Конвенциональные широкополосные технологические радиосети обмена данными повышенной надежности и живучести

Оборудование УКВ-диапазона на практике является идеальным выбором при создании технологических радиосетей обмена данными в большинстве ответственных применений. Поэтому на протяжении последних десятилетий узкополосные технологические радиосети обмена данными оставались основным инструментом сбора данных и управления. Однако с развитием информационных технологий возросли потребности в пропускной способности радиосетей, в связи с чем были созданы образцы аппаратуры УКВ-диапазона, имеющие более высокие технические характеристики и позволяющие обеспечить передачу в оперативном режиме достаточно большого объема данных. Для достижения таких характеристик были использованы широкополосные сигналы, что позволило увеличить скорость обмена данными и пропускную способность радиосетей, сохранив дальность передачи, характерную для УКВ-диапазона.

В настоящее время количество представленных на российском рынке моделей широкополосной аппаратуры, работающей в УКВ-диапазоне, относительно невелико. Все широкополосные радиомодемы обеспечивают работу в радиосетях с архитектурой "точка – много точек". Так, радиомодемы Mercury-900 (GE MDS, США) и Sentry-4G-900 (CalAmp, США) могут использоваться для строительства как подвижных, так и стационарных радиосетей (в последнем случае поставляются без встроенного навигационного приемника). Надежность работы этих устройств в составе радиосети обеспечивается реализацией разнесенного приема (технология MIMO – multiple in multiple out), при котором радиосигнал принимается одновременно на две антенны, установленные на расстоянии одна от другой. В Mercury-900 разнесенный прием используется для работы в радиосети WiMax, в Sentry-4G-900 – в радиосетях WiMax и WiFi.

Построение технологической радиосетей на базе Sentry-4G-900

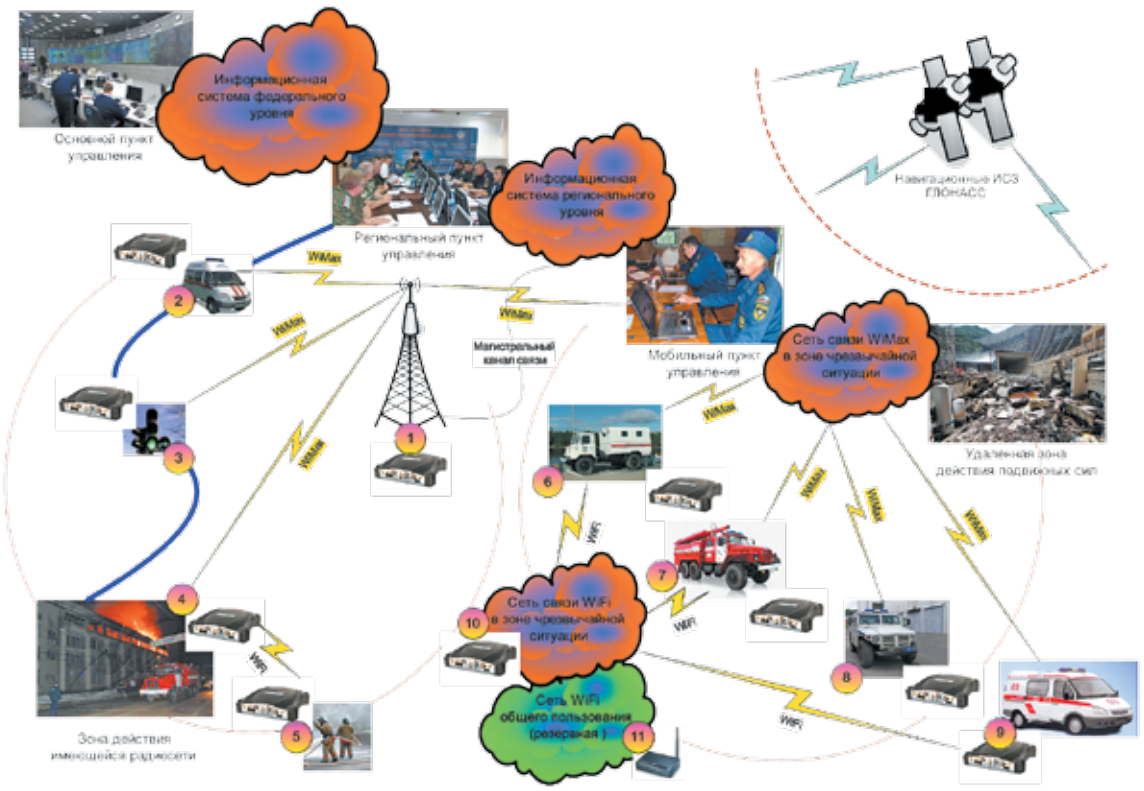
Надежность и живучесть технологических радиосетей на перспективном оборудовании Sentry-4G-900 обеспечивается за счет возможности создания на их базе единого информационного поля, функционирующего по IP-протоколу, доступ к которому с каждого устройства организуется по двум выделенным каналам – 900 МГц IEEE 802.16e-2005 WiMax и IEEE 802.11b/g WiFi. Кроме того, при наличии в оперативной зоне радиосетей стандарта WiFi общего пользования они могут использоваться в качестве резервных каналов доставки информации, повышая живучесть разворачиваемой технологической радиосети.

Упрощенная схема радиосети обмена данными МЧС России, построенная на радиомодемах Sentry-4G-900, представлена на рисунке. Радиосеть функционирует по IP-протоколу и является "прозрачной" для любого программного обеспечения, поддерживающего работу через локальную или глобальную вычислительную сеть. Задействуемая для работы в составе радиосети аппаратура может автоматически сопрягаться между собой по каналам WiMax или WiFi, используя автоматическую маршрутизацию сообщений и прозрачное объединение обеих технологий, чем обеспечивается высокая надежность и живучесть радиосети и функционирующей на ее базе информационной системы в целом.

Радиосеть имеет следующие функциональные возможности и порядок функционирования:

1. стационарная базовая станция WiMax широкополосной технологической радиосети обмена данными;
2. мониторинг и оперативно-диспетчерское управление подвижными дежурными силами в зоне работы постоянно действующей технологической радиосети;
3. управление светофорными комплексами по каналам технологической радиосети в интересах приоритетного пропуска подвижных дежурных сил;
4. оперативное управление и информационное обеспечение сил и средств служб общественной безопасности в районе проведения оперативных действий, находящемся в зоне действия технологической радиосети, по каналам связи WiMax;
5. локальная сеть управления силами и средствами служб общественной безопасности в районе оперативных действий по каналам связи WiFi;
6-9. разнородные подвижные силы и средства служб общественной безопасности различной ведомственной принадлежности в удаленной зоне;
10. локальная сеть WiFi для взаимодействия разнородных подвижных сил и средств служб общественной безопасности;
11. локальная сеть WiFi общего пользования.

Широкополосная технологическая радиосеть обмена данными имеет в своем составе группу стационарных ба-



Условные обозначения:

радиомодем Sentry-4G-900

точка доступа WiFi радиосети связи и передачи данных общего пользования

канал связи IEEE802.16e-2005 WiMax

канал связи IEEE802.11b/g WiFi

зовых станций WiMax и обеспечивает функционирование подвижных и стационарных объектов в оперативной зоне. Встроенный протокол позволяет организовать автоматический перевод подвижных объектов между соседними базовыми станциями с минимальной задержкой по времени. Базовые станции подключаются к региональному пункту управления по проводным или беспроводным магистральным каналам связи, работающим по IP-протоколу.

Региональный пункт управления осуществляет мониторинг и оперативно-диспетчерское управление подвижными дежурными силами при их выдвижении в ходе решения функциональных задач в районе оперативного предназначения в зоне работы постоянной действующей технологической радиосети. Он обеспечивает автоматизированный контроль за действиями подвижных сил с самого начала их оперативного использования и до завершения операции. По каналам радиосети с заданной периодичностью транслируются данные о текущем местоположении подвижных сил и средств и характере их использования, передаются команды управления и сигналы оповещения, а также обеспечивается удаленный доступ к массивам информации, которая может потребоваться в процессе решения оперативных задач.

По каналам технологической радиосети осуществляется оперативно-техническое управление стационарной инфраструктурой, в частности светофорными комплексами. Наличие такой возможности позволяет организовать приоритетный пропуск подвижных средств дежурных сил служб общественной безопасности на регулируемых перекрестках при их выдвижении в район оперативных действий. Реализация данной задачи позволяет существенно сократить время реагирования на аварии и происшествия и свести к минимуму тяжесть их последствий.

Оперативное управление и информационное обеспечение сил и средств служб общественной безопасности в районе проведения операции, находящемся в зоне действия технологической радиосети, осуществляется по каналам связи WiMax, которые обеспечивают обмен мультимедийной информацией. Относительно высокая пропускная способность радиосети позволяет передавать достаточно большие массивы графической и видеоинформации.

В районе оперативных действий разворачивается беспроводная локальная сеть управления силами и средствами служб общественной безопасности по каналам связи WiFi. Она сопрягается с действующей стационарной технологической радиосетью обмена данными WiMax и обеспечивает доступ пользователей к ресурсам информационной системы на региональном и федеральном уровнях. В результате подвижные силы имеют функциональные возможности, аналогичные тем,

которыми они располагают при работе в стационарных условиях. Применение WiFi позволяет организовать подключение к сети абонентов различной ведомственной принадлежности и использовать для подключения коммерческие терминалы и стандартное программное обеспечение, используемое в сетях данного типа.

Полевой (мобильный) пункт управления подвижными силами служб общественной безопасности может разворачиваться в удаленном районе при отсутствии постоянно действующей технологической радиосети обмена данными либо на границе данной сети. В последнем случае он может выступать как ретранслятор, увеличивая дальность связи. Связь обеспечивается техническими средствами, разворачиваемыми в оперативной зоне на период проведения совместной операции. Технологическая радиосеть обеспечивает обмен данными между всеми участниками операции, независимо от их ведомственной принадлежности.

Обеспечение участников операции навигационными данными от системы спутниковой связи ГЛОНАСС осуществляется через внешние или встроенные навигационные приемники аппаратуры Sentry-4G-900.

Таким образом, рассмотренная технология широкополосной передачи данных и реализованные на ее основе образцы оборудования позволяют создавать мобильные и стационарные интегрированные технологические радиосети обмена данными повышенной надежности и живучести для служб общественной безопасности и управления удаленными объектами.

Обеспечение безопасности информации в стационарных и подвижных радиосетях обмена данными

Безопасность данных в стационарных и подвижных технологических радиосетях является одним из ключевых условий их использования, а строительство таких радиосетей осуществляется с учетом необходимости полного исключения или максимального затруднения искажения передаваемой по ним информации. Степень защиты данных оказывает непосредственное влияние на надежность радиосети и ее живучесть, поскольку постороннее вмешательство в работу может существенно снизить эти параметры. В радиосетях обмена данными широко применяются различные методы и способы защиты информации. Ниже представлена информация о возможностях данных радиосетей противостоять основным угрозам: перехвату данных, несанкционированной работе в составе радиосети и радиоэлектронным помехам (вопросы противодействия профессиональным средствам радиоэлектронной борьбы и радиоэлектронного подавления в настоящей статье не рассматриваются).

Обеспечение безопасности данных в стационарных радиосетях

Одним из наиболее важных требований к технологическим радиосетям обмена данными является обеспечение их безопасности. Следует отметить, что защита данных в любой системе представляет собой комплекс непрерывных организационно-технических и специальных мероприятий, ни одно из которых в отдельности не позволяет добиться поставленной задачи. Тем не менее, рассматриваемые средства обмена данными обладают возможностями, позволяющими существенно снизить существующие угрозы, главными из которых являются перехват и несанкционированный доступ к работе в радиосети, что обусловлено уже самой средой передачи.

Устойчивость к перехвату данных

На первый взгляд, перехват данных в проводных технологических сетях связи сопряжен с серьезными трудностями. Однако эта задача не так сложна для специалиста, имеющего соответствующую подготовку (подтверждением этому являются многочисленные успешные атаки хакеров на информационные системы): кабельная сеть прокладывается внутри здания или комплекса зданий, при этом отдельные сегменты могут укладываться в подвалах зданий, коллекторах, патернах и т.п., то есть в местах, не контролируемых службами безопасности и представляющих собой, таким образом, потенциальные точки для несанкционированного подключения. Теоретически любой человек, знающий структуру кабельной системы, может получить доступ к ней в этих точках. После подключения к проводной системе связи получение доступа к информации является делом техники, поскольку во всех открытых проводных сетях используются стандартные протоколы связи и обмена данными, а также серийно выпускаемые и общедоступные программно-технические средства.

Средой передачи данных в радиосетях являются радиоволны, которые могут приниматься любым приемником на относительно большом расстоянии от передатчика. Однако радиосигналы, передаваемые в системах обмена данными с использованием современных радиомодемов, не так доступны, как это может показаться на первый взгляд.

Во-первых, для организации перехвата необходимо точно знать номинал рабочей частоты, используемой для обмена данными. При соблюдении пользователями минимальных правил безопасности получение этой информации крайне затруднено. Поскольку передаваемые данные не могут восприниматься на слух, то при использовании для определения номинала рабочей частоты доступных средств перехвата, например частотных сканеров, фиксируется только факт передачи сигналов на определенной частоте, которые представляются как набор шумов. Определение принадлежности этих сигналов тому объекту, поиск которого ведется, без доступа к передаваемой информации оказывается практически невозможным.

Во-вторых, оборудование использует специальные схемы модуляции сигнала и собственные преамбулы (структуру пакета данных). На практике это выливается в невозможность получения доступа к собственно передаваемой информации при отсутствии соответствующего радиомодема или специального оборудования для анализа сигналов. В отличие от проводных модемов распространение радиотехнического оборудования имеет известные ограничения, а все его пользователи регистрируются. В связи с этим вероятность легального

приобретения оборудования, которое может использоваться для обеспечения доступа к передаваемой в технологических радиосетях информации, практически равна нулю.

В-третьих, в большинстве радиосетей, особенно имеющих топологию типа "звезда", в которых обмен данными производится через базовую станцию, в отдельно взятой точке могут приниматься только данные, передаваемые в одном направлении (от базовой станции к удаленному объекту). Это связано с принципами построения сети, в которой базовая станция разворачивается на возвышенности и имеет высоко подвешенную приемо-передающую антенну, что обеспечивает возможность организации связи со всеми удаленными станциями сети. Для организации перехвата используемое для него оборудование необходимо разместить на такой же выгодной позиции, что в большинстве случаев оказывается невозможным. В противном случае обеспечивается перехват только данных от базовой станции, которые в большинстве стационарных технологических радиосетей представляют наименьший с точки зрения перехвата интерес (например запросы, которые дают минимальное представление о работе информационной системы).

И наконец, в отличие от проводных сетей обмена данными, где кабельная инфраструктура и аппаратура для ретрансляции сигналов распределены на больших территориях, радиооборудование передачи данных может быть полностью развернуто в охраняемых помещениях, физический доступ в которые строго ограничен.

Совокупность всех перечисленных выше качеств делает радиосети обмена данными более безопасными по сравнению с технологическими проводными сетями связи и обмена данными в части перехвата данных.

Устойчивость к несанкционированному подключению

При подключении к сети обмена данными обычно ставится цель получения доступа для работы в составе информационной системы или к "просмотру" передаваемых данных. Для решения этой задачи требуется соответствующий терминал, поддерживающий используемые в сети обмена данными протоколы. Такой терминал может быть легко реализован на базе современного компьютера, но решение второй части задачи представляется не таким простым.

Перечисленные выше трудности, возникающие при организации перехвата, встают и при попытке получить доступ к работе в составе сети обмена данными. Кратко описанные ниже свойства применяемых протоколов связи и обмена данными в равной степени относятся к радио- и проводным сетям и характеризуют их возможности по обеспечению безопасности информации.

Большинство коммерческих пользователей синхронных систем (например банков) используют протоколы "опроса" (например синхронный протокол SDLC), в которых заложены определенные возможности по обеспечению безопасности. Чтобы терминал распознавался системой, он должен быть внесен в "опросную таблицу", которая ведется и поддерживается на цен-

КОНТРОЛИРУЙ
скорость
время
маршрут
объем
направление
потоки
безопасность
ВСЁ,
ИСПОЛЬЗУЯ РАБОТАЮЩУЮ
в любых условиях,
в том числе в полевых,
в любой обстановке,
в том числе
в чрезвычайных ситуациях
и особых периодах,
безотказно,
надежно,
безопасно
ВСЕГДА
РАДИОСЕТЬ
DATARADIO®

ПОДВИЖНЫЕ и СТАЦИОНАРНЫЕ
радиосети обмена данными
Рабочий диапазон:
132-174, 380,-512, 700, 800,
900 МГц
Скорость: 4800-128000 бит/сек
Радиомодемы:
ParagonG3, GeminiG3, I-Base,
Senrty-4G-900, Viper-100/400,
Phantom, Integra-TR, T-Base,
T-96SR, TSLM
РОДНИК
СИСТЕМНЫЙ ИНТЕГРАТОР
+7 (499) 613-70-01, www.rodnik.ru
Вместе мы можем все

тральном компьютере. Несмотря на то, что система может самостоятельно распознавать новые терминалы и автоматически вносить их в таблицу, содержание таблицы постоянно контролируется администратором сети и специальными программами, которые могут локализовать нового пользователя, получившего доступ к системе, и предпринять соответствующие меры по исключению возможности его работы в составе информационной системы. Если терминал не будет внесен в таблицу, он не сможет работать в составе сети.

Значительная часть стационарных технологических радиосетей (например технологические радиосети управления телемеханикой на объектах топливно-энергетического комплекса) используется для обслуживания строго определенного количества терминалов, поэтому появление в их составе новых терминалов вообще не предусматривается.

Возможно, что профессиональный крэкер или хакер сможет перепрограммировать компьютер таким образом, чтобы получать данные без внесения дополнительного адреса в "опросную таблицу", однако в этом случае он не сможет передавать свои данные в центральный компьютер (что в большинстве случаев является основной целью проникновения в систему).

Попытки работы через технологическую радиосеть обмена данными под "прикрытием" другого терминала за счет дублирования его идентификационного номера приводят к генерации некорректных данных и подтверждений, получаемых центральным компьютером. Этот факт незамедлительно привлечет внимание администратора сети. На данном этапе достаточно просто выявить попытку получения несанкционированного доступа к работе в сети и предпринять соответствующие меры. Поскольку основным условием успешного проникновения в сеть является скрытность, уже сам факт выявления попытки несанкционированного доступа делает дальнейшие действия злоумышленника бессмысленными.

На практике выявить и локализовать несанкционированную работу в технологической радиосети обмена данными намного проще, чем в проводной системе связи. В случае предоставления крэкеру или хакеру возможности продолжения контролируемой работы в сети излучаемые его приемопередатчиком сигналы при посылке запросов и подтверждении приема сообщений могут быть легко запеленгованы (а поскольку работа в сети управляется с базовой станции администратором, последний может инициировать работу передатчика злоумышленника с необходимой периодичностью), что существенно проще осуществить, чем определить точку подключения к проводной сети обмена данными.

Устойчивость к подавлению и к воздействию помех

Подавление или намеренная постановка помех работе радиосистемы – задача существенно более сложная, чем физическое нарушение соединения в проводной системе, и ее реализация для большинства коммерческих систем маловероятна. Для выполнения этой задачи необходимо знать номинал рабочей частоты системы обмена данными, установить который не так просто, поскольку передача ведется коротким сеансами. Факт появления помех немедленно выявляется администратором радиосети, а источник излучения становится объектом пеленгования и локализации, осуществляемых в том числе и при поддержке соответствующих организаций, контролирующих использование радиочастотного спектра. Таким образом, установка и использование специального оборудования радиопротиводействия требует времени и крупных финансовых затрат, но при этом его дееспособность не может быть продолжительной.

Сергей Маргарян, Александр Харламов,
Алексей Хромцев, Алексей Сабунин,
ЗАО "НПП "Родник"

Продолжение в следующем номере

НОВОСТИ

Сотрудничество DS и P&G

Компания Procter & Gamble (P&G), крупнейший в мире производитель потребительских товаров, расширила область применения технологий V6 PLM компании Dassault Systemes (DS) для разработки упаковки. Данный шаг укрепляет стратегическое сотрудничество компаний, в рамках которого DS является поставщиком PLM-решений в масштабе всего предприятия-партнера. Компании совместно разрабатывают интегрированный комплекс продуктов, который должен сделать упаковочный процесс более эффективным, сократить время выпуска продукции на рынок, повысить экспозиционную эффективность товара и, в конечном итоге, сделать его более удобным для потребителей.

В ходе реализации своих будущих проектов по разработке упаковки P&G будет использовать возможности виртуального и цифрового проектирования CATIA V6 и функции виртуального тестирования SIMULIA V6. Подобный подход обеспечит более тесное взаимодействие с поставщиками, позволяя ускорить процесс создания упаковки, которая бы максимально соответствовала требованиям потребителей и одновременно была бы оптимальна при производстве и размещении. Более того, CATIA V6 обеспечит возможности совместной работы дизайнерских групп по всему миру, повторного использования элементов упаковки, автоматизации повторяющихся задач и соответствия корпоративным стандартам при одновременном снижении стоимости и повышении эффективности упаковочного процесса.

Сегодня компания P&G эффективно использует различные решения DS, включая решение 3DVIA Virtools для реализации проекта Virtual View по виртуализации и оптимизации розничных сетей. В компании также используется система управления техническими характеристиками изделия ENOVIA и функция повторного использования знаний в сфере применения системы корпоративных стандартов (Corporate Standards System – CSS). Кроме того, у компании P&G значительный опыт работы с системой SIMULIA Abaqus для мультифизического моделирования, а ранее, в 2009 году, было объявлено о том, что компания планирует внедрение решения SIMULIA SLM для управления жизненным циклом моделирования.