пассивные инфракрасные извещатели и радиоволновые. Но это не всегда получается по различным причинам. Во-первых, это вызывает ощутимое удорожание системы. Во-вторых, не каждый захочет, чтобы все стены в его доме были утыканы датчиками. В таких случаях можно применить способ, который учитывает расположение самих извещателей. Например, если произошло срабатывание в одной из комнат, то это воспринимается как сигнал «Внимание». Если срабатывания в этой комнате продолжаются в течение некоторого времени, т. е. налицо факт постоянного движения в помещении или сработали датчики в других комнатах, тогда эта ситуация воспринимается как подтвержденная или верифицированная тревога и принимаются все необходимые меры. Недостатком этого способа может являться то, что для подтверждения тревоги потребуется некоторое время, которого потом как раз может и не хватить для предотвращения преступления.

ВИДЕОВЕРИФИКАЦИЯ

Сейчас редко какая система безопасности обходится без видеонаблюдения. Видеокамера на объекте зачастую больше, чем охранных извещателей. В связи с этим напрашивается возможность использования видеокамеры как устройства подтверждения тревоги. Все, в общем-то, просто: при срабатывании охранной сигнализации оператору системы безопасности автоматически выводится изображение с видеокамеры, в зоне видимости которых находится тревожная зона. Охранник может мгновенно оценить обстановку и



ПРИГЛАШАЕМ ПРИНЯТЬ УЧАСТИЕ В ВЫСТАВКЕ!

Комплексная Безопасность

IV ВСЕРОССИЙСКАЯ СПЕЦИАЛИЗИРОВАННАЯ ВЫСТАВКА

11-14 сентября/ 2012

ТЕМАТИКА ВЫСТАВКИ

- Безопасность в чрезвычайных ситуациях
- Пожарная безопасность
- Безопасность на воде
- Системы общественной безопасности
- Безопасность дорожного движения
- Системы охраны
- Банковская безопасность
- Экологическая и промышленная безопасность
- Безопасность труда
- Медицина катастроф
- Защита дома и офиса
- СМИ

Место проведения выставки:
г. Ижевск, ул. Кооперативная, 9

Выставочный центр «УДМУРТИЯ»
тел./факс: (3412) 731-171, 731-116, 733-624, 733-664
safe@vcudmurtia.ru; www.safe.vcudm.ru

Информационный
партнер:

ПОСТАВЩИКИ МАШИН
ОБОРУДОВАНИЯ

визуально определить, насколько ситуация серьезна и какие действия предпринять дальше. Если речь идет о системе безопасности относительно крупного объекта с собственным постом охраны, вопросов нет — так и нужно делать. Это самое разумное решение в рамках построения интегрированной системы. Даже самые простые видеорегистраторы, как правило, уже имеют тревожные входы для каждого видеоканала, что позволит реализовать подобную связку охранной сигнализации и видеонаблюдения. В более продвинутых системах можно связывать с охранными датчиками отдельные пресеты поворотных камер, что позволит точно позиционировать видеокамеру и настраивать трансфокатор и другие параметры на каждое тревожное срабатывание. Однако совсем другое дело, если мы говорим о централизованной охране частных владений. Здесь сразу появляется несколько проблемных моментов. Во-первых, картинку нужно как-то передать на пульт охраны. Традиционно каналы связи с ПЦО — это телефонная линия или специализированный радиоканал. В существующих системах передачи извещений (СПИ), которые используют эти каналы для передачи тревожного сигнала с объекта на пульт, применяются низкоскоростные и малоинформативные протоколы, которые годятся только для передачи факта срабатывания охранного датчика. В принципе, с этой задачей они вполне справляются, но никакого видео с помощью них передать нельзя. Однако ничто не стоит на месте, и сейчас на рынке появляются системы, которые используют более современные и скоростные каналы связи. Это может быть сеть оператора мобильной связи или провайдера интернет. И в том и в другом случае технически уже становится возможна доставка видеоконтента на пост охраны. Конечно, в случае использования сетей сотовой связи не стоит забывать о стоимости трафика, передача видео может влететь в копеечку. Да и пропускная способность каналов не везде позволит «гнать» видео. Тем не менее в каждом случае можно найти то или иное решение и снять все или почти все технические вопросы.



Но остается еще один очень важный момент. Как правило, никто из пользователей систем охраны не хочет, чтобы к видеокамерам, установленным в его доме или офисе, был доступ каких бы то ни было посторонних лиц, кроме них самих. И это можно понять. Вряд ли вы сможете себя нормально чувствовать, если будете знать, что потенциально кто-то может за вами подсматривать в вашем собственном доме! И здесь кроется самая главная проблема организации процедуры видеоверификации. Частично она может быть решена, если использовать не обычные камеры видеонаблюдения, а специальные видеокамеры, которые решают только одну узкую задачу — подтверждают факт срабатывания охранной сигнализации. Обычно для этого видеокамеру монтируют в корпус охранного пассивного инфракрасного извещателя. Когда система снята с охраны или стоит на охране, но охранный датчик находится в норме, изображение с камеры гарантированно не передается на пульт охраны. В крайнем случае доступ к видеоизображению может получить только владелец. Хотя кто знает, если может посмотреть хозяин, то при желании могут ведь и другие? Поэтому я бы лично предпочел безусловный режим работы: нет тревоги — нет картинки. Прошла тревога по этому датчику, изображение с видеокамеры на какое-то время начинает передаваться на ПЦО. Дальше уже оператор на основании полученных видеоданных принимает решение, была ли это тревога ложная или нужно вызывать наряд для выезда на объект. Кстати, видеоизображение можно дополнить и звуком: установить рядом с камерой микрофон — не проблема. Звуковой ряд может дать ценную оперативную информацию о намерениях злоумышленников, что позволит принять правильное решение и снизить риск для группы задержания при силовом контакте.



Мир безопасности велик,
но мы стараемся увидеть главное!

Интернет-портал "Безопасность для всех"
www.sec4all.net

В завершение хотелось бы отметить, что в целом внедрение технологий верификации тревог — направление очень правильное и нужное, так как по статистике около 80% срабатываний охранной сигнализации являются ложными. Поэтому эффективное использование верификации позволит сэкономить кучу времени, нервов и денег прежде всего владельцам объектов. [2]