Конвенциональные широкополосные технологические радиосети обмена данными повышенной надежности и живучести

В статье рассматриваются широкополосные технологические радиосети обмена данными повышенной надежности и живучести, приведены характеристики специализированных радиомодемов для подвижных и стационарных технологических радиосетей обмена данными.

ЗАО «НПП «Родник», г. Москва

Оборудование УКВ-диапазона на практике является идеальным решением для создания технологических радиосетей обмена данными для большинства ответственных приложений. В связи с этим 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, используемых для обеспечения работы отдельных ответственных приложений. С целью удовлетворения этих возросших потребностей 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 разработчикам пришлось использовать широкополосные сигналы. Данное решение позволило увеличить скорость обмена данными и пропускную способность радиосетей, сохранив дальность передачи, характерные для УКВ-диапазона.

Все широкополосные радиомодемы обеспечивают работу в радиосетях с архитектурой «точка – много точек». Так, радиомодемы Mercury-900 и Sentry 4G-900 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

Таблица 1. Характеристики специализированных радиомодемов для подвижных и стационарных технологических радиосетей обмена данными

Наименование радиомодема (производитель)	Рабочий диапазон частот, МГц	Полоса, кГц/Вид модуляции	Скорость передачи информации	Тип протокола	Выходная мощность передачи, Вт	Чувствительность приема
«ExaLink-900, 900M, 900MT» (Exergia Division II, США)	902–928	Нет данных	935 кбит/с	TCP/IP,	0,125	-101 дБм, BER $10x10^{-4}$
«Phantom-900» (CalAmp, США)	902–928	490 кГц/2FSK, 4FSK	256 или 512 кбит/с	Прозрачный, TCP/IP	0,1–1	-98 дБм, BER $10x10^{-6}$, 512 кбит/с -102 дБм, BER $10x10^{-6}$, 256 кбит/с
«Sentry 4G-900», бортовой радиомодем с встроенным навигационным приемником и встроенной точкой доступа WiFi IEEE802.11b/g (CalAmp, США)	902–928	3,5 МГц/OFDMA TDD (IEEE802.16e-2005 WiMax), QPSK, 16QAM, 64QAM	1–3 Мбит/с (6 Мбит/с пиковая)	TCP/IP	0,1–1	Нет данных
«Mercury- 900», бортовой радиомодем с встроенным навигационным приемником и встроенной точкой доступа WiFi (GE MDS, США)	902–928	1,75, 3,5 МГц/ OFDMA (IEEE802.16d-2004 WiMax)	800 кбит/с	Прозрачный, TCP/IP	0,1–1	Нет данных
«TransNET 900» (GE MDS, США)	902–928	CPFSK	115,2 кбит/с	Прозрачный	0,1–1	-108 дБм, BER $1x10^{-6}$

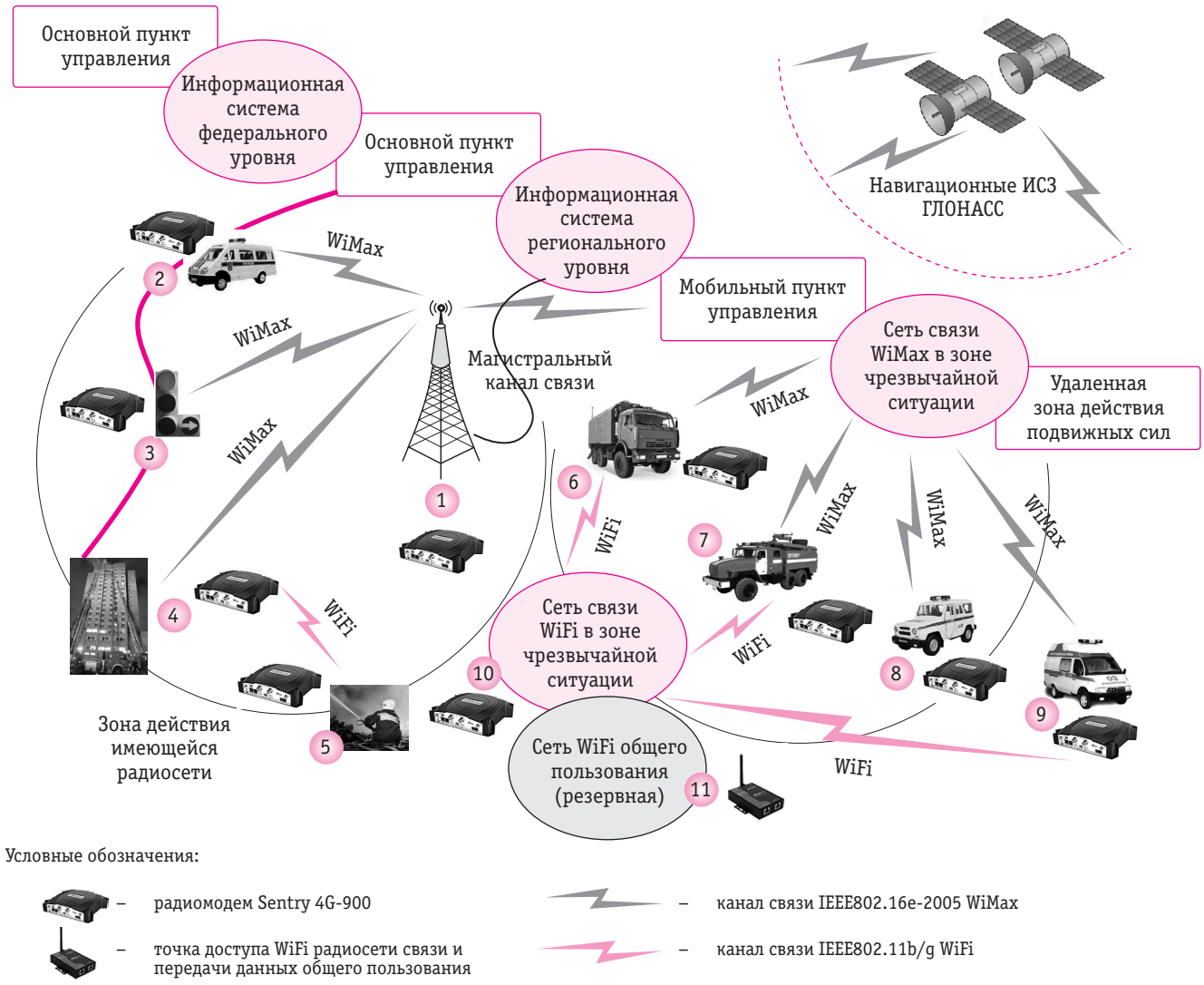

Рис. 1. Упрощенная схема радиосети обмена данными на радиомодемах Sentry 4G-900

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 технологических радиосетей повышенной надежности и живучести на оборудовании 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 IEEE802.16e-2005 WiMax и IEEE802.11b/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 на радиомодемах Sentry 4G-900 представлена на рис. 1.

Представленная на рис. 1 радиосеть обмена данными 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 при выдвижении в район оперативного предназначения в зоне работы постоянной действующей технологической радиосети.
3. Управление светофорными комплексами по каналам тех-

нологической радиосети в интересах приоритетного пропуска подвижных дежурных сил служб общественной безопасности на регулируемых перекрестках на маршруте выдвижения в район оперативного предназначения.

4 Оперативное управление и информационное обеспечение сил и средств служб общественной безопасности в районе оперативного назначения, находящемся в зоне действия технологической радиосети по каналам связи WiMax.

5 Локальная сеть управления силами и средствами служб общественной безопасности в районе оперативного предназначения по каналам связи WiFi в оперативной зоне постоянной действующей технологической радиосети.

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 различной ведомственной принадлежности в удаленной зоне.

11 Локальная сеть WiFi общего пользования.

Широкополосная технологическая радиосеть обмена данными имеет в своем составе группу стационарных базовых 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 выдвижении в ходе решения функциональных задач в районе оперативного предназначения в зоне работы постоянно 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 задач оперативного предназначения.

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 оперативного предназначения. Реализация данной функциональной 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 оперативного назначения, 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 оперативного предназначения 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. В рамках взаимодействия технологическая радиосеть обеспечивает обмен данными между всеми участниками операции, независимо от их ведомственной принадлежности.

Локальные подсети обмена данными разнородных подвижных сил и средств служб общественной безопасности различной ведомственной принадлежности в удаленной зоне разворачиваются на период проведения операции. Они позволяют предоставить подвижным силам функциональные возможности, аналогичные тем, которыми они располагают при работе в стационарных условиях. Разворачиваемая в удаленной зоне локальная вычислительная сеть на базе WiFi обеспечивает взаимодействие разнородных подвижных сил и средств служб общественной безопасности различной ведомственной принадлежности.

При наличии в удаленной зоне сети WiFi общего пользования она может использоваться в качестве резервной или аварийной для обеспечения обмена данными участников операции между собой и с соответствующими пунктами управления верхнего звена.

Навигационное обеспечение участников операции данными от системы спутниковой связи ГЛОНАСС осуществляется через внеш-

ние 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 технологических 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 полного исключения или максимального затруднения компрометации передаваемой по ним информации. В радиосетях обмена данными широко применяются различные методы и способы защиты информации. Степень защиты данных оказывает непосредственное влияние на надежность радиосети и ее живучесть, поскольку постороннее вмешательство в работу может существенно снизить эти параметры. Ниже представлена информация о возможностях данных радиосетей противостоять основным угрозам: перехвату данных, несанкционированной работе в составе радиосети и радиоэлектронным помехам.

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 непрерывный комплекс организационно-технических и специальных мероприятий, ни одно из которых самостоятельно не позволяет добиться поставленной задачи. Тем не менее рассматриваемые средства обмена данными обладают свойствами, позволяющими значительно 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, потернах и т.п., не контролируемых службами безопасности, и представлять собой 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 невозможно.

Во-вторых, оборудование использует специальные схемы модуляции сигнала и собственные преамбулы (структуру пакета данных). На практике это выливается в невозможность получения доступа собственно к 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 обмена данными 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 «просмотра» 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 способности 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 центральном 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).

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 для предоставления контролируемой работы или предотвращения доступа к сети. Поскольку основным условием успешного проникновения в сеть является скрытность, уже сам факт выявления попытки несанкционированного доступа делает его дальнейшие действия 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 (поскольку работа в сети управляется с базовой станции администратором, последний может инициировать работу передатчика злоумышленника с необходимой периодичностью), что существенно проще, чем определить точку подключения к проводной сети обмена данными.

Устойчивость к подавлению и воздействию помех

Подавление или намеренная постановка помех работе радиосистемы – задача существенно более сложная, чем физическое нарушение соединения в проводной системе, и для большинства коммерческих систем маловероятна.

Подверженность радиосигналов воздействию помех и возможность их подавления являются непреложным фактом. Однако для выполнения этой задачи необходимо знать номинал рабочей частоты системы обмена данными, установить который не так просто, поскольку передача ведется короткими сеансами. Факт появления помех немедленно выявляется администратором радиосети, а источник излучения становится объектом пеленгования и локализации, в том числе при поддержке соответствующих организаций, контролирующих использование радиочастотного спектра.

Поэтому гораздо проще незаметно перекусить кусачками пару проводов, чем поставить помеху радиосистеме, используя сложное и дорогостоящее специализированное оборудование, серьезно рискуя при этом быть пойманным. Работа кусачками займет не более 30 секунд, а установка и использование специального оборудования радиопротиводействия требует времени и крупных финансовых затрат, но при этом его воздействие не может быть продолжительным.

Подвижные радиосети

Подвижные технологические радиосети обмена данными подвергаются тем же угрозам, что и стаци-

онарные. Однако степень этих угроз существенно выше, поскольку удаленные объекты постоянно перемещаются, и их контроль оказывается более сложным по сравнению со стационарными радиосетями, а количество одновременно работающих в составе подвижной радиосети пользователей динамически изменяется. В подвижных радиосетях более высока угроза утраты радиотехнического оборудования и его использования для несанкционированного доступа в радиосеть.

Устойчивость к перехвату

Практический опыт эксплуатации подвижных технологических радиосетей обмена данными позволяет рассмотреть возможные угрозы на примере двух наиболее типовых ситуаций:

- целенаправленный перехват;
- угон служебного автомобиля, оснащенного бортовым радиотехническим оборудованием для работы в составе радиосети.

Прежде чем рассмотреть каждую из этих ситуаций, необходимо отметить, что в современных технологических подвижных радиосетях обмена данными используется схема централизованного управления радиосетью, а все данные передаются через базовые станции. В них применяется асимметричная схема адресации, то есть аппаратура базовой станции и подвижного объекта ведет себя по-разному, а сообщения, передаваемые в эфир одним подвижным объектом, не могут приниматься и использоваться другим без «разрешения» базовой станции. Таким образом, архитектура подвижной технологической радиосети обладает определенными свойствами, повышающими ее надежность и живучесть в условиях внешних воздействий.

Целенаправленный перехват

Организация перехвата сообщений в подвижной радиосети обмена данными связана с теми же трудностями, что и в стационарной. Дополнительные трудности создаются использованием уникальных адресов, которые «прошиваются» в радиотехническую аппаратуру в заводских условиях и не могут быть изменены пользователем. Каждый радиомодем для подвижного объекта имеет несколько адресов (индивидуальный, групповой и циркулярный). Все сообщения, за исключением циркулярных, направляются в адрес строго определенного пользователя и не могут приниматься другим радиомодемом, работающим в составе радиосети.

Таким образом, даже при наличии незарегистрированного в радиосети комплекта бортового радиотехнического оборудования можно получить доступ только к циркулярным сообщениям, транслируемым базовой станцией. Комплект базового оборудования теоретически позволяет принимать адресованные базовой станции сообщения. Однако для этого необходимо изменить адрес имеющегося базового радиомодема на адрес радиомодема, реально используемого в составе радиосети, и развернуть оборудование в точке, обеспечивающей прием сообщений от всех или значительной части подвижных объектов, работающих в достаточно большой зоне. Но даже в этом случае эффект от перехвата данных будет весьма мал, поскольку основную оперативную ценность в значительной части подвижных технологических радиосетей представляют собой исходящие данные (управляющие сигналы, команды, распоряжения, результаты обработки обращений к базам данных и т.д.), передаваемые в адрес мобильных пользователей со стороны базовой станции.

Дополнительная безопасность данных обеспечивается применяемыми в аппаратуре для подвижных радиосетей обмена данными методами и средствами, включая парольную защиту и закрытие данных. И хотя такое препятствие не может рассматриваться как серьезное для специалиста, оно достаточно надежно страхует от «случайного доступа» к данным. Обеспечение более высокого уровня безопасности информации достигается за счет применения штатной аппаратуры шифрования.

(Окончание статьи читайте в следующем номере)

ЗАО «НПП «Родник», г. Москва,
тел.: (499) 613-7001,
e-mail: sales@rodnik.ru