Защита периметра объекта (что полезно знать руководителю, принимающему решения)

Как театр начинается с вешалки, так и защита любого объекта начинается с защиты его периметра от проникновения нежелательных лиц. Это особенно верно для объектов больших, имеющих протяженный периметр (аэродромы, морские порты, железнодорожные парки, НПЗ и т. п.).

Protecting the perimeter of the facility (which is useful to decision makers)

As the theater begins with a hanger, and the facility protection begins with its perimeter defense against the penetration of undesirable persons. It is especially true for large facilities that have extended perimeter (airports, seaports, rail parks, refineries, etc.).

В.М. Крылов, кандидат технических наук, доцент, президент корпорации Пентакон
V.M. Krylov, Ph.D., associate professor

Что обсуждаем?

Поскольку необходимое противодействие нарушителю на практике может быть осуществлено только человеком, то одного ограждения территории очевидно недостаточно. Требуется оснащение периметра автоматизированным комплексом технических средств, обеспечивающих полное, достоверное и своевременное информирование службы охраны о происшествии, который включает систему периметральной сигнализации, телевизионное и (или) тепловизионное наблюдение, охранное освещение, контроль доступа и др.

Главной и системообразующей в этом комплексе является система периметральной сигнализации (СПС). Обсудим требования к ней в том порядке, в каком они обычно возникают у Заказчика при формировании требований к СПС. В силу небольшого размера статьи будем рассматривать чаще всего используемый для таких задач класс систем – СПС, располагаемые на ограждении. Отметим при этом, что общая логика анализа и основные выводы (с небольшими оговорками) будут справедливы и для систем других типов: систем подземного базирования (используются, когда рубеж охраны требуется сделать невидимым), радиолучевых датчиков (обычно применяются как второй рубеж охраны) и др.

Рис. 1

Вне зависимости от производителя и применяемых им технологий вибрационная СПС состоит из совокупности последовательно установленных на ограждении базовых элементов. Опуская несущественные для данного рассмотрения детали, базовый элемент представляет собой некий блок обработки (БО), к которому подсоединены два плеча виброчувствительного кабеля, длиной $l_{охр}$, закрепляемого на ограждении (рис. 1). Возникающие при проникновении вибрации ограждения преобразуются этим кабелем в электрический сигнал, который анализируется БО.

Где устанавливаем систему?

В принципе, годится любое вибрирующее под действием нарушителя ограждение: цельносварная сетка (СЦП), сетка «Рабица», профлист и т. п. В случае жестких (бетонных) заборов сверху надо установить АКЛ «Егоза» (хуже – проволочный козырек), на которой закрепить сенсорный кабель.

Рис. 2

В этом, кажется, совершенно простом вопросе таится, однако, одна важная «мелочь»: кабель-сенсор, устанавливаемый на АКЛ или колючую проволоку, должен обязательно иметь стальную защитную оболочку (броню). Если этим пренебречь, то уже через год система гарантированно выйдет из строя, поскольку острые края АКЛ под действием ветра прорежут пластиковую оболочку (рис. 2). Далее в прорезь попадет вода, мороз… и кабель выйдет из строя. Все кабельные СПС, построенные на основе трибоэлектрического эффекта («Гюрза», «Багульник», «Трезор», «Дельфин», «Годограф» и др.), не имеют бронированной версии кабеля (это связано с особенностью трибоэлектрического принципа детектирования). Бронированный кабель есть только в системе INTREPID MicroPoint, использующей для детектирования принцип проводной радиолокации.

И еще один не менее важный практический вопрос, часто возникающий у Заказчика в самом начале и существенно влияющий на общую стоимость решения: какую СПС можно использовать

ПЕНТАКОН, ЗАО
190000, Санкт-Петербург,
ул. Красного Курсанта, д. 25, лит. Д
Тел.: (812) 633-04-33, факс: (812) 633-04-37
E-mail: office@cctv.ru
www.cctv.ru

на уже существующем заборе, часто состоящем к тому же из ограждений разного типа, разумеется, не ухудшая при этом достоверность обнаружения нарушителя? Правильный ответ – только систему на базе технологии INTREPID, разработанную фирмой SouthWest MicroWave. Почему? Ответ в следующем разделе.

Главное в системе – правильно сигнализировать

От чего это зависит? Какие принципы должны быть использованы при построении СПС для обеспечения минимальных вероятностей ошибок обнаружения, нарушения периметра? Незнание правильных ответов на эти ключевые вопросы очень часто приводит к тому, что Заказчик получает систему с недопустимо большим уровнем ошибок. То есть фактически система не будет работать, будучи полностью функционально исправной. Так получается тем чаще, чем больше длина охраняемого периметра.

Подробный и обоснованный ответ на поставленные вопросы содержится в статье «Вероятность ошибок в системах периметральной сигнализации» (www.intrepidsys.ru). Здесь же мы приведем лишь принципиально значимые выводы. Однако, чтобы они не показались совершенно голословными, проиллюстрируем их.

На рис. 3 приведен пример того, как распределен по длине кабеля сигнал, снимаемый с одного его плеча. Здесь показано, что для всей длины плеча $l_{охр}$ при настройке задан лишь один уровень чувствительности v_o. В этом случае, если происходит проникновение на участке l_2, уровень сигнала превосходит заданный порог v_o и БО вырабатывает сигнал тревоги. На участке l_3 из-за случайных шумов и более высокой чувствительности кабеля в этой локальной точке происходит ложное срабатывание, тогда как на участке l_4 проникновение не обнаруживается (ошибка пропуска цели) несмотря на приблизительно такой же величины сигнал, возникший от нарушителя. Также рис. 3 иллюстрирует, как влияет регулировка порога срабатывания v на вероятность ошибок $P_{ложн}$, $P_{проп}$ (см. также рис. 4). Устанавливая большую чувствительность v_2, мы имеем шанс не пропустить сигнал тревоги на участке l_4, однако при этом увеличивается число ложных срабатываний. Напротив, меньшее значение чувствительности v_1 ложные срабатывания убирает, но мы имеем риск потерять сигнал тревоги (участок l_2).

Первый путь решения изложенных проблем – выровнять вибрационные свойства системы «ограждение + кабель» по длине каждого плеча. В практическом плане для реализации этого предложения необходимо максимально однородно (в смысле вибрационных свойств) выполнить установку ограждения и также очень качественно и однородно по всей длине осуществить крепление сенсорного кабеля. Поэтому (а не только для увеличения стоимости проекта) инсталляционные фирмы предлагают заказчику монтаж СПС вместе с установкой ограждения. Тем более, что некоторые из представленных на рынке СПС очень чувствительны к неравномерности вибрационных свойств ограждения. Предложение заново сделать ограждение значительно повышает стоимость СПС, и потому обычно не принимается. Тем более, что, хотя ошибки в работе системы уменьшаются, этим путем невозможно кардинально (в разы, а еще лучше на порядок) улучшить характеристики системы и, в первую очередь, допустимую длину охраняемого периметра.

Второй путь нам также подсказывается рис. 3: задавать чувствительность не одним значением на всю длину плеча (т. е. для 50…250 м) как некую «сред-

нюю температуру по больнице», а учитывать вибрационные свойства каждой секции ограждения, т. е. с точностью 1…3 м (показано на рис. 3 пунктиром).

В практическом плане возможны два способа осуществления этой идеи: аппаратный и программный.

В варианте аппаратного решения необходимо при установке системы делать длину каждого плеча сенсорного кабеля величиной 1…3 м. Но это совершенно нереально, поскольку увеличит и без того немалую стоимость СПС более, чем на два порядка. Увы, но только этот способ оказывается доступен для всех трибоэлектрических СПС («Багульник», «Гюрза», «Годограф», «Дельфин», «Трезор» и др.) Технология INTREPID – единственная из представленных на рынке СПС, в которой реализованы программный способ задания уровня чувствительности каждого 1,1 м кабеля для всей 220 м длины плеча. Это не только не приводит к повышению стоимости системы (см. далее), но и заодно бесплатно решает, по крайней мере, и еще две важнейшие задачи и позволяет:

- определять место проникновения с точностью, сопоставимой с размером секции ограждения, т. е. до 3 м;
- эффективно бороться с интегральными воздействиями, затрагивающими сразу несколько (много) рядом расположенных секций (ветер, осадки, проходящий транспорт и т. п.). Программный анализ и сопоставление сигналов от соседних элементов сенсора позволит не воспринимать как сигналы тревоги, пусть даже мощные, но приблизительно одинаковые, воздействия на соседние участки.

Проведенные эксперименты показали, что значительные вибрации ограждения, установленного на расстоянии 6 м от железнодорожного полотна, по которому проходит «Сапсан», не приводили к ложному срабатыванию. В то же время перелезание человека через забор надежно фиксировалось.

Аналогично ведет себя система INTREPID при охране периметра аэропортов, где помимо сильных ветровых нагрузок имеют место локальные воздушные потоки от авиационных двигателей.

Применяемый в технологии INTREPID программный учет вибрационных особенностей каждого метра уже инсталлированной системы «ограждение + кабель» дает также следующие важнейшие практические преимущества:

- полностью отсутствуют требования к однородности вибрационных характеристик ограждения, которое может состоять из различных конструкций разного качества (это ответ на вопрос, поставленный в конце предыдущего раздела);
- при прохождении кабелем-сенсором проездов и проходов в ограждении не требуется разрезать сам кабель. Его достаточно закопать под землю и программно задать нулевую чувствительность на этих участках. Т. е. возможно программно задать ситуацию, когда система не будет реагировать на КАМАЗ, переезжающий кабель, но выдаст сигнал на ворону, севшую на забор в метре от дороги;
- в процессе эксплуатации системы можно таким программным образом временно «выключить» участок периметра на период ремонтных или строительных работ.

Точная аналитическая оценка эффективности этого способа борьбы с ошибками путем калибровки чувствительности каждого метра сенсора весьма затруднена. Наш более чем 10-летний опыт работы с системой STRATUM, созданной на базе технологии INTREPID, позволяет утверждать, что ошибки в сопоставимых с другими системами случаях уменьшаются более чем в (10…20) раз. Или, что эквивалентно, в (10…20) раз увеличивается допустимая длина

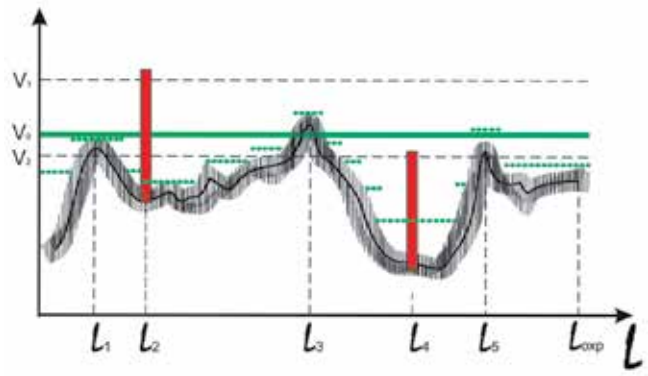


Рис. 3

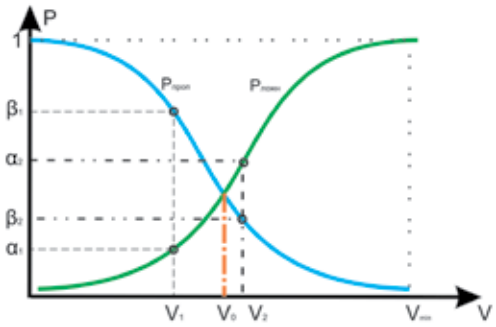


Рис. 4

охраняемого системой периметра. Этот вывод особенно полезно знать тем, кто выбирает СПС для охраны протяженного периметра, более 5…10 км (аэропорты, железнодорожные парки и т. п.).

Оценка вероятностей ошибок. Стоит ли доверять паспортным данным?

Как уже мы показывали выше вероятности ошибки ложного срабатывания ($P_{ложн}$) и ошибки необнаружения (пропуска) нарушителя ($P_{проп}$) взаимосвязаны и зависят в первую очередь от установленного порога чувствительности, при котором вырабатывается тревожный сигнал (рис. 3, 4). Вероятность правильного срабатывания системы ($P_{прав}$) в равной степени зависит от вероятностей обоих типов ошибок:

$$P_{прав} = 1 - P_{ложн} - P_{проп}.$$

Об этом часто забывают, требуя как от производителя, так и от инсталлятора уменьшить только одну из ошибок – $P_{ложн}$.

Здесь уместно отметить, что ошибки проявляют себя (воспринимаются сотрудниками охраны) сугубо по-разному. Большое значение вероятности ложного срабатывания $P_{ложн}$ (настройка v_2) означает также и большое беспокойство понапрасну сотрудников охраны. Поэтому через короткое время они психологически устают и перестают реагировать на каждое срабатывание системы (если вообще ее не выключат). И по факту оказывается, что вероятность правильной работы системы становится недопустимо малой и даже близкой к нулю $P_{прав} \sim 0$ ($P_{прав} = 0$, если систему выключают).

Возможна ситуация, когда вероятность правильной работы системы $P_{прав}$ также становится недопустимо малой, но только вследствие большого значения вероятности пропуска цели $P_{проп}$ (настройка v_1). Эта ситуация сама по себе без специальных проверочных мероприятий (и, следовательно, усилий) никак себя не проявляет. Не проявляет до наступления того момента, который и должна была предотвратить (но не предотвратила) система, и после наступления которого возможно уже «поздно пить «Боржоми».

Поэтому, если исходить из того, что возможные последствия, связанные с необнаружением проникновения, объективно более значимы, чем неудобства и беспокойства сотрудников охраны, то следует предпочесть настройку v_2. Увы, на практике, скорее всего, будет иметь место настройка v_1 – сработает «человеческий фактор» (усталость сотрудников охраны).

Таким образом, прежде чем проводить статистические испытания, необходимо определить значение уровня чувствительности v_0. А оно (точнее, множество их значений), в свою очередь, зависит от конкретной инсталляции (типа ограждения, особенностей его установки, крепления кабеля и т. д.). Кроме того, необходимо зафиксировать способ и место преодоления ограждения, размеры зон охраны и общую длину периметра, погодные факторы, имеющиеся сосредоточенные воздействия и т. д., таким образом, зафиксировав весь этот набор факторов и воспользовавшись, например, методикой ГОСТ 20.57.304-76, мы за 30–300 испытаний получим оценку вероятности ошибки обнаружения:

$$P_{обнаруж} = 1 - P_{проп.}$$

Получим оценку именно для этих фиксированных условий. Чтобы сделать перечисленные условия случайными, потребуется на порядки (!) больший объем испытаний, что практически нереализуемо. Да и полученное значение будет иметь небольшую ценность, типа «средней температуры по больнице».

А что сообщают производители оборудования? Они бодро указывают в паспортных данных $P_{обнаруж} = 0{,}95…0{,}98$. Без всяких оговорок, при каких условиях эти значения получены (если они действительно были получены). А без этих указаний неясно, что эти цифры означают.

Совсем грустная история с параметрами, которые приводятся в технической документации для оценки вероятности ложных срабатываний $P_{ложн}$. Точнее, вместо $P_{ложн}$ обычно принято оценивать ее производную величину $T_{ложн}$ – среднее время наработки на ложные срабатывания. Также без всяких оговорок об условиях испытаний в технической документации разных производителей указывается, что $T_{ложн} = 1..3$ мес. Тем не менее, отнесемся к данной величине с максимальным доверием и оценим смысл приведенного значения. Для этого надо прежде ответить на один вопрос – какой длине кабеля-сенсора соответствует приведенное значение? Логично предположить, что испытывался базовый элемент (рис. 1) с длиной плеча кабеля до 200...250 м (более часто используется зона размером 50…100 м). Тогда при длине периметра в 10 км $T_{ложн} = 2…6$ раз/день, а при длине 30 км – $T_{ложн} = 6…20$ раз/день, что вряд ли следует признать допустимым. А если такая система все же будет построена, то можно не сомневаться, что сотрудники службы охраны откорректируют ее работу до приемлемого для них значения частоты сигнала тревоги. Разумеется, что это и возможно, и будет сделано только за счет ухудшения вероятности обнаружения $P_{обнаруж}$.

Поэтому, основываясь на этих данных, которые приводят сами производители, следует заключить, что применение трибоэлектрических СПС («Багульник», «Трезор», «Гюрза», «Дельфин», «Годограф» и т. п.) может быть приемлемо только для периметра длиной не более 5…10 км и, следовательно, для охраны периметра аэропорта (10…30 км), НПЗ (до 70…80 км), железнодорожного парка их примене-

ние малоэффективно (если не бессмысленно). Применять следует систему на базе технологии INTREPID, для которой, как было показано в предыдущем разделе, предельная длина периметра в 10…20 раз больше, т. е. может составлять 50…200 км.

Итак, завершая анализ темы, мы приходим к печальному заключению, что указанные в техдокументации характеристики ошибок всего лишь цифры, которые хотел бы видеть покупатель. Или же это значения, которые могут быть достигнуты при некоторых условиях, о которых производитель умалчивает.

Но если это так, то как при отсутствии этих ключевых параметров осуществлять выбор системы? Теория хороша, но руководителю никуда не деться от принятия решения.

Предлагаю опираться на информацию, получаемую по трем направлениям.

Первое – подробнее знакомиться с теми принципами, которые используются в системе для уменьшения вероятностей ошибок. Надо оценить в сравнительном плане их потенциальные возможности так, как это было нами сделано в предыдущем разделе. Следует предпочесть (разумеется, с учетом сложившихся условий и ограничений) ту систему, которая имеет больший потенциал адаптации и возможных настроек (удобнее и эффективнее, если они будут программными). Анализ в предыдущем разделе однозначно отдает предпочтение технологии INTREPID, которая поэтому выбрана нами для построения комплексной защиты периметра STRATUM.

Второе направление – ознакомиться с опытом применения выбранной системы в схожих условиях: на других похожих объектах.

Третье – создать собственный испытательный полигон.

Сколько стоит? – Главный вопрос Заказчика

Очень часто представление о стоимости системы Заказчик основывает на оценке стоимости оборудования базового элемента, тем более, что функционально он одинаков для большинства систем (рис. 1). Однако такая оценка может быть приемлема только в случае, если в сравниваемых системах применяется один и тот же принцип работы. Как подробно показано в статьях «INTREPID MicroPoint – сравнительный анализ стоимости. ч. 1, 2, 3» (www.intrepidsys.ru), несмотря на в 2 раза большую стоимость оборудования INTREPID стоимость системы «под ключ», начиная с величины 1 км, оказывается в разы ниже (рис. 5). Причем это различие тем больше, чем больше длина периметра.

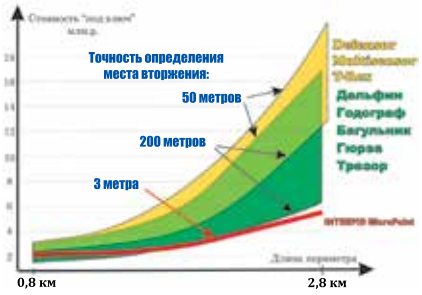
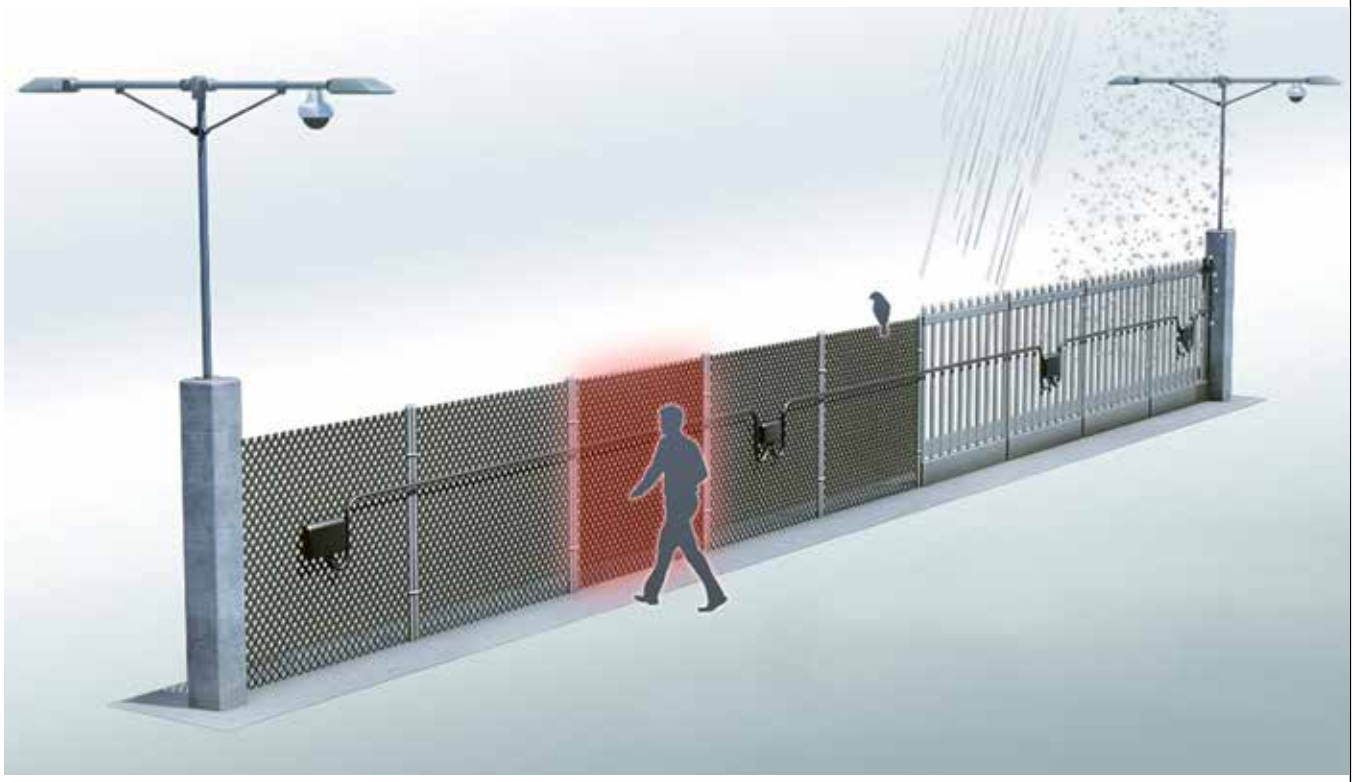


Рис. 5

Сигнал поступил. Что делать? – Интеграция

Чем важнее охраняемый объект и чем больше длина его периметра, тем более необходимо эффективное автоматизированное взаимодействие всех систем, входящих в комплекс охраны объекта: ТВ-наблюдение, охранное освещение, тепловизоры, контроль доступа на въездах и входах на террито-



рию. Большая часть из перечисленных в предыдущих разделах СПС располагает для целей интеграции только релейными выходами, так называемыми «сухими контактами»: возникла тревога – сработало реле – включилась ТВ-камера и/или освещение. Таких возможностей, однако, крайне недостаточно для создания комплексной системы защиты периметра объекта. Поэтому, выбирая для создания комплекса STRATUM технологию периметральной сигнализации INTREPID, мы приняли во внимание не только ее наилучшие обнаружительные возможности, не только ее наименьшую стоимость, но и максимально доступные возможности для интеграции.

Система комплексной защиты периметра STRATUM позволяет:

- отображать на графическом плане (спутниковой фотографии) объекта место нарушения периметра с точностью 3 м;
- управлять положением и углом поля зрения поворотных ТВ-камер и тепловизоров;
- синхронно включать при необходимости охранное освещение тревожного участка;
- обеспечивать, благодаря использованию управляемых ТВ-камер по сравнению с традиционной схемой расположения стационарных камер вдоль периметра, более понятное и эффективное отображение происходящего события. Общее число используемых ТВ-камер сокращается в 5…7 раз. При этом стоимость ТВ-системы сокращается в 1.5…2 раза! Плюс сокращение в 5..7 раз объема и стоимости видеоархива (существенное уменьшение стоимости системы с одновременным повышением ее качества и возможностей);
- обеспечить интеграцию любого другого оборудования обеспечения безопасности (радиолокационных станций, досмотрового оборудования, системы оповещения и др.).

О надежности и сопровождении системы

Если судить о надежности основных блоков систем, то, учитывая приблизительно одинаковую технологию их изготовления и используемые компоненты, разумно предположить, что она должна быть приблизительно одинаковой. Однако производители дают значение среднего времени наработки на отказ от 30 000 часов (3 года) у «Дельфина», до 60 000 часов (7 лет) у «Гюрзы». Почему так? Мы не знаем ответа.

Если одновременно с электронными блоками оценивается и надежность трибоэлектрического кабеля (важная часть системы), то в случае его установки на АКЛ выход системы через 1…1,5 года гарантирован.

Если судить о надежности системы по общему числу контактов и соединений в системе(по числу наименее надежных элементов), то и в этом сравнении лидирует система INTREPID, имеющая минимальное число блоков, кабелей и, следовательно, соединений. И действительно, есть опыт безотказной работы системы в условиях (-47 C^0…+ 45 C^0) на протяжении более 10 лет.

Ремонтопригодность всех систем хорошая и сопоставима по всем параметрам, кроме одного: место повреждения сенсорного кабеля в системе INTREPID определяется с точностью 1 м, у всех остальных систем – с точностью размера плеча (50…250 м).

К задачам сопровождения системы относятся, в первую очередь, коррекция настроек, в том числе сезонная калибровка, а также задание иной конфигурации зон охраны и взаимодействия подсистем. В системах INTREPID и STRATUM в отличие от других систем эти процедуры выполняются на программном, а не на аппаратном уровне. И поэтому выполняются быстро, просто и дешево.

Заключение

Проведенный анализ, в котором объективно и аргументированно рассмотрены основные факторы, влияющие на выбор системы защиты периметра, позволяет обоснованно сказать, что технология INTREPID и созданная на ее базе комплексная система защиты периметра STRATUM – это новое поколение периметральных систем. Новое поколение – это значит, что данные системы решают сложные задачи охраны периметра объекта (особенно протяженного периметра) не только с более высокими качеством и возможностями (функциональностью), но за меньшую стоимость.