

Многозонный комплекс дистанционного радиомониторинга ST 052

1. Варианты использования.

По своей структуре, и выполняемым задачам ST 052, является стационарным автоматизированным многоканальным комплексом радиомониторинга (АМКР) с пространственно разнесенными приемными блоками. Как уже отмечалось выше, комплекс состоит из базовой аппаратуры и периферийных модулей.

Связь между базовой аппаратурой и периферийными модулями осуществляется по радиомодему на реальном расстоянии до 100 м. Управление комплексом и контроль за его работой осуществляется при помощи ПК с установленным на него программным обеспечением. Основными отличиями структурной схемы ST 052 от «классических» АМКР являются:

- отсутствие кабельных линий, соединяющих базовую и периферийную аппаратуру;
- использование в приемной части комплекса не только сканирующего радиоприемника, но и детектора ЭМП;
- приемная аппаратура входит не в состав базового оборудования, а в состав периферийного;
- в каждом из контролируемых помещений располагается своя приемная часть, а не одна на все помещения как в «классических» АМКР.

Учитывая эти особенности, можно описать несколько вариантов использования ST 052.

Первый вариант рассчитан на объекты, где отсутствуют штатные специалисты по защите информации и вопросы выявления СТС НПИ решаются либо сотрудниками охраны, либо непосредственно лицом, кабинет которого является защищаемым. Уровень автоматизации процесса обнаружения и идентификации, позволяют использовать ST 052 лицами, не имеющими специальной подготовки. Естественно, на организационном уровне должны быть согласованы действия в случае обнаружения «опасного» сигнала. Этими действиями могут быть:

- прекращение режимного мероприятия;
- вызов поисковой бригады;
- принятие иных мер по блокировке угрозы.

При этом варианте, базовая аппаратура может быть размещена:

- на посту охраны (контроль ведет охранник);
- в приемной (контроль ведет секретарь);
- непосредственно в контролируемом помещении (контроль ведет сам хозяин кабинета).

Второй вариант использования ST 052 рассчитан на предприятия, где имеются специалисты по защите информации. Как правило, это крупные объекты, где уже есть технические средства защиты (возможно и «классические» АМКР). В этом случае если позволяет дальность действия радиомодема базовая аппаратура устанавливается в помещении службы безопасности (посту радиомониторинга). При наличии стационарного комплекса радиомониторинга, ST 052 выполняет роль вспомогательной аппаратуры, предназначенной для мгновенной реакции на возникающие угрозы и идентификации перехваченных цифровых протоколов.

Существует и **Третий вариант** использования комплекса. Условно его можно назвать быстроразворачиваемым. Так как для работы ST 052 не требуется прокладки кабельных линий, а процесс адаптации занимает от получаса до нескольких часов, его можно использовать на временных объектах. К таким объектам относятся номера гостиниц, временно арендуемые помещения, и пр. Естественно, перед началом процесса адаптации в контролируемом помещении необходимо провести мероприятие по выявлению СТС НПИ. После адаптации комплекса контроль может вестись как непосредственно самого помещения, так и из смежного. Кроме того, при наличии портативного ПК, временный пост радиомониторинга может быть развернут в автомобиле (если позволяет дальность

радиообмена). Такой вариант использования может быть интересен для группы личной охраны, при обеспечении безопасности «первых» лиц за пределами предприятия.

Из анализа приведенных технических возможностей и связанных с ними вариантов использования ST 052, можно сделать вывод о том, что комплекс является универсальным средством обнаружения и идентификации радиоэфирных СТС НПИ, как в совокупности с другими техническими средствами защиты информации, так и самостоятельно. При этом от оператора комплекса не требуется специальная техническая и методическая подготовка. Хотя, установку, настройку и адаптацию комплекса лучше проводить с привлечением специалистов по защите информации.

2. Сравнительный анализ возможностей, аппаратуры, предназначенной для обнаружения радиоэфирных СТС НПИ.

2.1 Общая классификация аппаратуры.

В настоящее время основными техническими средствами, предназначенными для выявления радиоэфирных СТС НПИ в стационарном режиме являются:

- стационарные детекторы ЭМП;
- скоростные приемники «ближней зоны»;
- автоматизированные многоканальные комплексы радиомониторинга.

Детекторы ЭМП (индикаторы электромагнитного поля). Принцип действия основан на широкополосном детектировании сигнала. Устанавливаются в контролируемом помещении. Наиболее распространенный диапазон: 50-3000 МГц (самые совершенные образцы, до 8 ГГц). Дальность обнаружения - от 0,3 до 3 м. (зависит от: электромагнитного фона в помещении и мощности передатчика СТС НПИ). Основной принцип обнаружения - амплитудный. Основные способы идентификации – индикатор уровня, частотомер, (у наиболее совершенных моделей – идентификация известных цифровых сигналов). Дополнительные возможности: ведение электронного протокола «тревог». Возможные виды индикации: световая звуковая, ЖКИ, (реже вибросигнал). Контроль производит лицо, осуществляющее режимное мероприятие. Ценовой диапазон детекторов ЭМП: от 150 до 800 долларов США.

Скоростные приемники «ближней зоны». По сути своей являются сканирующими радиоприемниками. Поиск сигналов производится путем последовательного прохода всего диапазона с узкой полосой обзора. Скорость обзора диапазона (с учетом обработки сигналов) составляет несколько минут.

Устанавливаются либо в контролируемом помещении, либо в помещении, смежном с контролируемым. Наиболее распространенный диапазон 50 – 3000 МГц. Дальность обнаружения – до 10-15 метров в зависимости от мощности передатчика СТС НПИ. Основной принцип идентификации «опасных» сигналов – анализ информации, заложенной в демодулированный сигнал (как частный случай - корреляционная обработка). Дополнительные возможности - создание списка «дружественных сигналов». Способы индикации – световая, звуковая, индикатор уровня, частотомер, возможность прослушивания демодулированного сигнала. Контроль может производить как лицо, проводящее режимное мероприятие, так и сотрудник, находящийся во время переговоров в смежном помещении. В последнем случае корреляционный приемник не сможет выполнить свою задачу по анализу демодулированного сигнала. Ценовой диапазон приемников «ближней зоны»: от 1000 до 1500 долларов США

Автоматизированные многоканальные комплексы радиомониторинга (АМКР).

В состав АМКР входят:

- радиоприемное устройство (как правило, сканирующий приемник);
- контроллер (для сопряжения приемника с персональным компьютером (ПК) и управления периферийными устройствами);
- ПК с установленным на него специальным программным обеспечением;
- антенный коммутатор (один или несколько);
- внутренние и наружные антенны;
- генератор «прицельной» помехи (один или несколько);
- СВЧ конверторы (для расширения диапазона принимаемых частот приемника).

ПК, приемник и контроллер составляют т.н. «ядро» АМКР и располагаются в помещении «поста» радиомониторинга, остальное оборудование является периферийным и устанавливается в контролируемых помещениях или на внешней стороне здания. Связь между аппаратурой «ядра» и периферийными устройствами осуществляется по кабельным линиям. Максимальное количество каналов приема в АМКР обычно не превышает 24. Управление комплексом производится из оболочки управляющей программы в автоматическом или ручном режимах. Основными принципами идентификации «опасного» сигнала в АМКР являются:

- *Принцип пространственно распределенных антенн.* Заключается в том, что в каждой контролируемой зоне располагается приемная антенна, а на внешней части здания располагается т.н. опорная антенна. Если уровень сигнала на опорной антенне превышает уровни сигналов на внутренних антеннах, то такой сигнал относится к «внешним» и с большой вероятностью не является опасным. Если имеет место ситуация, когда уровень сигнала на какой-либо из внутренних антенн превышает уровень сигнала на опорной антенне (и на других внутренних антеннах), то данный сигнал является «опасным», по крайней мере, его источник следует искать в том помещении, где его уровень наибольший.

- *Анализ гармоник.* Основан на предположении, что если антенна и радиопередающее СТС НПИ находятся в одном помещении, (а следовательно антенна – «в ближней» зоне передатчика), то помимо несущей частоты сигнала будут зарегистрированы и его гармоники. Т.е. наличие одной или нескольких гармоник позволяет сделать вывод о том, что источник ЭМП находится недалеко от приемной антенны.

- *Корреляционная обработка.* Заключается в сравнении акустического фона помещения со звуковой информацией, демодулированного сигнала. Существуют понятия «активная» и «пассивная» корреляция. Первый способ предполагает использование «контрольного звука», который модулирует сигнал радиомикрофона и в этом случае эффективность корреляционного анализа существенно повышается. Так, например, при активной корреляции возможна идентификация радиомикрофонов с простейшими видами аналогового «прикрытия». Однако активная корреляция невозможна при дистанционном радиомониторинге во время проведения важных переговоров и других режимных мероприятий. «Пассивная» корреляция не предполагает создания какого-либо специального звука, а использует естественные (фоновые) звуки помещения. Данный вид корреляционной обработки не так эффективен (при его помощи идентифицируются только «открытые» каналы СТС НПИ), зато его можно использовать во время проведения режимных мероприятий.

- *Соответствие принятого сигнала критериям.* Из всего множества принятых сигналов отбираются те из них, которые имеют некие признаки, характерные для СТС НПИ.

Стоимость базового комплекта АМКР, реализованного на основе сканирующего радиоприемника (типа AR5000) составляет от 7500 до 10 000 долларов США. Минимальный комплект периферийного оборудования состоит из одной внутренней антенны и стоит от 50 до 500 долларов США. Если в составе приемной аппаратуры содержится СВЧ конвертор, стоимость каждого приемного канала увеличивается до 1000 долларов США. Для эксплуатации комплекса необходим подготовленный специалист.

2.2. Достоинства и недостатки аппаратуры различных классов.

При анализе достоинств и недостатков аппаратуры, учитывались технические возможности и потребительские свойства лучших образцов в своем классе. Результаты анализ приведены в таблице.

Достоинства

Стационарный детектор ЭМП

Невысокая стоимость. Небольшие габариты и вес. Наличие автономного источника питания. Для эксплуатации не требуется специальная подготовка. Обнаружение СТС НПИ практически в режиме реального времени. Идентификация наиболее распространенных цифровых протоколов.

Недостатки

При высокой степени загруженности диапазона имеет место большое число «ложных тревог». При уменьшении чувствительности, и без того малая дальность обнаружения, снижается до недопустимых значений. Неоднозначная интерпретация обнаруженных сигналов.

Скоростной приемник «ближней зоны»

Относительно невысокая стоимость. Небольшие габариты и вес. Наличие автономного источника ГГц. При высокой степени загруженности диапазона время сканирования и анализа резко увеличивается. Однозначная идентификация СТС сигнала несколько минут. НПИ возможна только при «работе» по аналоговым

Возможность прослушать демодулированный сигнал без кодирования канала передачи. Для аналоговый сигнал. Возможность дистанционного автоматической идентификации СТС НПИ методом мониторинга из помещения смежного с корреляционной обработки, приемник должен контролируем. Корреляционная обработка находится в контролируемом помещении. принятых сигналов в автоматическом режиме. Создание списка «дружественных сигналов», которые игнорируются в режиме поиска.

Автоматизированный многоканальный комплекс радиомониторинга

Высокая стоимость. Сложность в эксплуатации. Процесс идентификации сигналов оператор должен иметь специальную подготовку. автоматизирован. Для обработки результатов измерений используются возможности ПК. кабельных линий из контролируемых помещений в нескольких помещениях одновременно. комплекс должен быть предусмотрен. Возможность исследовать принятый сигнал в выделенный компьютер. Так как приемной частью ручном режиме, используя анализатор спектра, является сканирующий радиоприемник, векторный анализатор и т.п. Возможность возможности комплекса по выявлению «сложных» расширения диапазона принимаемых частот за каналов передачи СТС НПИ ограничены. счет использования СВЧ конвертора. Модульный обнаружение таких каналов возможно только при принципе построения позволяет, по мере большого времени наблюдения и детальном необходимости наращивать «периферию». анализе полученных результатов. Аппаратура сугубо стационарная, адаптированная к условиям конкретного объекта.

Определенное превосходство перед остальными классами аналогичной по назначению аппаратуры имеют детекторы ЭМП. Это определяется, прежде всего, низкой стоимостью, простотой в эксплуатации, широким диапазоном, возможностью обнаруживать и идентифицировать наиболее распространенные цифровые каналы передачи СТС НПИ. Однако, когда мы говорим о стационарных приборах этого класса, следует отметить их крайне низкую эффективность. Это объясняется тем, что в условиях сильных помех, отстроиться от них можно только путем загробления чувствительности, что приводит к снижению дальности обнаружения.

Приемники ближней зоны лишены основного недостатка детекторов ЭМП – неспособности эффективно работать в условиях мощных помех. Но зато они ограничены по верхней части диапазона. На сегодняшний день, 3 ГГц уже не достаточно. Главное достоинством приемников «ближней зоны» - возможность в автоматическом режиме пройти весь диапазон, обнаружить наиболее сильные сигналы, обработать их при помощи коррелятора и дать возможность оператору услышать демодулированный сигнал. При ближайшем рассмотрении можно утверждать, что данный класс аппаратуры рассчитан исключительно для обнаружения аналоговых радиомикрофонов с открытым каналом передачи.

АМКР несомненно являются наиболее эффективным техническим средством (из числа указанных). При несомненных достоинствах данного класса аппаратуры, у нее имеется и ряд недостатков, главными из которых являются:

- высокая стоимость аппаратуры;
- высокие требования, предъявляемые к подготовке оператора;
- несмотря на высокую стоимость и сложность неспособность обнаружить и однозначно идентифицировать некоторые типы «нестандартных» каналов передачи и большую часть стандартных цифровых протоколов.

Последний недостаток устраняется за счет замены сканирующих радиоприемников в составе АМКР на анализаторы спектра (чаще всего HP), или цифровые панорамные приемники. Стоимость комплекса при этом существенно повышается, а требования к оператору становятся еще более высокие.

Комплекс ST 052, как уже отмечалось выше, является частным случаем АМКР. Но при разработке этого комплекса, несомненно, учитывались указанные недостатки АМКР. Экономический аспект использования ST 052 будет рассмотрен в следующем разделе.

АМКР на базе сканирующего приемника

Комплекс ST 05

Сложность в эксплуатации.

Эксплуатация комплекса не требует от оператора специальной подготовки.

Необходимость прокладки кабельных линий из контролируемых помещений в «пост» радиомониторинга

Обмен информацией базовой и периферийной аппаратуры осуществляется по радиомодему.

Так как приемной частью является сканирующий радиоприемник, возможности комплекса по выявлению «сложных» каналов передачи СТС НПИ ограничены. Обнаружение таких каналов возможно только при большом времени наблюдения и детальном анализе полученных результатов.

Приемная часть состоит из детектора ЭМП и сканирующего радиоприемника. За счет этого недостатки каждого из этих приборов компенсируются за счет достоинств другого.

Для управления комплексом должен быть предусмотрен выделенный компьютер.

В диапазоне детектора ЭМП возможна автоматическая идентификация «цифровых» протоколов и обнаружение «нестандартных» каналов передачи СТС НПИ.

Аппаратура сугубо стационарная, адаптированная к условиям конкретного объекта.

Требования к ПК минимальные. Программа может работать в фоновом режиме, например на компьютере секретаря.

Возможность быстрого развертывания и адаптации к условиям новому объекту. Это позволяет использовать аппаратуру на «выезде».

К недостаткам ST 052 можно отнести невозможность демодулировать принятый сигнал и реализовать тем самым один из аспектов информационного способа идентификации сигналов. Не отрицая полезности этой процедуры для большинства практических задач, следует отметить ее ограниченность для СТС НПИ, которые не имеют аналоговых видов модуляции, не предназначены для передачи речевой информации (видеопередатчики), используют сложные виды модуляции, кодирования и прикрытия. С учетом перспектив развития техники передачи информации, в том числе и для СТС НПИ, и теоретических способов применения систем шумоподобных сигналов, возможность идентификации сигналов по информационным признакам сводятся к минимуму.

В настоящее время сигнал, излучаемый СТС НПИ, следует рассматривать как шумовой, что исключает возможности его демодуляции без знания способа преобразования исходной информации и, более того, наличие опций демодуляции не является необходимым для эффективного обнаружения сигналов СТС НПИ.

Таким образом, для достижения максимальной эффективности, в комплексе ST 052 учтены основные недостатки аналогичных по назначению классов аппаратуры. При этом реализованы главные достоинства:

- **от детекторов ЭМП:** - мгновенная реакция на угрозы, идентификация цифровых каналов передачи;
- **от приемников:** возможность работы в условиях мощных помех, определение спектральных характеристик сигнала;
- **от АМКР:** высокий уровень автоматизации процесса обнаружения и идентификации СТС НПИ.

При этом особое внимание в комплексе уделяется отражению наиболее современных радиоэфирных СТС НПИ, при относительно невысокой стоимости и сложности в эксплуатации.

2.3. Экономические аспекты использования ST 052.

Учитывая возможности аппаратуры обнаружения радиоэфирных СТС НПИ можно отметить, что детекторы ЭМП и портативные скоростные приемники «ближней зоны» более приспособлены для выявления источников ЭМП в «поисковом режиме», а не стационарном. Поэтому их нельзя однозначно классифицировать, как «объектовую» аппаратуру. Функция обнаружения и идентификации радиоэфирных СТС НПИ в стационарном режиме наиболее полно реализована в АМКР, частным случаем которой и является ST 052. Исходя из этого, при анализе экономической целесообразности использования данного комплекса, в настоящем разделе будут анализироваться экономические аспекты использования «классического» АМКР, созданного на базе широкополосного сканирующего радиоприемника и комплекса ST 052.

Причем необходимо рассматривать АМКР не только в стандартной комплектации, но и в расширенной периферии (с возможностью приема сигналов в диапазоне свыше 6 ГГц), так как «модель угроз» предполагает возможность использования этой части диапазона.

Для начала необходимо определить стоимость аппаратуры комплексов для одноканального варианта.

	АМКР диапазон до 2,5 ГГц	АМКР диапазон до 8 ГГц	Комплекс ST 052
Состав базовой аппаратуры	Сканирующий радиоприемник; Контроллер; Антенный коммутатор; ПК с ПО	Сканирующий радиоприемник; Контроллер; Антенный коммутатор; ПК с ПО	БППМ ПК с ПО
Состав периферийной аппаратуры	Одна внутренняя антенна; Одна опорная антенна.	Одна внутренняя антенна; Одна опорная антенна; СВЧ конверторы (до 8 ГГц).	
Стоимость (руб.)	221 600	307 800	104 000

Затем, увеличивая количество периферийного оборудования, необходимо проследить зависимость стоимости каждого из комплексов от количества каналов. Как отмечалось ранее, максимальное количество каналов в ST 052 может достигать 32, а в АМКР – 24. Исходя из этого, анализ зависимости производится на максимальной периферии АМКР. График этой зависимости представлен на рисунке.

Из приведенного графика видно, что при количестве каналов от 1 до 6, стоимость ST 052 ниже, чем у любого из АМКР. При увеличении количества каналов от 6 до 24, стоимость ST 052 превышает стоимость АМКР, работающего в диапазоне до 2,5 ГГц. Цена АМКР, работающего в диапазоне, аналогичном ST 052 существенно выше при любом количестве каналов.

Учитывая приведенные в предыдущих разделах достоинства и недостатки комплекса ST 052 по отношению к АМКР, созданным на базе сканирующих приемников, а также результаты анализа стоимости, можно отметить, что при количестве каналов от 1 до 6, соотношение «цена/возможности» ST 052 выглядит более предпочтительным.

При увеличении количества приемных каналов от 6 до 24, стоимость АМКР, не имеющего в своем составе СВЧ конвертеров ниже, чем у ST 052, но при этом обнаружение сигналов в диапазоне от 2,5 до 6 ГГц невозможно. Включение в состав АМКР СВЧ конвертеров приводит к тому, что по соотношению «цена/возможности» такой комплекс проигрывает комплексу ST 052.

2.4. Перспективы развития комплекса ST 052.

Несмотря на то, что комплекс ST 052 серийно выпускается только в течение полугода, разработчики данной аппаратуры ведут работы по дальнейшему ее совершенствованию. Основными направлениями этих работ являются:

- Разработка комплекса с возможностью передачи сообщений о состоянии объекта защиты по GSM каналу. Данная модификация будет позволять получать информацию о работе комплекса на любом

расстоянии. Такой вариант комплекса не предполагает использования ПК и ориентирован на небольшие объекты, где нет штатной службы безопасности, и эксплуатацией комплекса занимается «хозяин» контролируемого помещения.

- Разработка варианта комплекса, где удаленные модули и базовая аппаратура будут обмениваться информацией по проводным линиям (в том числе штатным проводным линиям объекта). Данный вариант предполагает большое количество периферийных модулей.

- Разработка сетевого варианта, позволяющего управлять аппаратурой с удаленного компьютера по локальной сети предприятия. Данный вариант предпочтителен для использования на объекте, где эксплуатация комплекса осуществляется силами штатной службы безопасности.

Сведения о перспективных направлениях развития комплекса ST 052 предоставлены фирмой разработчиком данной аппаратуры - ООО «Смерш-Техникс», Санкт-Петербург.

3. Общие выводы.

· Исходя из возможностей серийно выпускаемого изделия и основных направлений развития комплекса ST 052, можно сделать вывод о том, что использование комплекса возможно на объектах различной конфигурации и с различным уровнем подготовки персонала.

· Модульный принцип построения комплекса, гибкая адаптация структуры комплекса к условиям конкретного объекта, а также возможность его интеграции в уже существующую систему защиты информации, позволяют рассматривать ST 052, как одно из наиболее удобных и недорогих технических средств, предназначенных для радиомониторинга.

· Несмотря на простоту в эксплуатации, уровень обнаруживаемых угроз позволяет отнести ST 052 к классу профессиональной аппаратуры.

· Исходя из соотношения показателей «цена/возможности», при небольшом количестве периферийных модулей (от 1 до 6), комплекс ST 052 является оптимальным средством обнаружения радиоэфирных СТС НПИ.

· С учетом приведенных выше выводов можно рекомендовать использование комплекса ST 052 для решения практических задач по защите информации, как в автономном режиме, так и в составе существующих систем обеспечения комплексной безопасности объекта.