Радиоразведка в задачах антитеррора

Д. И. Васильев, генеральный директор ОАО НПО «Завод Волна»
М. А. Вознюк, доктор военных наук, профессор, академик МАС, заместитель директора НИЦ НПО «Завод Волна» по научной работе

Способы ведения антитеррористической деятельности тесно связаны с условиями, определяющими степень вскрытия замысла и тактики действия террористов.

Сегодняшнее время способствует широкому использованию преступниками новых информационных технологий в своих антизаконных (бандитских) действиях, в результате которых страдает в большей степени мирное население. Это, прежде всего использование средств радио и теле вещания с целью влияния на массы людей. Например, вызывать у населения панику, дать искаженную информацию в оценке какого то факта чем вызвать недовольство у мирных граждан. Использование средств связи и управления (компьютеров и сети Интернет или системы связи) для управления диверсионным ресурсом (взрывными закладками).

Следовательно, еще на стадии разработки новых технологий способных на расстояниях исполнять указания оператора, необходимо предусматривать возможность их блокирования при несанкционированном использовании. А на практике это энергетическое подавление шумовыми сигналами или специальными сигналами радиоуправляемых агрегатов, то есть создавать условия блокировки систем управления подрывами или другим враждебным действиями. Эта задача может и должна успешно решаться правоохранительными органами и любыми охранными структурами при условии если у них на достаточном техническом уровне решена задача радиоразведки в зоне охраняемого объекта. В нашем случае она сводится больше к задаче радиомониторинга эфира в зоне охраняемого объекта.

Постоянный контроль эфира, в наиболее вероятных для использования в целях террора участках радиочастотного диапазона, позволит набрать статистику характеризующую состояние эфира на любой рассматриваемый момент времени и определять несанкционированное использование эфира и в каких целях любым источником с определением его местоположения. Такая информация позволит существенно сократить время вскрытия замысла бандитов и их ликвидации.

Рис. 1 **ПОСТ МОНИТОРИНГА НА ОСНОВЕ ЦИФРОВОГО ПРИЕМНИКА**

Технология создания поста мониторинга в настоящее время вполне доступна как государственным органам правопорядка и защиты граждан, так и коммерческим органам охраны объектов и VIP-персон. Такие посты, создаются, как в стацио-

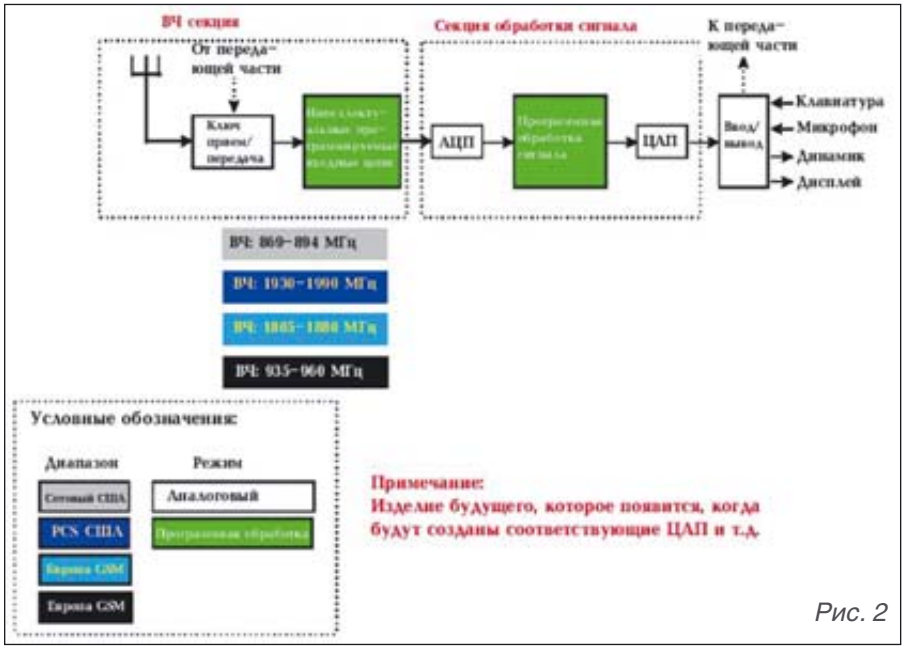

Рис. 2

Рис. 3

нарном исполнении, так и мобильном (носимая или перевозимая). Основное различие в объеме памяти ПЭВМ, в использовании антенных системам и систем электропитания. Наиболее распространенными являются мобильные посты РР располагаемые на любом типе автомобиля в зависимости от легенды прикрытия, но требующего специальной промышленной подготовки (монтажа скрытых антенн).

В аппаратную основу поста мониторинга положен базовый компьютер на основе ПЭВМ-Pentium-3(4) (Рис. 1) со специальным программным обеспечением, антенной системой (комплектуется под задачу), входным устройством радиоприемника, блоком аналогового–цифрового преобразователя, блока цифровой фильтрации и демодуляции. Все указанные блоки соединены ПЭВМ, которая управляет процессом сбора, обработки, и представления информации о состоянии эфира в любой момент времени текучего и прошедшего с возможностью предсказания по статистическим данным.

Классическая структурная схема приемного тракта поста радиомониторинга и определения места положения источника излучения приведена на рис. 2. [1]

На рис. 3 приведены фотографии рабочего места оператора поста радиоразведки комплекса РЭБ (внизу справа). На мониторах (слева) приведены три варианта обзора эфира: на верхнем отображается текущий обзор в полосе КВ диапазона 1,5–30 МГц с регистрацией источников излучения в электронном аппаратном журнале, а также идет отображение текущей оперативной информации; на среднем мониторе идет параллельное отображение спектра сигнала в полосе 30 МГц и детальный контроль в полосе 10 МГц любого участка диапазона (эта полоса определяется оператором). На третьем мониторе, показан индивидуальный контроль четырех источников в полосе каждого (потенциально один пост в состоянии сопровождать 32 источника в автоматизированном режиме с выводом на обзор до 6 источников).

На рис. 4 приведена схема автоматизированного интегрального комплекса анализа и обработки данных панорамного обзора сигнально-помеховой обстановки и пелленга КВ диапазона.

На рис. 1 приведен пример функционального сбора аппаратуры позволяющей создать пост мониторинга эфира, однако, следует заметить, что программное обеспечение создается индивидуально для каждого объекта.

В данной статье авторы ставили цель привлечения внимания специалистов оперативных служб по борьбе с терроризмом и вообще органов охраны жизненноважных для населения объектов к необходимости привлечения в качестве оружия современных информационных технологий.

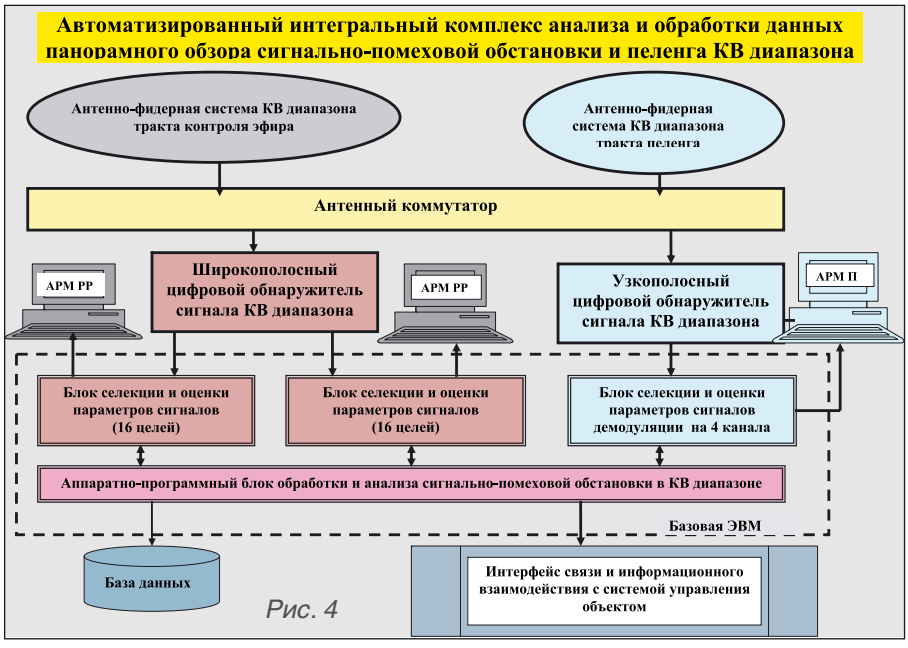

Рис. 4

Литература

1. Информост №3(51) 2007 г.

ОАО «НПО Завод «Волна»
Россия, 198095, г. Санкт-Петербург
Маршала Говорова ул., д. 29
Тел./факс: (812) 252-0914
E-mail: info@volnaspb.ru
http://www.volnaspb.ru