# Совершенствование охраны традиционного и виртуального периметров, границы

**Необходимость противодействовать угрозе терроризма заставляет постоянно совершенствовать системы, отвечающие за безопасность и мониторинг объектов**

**В.А. Юдинцев**
Ведущий инженер ГУП НЦП "Элвис"

Акцент делается на системы, которые содействуют идентификации угрозы и принятию адекватных мер в случае нарушения, позволяют отслеживать и распознавать людей в зонах, расположенных внутри, вне и вдоль периметра объектов.

## Основные характеристики периметровых систем

Важнейший элемент всех типов периметровых охранных систем – электронное оборудование, обладающее следующими характеристиками:

- вероятность обнаружения, определяющая надежность рубежа охраны, не менее 0,9–0,95;
- устойчивость к электромагнитным, индустриальным помехам, шуму транспорта, вторжению мелких животных и птиц;
- частота ложных срабатываний не более раза за десять суток на участке длиной 250 м;
- работа в широком диапазоне условий;
- маскируемость (визуальная и техническая) средств обнаружения;
- надежность, простота монтажа и эксплуатации;
- интеграция с другими охранными системами.

Один из основных путей развития систем охраны периметра – их интеллектуализация, переход от датчиков порогового типа, выдающих сигнал типа "да/нет", к устройствам с функциями распознавания нарушителя.

Наиболее совершенные из таких систем позволяют реализовать интегрированные с существующей инфраструктурой решения, предназначенные для обеспечения безопасности периметра.

## Охрана традиционного периметра

Интегрированная система охраны традиционного периметра (ИСОТП) конструируется из расчета масштабирования согласно размерам объекта и использует одни и те же аппаратные и программные средства как для небольших местных, так и для крупных международных аэропортов.

### Этапы создания ИСОТП

Создание системы начинается с анализа угрозы, который включает в себя детальное исследование слабых мест объекта. Когда угрозы идентифицированы, риск, связанный с каждой их них, ранжируется по их вкладу, критичности и т.д. Затем принимается решение, какие риски следует смягчить, а какие принять. Этот этап чрезвычайно важен, поскольку определяет весь последующий ход разработки системы, а также ее стоимость.

Архитектура физической системы может быть разработана сразу после того, как определены основные параметры: параметры цели, эксплуатационная готовность ($A_0$), факторы окружающей среды, вероятность обнаружения ($P_d$), вероятность сигналов ложной тревоги ($P_{fa}$), сигнальные помехи (NAR).

Конструирование архитектуры начинается с составления чертежей объекта с увеличенным картированием мест работ. На чертежах указываются места расположения имеющихся источников электропитания и фиксированных узлов связи.

Осуществляется разработка точных моделей датчиков, как радиолокационных систем (РЛС), так и камер (видимого и ИК-диапазона) по диапазону кривых, учитывающих влияние погодных условий и характеристики цели, наряду со специфическими характеристиками датчика. Моделирование позволяет определить максимально используемый диапазон датчика для данного типа цели. Например, РЛС, при хороших погодных условиях работающая в диапазоне 1500 м (в этом диапазоне цель в 1 м$^2$ будет иметь $P_d$, равный 95%), станет использовать диапазон лишь 1000 м для той же цели при дожде 20 мм/час.

### Разработка топологии датчиков

Для разработки топологии сети датчиков информация о местах расположения источников питания и узлов связи, содержащаяся на чертежах объекта, используется в сочетании с данными о моделях датчиков. Например, в системе анализа сенсорной топографии (STAT), в которой используются значения $P_d$ по диапазонам кривых, для этой цели применяются данные топографии (включая здания), ограничения по высоте и другие топографические ограничения. Система STAT воспроизводит карту значений $P_d$ всего объекта в цвете. Нижние области $P_d$ корректируются с использованием дополнительных датчиков.

На рис. 1 показан пример использования STAT для разработки топологии датчиков аэропорта. Две наземные РЛС наблюдения (GSR) располагаются на противоположных концах аэропорта. Наличие очевидных пустот свидетельствует о необходимости установки дополнительных датчиков.

Датчики обеспечены резервными линиями связи, системами электропитания и компьютерными ресурсами. Такая система продолжает функционировать без ухудшения характеристик даже при выходе из строя какого-либо из компонентов.

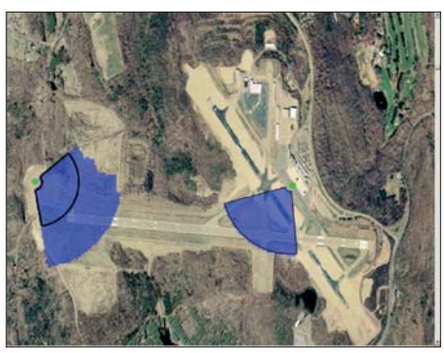

**Рис. 1. Пример использования системы анализа сенсорной топографии для разработки топологии датчиков аэропорта**

### Подсистемы ИСОТП

Как показано на рис. 2, ИСОТП состоит из шести подсистем, имеющих модульную конструкцию с хорошо проработанными интерфейсами. Это обеспечивает поддержку использования как новых, так и усовершенствованных элементов конструкции.

Подсистема обнаружения и отслеживания вторжения (IDTS) функционирует, как входной датчик наблюдения ИСОТП. Любые типы датчиков могут быть интегрированы в ИСОТП, однако предпочтение отдается трем основным типам:

1) наземная РЛС наблюдения (GSR) используется в местах полной видимости, как главное средство обнаружения и отслеживания целей, что объясняется всепогодными возможностями ее работы при невысокой стоимости эксплуатации;
2) видеокамеры, снабженные кабельной телевизионной сетью, и ИК-камеры используются в загроможденных местах, обычно вблизи строений;
3) сеть РЛС дальнего обнаружения применяется в областях с низким трафиком, как дополнительное средство обнаружения вторжения.

Входные данные от датчиков наблюдения собираются, обрабатываются и сохраняются, как и сигналы тревоги, которые генерируются и передаются на подсистему контроля и подачи команд (Command and Control Subsystem – C2S). События, генерируемые системой контроля доступа, также обрабатываются в IDTS и поступают в C2S.

Подсистема оценки вторжения (Intrusion Assessment Subsystem – IAS) осуществляет круглосуточную оценку событий вторжения при неблагоприятных погодных условиях. Комбинация камер видимого света и ИК-камер используется для выполнения оценки в полном диапазоне световых и погодных условий. Камеры могут работать в ручном, автоматическом и походном режиме. В автоматическом режиме данные положения, генерируемые IDTS, автоматически направляют

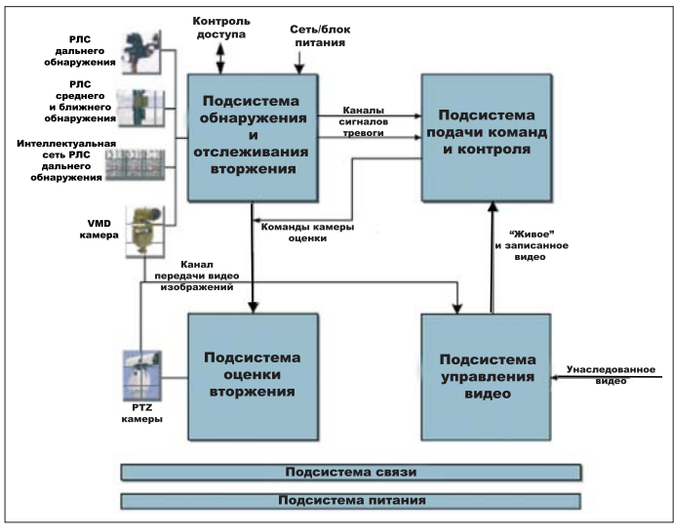


**Рис. 2. Блок-схема интегрированной системы охраны традиционного периметра**

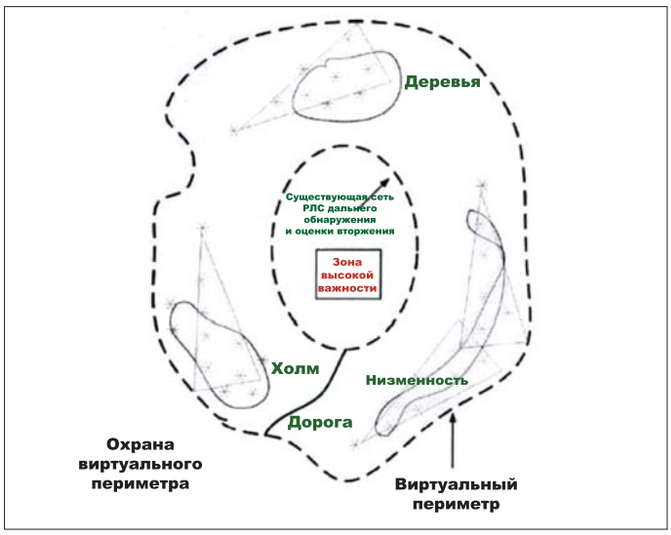


**Рис. 3. Общая концепция охраны виртуального периметра**

камеру на движущуюся цель. В походном режиме камера автоматически перемещается по местам в последовательности, определенной оператором, и с заданной задержкой в каждом месте. Все видеоизображения записываются.

Подсистема контроля и подачи команд (Command and Control Subsystem – C2S) обеспечивает оператору интерфейс с функциями управления событиями. Для оператора отображаются как географическая карта, так и табличные данные. В данной подсистеме осуществляется обработка сигналов тревоги от различных источников, в том числе сигналов от систем контроля доступа, сигналов о нарушении периметра, потере связи, нарушении питания, о злоумышленных действиях и пр. Далее устанавливается приоритетность сигналов тревоги по правилам, определенным пользователем. Сигнал наивысшего приоритета всегда представляется оператору для принятия мер. Он оценивает ситуации по видеоизображениям, поступающим от камер, подтверждает сигнал тревоги и принимает соответствующие решения, при необходимости привлекая персонал служб обеспечения безопасности. C2S также регистрирует все действия оператора и данные происшествия.

Подсистема связи (Communications Subsystem – CS) соединяет все рабочие элементы, включая датчики с вычислительными ресурсами, расположенными в серверных помещениях. В подсистеме используется оптоволоконная Ethernet-сеть с высокой скоростью передачи данных. Также обеспечивается мобильная связь (в том числе видео) с силами реагирования.

Подсистема питания (Power Subsystem – PS) представляет собой источники бесперебойного электропитания для всех компонентов системы.

Подсистема управления видео (Video Management Subsystem –VMS) управляет всеми операциями видео, включая отображение в режиме реального времени, воспроизведение, хранение и архивирование.

## Охрана виртуального периметра

В системе охраны виртуального периметра (СОВП) используются беспроводные датчики вторжения и беспроводное оборудование для оценки видеоизображений.

### Архитектура СОВП

Обычно применяется модульная системная архитектура, включающая в себя несколько типов протоколов и аппаратных средств.

Модульная системная архитектура облегчает интеграцию аппаратных средств и технических решений, обеспечивает мониторинг и контроль рассредоточенных по большому объекту сенсорных систем и систем оценки видеоизображений и интерфейс с внутренней и внешней системами командования и контроля.

Для СОВП характерна трехуровневая системная архитектура. Первичные датчики дальнего действия (типа РЛС) могут охватывать большую часть поверхности периметра. Вторичные датчики среднего действия необходимы для охвата пустот местности и долин. Кроме того, СОВП специально ориентирована на использование множества сенсорных датчиков ближнего действия. Каждый узел оценки поддерживает до трех видеокамер и двухстороннюю звуковую связь.

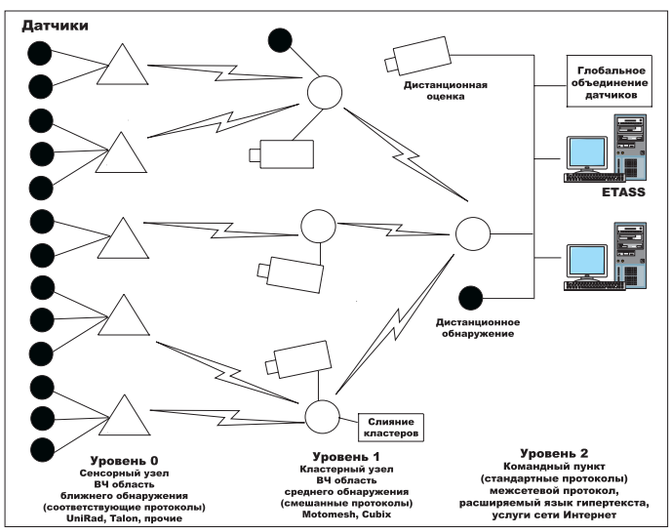


**Рис. 4. Графическое представление архитектуры системы охраны виртуального периметра**

### Особенности использования СОВП

СОВП предназначена для развертывания на территории, являющейся собственностью объекта, где доступ к местам общего пользования ограничен. Здесь отсутствует необходимость скрывать демонстрационные возможности системы, а питание осуществляется от солнечных батарей. Однако к СОВП предъявляются определенные требования, которые непросто реализовать. Система должна обеспечивать операторов информацией, достаточной для соответствующего реагирования. Это может быть выполнено за счет применения набора многоплановых датчиков с перекрывающимися рабочими зонами, предназначенных для обнаружения различных видов излучения, позволяющего выявить нарушителя, и связанных с визуальной оценкой.

СОВП должны быть удобными для размещения на местах, достаточно гибкими для адаптации к изменяющимся угрозам, а также должны позволять дистанционно настраивать или перепрограммировать значения чувствительности датчиков, алгоритмы слияния датчиков, программы. На рис. 3 показана общая концепция СОВП.

Графическое изображение аппаратной архитектуры СОВП представлено на рис. 4. Датчики объединяются в узлы датчиков (SN, уровень 0), которые связаны с кластерными узлами (CN, уровень 1), в свою очередь они соединены с сетью связи командного центра (CC, уровень 2).

### Некоторые итоги испытаний СОВП

В ходе демонстрационных испытаний СОВП в 2005 г. на базе ВВС в Киртланде было выявлено, что системные операторы имеют тенденцию отключать систему при избыточном уровне преднамеренных помех, ложных сигналов, интенсивности помех (NAR/FAR) в физических системах безопасности.

Работа внешних датчиков лучше всего осуществляется в контролируемых средах, например в

областях между сетями РЛС дальнего обнаружения или на гравийном участке без растительности. В СОВП-средах такие контролируемые условия отсутствуют, и предполагается, что система будет развернута на местности, не охваченной технической поддержкой. Таким образом, можно ожидать высокой интенсивности преднамеренных помех и ложных сигналов.

В ходе указанных испытаний система продемонстрировала способность обнаруживать и визуально оценивать вторжение человека и транспортного средства в пяти областях с отсутствием прямой видимости (Eintrusion at five non-line-of-sight areas). Была также продемонстрирована способность оценивать визуально низкопрофильных (low-profile) нарушителей. Передача беспроводных данных осуществлялась с расстояния в несколько километров, хотя оно может быть больше.

Используемые аппаратные средства работали в течение года при соблюдении минимального ухода, который требовался из-за влияния сезонных изменений на чувствительность датчиков. В будущем это обслуживание будет выполняться дистанционно.

## Охрана границы

### Типы датчиков

Рассмотрим два типа датчиков, применяемых для расширения зоны действия систем наблюдения периметра (границы): скрытые дальномерные направленные радиолокационные датчики и скрытые дальномерные оптоволоконные датчики.

Скрытые направленные радиолокационные датчики, называемые также канальными коаксиальными кабелями, являются, по сути, объемными датчиками и осуществляют защиту периметра более 30 лет. В этом случае СВЧ-энергия реализуется между двумя параллельными коаксиальными кабелями. Один кабель действует как передающая антенна, другой – как приемная антенна. Оба кабеля утапливаются в почву на глубину 23 см. Обнаружение является результатом того, что объекты с достаточным радиолокационным поперечным сечением на рабочей системной частоте нарушают поле с силой, достаточной для подачи сигнала тревоги. Объемное поле позволяет сенсорным кабелям демонстрировать исключительно большую вероятность обнаружения: более 99% – для человека, 95% – для небольших животных и птиц и естественных природных явлений (дождь, снег, ветер и т.д.). Канальные коаксиальные системы становятся менее устойчивыми, если сенсорные кабели располагаются на поверхности, а проводимость утопленной среды влияет на силу поля. Это означает, что их применение в горных местах и/или в местах с изменяющимися характеристиками почвы требует использования специальной техники монтажа и/или дополнительных зон, что приводит к значительному увеличению стоимости.

Заглубленные волоконно-оптические датчики являются сейсмическими датчиками, измеряют волны давления в земле, вызванные нарушителями. Сейсмические датчики используются в системах внешней безопасности давно, однако их противоречивые характеристики привели к большему распространению и развитию других сенсорных технологий. В настоящее время сейсмические датчики преимущественно используются для защиты подземных трубопроводов и обнаружения пустот по длине шва, теоретически могут защищать десятки километров границы без источника питания, обеспечивая значительную экономию средств.

### Дальномерные управляемые РЛС

В основе таких систем находится новый сверхширокополосный спектр, обладающий возможностями:

- обнаружения с точностью до 1 м;
- программного зонирования для адаптации системы к изменяющимся требованиям рабочей среды;
- нормализованного установления порогов для адаптации системы к изменяющейся топографии;
- глобального анализа отклика для сведения до минимума преднамеренных помех;
- интегрирования устройств питания и данных, что позволяет минимизировать требования к инфраструктуре;
- дистанционной диагностики, позволяющей уменьшить стоимость обслуживания на протяжении жизненного цикла системы.

Эта система безопасности границы включает в себя C⁴I-систему, основанную на GIS/GPS, которая может отслеживать координаты потенциальных целей и сил реагирования.

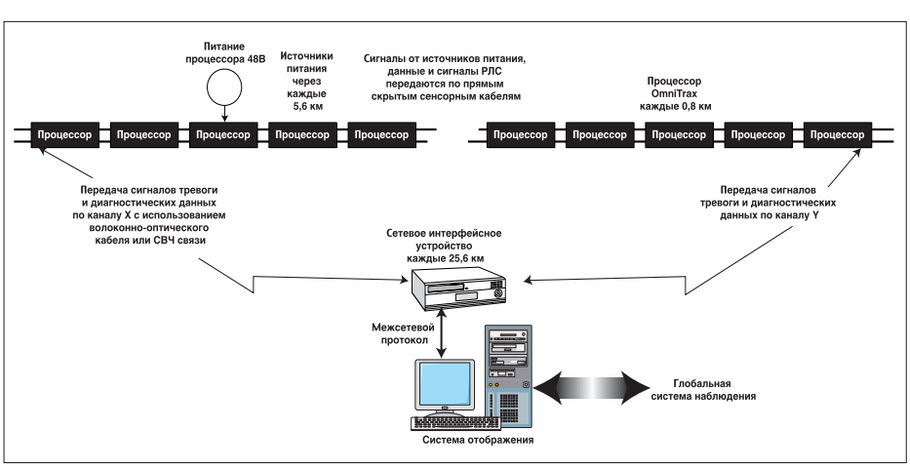


**Рис. 5. Концепция системы охраны границы**

### Концепция системы охраны границы

Архитектура системы (рис. 5) является чрезвычайно отказоустойчивой, характеризуется разделением каналов данных и источников питания для каждого сенсорного кабеля, а также использованием батарейного питания и схемы зарядки для каждого процессора. Процессоры работают в широком температурном диапазоне, как и вся система, они могут быть заглублены в целях защиты от вандализма. Кроме того, в систему включены многочисленные диагностические устройства для установления и устранения вероятных неисправностей, имеется возможность дистанционной настройки порогов сигналов тревоги.

Новые системы будут иметь возможность определять направление движения объекта, пересекающего кабель, и возможность поверхностного монтажа сенсорных кабелей.

## Решение задачи охраны периметра в России

Разработаны и используются на практике интеллектуальные системы видеонаблюдения, в которых функции видеообработки и анализа ситуаций осуществляются компьютером, благодаря чему отпадает необходимость следить за событиями, отображаемыми на экране монитора. Системы непрерывно и автоматически анализируют обстановку на охраняемом объекте и в случае необходимости поднимают тревогу.

Такие системы имеют следующие функциональные возможности:

- трансляция изображения на экран монитора компьютера;
- создание многоуровневого видеоархива, при котором записывается не только видеоизображение, но и на каждый подвижный объект заводится специальная карточка с описанием признаков и крупной фотографией объекта;
- детектирование движения;
- обнаружение и захват целей – до 50 подвижных объектов одновременно;
- целеуказание и автоматическое сопровождение объектов;
- создание базы данных объектов с возможностью интерактивного поиска по признакам (тип, цвет, скорость и т.д);
- задание тревожных зон и распознавание ситуаций;
- возможность получения детального изображения цели оптическим приближением в автоматическом режиме;
- автоматическое слежение за выбранной целью и получение траектории ее движения;
- привязка к карте местности – система позволяет отображать на карте мнемознаками, символами все обнаруженные объекты;
- передача информации и изображения через любые каналы связи, включая узкополосные (GPRS, Blue Tooth).

Использование подобных технологий видеонаблюдения позволит реализовать принципиально новые, сотовые концепции безопасности. ■

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