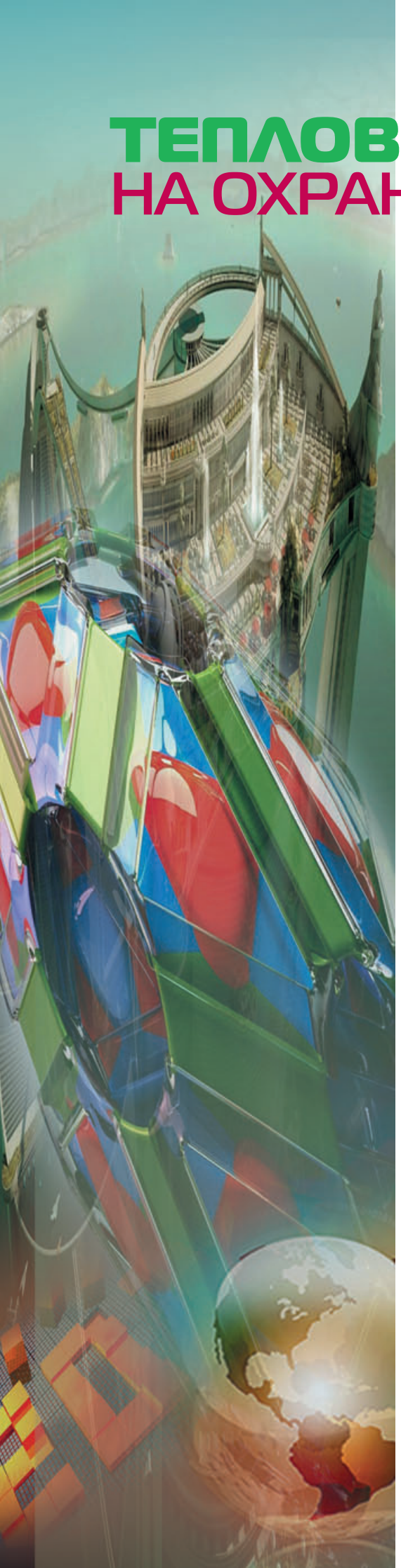
# ТЕПЛОВИЗОРЫ НА ОХРАНЕ ПЕРИМЕТРА



***С. Никитин***
*ООО «СКН»*

## ИЗ КОСМОСА НА ЗЕМЛЮ

Тепловизоры давно применяются в наиболее совершенных системах безопасности. Примером такой системы может служить система предупреждения о ракетном нападении (СПРН). Она имеет в составе спутники, размещенные на высокоэллиптических и геостационарных орбитах, которые осуществляют наблюдение за районами размещения межконтинентальных баллистических ракет. Спутники оснащены охлаждаемыми тепловизорами, работающими в диапазоне 3-5 микрон, которые позволяют обнаружить «факел» стартовавшей ракеты в любое время суток с расстояния 40 000 км. Работа аппаратуры СПРН невозможна без совершенных устройств видеоаналитики, работа над которыми длилась десятилетиями. В результате были созданы изощренные алгоритмы селекции подвижных объектов на неподвижном и малоподвижном фоне, которые только сегодня начинают появляться на открытом рынке. Тепловизионные системы обнаружения стартов баллистических ракет были приняты на вооружение в конце XX века СССР и США, и с тех пор эти системы постоянно совершенствуются. Серьезность угрозы подразумевает адекватные средства противодействия – поэтому можно сказать, что применение тепловизоров для обеспечения безопасности целой страны доказывает их эффективность.

В настоящей статье мы рассмотрим роль тепловизоров в системе охраны периметра объектов меньших масштабов. Государственные, в т.ч. военные объекты, заводы, электростанции, объекты транспорта и многие другие имеют высокие требования к системе безопасности. Постараемся доказать, что тепловизор с устройством видеоаналитики на сегодняшний день является высокоэффективным и экономически оправданным средством защиты периметра особо важного объекта. Следует сказать, что под особо важным объектом подразумевается такой объект, проникновение злоумышленников на который может создать угрозу здоровью и жизни большого числа людей или привести к другим тяжелым потерям.

## ОСНОВНЫЕ ПОНЯТИЯ

Дадим определения основным терминам и понятиям, используемым в этой статье. Под обнаружением понимается раскрытие действий, совершаемых нарушителями. Эффективность обнаружения зависит от вероятности обнаружения и времени, необходимого на передачу сигнала тревоги и оценки его достоверности. В связи с этим вероятность обнаружения разделяют на первичную $P_1$ (датчиком) и системную $P_D$. В случае с тепловизором $P_1$ – это вероятность того, что при попадании нарушителя в зону обзора тепловизор сформирует изображение с достаточным для обнаружения соотношением «сигнал/шум», а устройство видеоаналитики сформирует сигнал тревоги. Системная вероятность обнаружения – это шанс того, что оператор системы на основании данных, полученных от средств охраны, обнаружит нарушителя. Системная вероятность обнаружения снижается с увеличением времени, необходимого для передачи сигнала оператору, анализа данных и связи с силами охраны, следовательно, необходимо минимизировать этот временной интервал. Минимизация этого интервала и достигается использованием устройств видеоаналитики. Таким образом, удается максимально использовать обнаружительную эффективность тепловизора и повысить качество работы оператора.

Рассмотрим параметры, влияющие на эффективность работы устройства обнаружения в составе системы охраны периметра. Некоторые производители указывают, например, что вероятность обнаружения – 99%. Это, мягко говоря, неверно. Конкретный извещатель характеризуется двумя параметрами – вероятностью обнаружения $P_1$ и доверительным уровнем $C$. Датчик обнаруживает нарушителя с вероятностью при доверительном уровне $C$. Это означает, что на основе результатов испытаний можно сделать вывод, что с вероятностью $C$ реальная, но точно неизвестная вероятность обнаружения датчика будет не меньше $P_1$. Для различных $C$ могут получиться различные $P_1$ – снижая $C$, можно увеличить $P_1$, и наоборот. На *рисунке 1* мы привели различные соотношения, полученные экспериментальным путем. Слева показано обнаружение человека в зоне, обведенной желтой линией. Вероятность обнаружения составляет 96% при доверительном уровне 95%. Справа показано обнаружение объекта, пересекающего голубую линию. Мы снизили доверительный уровень до 85% и получили вероятность обнаружения в 100%. Как видите, варьируя величину доверительного уровня, можно получить различные значения вероятности обнаружения.

Необходимо также определиться с критерием, на основании которого извещатель или их система будет формировать сигнал тревоги. Примером критерия обнаружения

для пары тепловизор – устройство видеоаналитики может быть следующий: система должна обнаруживать с вероятностью 95 % при доверительном уровне 95 % человека или группу людей, двигающихся со скоростью от 0,1 до 5 м/с и пересекающих охраняемую зону шагом, бегом или ползком в любое время суток на расстоянии не менее 200 м от точки установки тепловизора. Профессиональное оборудование, как правило, проходит испытания на вероятность обнаружения различных целей. Методика таких испытаний может включать обнаружение отдельных людей или групп лиц, передвигающихся в различных направлениях с различной скоростью и т.п. На основании таких испытаний делается заключение о пригодности применения оборудования в особо ответственных приложениях.

Вероятность обнаружения зависит от многих факторов, среди которых можно выделить основные:

1. Цели, которые нужно обнаружить (идущий, ползущий нарушитель, группа людей, техника и т.п.).
2. Конструкции тепловизора.
3. Условия установки тепловизора.
4. Настройки чувствительности.
5. Техническое состояние аппаратуры, условия эксплуатации.
6. Наличие дополнительных систем безопасности, например, сейсмического датчика, установленного на ограждении.

При работе в реальных условиях возможно появление ложных тревог. Ложным называют любой сигнал тревоги, не вызванный вторжением. Для идеальной системы датчиков (принимая, что $P_D = 1$) частота ложных тревог должна быть равна нулю. Однако любой реальный датчик (в т.ч. и тепловизор) взаимодействует с окружающей средой и может не отличить вторжение от другого события в зоне обнаружения. Именно поэтому и необходима оценка, без которой обнаружение нельзя считать полным.

Ложные тревоги принято классифицировать по источнику. Естественными источниками ложных тревог являются растительность, животные, погодные условия и т.п. К техногенным источникам относятся, например, переносимые ветром предметы, электромагнитные помехи. Наконец, ряд ложных тревог может создаваться непосредственно оборудованием: неисправностью или неудачной конструкцией, некачественным обслуживанием. Важно определить максимально допустимую частоту ложных тревог. Например, для комплекса авиационных сооружений была установлена максимально допустимая частота ложных тревог: не более одной тревоги в 14 суток на 1 км периметра. Также установленная частота ложных тревог позволяет оператору определить, когда следует обратиться в службу технического обслуживания.

Существует зависимость между вероятностью ложной тревоги за определенный период времени и частотой ложных тревог. Эта зависимость в большинстве случаев описывается упрощенной формулой $P_{лт} = 1 - e^{-t/T}$, где $T$ – среднее время наработки на одно ложное срабатывание (например, тридцать дней), а $t$ – период наблюдения. Обратный переход можно осуществить по формуле $T = t/ln(1 - P_{лт})$. Важно помнить, что если в интенсивности фигурируют дни, то и период наблюдения должен исчисляться в днях.

Также следует сказать о защите от вмешательства в работу технических средств охраны и самопроверке системы и ее элементов. Это нужно, чтобы внешние факторы (в т.ч. действия злоумышленников) не влияли на работу системы безопасности и время от времени оператор мог проверить работоспособность системы. Вышесказанное также говорит в пользу применения видеоаналитики совместно с тепловизорами. Современные устройства отслеживают изменение поля зрения и способны формировать сигнал тревоги как в случае естественной причины такого изменения (например, от порыва ветра), так и в случае умышленного саботажа. Также тепловизор позволяет с легкостью оценить собственную работоспособность – оператор способен быстро заметить пропадание или серьезное ухудшение качества видеосигнала и без видеоаналитики.

## ДОКАЗАТЕЛЬСТВА ПРЕВОСХОДСТВА: НАГЛЯДНОСТЬ

Попробуем на примере доказать читателю, что тепловизионная система охраны периметра обладает рядом несомненных преимуществ. Мы уже сказали, что системная вероятность обнаружения зависит от времени оценки. На *рисунке 2* приведены два кадра с тепловизора.

На кадре слева вдоль забора бежит крупное животное, а на кадре справа видна группа людей. Чтобы понять это, требуется около секунды. Конечно, нельзя сбрасывать со счетов погоду, расстояние до цели, скорость перемещения, разрешение тепловизора и т.п. Но можно сказать точно: сигнал с тепловизора предоставляет оператору гораздо больше информации, чем сигнал тревоги от датчика периметровой сигнализации.

На *рисунке 3* продемонстрирована работа тепловизора совместно с устройством видеоаналитики. Как видите, если человека на расстоянии 60 метров оператор может с легкостью распознать, то разобраться в происходящем на заднем плане (расстояние более 100 м) уже гораздо сложнее. Тем не менее устройство видеоаналитики справляется с этой задачей, выделяя оператору зону интереса.

## ДОКАЗАТЕЛЬСТВА ПРЕВОСХОДСТВА: СВЕРХРАННЕЕ ОБНАРУЖЕНИЕ

Вообще тепловизор с аналитикой представляет собой одно из лучших устройств по своевременному формированию сигнала предтревоги. Ранее мы упоминали («Алгоритм Безопасности» №6, 2011), что устрой-

***Рис. 1.*** Вероятность обнаружения и доверительный уровень

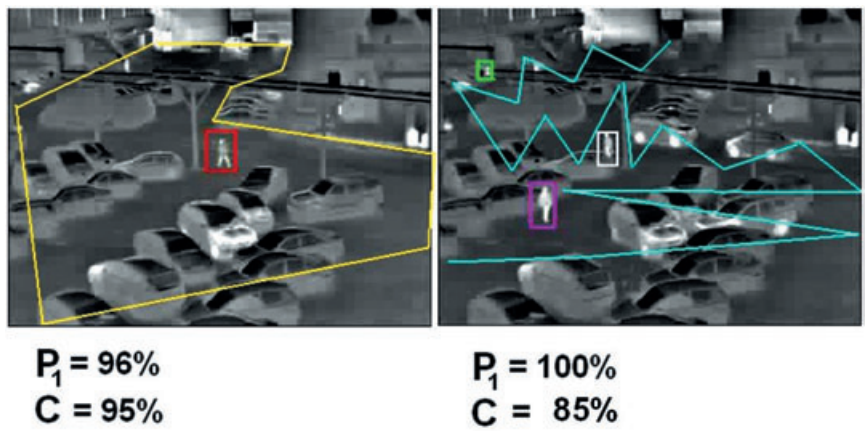
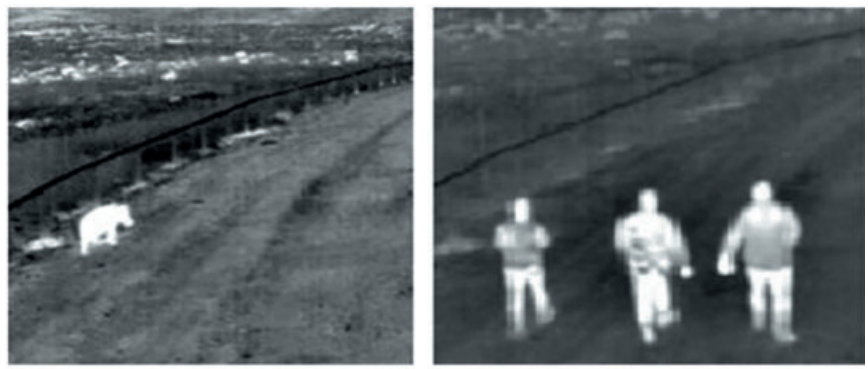



***Рис. 2.*** Оценка характера тревоги



ство видеоаналитики сможет обнаружить малоконтрастный точечный сигнал на максимально возможном расстоянии, сопоставить его с критерием оценки и обратить внимание оператора на потенциальную угрозу задолго до того, как нарушитель приблизится к забору вокруг объекта. В самом деле, если тепловизор с объективом 100 мм может обнаружить человека на расстоянии до 2 км, а средняя скорость человека 5 км/ч, то оператор получит информацию о приближающемся человеке за 20-25 минут до возможного пересечения человеком границы охраняемого объекта.

На *рисунке 4* показано, что СФЗ только тогда выполняет свою функцию, когда время защиты меньше, чем время, необходимое нарушителям для выполнения своей задачи. Допустим, что первый сигнал тревоги приходит от лучевого датчика, установленного на заборе, а оценка ведется при помощи камеры наблюдения. Тогда, если заменить существующую систему обнаружения на тепловизор (фокусное расстояние объектива 100 мм) с устройством аналитики, зависимость, на *рисунке 3* приобретет вид, изображенный на *рисунке 5*.

Дадим пояснения. В момент времени $t_0$ нарушитель начинает свое движение в сторону объекта защиты. Время предтревоги обозначено интервалом ПТ. В это время оператор получает информацию от тепловизора с устройством видеоаналитики, что на расстоянии до 2 км обнаружен потенциальный нарушитель. В этот момент оператор может оповестить службу охраны о возможном нападении. В интервал РО (распознавания и оценки) оператор принимает решение – есть ли потенциальная угроза объекту или тревога была ложной. В момент времени $t_1$ нарушитель (теоретически) мог бы преодолевать первый рубеж охраны (например, забор с датчиками), но так как перехват может быть осуществлен раньше, то этого может и не случиться. Восточная мудрость гласит: «выигранный бой – это тот, который закончился, не начавшись». Эта фраза применима и в нашем случае: противник может быть обезврежен еще до вторжения на объект.

*Рис. 3.* Обнаружение людей

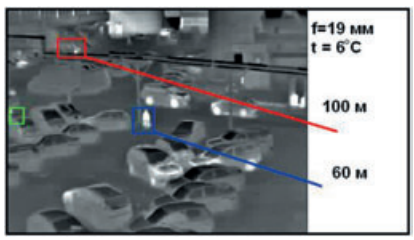



*Рис. 4.* Зависимость времени выполнения задачи нарушителей от СФЗ

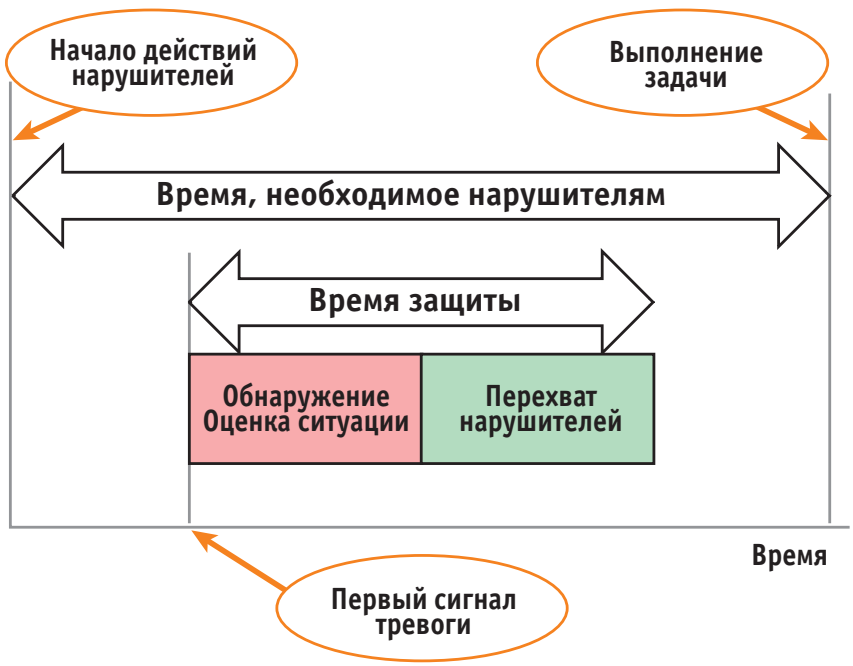
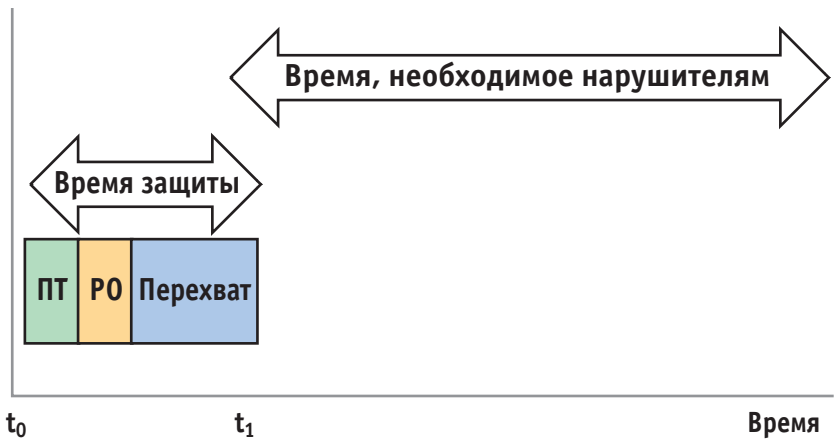



*Рис. 5.* Эффект применения тепловизора




## ДОКАЗАТЕЛЬСТВА ПРЕВОСХОДСТВА: ДЕШЕВЛЕ, ЧЕМ КАЖЕТСЯ

Наконец, приведем экономическое обоснование. Допустим, нам необходимо обнаружить нарушителя за 700 метров от объекта, чтобы обеспечить его задержание. Длина окружности ($L=2\pi R$ ) примерно равна 4400 м. Для защиты данного периметра чувствительным кабелем потребуется около 4,5 миллионов рублей. Стоимость забора высотой 2 м составит ориентировочно 1-2 миллиона рублей. Также необходима система видеонаблюдения для оценки сигнала тревоги. Предположим, что камеры устанавливаются из расчета одна камера на 100 метров периметра. Тогда потребуется 44 камеры, устройства записи, система передачи данных. Это еще ориентировочно 2-3 миллиона рублей. Если мы остановим свой выбор на тепловизорах с видеоаналитикой и установим их так, чтобы обеспечить обзор в 360°, то потребуется около 7 миллионов рублей (против 8,5). Экономия составит около 15-20%. Разумеется, это очень приблизительный расчет, который лишь призван показать экономическое обоснование применения тепловизоров. В реальной жизни каждый объект требует индивидуального подхода.

## ОДИН ДАТЧИК ХОРОШО, А СИСТЕМА – ЛУЧШЕ

Для улучшения параметров системы охраны периметра тепловизоры можно объединить с другими средствами охраны, использующими иной принцип обнаружения. Проведем небольшой расчет, чтобы показать, как различные схемы включения влияют на частоту ложных тревог и обнаружительную способность системы датчиков.

Любой датчик имеет такие параметры, как вероятность обнаружения и вероятность ложной тревоги. Как правило, производители не указывают вероятность ложной тревоги, а приводят частоту ложных тревог, например, не более одного ложного срабатывания в девяносто дней. Перейдем к вероятности, воспользовавшись фор-

мулой: $P_{лт} = 1 - e^{-t/T}$, где $T$ – среднее время наработки на ложную тревогу одного датчика, а $t$ – период наблюдения. Мы приняли $T$ = 90 дней согласно документации на датчик. Подставив величины в формулу для вероятности, получим $P_{лт} = 1{,}1\%$ в день. Также производитель заявляет вероятность обнаружения $P_{об}$ = 98%. Для тепловизора с устройством аналитики нами в ходе испытаний были получены следующие данные: $P_{лт}$ = 6,65% в день, $P_{об}$ = 99%.

***Табл. 1.*** Вероятности событий в системе датчиков

| **Вероятность** | **Схема «И»** | **Схема «ИЛИ»** |
|---|---|---|
| Ложная тревога в системе | $P_{лт1}P_{лт2} << P_{лт1}, P_{лт2}$ | $P_{лт1} + P_{лт2} - P_{лт1}P_{лт2} >> P_{лт1}, P_{лт2}$ |
| Пропуск нарушителей системой | $P_{пр1} + P_{пр2} - P_{пр1}P_{пр2} >> P_{пр1}, P_{пр2}$ | $P_{пр1}P_{пр2} << P_{пр1}, P_{пр2}$ |

В *таблице 1* рассмотрены два простейших случая включения датчиков. Как видно, при схеме «И» уменьшается вероятность ложной тревоги, а при схеме «ИЛИ» – вероятность пропуска нарушителей системой. Подставим указанные выше значения. Тогда данные в таблице примут следующие значения:

| **Вероятность** | **Схема «И»** | **Схема «ИЛИ»** |
|---|---|---|
| Ложная тревога в системе | *0,066% (вместо 1,1% минимум)* | *7,68% (вместо 6,65% максимум)* |
| Пропуск нарушителей системой | *2,98% (вместо 2% максимум)* | *0,02% (вместо 1% минимум)* |

Как видите, используя различные схемы включения, можно оптимизировать параметры исходя из требований к безопасности объекта. Например, согласно требованиям нормативных документов МВД РФ, для особо важного объекта с повышенной значимостью потерь требуется обеспечить вероятность обнаружения 99,5%. Для решения этой задачи можно рекомендовать объединение описанных выше датчиков по схеме «ИЛИ», так как ни один из них по отдельности не удовлетворяет требованиям. Разумеется, схемы включения не ограничиваются только этими двумя способами. Существуют комбинации логических элементов, при которых возможно достичь и снижения количества ложных тревог в системе, и увеличить вероятность обнаружения, но синтез таких схем выходит за рамки этой статьи.

Разумеется, при проектировании реальной системы охраны периметра следует учитывать и множество других факторов. Но мы надеемся, что материал, изложенный в статье, найдет своих сторонников и специалисты будут расценивать тепловизор как высокоэффективное средство охраны периметра.