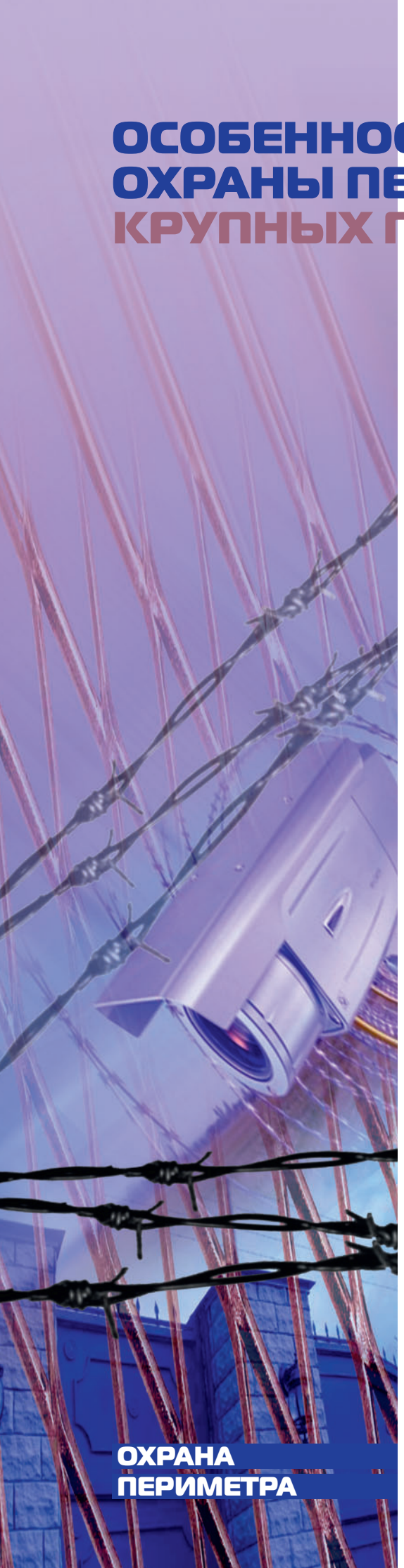
ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОХРАНЫ ПЕРИМЕТРА КРУПНЫХ ГОРОДСКИХ ОБЪЕКТОВ

Звежинский Станислав Сигизмундович
д.т.н., профессор МТУСИ



ОХРАНА ПЕРИМЕТРА

Надежная охрана периметра крупного (важного, особо или критически важного) объекта является, безусловно, необходимой составляющей успешности системы физической защиты (СФЗ), поскольку «раннее» обнаружение вторжения потенциального нарушителя (злоумышленника, вора, террориста и пр.) на границе контролируемой зоны обеспечивает временной интервал силам охраны и безопасности для организации эффективного противодействия [1]. Существует множество литературы, как отечественной, так и зарубежной, описывающей различные аспекты охраны периметра объекта [2-7]. Однако известная вариативность внешней среды (физико-географические условия, климатика, антропогенные и политические факторы) и внутренних условий (специфика объектов, их «слабые места» или уязвимости, организация службы охраны и пр.) обусловливают широкий диапазон кажущихся возможностей для заказчиков и проектантов, который не обязательно приводит к нужному, рациональному результату. Тем более это проявляется в условиях городской среды, при концентрации индустриальных помеховых факторов, отсутствии (или существенной ограниченности) пространства для организации более эффективного многорубежного периметра, повышенных требованиях к эстетике инженерных и технических средств физической защиты (ТСФЗ) и т. д.

Тематика статьи обусловлена интересом потенциальных заказчиков и проектантов к повышению эффективности охраны городских объектов в новых условиях, наметившихся в последнее время:

- известные затруднения в финансировании работ и закупок оборудования по СФЗ;
- «вежливый» отказ многих (прежде всего, государственных) заказчиков от импортного оборудования (усиление требований по ПДИТР и импортозамещению);
- реальное, ненадуманное возрастание террористических угроз в крупных городах, что обусловливает изменение, усложнение модели злоумышленника, под которой ранее типично понимался безоружный «случайный» или неподготовленный нарушитель (из «печальной» географии за последние 4 года – Волгоград, Дербент, Грозный, Санкт-Петербург, Астрахань; информация НАК в марте-апреле 2017 о предотвращенных терактах в крупных городах).

Недавним примером повышенного внимания государства к блокированию террористических угроз в городской среде служит Постановление Правительства РФ «Об утверждении требований к антитеррористической защищенности гостиниц…» от 14.04.2017 [8], где, однако, из обязательных технических мер предусматривается только видеонаблюдение (дополнительно – освещение, тревожно-вызывная сигнализация) с архивированием информации на срок не менее 30 дней. Но это связано, по-видимому, с тем, что городские гостиницы, как правило, не имеют примыкающей территории, и их периметром фактически являются стены зданий. В этом же Постановлении отмечается, что антитеррористическая защищенность обеспечивается, в том числе, другими инженерно-техническими средствами СФЗ.

Охрана городского объекта (периметра, внутренней территории, отдельных помещений и предметов) обеспечивается техническими средствами трех систем (подсистем) в составе СФЗ: охранной сигнализации (СОС), охранного телевидения (СОТ), контроля и управления доступом (СКУД); защита же в основном обеспечивается инженерными сооружениями (заграждения, заборы и пр.) и средствами укрепленности (решетки, жалюзи, пленки и пр.). Кроме того, используются специальные ТСФЗ по досмотру посетителей и транспорта, технической защите информации и др., рассмотрение которых выходит за рамки данной статьи, как и организация сил охраны и безопасности, их техническое обеспечение и вооружение. Можно, конечно, обсуж-

дать, какие инженерные заграждения в наилучшей степени подходят для объекта в городской черте, но, во-первых, эта тема уже поднималась в литературе [2, 9], а во-вторых, зачастую такая возможность просто отсутствует – либо забора по периметру нет, либо он такой, какой есть (например, гостиница «Президент-отель», Дом Правительства), и изменить его вид невозможно по разным причинам.

Необходимо отметить, что пока основную роль при организации защиты периметра городского объекта, как правило, несет СОС. Однако опережающее развитие СОТ позволяет в обозримом будущем спрогнозировать основной упор в охране периметра на подсистему интеллектуального видеонаблюдения с сигнализационными программными детекторами движения, способными обнаружить «ухищренные» способы вторжения, отличить человека-нарушителя от крупного животного (например, собаки) или стаи птиц, устранить последствия неблагоприятных погодных условий (например, сильный снег, дождь, обледенение) и пр. За рубежом, например, в Великобритании, «ставка» в охране городских объектов уже давно сделана на видеонаблюдение, дополняя его сигнализационными средствами обнаружения (СО) с повышенной информативностью и сигнализационной надежностью (возможностью классификации типов нарушителя, уточнения места вторжения и пр.).

В городе, по сравнению с «сельскими» условиями, для ускоренного продвижения интеллектуального видеонаблюдения имеется три важных преимущества:

- доступность сетевого электропитания и отсутствие ограничений на потребляемую мощность;
- доступность IP или WiFi – коммуникационной среды;
- как правило, наличие «фонового» ночного освещения на уровне не менее 0,01 лк (обусловленного городским освещением), что позволяет использовать для СОТ низкоуровневые телевизионные камеры (ТВК) без дорогостоящего освещения или малоэффективной подсветки (на дальности более 50 м).

Заметим, что тематика интеллектуального видеонаблюдения достаточно широко представлена в отечественной специальной периодике (в том числе в данном журнале), продолжает нарастать и здесь подробно не рассматривается.

НОРМАТИВНАЯ БАЗА ДЛЯ ОРГАНИЗАЦИИ ОХРАНЫ ПЕРИМЕТРА НА ГОРОДСКОМ ОБЪЕКТЕ

Нормативные документы первого, федерального уровня значимости – законы и указы, имеющие отношение к рассматриваемой теме, носят общий методологический и организационный характер, не раскрывая конкретики, интересной специалистам. Примером тому являются, например, ФЗ № 35 «О противодействии терроризму» от 06.03.2006 или Указ Президента РФ от 10.11.2007 № 1495 «Об утверждении общевоинских уставов…», более информативными являются Постановления Правительства РФ.

Особый интерес представляют «Правила по обеспечению безопасности и антитеррористической защищенности объектов топливно-энергетического комплекса» от 05.05.2012, утвержденные избранным Президентом РФ В. Путиным в последний день его работы в должности Председателя Правительства [10]. В этом Постановлении изложена методология построения СФЗ объектов ТЭК по обеспечению заданного уровня защищенности, зависящего от их категории, которая в свою очередь определяется масштабом потенциального ущерба. К положительным сторонам документа можно отнести выверенный тезаурус и понятийный аппарат, к отрицательным – большой объем. В нем достаточно подробно описаны требования и рекомендации к периметральным инженерно-техническим средствам защиты, к техническим средствам СОС, СОТ и СКУД (а также вспомогательным системам – связи, оповещения, освещения и пр.), установленным на периметре и внутри зданий (помещений). На наш взгляд, этот документ может служить реальной основой для построения (проектирования, модернизации) СФЗ любого крупного городского объекта. Требуется лишь его творческое переосмысление под специфические условия.

На втором – ведомственном и межведомственном – уровне значимости нормативных документов по вопросам СФЗ, где еще больше конкретики, следует отметить определенный «разнобой». Он проистекает еще с советских времен, когда два больших ведомства – КГБ и МВД (наследники огромной, но единой НКВД) – так и не смогли «договориться» о реализации **единой** (выделено автором) технической политики государства в области СФЗ, тогда эта область называлась несколько иначе – технические средства охраны (ТСО). Вследствие этого в настоящий момент в различных ведомствах и корпорациях страны существует большое количество внутренних документов (ОСТы, руководящие документы, приказы по ведомствам, технические правила и пр.), определяющих порядок проектирования и построения СФЗ, слабо коррелированных друг с другом. Можно выделить пять «семейств» близких по сути нормативных документов, которые сгруппированы вокруг:

1) Росатома и Пограничной службы ФСБ РФ (АО «СНПО «Элерон»);
2) МВД и Росгвардии (НИЦ «Охрана»);
3) Министерства обороны (12 ЦНИИ МО РФ);
4) Минэнерго (Газпром, Роснефть, Транснефть);
5) Министерства транспорта («Ассоциация» и др.).

Некоторые из этих документов являются недоступными (закрытыми), соответствующие требования в них зачастую противоречат друг другу, но самым неприятным следствием ведомственного «разнобоя» является большое число т. н. «перечней», где указаны только те технические средства СФЗ (ТСФЗ), которые можно применять на объектах данного ведомства. К сожалению, объективного мониторинга целесообразности применения (эффективности) ТСФЗ в масштабах страны не было и нет, в отличие, например, от США, где это осуществляет государственная компания Sandia Lab [1]. Фактически получается, что в РФ большая часть рынка СФЗ «разделена» по ведомствам (куда относятся оборудуемые объекты), но даже внутри ведомства возможны различные «перечни» больших корпораций (например, в Минэнерго). Если же городской объект охраны напрямую не относится к какому-либо ведомству, но может относиться косвенно – по используемым в СФЗ силам охраны и безопасности (например, Росгвардия, МВД, Минобороны). Для разработчиков ТСФЗ наличие ведомственных перечней, конечно, затрудняет справедливую конкуренцию, но пока не выявлено тенденции к их уменьшению.

В 2000-е годы в РФ разработано множество ГОСТов (национальных стандартов) по различным вопросам создания компонентов и СФЗ в целом, в основном специалистами первых 3 ведомств из вышеприведенного списка «семейств», которые несут в себе некоторые «родовые» черты. В последнее время эти ГОСТы заменяются техническими регламентами (на основании ФЗ РФ «О техническом регулировании» от 27.12.2002, № 184), из которых безусловный интерес представляют: «О безопасности зданий и сооружений» (ФЗ РФ от 02.07.2013 № 185), «О технических средствах обеспечения противокриминальной защиты объектов и имущества» (проект ФЗ), «Проектирование систем антитеррористической защищенности и комплексной безопасности высотных и уникальных зданий» (технический регламент П-119-05-СБ-01-2010).

Из других нормативных документов следует выделить важный, на мой взгляд, ГОСТ Р 52860-2007 «Технические средства физической защиты. Общие технические требования», действующий в Росатоме. Интерес представляют ГОСТ Р 51558-2008 («Средства и системы охранные телеви-

зионные…), ГОСТ Р 51241-2008 («Средства и системы контроля и управления доступом…»), а также устаревшие руководящие документы (РД) системы МВД РФ, например, РД 78.36.007-99 «Выбор и применение средств охранно-пожарной сигнализации и средств технической укрепленности для оборудования объектов». Изучение этих документов повышает, как сейчас принято говорить, уровень компетенций по выбранной тематике.

МОДЕЛИ НАРУШИТЕЛЕЙ И ИХ ВЛИЯНИЕ НА ПОСТРОЕНИЕ СФЗ

Под моделью нарушителя понимается тип злоумышленника, который обусловлен его подготовленностью и снаряжением, целью и возможным сценарием вторжения на объект охраны. Условно они подразделяются на внешних (вторгающихся на объект из внешней среды) и внутренних, которые мы не рассматриваем. Существует несколько классификаций внешних нарушителей, отличающихся друг от друга и зависящих от множества факторов: местоположения, политической и криминальной обстановки и пр. Для наших условий можно предложить три основных типа, приведенных ниже в порядке возрастания опасности:

1) **случайный или неподготовленный**, целью которого является спонтанное желание проникнуть на городской объект для мелкой кражи, порчи имущества (саботаж) и пр., возможно использующий для вторжения подручные средства, не знакомый с элементами существующей СФЗ;
2) **подготовленный**, подготавливающий акцию вторжения заранее (знакомясь с видимыми элементами существующей СФЗ), типовыми целями которого являются кража или сбор компрометирующей информации, использующий инженерные средства для облегчения вторжения;
3) **осведомленный или хорошо подготовленный** (в том числе в составе группы), задолго планирующий акцию вторжения, собирая информацию об СФЗ в целом (в том числе с использованием специальных технических средств, путем подкупа сотрудников-сообщников), типовыми целями которого являются крупная кража, диверсия, террористический акт, сбор особо важной информации, использующий специальные технические (например, для постановки помех) или инженерные средства для сокрытия вторжения и последующего отхода.

Следует понимать, что типовые ТСФЗ (главным образом, средства обнаружения нарушителей) в нашей стране и за рубежом разрабатываются и проверяются (на предмет соответствия заданной вероятности обнаружения) только для первого, наименее опасного типа [4, 11]. Для второго и, особенно, третьего типа нарушителя сигнализационная надежность СО снижается, в неблагоприятных условиях – до практического нуля. Это обусловлено существованием т. н. «дыр» или зон пониженной чувствительности в зоне обнаружения СО, а также принципиальными ограничениями на физический принцип регистрации полезных сигналов. Не существует таковых без недостатков, иначе СО разрабатывались и выпускались бы только одного принципа действия вместо существующих около 20 [6, 7, 12].

Если заказчика (проектировщика) **действительно** (подчеркнуто автором) волнует проблема обнаружения осведомленного нарушителя, то следует уяснить соответствующие основные базовые требования к периметральным компонентам СФЗ:

- выигрывают маскируемые СО, чувствительный элемент (преобразователь контролируемой физической величины в электрический сигнал) которой не виден как с внешней стороны периметра (это понятно), так и с внутренней (затрудняя действия возможного внутреннего сообщника);
- преимущества имеют СО пассивного физического принципа действия, который невозможно (или крайне тяжело) выявить путем регистрации вблизи электромагнитных полей или однократными физическими воздействиями якобы случайных «прохожих» или «играющих детей»;
- преимущества имеют СО с объемной зоной обнаружения, которую трудно «обойти» (перепрыгнуть, переползти и пр.), даже применив определенную осведомленность;
- необходимо на рубеже охраны в пределах одного участка устанавливать 2 или 3 СО с разнесенными зонами обнаружения, основанными на различных физических принципах действия, у которых «дыры» проявляются в несовместимо разных условиях;
- использование «замкнутой» СОТ типа CCTV, лучше малозаметной или замаскированной под освещение, оповещение и пр.;
- ограничение протяженности одного участка охраны величиной не более 100 м (как в действующем стандарте США для охраны особо важных объектов) для более точной установки места предполагаемого вторжения и улучшения помехоустойчивости СО;
- обеспечение полосы отчуждения (например, путем установки внутреннего ограждения) между внешним периметральным заграждением объекта и внутренней территорией, по которой могут передвигаться штатные сотрудники и посетители; ширина такой полосы, как показывает практика, должна быть не менее 3 м;
- учет новых возможностей осведомленного нарушителя по совершению противоправных действий, прежде всего, с помощью БЛА вертолетного типа (например, заброс взрывоопасных предметов, шпионских устройств на территорию объекта), когда периметральные СО не в состоянии обнаружить такие инциденты.

Конечно, совокупность вышеуказанных требований (а только она дает гарантированную эффективность), к сожалению, очень трудно (если возможно) реализовать на практике в городских условиях, но стремиться к этому надо.

СПЕЦИФИКА ГОРОДСКИХ УСЛОВИЙ, ВЛИЯЮЩАЯ НА ОРГАНИЗАЦИЮ ОХРАНЫ ПЕРИМЕТРА

Условия крупного города обуславливают нижеследующие характерные особенности, которые необходимо учитывать при выборе оборудования СФЗ.

Уровни электромагнитных помех на 3-5 порядков (в разных диапазонах частот и разных частях города) превышают фоновые величины, свойственные безлюдным территориям или даже сельской местности, что обусловлено, в основном, влиянием и насыщенностью высоковольтных ЛЭП, городского транспорта (не обязательно электрифицированного), разнообразных и разветвленных систем радиосвязи. Это ставит «крест» на применении ТСФЗ с относительно низкой электромагнитной совместимостью, например, пассивных маскируемых магнитометрических, вибромагнитометрических или сейсмомагнитометрических СО [4, 6]. Хотя в Израиле магнитометрические СО с «небольшим» чувствительным элементом, вмурованным в кирпичное или бетонное заграждение, используются в сельской местности для сигнализационного блокирования «перелаза» вооруженным нарушителем. Вблизи границы городского объекта могут случайно появляться и исчезать источники мощных импульсных (а значит широкополосных) электромагнитных полей, например, от сварочных аппаратов, что также предъявляет требования к повышенной электромагнитной совместимости ТСФЗ.

Уровни сейсмических помех на 4-6 порядков (в разных диапазонах частот и разных частях города) превышают фоновые величины, свойственные безлюдным территориям, что также обусловлено, в основном, влиянием городского транспорта и строительной активностью. Это практически исключает применение в городских

условиях пассивных сейсмических СО [4, 6, 12], за исключением изделий с «узкой» ЗО, регистрирующих волны давления; но такие СО в зимних условиях РФ, как показывает практика, работают неустойчиво [2] в отличие, например, от Вашингтона, где они используются при охране лужайки Белого Дома. Заметим, что точечные сейсмоприемники (геофоны, акселерометры, пьезодатчики), установленные на ограждении, уже образуют ЧЭ не сейсмических, а вибрационных СО, которые широко (и справедливо) используются при охране периметра [13].

Заграждение по периметру объекта, которое трудно или невозможно заменить или оптимизировать, имеет зачастую разнородный характер: кирпичный забор, бетонные плиты, сетка, металлическая решетка и т. д., в промежутках «разрываемые» стенами зданий и сооружений. Линия периметра может быть весьма ломаной, а по высоте различной и уступами (на склоне). Это ограничивает широкое использование в составе СФЗ городского объекта двухпозиционных радиолучевых и ИК-активных СО, у которых ЗО распространяется прямолинейно; кроме того, их трудно замаскировать или закамуфлировать. В местах сочленения различных типов заграждений, зданий и сооружений, где возникают предпосылки вторжения подготовленного нарушителя, возможно использование однопозиционных радиолучевых СО, основанных на эффекте Доплера.

Трудность организации необходимой для надежной охраны полосы отчуждения, а также невозможность крупной растительности по периметру снаружи и внутри объекта, во-первых, создают уязвимости для вторжения (например, с использованием деревьев), во-вторых, создают сильные помехи, связанные с раскачиванием кустов, стволов и крон деревьев при ветре. Это ограничивает использование СО, чувствительных к такого рода помехам, например, емкостных (электростатических), радиолучевых с относительно широкой ЗО [6, 7].

Усиление аэродинамического фактора заключается в увеличении скорости и турбулентности ветровых потоков в условиях сложной пространственной конфигурации городских сооружений. Это предъявляет повышенные требования к ветровой помехоустойчивости применяемых СО. При этом не рекомендуется применять т. н. адаптивное регулирование порога обнаружения (когда его величина плавно увеличивается с увеличением монотонного шума с ЧЭ, то есть скорости ветра), поскольку можно быть уверенным, что подготовленный нарушитель тоже об этом знает – во время ветра (дождя, снегопада с ветром) вероятность обнаружения таких СО значительно уменьшается.

Другие требования к периметральным СО общего характера можно найти в литературе.

ОСНОВНЫЕ РЕКОМЕНДАЦИИ ПО ВЫБОРУ ОБОРУДОВАНИЯ ОХРАНЫ ПЕРИМЕТРА

Городской объект охраны, как правило, имеет относительно небольшую протяженность периметра – не более 1 км, при этом может использоваться кабельная система сбора и обработки информации (ССОИ) любого типа. Применение радиоканальной ССОИ нежелательно ввиду большей уязвимости к специально создаваемым радиочастотным помехам, а также с точки зрения защиты циркулирующей в системе информации. Предпочтительным решением являются оптоволоконные линии связи.

Опыт и анализ объема рынка ТСО в мире показывают, что альтернативы

вибрационным СО, осуществляющим сигнализационное блокирование периметральных заграждений, не существует [6, 13]. В их пользу – пассивный характер действия, малозаметность или маскируемость (под освещение, линии связи), строго ограниченная плоскостью заграждения. При этом надо понимать, что универсальных изделий, предназначенных для установки на любые заграждения, нет – оптимальные характеристики СО достигаются только для определенного типа заграждений, для других – хуже.

В РФ в основном разработаны и производятся вибрационные СО с трибоэлектрическим кабельным ЧЭ, принцип действия которого основан на паразитном электрическом эффекте [13-15]. Такие изделия достаточно надежно функционируют на «мягких» сеточных заграждениях, в то время как на решетчатых – намного хуже, не хватает банальной чувствительности. На бетонных, кирпичных заграждениях применять трибоэлектрический ЧЭ нельзя, поэтому организовывают козырек (как правило, «колючий»), который и блокируют от «перелаза» и «перекуса». Но такой козырек портит эстетику объекта охраны и не всегда допустим.

Зарубежные вибрационные СО используют специализированный высокочувствительный кабельный ЧЭ (электретный, гибкий пьезоэлектрический, магнитоэластичный), поэтому проявляют повышенную сигнализационную надежность именно на «жестких» и монолитных заграждениях [5, 13]. Отечественную альтернативу им дает вибрационное СО с оптоволоконным ЧЭ, которое использует эффект изменения параметров ИК излучения (фаза, поляризация, спекл-структура), распространяющегося в оптоволокне (одномодовом, многомодовом) под действием вибраций контролируемого заграждения. Дополнительно, оптоволоконный ЧЭ не чувствителен к электромагнитным помехам (высочайшая электромагнитная совместимость), что делает такие СО весьма перспективными для использования в городских условиях.

Типичное современное вибрационное оптоволоконное СО, по сути, представляет собой систему обнаружения с явно выраженной центральной станционной частью, куда со всего периметра «стекаются» сигналы с участков периметра и где при помощи достаточно мощного компьютера происходит их обработка и распознавание (тревога/дежурный режим) [4, 13, 15]. Алгоритм обработки информации основан, как правило, на технологии искусственных нейронных сетей, когда наилучшие параметры автоматически выбираются на основе сформированного (на конкретном объекте) «учебника», состоящего, с одной стороны, из тренировочных и реальных полезных сигналов, а с другой стороны, зарегистрированных помеховых воздействий. Учебник формируется в процессе пуско-наладки и по мере необходимости примеры для дообучения добавляются в него в процессе эксплуатации системы обнаружения.

Относительная трудность ремонта оптоволоконного ЧЭ в городских условиях по понятным причинам не является недостатком. Дополнительным преимуществом оптоволоконных систем является возможность дополнительной передачи (по используемому оптоволокну) видеосигналов с СОТ, другой информации.

Единственным значимым недостатком вибрационных оптоволоконных систем обнаружения является их повышенная погонная стоимость, которая приблизительно сравнивается с погонной стоимостью типичных трибоэлектрических СО при протяженности периметра свыше 3-5 км. Поэтому в настоящее время осуществляются работы по удешевлению оборудования таких систем.

Итак, надежные вибрационные СО – «каркас» построения СФЗ периметра. Второе, на что хотелось бы обратить внимание, это активные радиоволновые кабельные СО, основанные на эффекте линии вытекающей волны (ЛВВ) и работающие в УКВ-диапазоне частот 50±10 МГц. Два или даже один коаксиальные кабельные (с перфорацией) ЧЭ формируют объемную, но достаточно компактную зону обнаружения вблизи периметра. Причем один кабель может находиться на заграждении (неметаллическом) в коробе, а второй – в грунте, могут оба находиться в грунте, то есть СО может быть полностью маскируемым. Как показывают зарубежные исследования [1, 6, 7], ЛВВ СО имеет максимальный т. н. «потенциал обнаружения», то есть по совокупности сигнализационных параметров является лидером среди других типов, пусть и не особо выраженным. Современные зарубежные изделия, недоступные на отечественном рынке, объективно лучше отечественных СО, однако и намного дороже. Отечественная техника такого типа выпускается несколькими компаниями, но пока не очень востребована в силу разных причин.

Возможность анализа других средств или систем раннего обнаружения нарушителей на периметре городского объекта упирается в формат статьи. Кроме приведенной, существует и другая литература по этой проблеме. Выражаем надежду, что высказанные здесь мысли поспособствуют заказчикам и проектантам в новых условиях (и соответственно повышенных требований к сигнализационной надежности) создавать более эффективные СФЗ. Тематика статьи широка, и хотелось бы увидеть продолжение в лице других авторов, в том числе по техническим средствам СКУД и, конечно же, по новым возможностям интеллектуальных систем видеонаблюдения на периметре.

ЛИТЕРАТУРА

1. *Гарсиа М. Проектирование и оценка систем физической защиты. М.: Мир, АСТ, 2002.*
2. *Иванов И. В. Охрана периметров-2. М.: Паритет-Граф, 2000.*
3. *Магауенов Р. Г. Системы охранной сигнализации: основы теории и принципы построения. М.: Горячая линия – Телеком, 2004.*
4. *Звежинский С. С. Проблема выбора периметровых средств обнаружения // БДИ. 2002. № 4.*
5. *Введенский Б. С. Оборудование для охраны периметров. М.: Мир безопасности, 2002.*
6. *Report TCRP-86-4. Intrusion detection for public transportation facilities handbook. Transit Cooperative Research Program. Washington, 2003. November.*
7. *Perimeter Security Sensor Technologies Handbook for DARPA and JPSG. NISE East Electronic Security Systems. 1997.*
8. *Постановление Правительства РФ «Об утверждении требований к антитеррористической защищенности гостиниц и иных средств размещения, оказывающих гостиничные услуги, и формы паспорта безопасности данных объектов» от 14.04.2017, № 447.*
9. *Ларин А. И., Звежинский С. С. Заграждение как элемент комплекса ТСО объекта // Специальная техника. 2002. № 3.*
10. *Постановление Правительства РФ «Правила по обеспечению безопасности и антитеррористической защищенности объектов топливно-энергетического комплекса» от 05.05.2012, № 458.*
11. *Звежинский С. С. О сигнализационной надежности периметровых средств обнаружения // БДИ. 2004. № 2.*
12. *Груба И. И. Системы охранной сигнализации: Технические средства обнаружения. М.: Солон-Пресс, 2012.*
13. *Звежинский С. С. Технические особенности построения периметровых вибрационных средств обнаружения // БДИ. 2004. № 4-5.*
14. *www.dedal.ru.*
15. *www.neurophotonica.ru.*