

# ПОДВИЖНЫЕ РАДИОСЕТИ ОБМЕНА ДАННЫМИ ДЛЯ СИЛ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

ООО «НЦПР» (Технический бюллетень)

---

## 1. Общие положения

Эффективность решения задач, стоящих перед подвижными подразделениями служб общественной безопасности различной ведомственной принадлежности (МВД, МЧС, Минздрава и др.), может быть существенно повышена в результате совершенствования их информационной инфраструктуры и создания единого информационного пространства для стационарных органов управления и подвижных сил. Данная задача может решаться в рамках развертывания Автоматизированных систем оперативно-диспетчерского управления (АСОДУ), предназначенных для планирования использования, мониторинга работы, управления действиями и информационного обеспечения мобильных подразделений в оперативной зоне. Важнейшим элементом информационной инфраструктуры следует считать средства управления и информационного обеспечения, которые, в значительной степени, определяют возможности отдельных подразделений и дежурных частей по решению стоящих оперативных задач.

Автоматизация процессов управления подчиненными силами и средствами в ходе повседневной деятельности и при проведении специальных операций, своевременного и полного информационного обеспечения и координации их действий с силами взаимодействующих министерств и ведомств позволяет без существенного расширения штатного состава повысить эффективность работы подразделений и частей, оперативность действий в зоне ответственности.

Внедрение и эксплуатация АСОДУ обуславливают формирование требований к обслуживающим их радиосетям обмена данными, которые должны обеспечить решение следующих основных функциональных задач, значительная часть которых должна решаться в масштабе времени, близком к реальному:

- оперативного и надежного доведения распоряжений и сигналов управления до подвижных групп при выполнении ими задач оперативного предназначения;
- автоматического гарантированного доведения до исполнителей сигналов оповещения;
- передачи и приёма докладов о ходе и результатах выполнения поставленных задач;
- информационного обеспечения подвижных групп с удаленным доступом в базы данных по угнанным автомобилям, преступникам, оружию, украденным драгоценностям и т.д.;
- мониторинга и контроля местоположения и перемещения подвижных сил и средств с автоматическим отображением данных о местоположении и характере выполняемой задачи на фоне цифровой карты;
- организации взаимодействия с соседними подразделениями и подвижными силами другой ведомственной принадлежности;

- своевременного автоматизированного анализа и оценки результатов использования дежурных подвижных сил на основе поступающих по радиосети данных;
- оперативной автоматизированной оценки обстановки и поддержки принятия решений на различных уровнях управления;
- автоматического мониторинга технического состояния аппаратуры обмена данными с целью обеспечения высокой надёжности и живучести системы оперативно-диспетчерского управления.

Наиболее полно предъявляемым требованиям удовлетворяют технологические радиосети обмена данными УКВ-диапазона, обладающие следующими основными оперативно-техническими возможностями и преимуществами:

- надёжность среды передачи (линия передачи не подвергается механическим повреждениям и разрушающему влиянию окружающей среды, а ее качество контролируется соответствующими государственными органами);
- обширная оперативная зона с возможностью ее расширения за счет ретрансляции сигнала (некоторые реально построенные и успешно эксплуатирующиеся радиосети имеют сплошную оперативную зону более миллиона квадратных километров, что сопоставимо со всей территорией Европейской части Российской Федерации);
- применение детерминированных протоколов обмена данными, поддерживающих работу в близком к реальному масштабе времени и обеспечивающих гарантированную доставку данных в установленные регламентом работы радиосети сроки;
- относительно небольшое время доступа к каналу передачи данных, обеспечивающее незначительные и приемлемые для большинства использующих радиосеть автоматизированных систем управления задержки в доставке данных;
- высокая безопасность данных, циркулирующих в технологической радиосети (применяемые технологии обеспечивают защиту от подавления, перехвата или несанкционированного доступа к работе в составе технологической радиосети);
- относительно низкая совокупная стоимость владения (отсутствие платежей за аренду оборудования и информационные потоки);
- независимость от «чужой» инфраструктуры связи и возможность развивать ее исходя из реальных требований (радиосеть принадлежит собственно пользователю, параметры ее работы и оперативная зона могут изменяться им самостоятельно);
- совместимость с разнородным оборудованием сбора и обработки данных по широко применяемым и детально отработанным интерфейсам (поддерживается работа по IP-протоколу и специализированным полицейским протоколам);
- простота перемещения и оперативность развертывания в новом районе;
- возможность эксплуатации в жестких условиях, в том числе, в экстремальных климатических условиях.

Технологическая радиосеть обмена данными, работающая в УКВ-диапазоне и позволяющая организовать обмен информацией между стационарными пунктами управления и подвижными группами, а также подвижных групп между собой, является идеальным средством для управления подчиненными силами в обширной оперативной зоне, не требующим развертывания сложной технической инфраструктуры и способная функционировать с использованием имеющегося радиочастотного ресурса. Она может использоваться также в составе систем дистанционного управления техническими средствами, сбора данных, идентификации и контроля, обеспечивая возможность их быстрого монтажа на заданном объекте и оперативного перемещения в другой район в случае изменения стоящей задачи.

## 2. Оперативно-технические задачи АСОДУ

Современная технологическая радиосеть позволяет эффективно решать комплекс оперативно-технических задач, стоящих перед подвижными подразделениями дежурных сил общественной безопасности в рамках развертывания и функционирования современных АСОДУ. В этом случае некоторыми общими типовыми задачами для всех подвижных подразделений, решаемых с использованием технологической радиосети обмена данными, являются (ниже представлены данные применительно к одной из наиболее современных зарубежных полицейских систем рассматриваемого типа, использующих аппаратуру связи APCO25 и аппаратуру передачи данных ParagonG3/GeminiG3):

- **Мониторинг работы подвижных сил и средств.** Объективная (инструментальная) информация о местоположении и параметрах движения контролируемых подвижных объектов (транспортных и специальных средств МВД, ГИБДД, вневедомственной охраны и др.) в реальном масштабе времени поступает на рабочее место диспетчера и отображается на экране его рабочего места на фоне цифровой карты или электронного плана оперативного района. Дополнительно от каждого подвижного объекта поступает информация о его оперативном (например, находится на задании, ведет патрулирование, приступил к задержанию и т.п.) и техническом (например, полностью или частично работоспособен, либо не в состоянии решать поставленную задачу по техническим причинам). Средства перспективной АСОДУ контролируют общую обстановку и отслеживают изменения состояния подвижных объектов (отклонение от заданного маршрута движения, выход из назначенной оперативной зоны, начало и завершение выполнения плановых мероприятий и т.п.). При выявлении отклонений генерируются соответствующие сигналы тревог.

Обработка данных выполняется на средствах вычислительного комплекса повышенной надёжности и живучести, коэффициент оперативной готовности которого составляет 99,999%, что полностью удовлетворяет требованиям, предъявляемым к ответственным информационным системам. Технологическая радиосеть позволяет организовать приём в одном радиоканале УКВ-диапазона через каждую базовую станцию сообщений от более 300 подвижных объектов с периодичностью обновления навигационных данных о каждом объекте раз в минуту. Таким образом, диспетчер располагает объективной информацией о задействовании подчиненных сил и средств практически в реальном масштабе времени.

- **Оперативно-диспетчерское управление подвижными силами и средствами.** Осуществляется на основании данных мониторинга с учетом текущих и планируемых задач. При возникновении новой оперативной задачи система выдает рекомендации диспетчеру по распределению

подвижных сил и средств с учетом их текущего местоположения (ближайший к району происшествия), характера использования (свободен, решает задачу более низкого приоритета и т.п.), степени готовности (начало патрулирования, завершение дежурства, смена экипажа и т.п.) и технического состояния (исправен, на заправке, техническая проблема, например, прокол шины и т.п.). Команды и инструкции диспетчера гарантированно доводятся до отдельных подвижных подразделений, групп пользователей или циркулярно в автоматическом режиме с подтверждением получения. Порядок их доведения и состояние связи контролируются системой автоматически. Наличие единого информационного пространства и использование единого протокола для обмена данными предоставляет техническую возможность передачи данных из пункта управления федерального уровня (применительно к Российской Федерации — из г.Москвы) на любой подключенный к радиосети обмена данными удаленный подвижный объект (например, в г.г.Владивостоке или Калининграде), в реальном масштабе времени.

Современная автоматизированная система позволяет организовать эффективное оперативно-диспетчерское управление несколькими сотнями подвижных объектов с привлечением ограниченного числа диспетчеров. На практике сообщение объемом в страницу машинописного текста в адрес группы из 300 подвижных объектов может быть доведено в течение доли секунды и подтверждено в течение минуты. Диспетчер может также получить уведомление о том, что адресат реально ознакомился с сообщением, а система обеспечит гарантированное доведение информации не только до заданного транспортного средства, но и до конкретного исполнителя даже в случае смены им транспортного средства.

- **Информационное обеспечение подвижных сил.** В отличие от радиосетей голосовой связи выполняется без привлечения диспетчера путем прямого обращения к информационным базам данных. Экипаж подвижного объекта обращается к базе данных и в близком к реальному масштабе времени получает необходимую ему информацию (удаленная идентификация личности по отпечаткам пальцев, контроль лицензий на ношение оружия, проверка автомобилей на угон и т.п.). Обращение может выполняться с борта патрульного автомобиля к локальной, региональной или федеральной базе данных по каналам существующей ведомственной сети обмена данными с контролем и разграничением доступа к информации и функциям.

Современная АСОДУ позволяет расширить возможности технических комплексов контроля. Наличие радиоканала обмена данными с адекватной пропускной способностью позволяет в полной мере использовать ее возможности на подвижных объектах. Например, комплекс «Сова» может применяться в движении на борту патрульного автомобиля и обеспечивать выборочную проверку транспортных средств непосредственно в потоке транспорта без их остановки. Комплекс «Папиллон» может использоваться для идентификации личности по отпечаткам пальцев с временных позиций, положение которых меняется в зависимости от оперативной обстановки. Зарегистрированные системой исходные данные (номера автотранспортных средств или отпечатки пальцев) могут автоматически проверяться по удаленной централизованной базе данных, которая пополняется в реальном масштабе времени. Применение IP-протокола в канале радиосвязи между специальным транспортным средством и диспетчером позволяет организовать обращение в удаленные базы данных на любом уровне управления

(локальном, региональном или федеральном). Такие возможности позволят увеличить число проверяемых транспортных средств и подозреваемых и повысить эффективность оперативно-розыскных мероприятий по горячим следам.

Рассмотренный вариант оперативного использования комплексов дополнительно позволяет:

- повысить безопасность личного состава при проверках (за счет того, что, например, при остановке транспортного средства наряд заранее знает, кому это транспортное средство принадлежит и может более точно оценить складывающуюся обстановку).
- объективно оценить интенсивность работы подвижных дежурных сил и эксплуатации системы по количеству запросов, сделанных в базу данных, например, по угнанным автотранспортным средствам и находящимся в розыске преступникам.

Сопряжение с современными автоматизированными системами управления других министерств и ведомств, использующими радиосети обмена данными с подвижными объектами, позволяет решать комплекс технически сложных задач, связанных с управлением и обеспечением безопасности дорожного движения в крупных населенных пунктах и на междугородных трассах. Актуальность такой задачи возрастает в период проведения массовых мероприятий, таких как «Универсиада-2013» в г.Казани и «Олимпиада-2014» в г.Сочи.

Типовыми задачами, связанными с совместным использованием возможностей современных автоматизированных систем управления подвижными силами служб общественной безопасности и пассажирскими, грузовыми и специальными перевозками, могут быть следующие:

- **Мониторинг транспортных потоков.** Выполняется на основе данных, поступающих от автомобильных и электрических транспортных средств, оснащенных радионавигационной аппаратурой. Позволяет получать достаточно точную и детальную информацию о скоростях движения по улицам и на перекрестках, не оснащенных системами видео наблюдения.

Такое техническое решение является практически единственным способом оперативного автоматического получения полной информации о дорожной обстановке (в части скорости транспортных потоков). Оно предоставляет уникальную возможность организации управления дорожным движением на основе реально складывающейся дорожной обстановки на всей территории крупного города.

- **Профилактика дорожно-транспортных происшествий.** Удаленное подключение дежурных подразделений ГИБДД к текущей базе данных о работе городского пассажирского транспорта, отражающей информацию о находящихся на маршрутах транспортных средствах и параметрах их движения (местоположение и скорость), позволяют автоматически регистрировать и выявлять факты нарушения водителями скоростного режима как в реальном масштабе времени, так и за определенный период времени или на определенном участке маршрута. Все данные являются документированными и могут использоваться для проведения разборов причин дорожно-транспортных происшествий. Для анализа могут использоваться не только параметры движения транспортных средств, но и время работы (перерывов в работе) водителей, соблюдение сроков проведения технического обслуживания транспортных средств и т.п.

По данным статистики ДТП с наиболее тяжкими последствиями связаны с участием в них общественного транспорта. Получение объективной детальной информации о работе этого вида транспорта и наличие возможности ее автоматизированного анализа (по конкретному транспортному средству и водителю) позволяет организовать профилактические мероприятия адресно и на качественно новом уровне.

- **Приоритетный пропуск общественного транспорта на регулируемых перекрестках.** Доступ в реальном масштабе времени к навигационной информации о работе пассажирского транспорта позволяет организовать приоритетный пропуск крупногабаритного транспорта (автобусов, троллейбусов, трамваев) на регулируемых перекрестках и обеспечить повышение существующей пропускной способности улиц и магистралей без их модернизации. Одновременно создаются условия для увеличения средней скорости движения и снижения напряженности в дорожной обстановке, особенно в часы пиковых нагрузок.

По данным мировой практики организация движения в крупных городах с приоритетным пропуском крупногабаритного транспорта позволяет не только снизить расходы моторесурса (до 5%) и выбросы выхлопных газов в атмосферу, но и увеличить пропускную способность улиц и магистралей за счет исключения остановок крупногабаритного транспорта на светофорах на 5-15%.

Типовыми задачами, связанными с совместным использованием возможностей современных автоматизированных систем управления других ведомств, могут быть следующие:

- **Информационное взаимодействие при выполнении специальных задач в ходе чрезвычайных ситуаций.** Формирование временных сводных подразделений сил МВД и других ведомств (в частности, МО и МЧС) позволяет обеспечить их координированное использование по планам различных ведомств. При использовании интегрированной радиосети обмена данными создается единое информационное пространство, в рамках которого вышеуказанные формирования могут действовать с высокой эффективностью при обеспечении адекватного уровня безопасности личного состава, техники и специальных средств.

Перспективная АСОДУ позволяет решать ряд вспомогательных задач, связанных с эксплуатацией технических средств и специальной техники МВД РФ. Примерами таких задач являются:

- **Дистанционное управление робототехническими комплексами специального назначения.** Эффективно применяется в условиях, когда управление должно быть организовано на дальность, превышающую длину управляющего кабеля или когда использование управляющего кабеля оказывается невозможным (при работе внутри зданий и помещений, в завалах и т.п.). Дооснащение имеющихся технических средств позволяет расширить их функциональные и тактико-технические возможности, исключив приобретение дополнительных специальных средств.
- **Управление светофорами, временными знаками и дорожными табло.** Возможности технологической радиосети позволяют оперативно развернуть резервные системы управления средствами дорожного движения в случае аварий и сбоев, а также расширить возможности по информированию участников дорожного движения в повседневной обстановке и в условиях ухудшения метеорологических и дорожных условий.

Весь комплекс вышеперечисленных задач может решаться в рамках перспективной АСОДУ с жестким разграничений доступа к ресурсам радиосети и функционирующей в ее составе информации.

### **3. Функциональные возможности информационной системы, обеспечиваемые технологической радиосетью обмена данными**

Оперативно-технические возможности технологической радиосети обмена данными УКВ-диапазона расширяют функциональные возможности информационной системы МВД РФ и существенно дополняют возможности современных голосовых радиосетей, включая цифровые транковые радиосети стандартов APCO25 или TETRA, в части обмена данными с подвижными объектами. Основными из них являются следующие:

- **Обмен сообщениями в реальном масштабе времени.** Обмен сообщениями подвижных объектов с диспетчером и между собой в реальном масштабе времени производится через базовую станцию. Например, пользователь направляет сообщение: «ОГ086 встреча в точке Т01 в 10.00». В этом случае направленное сообщение принимается базовой станцией автоматически передается в адрес другого подвижного объекта, где высвечивается на дисплее пользователя (в данном случае — оперативной группы 086) и сопровождается звуковым сигналом. В случае если адресат завершил работу в системе, поступающие в его адрес сообщения ставятся в очередь и автоматически доводятся до него при подключении к системе. Все сообщения, передаваемые между двумя или несколькими подвижными объектами, автоматически фиксируются на стационарном пункте управления. Сообщение может быть сгенерировано на любом уровне управления (локальном, региональном или федеральном) и оперативно доведено до конкретных непосредственных исполнителей на борту удаленного специального автомобиля.
- **Объявления.** Любое сообщение может быть направлено всем или определенной группе пользователей, работающих в системе. Например, сообщение может быть направлено всем оперативным группам или машинам, включая взаимодействующие. Любое объявление передается только пользователям, которым оно адресовано.
- **Доступ к предметной базе данных** (например, перечню происшествий или угнанных транспортных средств). Предоставляемые интерфейсы с базами данных (на локальном, региональном или федеральном уровнях с использованием принятых разграничений доступа к данным и функциям) позволяют подвижному пользователю автоматически получить санкционированный доступ к важной оперативной информации без риска перехвата этой информации лицами, не имеющими соответствующего доступа к ней. Например, сотрудник может произвести проверку подозрительного транспортного средства по его государственному номерному знаку без остановки самого средства. В этом случае сотрудник стационарного поста или патрульного автомобиля обращается к базе данных и получает полную информацию о транспортном средстве и его владельце.
- **Передача докладов.** Оперативное доведение сообщения повышенной размерности, подготовленного подвижным пользователем на установленном в автомобиле терминале, до заинтересованных лиц и инстанций позволяет увеличить общий срок патрулирования за счет

сокращения времени на подготовку отчетов в стационарных условиях. Например, сотрудник может передать в адрес диспетчера полный доклад о результатах работы в течение всего дежурства не покидая автомобиля.

- **Автоматическое определение местоположения подвижного объекта.** Каждый подвижный объект оснащается приемником спутниковой навигационной системы ГЛОНАСС/GPS «Навстар», позволяющим определять собственное местоположение с высокой точностью. При этом специальный модуль обеспечивает автоматическую передачу данных о его местоположении с каждым сообщением, с заданной периодичностью или по заданной программе. Таким образом, диспетчер постоянно имеет информацию о местоположении подвижных объектов. Полученная навигационная информация представляется в различных табличных формах, либо выводится на карту в графическом виде.
- **Электронная почта.** Сообщения пользователям системы могут направляться независимо от того, подключены ли они к радиосети в данный момент времени или нет. При отсутствии абонента, которому адресовано сообщение, все сообщения хранятся в центральном компьютере и доводятся до адресата в момент его подключения к радиосети. Сообщения могут адресоваться отдельному пользователю, определенной группе или всем пользователям.
- **Конференц-связь.** Любой пользователь радиосети может организовать конференцию, в которой одновременно могут работать два и более пользователей. Участниками конференции могут быть пользователи, работающие в зоне действия одной или различных базовых станций (например, базовых станций радиосети, развернутых в других населенных пунктах).
- **Удаленный доступ к данным.** Пользователи, в зависимости от уровня доступа, могут удаленно просматривать и редактировать данные. Например, старший подвижной оперативной группы может получить доступ к информационным файлам по закреплению жилых помещений и адресов, разрешений на ношение оружия, владельцев транспортных средств, списку происшествий, графикам работы организаций и учреждений, телефонному справочнику, планам строений, картам местности, оперативным данным об обстановке в заданном районе, метеорологическим данным и др.
- **Интерфейс диспетчерской системы/системы распределения сообщений.** Система может быть настроена для организации обмена данными с взаимодействующими подразделениями (например, подразделениями дежурных сил различной ведомственной принадлежности) и другими автоматизированными диспетчерскими системами, что позволяет подвижным подразделениям оперативно получать необходимую информацию (информацию для идентификации личности, адресные данные, данные о транспортных средствах, проверять подлинность отдельных документов).
- **Безопасность данных.** Радиосеть обеспечивает закрытие всей передаваемой информации. Кроме того, доступ к системе могут получить только пользователи, внесенные в соответствующий перечень. Система позволяет вести протокол всех попыток подключения, запросов на получение информации и передачи данных с регистрацией времени события. (Информация о безопасности технологической радиосети обмена данными представлена ниже).
- **Приоритеты и разграничение доступа.** Любой пользователь радиосети может использовать имеющиеся приоритеты и доступ или ограничение доступа к выполнению любой функции.

- **Имена пользователей.** Каждый пользователь радиосети прописывается в системе с использованием имени и пароля, поэтому может получать сообщения, адресованные его подразделению (Например: «ОГ086») или на его имя (Например: «ОГ086/Иванову В.П.»). Такой алгоритм позволяет направлять сообщения пользователям при отсутствии данных о принадлежности их к конкретному подразделению. В этом случае абонент получит адресованное ему сообщение даже в случае смены транспортного средства и подключения к системе с другого бортового или стационарного терминала.
- **Диспетчерская консоль.** В ходе обычной работы на экране диспетчерской консоли отображается информация о номере подразделения и имени каждого работающего в системе пользователя, а также данные о его статусе (в оперативном использовании, временно не функционирует и т.д.). Диспетчер имеет возможность контролировать весь поток сообщений и работать в системе как обычный пользователь.
- **Пропускная способность.** Максимальное количество пользователей зависит от интенсивности и объёма передаваемых сообщений, скорости обмена данными в радиосети и времени доступа к канальным ресурсам. При идентичном трафике скорость обмена данными при использовании рассматриваемой в качестве примера аппаратуры ParagonG3/GeminiG3 производства американской компании CalAmp ([www.calamp.com](http://www.calamp.com)) в восемь раз выше (составляет 64 кбит/с в движении), а время доступа к радиоканалу (15 мс, основной параметр, влияющий на пропускную способность) в 30 раз меньше, чем в современной цифровой транковой системе для силовых структур APCO25. Более высокий, по сравнению с речевыми радиосетями, уровень автоматизации позволяет сократить количество диспетчеров не менее чем в пять раз, необходимый радиочастотный ресурс — в два-три раза, количество базовых станций в несколько раз.
- **Сопряжение комплексов информационной системы.** Вычислительные комплексы информационной системы, эксплуатируемые в различных населенных пунктах или находящиеся в различном оперативном подчинении, могут сопрягаться между собой, образуя единое информационное поле. В варианте исполнения с повышенной надёжностью и живучестью узлы одного вычислительного комплекса могут быть разнесены на сотни километров и развернуты в различных населенных пунктах. После подключения к такой информационной системе пользователь получает возможность использования всего набора функций информационной системы при обмене данными с любым пользователем другого комплекса. Поскольку система не накладывает ограничений на количество сопрягаемых между собой комплексов, ее размеры практически не ограничены.
- **Фотографические изображения.** При наличии базы данных цифровых изображений они могут передаваться по каналам технологической радиосети обмена данными. Данная функция позволяет существенно повысить возможности по идентификации личности подвижными подразделениями и информационному обеспечению специальных операций.

#### 4. Интегрированные межведомственные узкополосные технологические радиосети обмена данными

Одним из перспективных направлений развития узкополосных радиосетей обмена данными является разработка технических решений для создания интегрированных технологических радиосетей (ИТРС), которые могут эксплуатироваться одновременно пользователями различной ведомственной

принадлежности и обеспечивать исключение компрометации передаваемой в радиосети информации за счет разграничения доступа к транслируемым в радиосети данным. Как правило, такие интегрированные радиосети позволяют поддерживать связь с подвижными и стационарными объектами и используют для обмена универсальный IP-протокол, позволяющий сделать доступ к радиосети прозрачным для различных приложений, способных успешно функционировать в обычных локальных вычислительных сетях (ЛВС).

Интегрированные радиосети могут в полной мере использовать описанные в настоящей статье решения, направленные на повышение их надёжности и живучести. Вместе с тем, они обладают дополнительными преимуществами, поскольку строятся на единых технических принципах и используют единую инфраструктуру. Кроме того, правильное распределение функций между владельцами сетей с учетом специфических возможностей каждого из них позволяет упростить выполнение организационно-технических мероприятий, связанных с их эксплуатацией. Например, в случае создания единой сети для всех служб общественной безопасности города каждая из служб может обеспечивать эксплуатацию собственного сегмента радиосети, отдельные службы — отвечать за эксплуатацию совместно используемых сегментов, а подразделения полиции дополнительно — осуществлять физическую охрану всех объектов, на которых размещается аппаратура связи. Радиочастотный ресурс для создания ИТРС может выделяться всеми службами общественной безопасности с учетом возможностей каждой из служб, а использоваться в зависимости от текущих потребностей каждой из них. Наиболее сложным в реализации такого подхода представляется слабое межведомственное взаимодействие и существующие правила и особенности финансирования служб общественной безопасности, однако и эти проблемы не являются непреодолимыми, если задача решается в рамках муниципального образования или субъекта Российской Федерации.

Вариант интегрированной технологической радиосети обмена данными повышенной надёжности и живучести представлен на Рис. 11.

[изображение отсутствует: 2f6432f1fd37-1095.png]

<b><u>Условные обозначения:</u></b>				
БС ИТРС	–	базовая станция Интегрированной технологической радиосети (ИТРС) обмена данными		– радиомодем базовой станции ParagonG3 подвижной технологической подсети ведомств (служб общественной безопасности)
ВОЛС	–	волоконно-оптическая линия связи		– бортовой радиомодем GeminiG3 подвижной технологической подсети ведомств (служб общественной безопасности)



–	<b>Вычислительный узел Центра управления дорожным движением.</b>
–	Городская маршрутная сеть.

Предполагается, что ИТРС обслуживает подвижные дежурные силы и функционирование объектов инфраструктуры Министерства транспорта (в части пассажирского транспорта), Министерства внутренних дел, Министерства по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, а также городских аварийных служб муниципальных образований в повседневной деятельности и при проведении совместных операций (в части специального транспорта подвижных дежурных сил).

Вычислительный узел Центра управления дорожным движением реализуется на базе серверов повышенной надёжности и живучести с использованием технологий виртуализации Stratus everRun<sup>®</sup> с физическим разнесением вычислительных узлов. Он сопрягается с вычислительным узлом Центра управления перевозками [3]. Доступ к инфраструктуре ИТРС обеспечивается по выделенным проводным каналам связи. Центр управления дорожным движением осуществляет управление светофорными комплексами с учетом реальной дорожной обстановки. Связь со светофорными комплексами организуется по ВОЛС и/или радиоканалам единой стационарной подсети [7]. Управление светофорами организуется с учетом поступающих в реальном масштабе времени данных от Центра управления перевозками и транспортных средств (пассажирского и специального транспорта), находящихся на маршрутах движения.

Диспетчеры ведомственной службы (служб общественной безопасности) подключаются к Центру управления дорожным движением и Центру управления перевозками по выделенным каналам связи или существующим каналам связи общего пользования. Они имеют доступ к инфраструктуре Интегрированной технологической радиосети обмена данными по выделенным проводным каналам связи и взаимодействуют с Центром управления дорожным движением в части приоритетного пропуска транспорта подвижных дежурных сил служб общественной безопасности на регулируемых дорожных перекрестках с учетом реально складывающейся оперативной и дорожной обстановки.

Вычислительный узел Центра управления перевозками реализуется на базе виртуальных серверов повышенной надёжности и живучести с физическим разнесением вычислительных узлов. Он сопрягается с вычислительным узлом Центра управления дорожным движением [1], формируя единый вычислительный комплекс. Доступ к инфраструктуре Интегрированной технологической радиосети обмена данными обеспечивается по выделенным проводным каналам связи. Вычислительный узел обеспечивает мониторинг, оперативно-диспетчерское управление и информационное обеспечение всех участников перевозочного процесса, включая информирование пассажиров на остановках общественного транспорта. Он взаимодействует с Центром управления дорожным движением в части приоритетного пропуска пассажирского транспорта на регулируемых дорожных перекрестках с учетом реальных потребностей.

Вычислительный комплекс диспетчерского пункта пассажирского автотранспортного предприятия или трамвайно-троллейбусного депо решает задачи, связанные с выделением транспортных средств и поддержанием их готовности к выполнению пассажирских перевозок в процессе их выполнения под руководством Центра управления перевозками. Он получает полную информацию о работе пассажирского транспорта в масштабе времени, близком к реальному.

Базовая инфраструктура подвижной оперативной подсети ИТРС обмена данными, обеспечивающая обмен данными средств дежурных подвижных сил служб общественной безопасности [6] с диспетчерами ведомственной службы [2] и между собой. Она создается на специализированной базовой аппаратуре передачи данных, радиомодемах ParagonG3, обеспечивающих обмен данными в движении со скоростью 64-128 кбит/с с использованием IP-протокола.

Бортовое оборудование подвижной оперативной подсети ИТРС обмена данными реализуется на специализированной бортовой аппаратуре передачи данных, радиомодемах GeminiG3, обеспечивающих обмен данными в движении со скоростью 64-128 кбит/с с использованием IP-протокола.

Базовая инфраструктура единой стационарной подсети обмена данными, реализованная на радиомодемах Viper-SC, обеспечивает обмен данными со скоростями 32-128 кбит/с с использованием IP-протокола. Она используется для обеспечения связи со светофорными комплексами (включая временные) [9], не имеющими постоянной проводной связи, а также информационными средствами остановочных пунктов пассажирского транспорта [10]. Каналы стационарной подсети обмена данными обеспечивают выполнение функций сбора данных и управления работой светофорных комплексов в интересах организации приоритетного пропуски через регулируемые дорожные перекрестки пассажирского и специального транспорта, а также трансляции данных о расписаниях и реальных графиках движения пассажирского транспорта в интересах информирования населения на пассажирообразующих остановках.

Интеллектуальный светофорный комплекс, подключенный по волоконно-оптической линии связи, обеспечивает получение данных от бортового радиотехнического комплекса пассажирского транспортного средства [12] и их трансляцию в адрес Центра управления перевозками [1] по волоконно-оптической линии связи в интересах принятия решения о приоритетном пропуске через регулируемый дорожный перекресток.

Интеллектуальный светофорный комплекс, подключенный по радиоканалу Единой стационарной подсети, обеспечивает получение данных от бортового радиотехнического комплекса пассажирского транспортного средства [12] и их трансляцию в адрес Центра управления перевозками [1] по каналам единой стационарной подсети в интересах принятия решения о приоритетном пропуске через регулируемый дорожный перекресток.

Информационный комплекс остановочного пункта обеспечивает информирование населения на пассажирообразующих остановках и предоставление информации о расписаниях и реальных графиках движения пассажирского транспорта, а также любой другой информации, включая рекламу. Он является составным элементом городской системы оповещения населения в чрезвычайных ситуациях.

Базовая инфраструктура подвижной оперативной подсети обмена данными пассажирского транспорта, реализованная на радиомодемах Viper-SC, обеспечивает обмен данными со скоростью 64 кбит/с с использованием IP-протокола средств пассажирского транспорта с диспетчерами Центра управления перевозками и между собой. Она используется для обеспечения мониторинга и оперативно-диспетчерского управления пассажирскими перевозками, включая перевозки речным транспортом.

Бортовой радиотехнический комплекс пассажирского транспорта, оснащенный техническими средствами, обеспечивающими работу в составе подвижной оперативной подсети ИТРС обмена данными [6] со скоростью 64 кбит/с и стационарной технологической подсети автотранспортных предприятий и трамвайно-троллейбусных депо [14] со скоростью до 54 Мбит/с, позволяет организовать

оперативный обмен данными с диспетчером Центра управления перевозками [3] и автоматическую связь с аппаратурой светофорных комплексов [8, 9] в интересах организации приоритетного пропуски через регулируемые дорожные перекрестки, а также автоматический обмен служебной информацией с вычислительным комплексом транспортного предприятия [4] при выходе и возвращении в парк или депо.

Бортовой радиомодем Viper-SC обеспечивает обмен данными с вычислительным комплексом и диспетчерами Центра управления перевозками по радиоканалам подвижной оперативной подсети транспорта на скорости 64 кбит/с. Он используется для трансляции навигационных и телеметрических данных, команд управления и сигналов оповещения.

Стационарная технологическая подсеть предприятия пассажирского транспорта обеспечивает автоматический обмен данными с бортовым радиотехническим комплексом в интересах поддержания в актуальном состоянии технологической информации на борту, а также съема данных о результатах эксплуатации за заданный период. Позволяет организовать обмен данными в автоматическом режиме по IP-протоколу на скорости до 54 Мбит/с и автоматический сбор данных с борта пассажирских транспортных средств на территории парка или депо.

Спутниковая радионавигационная система ГЛОНАСС/GPS «Навстар», выполняющая функции навигационного обеспечения функционирования пассажирского и специального транспорта.

Городская маршрутная сеть формируется с учетом объективных данных о пассажиропотоках. Движение организуется по единому согласованному графику для автомобильного и электрического транспорта с учетом требований по обеспечению интермодальности (согласованности с возможностью выбора наиболее подходящего для конкретного пассажира) перевозок, включая расписания движения авиационного и речного (морского) транспорта.

Широкие возможности радиосети позволяют эффективно использовать ее в интересах решения задач эвакуации населения в чрезвычайных ситуациях, а также обеспечения мобилизационного развертывания вооруженных сил в особый период.

В рассматриваемом варианте интегрированная технологическая радиосеть обмена данными становится компонентом единой городской информационной инфраструктуры. Она обеспечивает взаимодействие между подвижными силами и средствами различной ведомственной принадлежности и функционирование стационарных элементов городской и транспортной инфраструктуры. Радиосеть используется для решения различных функциональных задач, в связи с чем в ее составе применяются аппаратно-программные средства с различными техническими характеристиками, выбор которых производится исходя из требований решения конкретных задач. Поскольку основная часть вышеуказанных задач относится к категории ответственных, при создании радиосети должно быть предусмотрено выполнение требований к ее повышенной надёжности и живучести.

## **5. Обеспечение безопасности в технологической радиосети обмена данными**

Технологическая радиосеть обмена данными является основным элементом, обеспечивающим функционирование АСОДУ. Она должна строиться в соответствии с решениями руководства Министерства внутренних дел Российской Федерации, ГУВД, УВД республик, краев и областей, указаниями начальника Главного штаба МВД России, распоряжением по связи Главного штаба с учетом

наличия и состояния сил и средств связи, времени на развертывание системы и возможного на нее воздействия, Концепцией развития ведомственной сети связи и передачи данных МВД России, регламентирующей основы создания и совершенствования системы связи в каждом конкретном регионе.

Технологическая радиосеть обмена данными должна формироваться в соответствии со структурой управления органов внутренних дел, характером выполняемых ими задач, геополитических и географических условий и необходимостью взаимодействия структурных подразделений при проведении оперативно-розыскных и иных мероприятий с использованием обходных каналов связи, в том числе других министерств и ведомств.

Для управления органами внутренних дел Российской Федерации создается ведомственная система связи и передачи данных, в том числе и защищенная, являющаяся составной частью интегрированной государственной системы связи России и состоящая из стационарных и подвижных узлов связи территориальных органов внутренних дел — пунктов управления, каналов и линий связи между пунктами управления, линий привязки узлов связи пунктов управления к стационарным узлам связи общегосударственной сети связи.

*Из инструктивного доклада заместителя начальника Главного штаба — начальника Управления связи и автоматизации МВД РФ на Всероссийском совещании-семинаре начальников штабов МВД, ГУВД, УВД, УВДТ, УВД УРО: «Задачи штабов по организации ведомственной системы связи, сети передачи данных, автоматизации органов внутренних дел и пути их решения»*

В связи с этим 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 существенно снизить существующие угрозы.

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 надёжность 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<sup>1</sup>.

## **6. 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»<sup>2</sup> на информационные системы различных ведомств и организаций). 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 стационарных и подвижных радиосетях являются радиоволны, которые могут приниматься любым приемником на относительно большом расстоянии от передатчика. Однако, радиосигналы, передаваемые в радиосетях обмена данными с использованием современного радиотехнического оборудования, 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 собственно к передаваемой информации при отсутствии соответствующего приемного оборудования или специальных приборов для анализа сигналов. В отличие от проводных средств связи, 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, в то время как удаленные объекты такой возможности не имеют. 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 стационарные и подвижные радиосети обмена данными более безопасными по сравнению с технологическими проводными сетями связи и обмена данными в части перехвата информации.

## 2. Устойчивость к несанкционированному подключению

При подключении к сети обмена данными обычно ставится цель получение доступа для работы в составе информационной системы или «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 способности по обеспечению безопасности информации.

Часть технологических радиосетей обмена данными (в первую очередь, стационарных) использует протоколы «опроса», в которых заложены определенные возможности по обеспечению безопасности. Чтобы терминал пользователя распознавался информационной 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, который может локализовать нового пользователя, получившего доступ к сети, 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 технологических радиосетей используется для обслуживания строго определенного количества терминалов, поэтому появление в их составе новых терминалов вообще не предусматривается.

Возможно, что профессиональный «крэкер»<sup>3</sup> 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 информационной системе. 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 приёма 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, чем определить точку подключения к проводной сети обмена данными.

### **3. Устойчивость к подавлению и воздействию помех**

Подавление или намеренная постанковка помех работе радиосети задача существенно более сложная, чем физическое нарушение соединения в проводной системе, и для большинства технологических радиосетей маловероятна.

Подверженность радиосигналов воздействию помех и возможность их подавления являются непреложным фактом. Однако для выполнения этой задачи необходимо знать номинал рабочей частоты радиосети 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, в том числе, при поддержке соответствующих организаций, контролирующих использование радиочастотного спектра.

Поэтому на практике оказывается 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.

### **4. Особенности обеспечения безопасности работы подвижных технологических радиосетей**

Подвижные технологические радиосети обмена данными подвергаются всем описанным выше угрозам, 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.

Практический опыт эксплуатации подвижных технологических радиосетей обмена данными служб общественной безопасности 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 подвижных технологических 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 ведут 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 надёжность и живучесть в условиях внешних воздействий.

## 5. Целенаправленный перехват

Организация перехвата сообщений в подвижной радиосети, использующей современные протоколы обмена, реализующие возможность инициализации работы по инициативе подвижного объекта, связана с теми же трудностями, что и в радиосетях, применяющих более простые протоколы «опроса». Дополнительные трудности для перехвата создаются наличием уникальных адресов, которые «прошиваются» в радиотехническую аппаратуру в заводских условиях и не могут быть изменены пользователем. Каждое устройство связи (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 не зарегистрированного 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 приём 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 рассматриваемых современных подвижных технологических радиосетей, представляют 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 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.

### 1. Угон служебного автомобиля с подключенным к радиосети радиотехническим оборудованием

В случае угона служебного автомобиля при включении установленного в нем оборудования невозможно получить полный доступ ко всей информации, как в голосовой радиосети. В отличие от конвенциональных голосовых радиосетей, где каждый подключившийся к сети пользователь может принимать циркулирующие в ней сообщения, в радиосетях обмена данными это полностью исключено.

Поскольку устанавливаемая на подвижных объектах радиотехническая аппаратура имеет свой уникальный адрес, она может принимать только общие циркулярные сообщения и сообщения, адресованные только данному подвижному объекту в составе группы или индивидуально. Но при получении администратором информационной системы информации об угоне служебного автомобиля он может оперативно исключить адрес установленного на этом автомобиле оборудования из общего списка

адресов и предотвратить передачу данных на установленный в угнанном автомобиле компьютер. Передача циркулярных сообщений на период локализации ситуации с угоном служебного автомобиля также может быть временно прекращена, а доведение данных до остальных пользователей производится с использованием групповых и индивидуальных адресов.

Поскольку управление работой всей сети обмена данными строго централизовано и обеспечивается дистанционно с базовой станции, аппаратура на угнанном автомобиле может быть просто дистанционно отключена. Факт отключения радиомодема легко подтверждается, поскольку каждая переданная в его адрес команда, включая команду на отключение, автоматически контролируется и фиксируется. В этом случае передача циркулярных сообщений в радиосети обмена данными может беспрепятственно продолжаться.

В некоторых реально действующих автоматизированных системах оперативно-диспетчерского управления реализована специальная функция, обеспечивающая трансляцию ложных сообщений на компьютер в похищенном автомобиле, имитирующих реальный радиообмен, которая позволяет ввести похитителя в заблуждение и, в большинстве случаев, побудить его к выполнению действий, гарантирующих его задержание.

В современных системах, использующих навигационные средства, обеспечивается автоматическая передача диспетчеру данных о местоположении подвижного объекта. Таким образом, в случае угона служебного автомобиля администратор радиосети имеет возможность дистанционного его контролировать. Поскольку управление работой бортовой аппаратуры и передачей навигационной информации с подвижного объекта также производится дистанционно через базовую станцию, имеется возможность изменения режима ее работы в сторону увеличения интенсивности трансляции навигационных данных с борта угнанного автомобиля, что гарантирует задержание угонщика и возврат автомобиля.

#### **6. Технология параллельного декодирования/интеллектуального объединения радиосигналов как средство повышения пропускной способности, надёжности и живучести подвижных технологических радиосетей обмена данными**

Современные подвижные узкополосные технологические радиосети обмена данными строятся на специализированном оборудовании, позволяющем наряду с увеличением их пропускной способности поддерживать высокие характеристики надёжности и живучести. Функционирование таких радиосетей организуется, как правило, на базе IP-протокола, что обеспечивает их совместимость с любым программным обеспечением, поддерживающим этот протокол.

Использование IP-протокола стало возможным и целесообразным только после достижения достаточно высоких скоростей обмена данными в радиосети (выше 19,2 кбит/с<sup>4</sup>). Однако повышение скорости обмена связано с решением ряда технических задач. Известно, что увеличение скорости обмена данными требует дополнительных энергетических затрат. Расчеты и практические измерения показывают, что, при прочих равных, радиосеть обмена данными, работающая на скорости 19,2 кбитс, имеет рабочую зону примерно в четыре раза меньше, чем аналогичная радиосеть, работающая на скорости 4,8 кбитс, при одинаковом соотношении сигналшум. При удвоении скорости для обеспечения той же чувствительности необходимо увеличить мощность выходного сигнала на 3 дБ. Увеличение скорости обмена данными с 4,8 до 19,2 кбит/с приводит к минимально возможной потере чувствительности в 6 дБ или выходной мощности в четыре раза.

На практике потери составляют около 9 дБ, поскольку теоретический минимум потерь рассчитан для идеальных условий распространения сигнала. Компенсация потери в 9 дБ требует увеличения выходной мощности применяемой аппаратуры примерно в восемь раз или до 250 Вт для подвижного объекта и 800 Вт для базовой станции. Использование таких мощностей в реальных системах невозможно. Потери в 9 дБ относятся к стационарным системам. Значение этого параметра ещё более возрастает в подвижных системах, где более ощутимо влияние эффекта замирания в результате многолучевого распространения сигнала.

Взаимосвязь скорости обмена данными и соотношения сигналшум хорошо известна. Более 50 лет назад она была описана теоремой Шэннона, а приведенный выше вывод подтверждается расчетами, выполненными по следующей формуле:

$$C = BW \log_2 (1 + S/N)$$

где:

$C$  — пропускная способность канала (в бодах);

$BW$  — ширина канала (Гц);

$S/N$  — соотношение сигналшум.

Даже не выполняя операцию с логарифмами, можно легко заметить, что если соотношение сигналшум равно 1, пропускная способность канала равна  $BW$ , а если соотношение сигналшум равно 3, то пропускная способность канала равна  $2BW$  или удваивается. Другими словами, при увеличении соотношения сигналшум увеличивается пропускная способность канала передачи данных. И наоборот, при уменьшении соотношения сигналшум пропускная способность канала уменьшается.

Отношение энергетических затрат на бит данных в зависимости от уровня шума можно определить по следующей формуле:

$$E_b/N_0 = (S/N) (W/R)$$

где:

$E_b/N_0$  — отношение энергетических затрат на бит данных в зависимости от уровня шума;

$S/N$  — соотношение сигналшум несущей частоты;

$W$  — ширина канала в Гц;

$R$  — скорость передачи в битах.

Для упрощения расчетов можно предположить, что величина  $S/N = 1$  и величина  $WR = 1$ . В этом случае значение  $E_b/N_0 = 1$ . Таким образом, при прочих равных, в случае удвоения скорости передачи  $R$  до  $2R$ , величина  $E_b/N_0$  будет равна 0,5. Переведя ее в дБ (мощность сигнала) получаем значение 3 дБ. Другими словами, на передаче одного бита данных теряются 3 дБ. Для достижения одинаковой производительности системы необходимо увеличить значение соотношения сигналшум на 3 дБ, либо увеличить ширину канала до  $2W$ , то есть удвоить ее.

Если величина  $E_b/N_0$  не увеличивается, то это приводит к возрастанию вероятных ошибок при передаче. Для обеспечения заданного числа минимальных вероятных ошибок в случае увеличения скорости передачи необходимо увеличить ширину канала или мощность сигнала, либо обоих параметров

одновременно.

Поскольку ширина канала является величиной постоянной, единственным способом добиться необходимого значения вероятных ошибок при передаче является увеличение соотношения сигнал/шум. В этом случае для компенсации потерь, например, в 8 дБ теоретически необходимо увеличить мощность сигнала в 6,3 раза, то есть, если в системе со скоростью обмена данными 4,8 кбит/с удовлетворительная работа обеспечивается при использовании передатчика мощностью 25 Вт, то для работы с такой же достоверностью доведения данных на скорости 19,2 кбит/с потребуется передатчик мощностью более 150 Вт.

Как следует из представленных выше расчетов, увеличение мощности передатчика не может считаться эффективным решением. Одним из достаточно простых решений является увеличение количества базовых станций при уменьшении оперативной зоны каждой из них (как это делается в сотовой связи). В этом случае потери мощности сигнала при передаче снижаются, поскольку мобильные пользователи находятся на более близком расстоянии от базовой станции. При этом для рассмотренного выше варианта, в котором потери мощности сигнала составляют 8-9 дБ, число базовых станций, которые смогут обеспечить работу в заданной зоне на скорости 19,2 кбит/с, должно быть увеличено в четыре раза по сравнению с аналогичной системой, работающей на скорости 4,8 кбит/с.

Как правило, владелец технологической радиосети обмена данными имеет ограниченные возможности по расширению базовой инфраструктуры, которая связана, в частности, с дополнительными затратами на обеспечение безопасности системы и увеличением эксплуатационных затрат. В связи с этим в современных технологических радиосетях применяется специализированное оборудование, реализующее методы работы и алгоритмы обработки сигналов, позволяющие сохранить приемлемые размеры оперативной зоны базовой станции при наращивании скорости обмена данными.

Наряду с сокращением оперативной зоны базовой станции возрастает количество ошибок при передаче, которые обусловлены замираниями сигнала при многолучевом распространении в результате того, что радиоволны достигают приемной антенны, проходя путь различной длины. Одни сигналы приходят в точку приёма по прямой, другие — многократно отражаясь от местных предметов (зданий, складов местности, автомобилей и т.д.). Такая ситуация наиболее типична для крупных городов.

Замирание сигнала возникает в результате того, что различные радиосигналы, проходя различное расстояние и достигая приемной антенны в различное время, усиливают или, наоборот, подавляют друг друга. Обычно подавление сигнала составляет 30 дБ (то есть коэффициент подавления составляет 1000).

Любой пользователь сотового телефона испытывал отрицательное воздействие замирания сигнала на качество связи. Изменение положения сотового телефона всего на несколько десятков сантиметров может очень сильно влиять на качество принимаемого сигнала. Обмен данными подвержен более серьезному влиянию затухания по сравнению с речевым обменом.

В определенной степени влияние затухания сигнала может быть компенсировано за счет восстановления потерянных во время передачи данных. Оно производится за счет использования избыточных данных, добавляемых к исходному сообщению перед его передачей. Эта технология, получившая наименование «коррекция ошибки» (FEC — Forward Error Correction), основывается на том, что лучше пожертвовать частью пропускной способности радиоканала и передать сообщение увеличенного объёма, чем повторно передавать сообщение полностью (в последнем случае потери пропускной способности радиосети и задержки в доставке данных будут значительно выше).

Как и любая другая, технология коррекция ошибки имеет свои ограничения. На определенном этапе объём избыточных данных, необходимых для надежной передачи сообщения, приводит к заметному снижению эффективности работы радиосети и увеличению накладных расходов, поскольку наиболее мощные алгоритмы коррекции ошибок требуют увеличения объёма исходного сообщения в два раза.

С увеличением скорости обмена возрастает и объём избыточных данных, необходимых для восстановления переданного сообщения, поскольку удвоение скорости обмена данными приводит к увеличению в два раза потерь в результате затухания. Таким образом, при увеличении скорости обмена данными в два раза (например, с 9,6 до 19,2 кбит/с) для компенсации этого эффекта необходимо увеличить объём избыточных данных в четыре раза. В случае применения IP-протокола объём передаваемых в радиосети данных существенно увеличивается за счет служебной информации, связанной с использованием самого протокола. Все это ведет к заметному снижению эффективности радиоканала с точки зрения его пропускной способности.

Связанные с наращиванием скорости обмена данными технические проблемы получили решение в современных образцах радиомодемов, использующих технологию «параллельного декодирования/интеллектуального объединения» радиосигналов (Parallel Decoding/Smart Combining). Такие радиомодемы обеспечивают устойчивую работу на скоростях 64 кбит/с в радиосетях с шагом сетки радиочастот 25 кГц и 128 кбит/с — с шагом сетки радиочастот 50 кГц. Затухания радиосигнала возникают в определенных точках оперативной зоны базовой станции. На практике расположение таких точек определяется комбинацией сигналов, принимаемых в заданной точке оперативной зоны, и соотносится с длиной их волны. Если использовать два приемника с двумя разнесенными антеннами, то вероятность одновременного попадания двух антенн в точку затухания сигнала существенно снижается. Другими словами, если одна антенна попадет в зону затухания сигнала, вторая, как правило, будет находиться вне этой зоны.

Впервые данный принцип был реализован в радиомодемах ParagonPD/GeminiPD и получил дальнейшее развитие в радиомодемах ParagonG3/GeminiG3. Пространственное разнесение приемных антенн не является новым методом, но представляется чрезвычайно эффективным. Радиомодемы оснащены двумя приемниками с антеннами, позволяющими использовать данный принцип.

Пространственно разнесенный приём может быть реализован двумя способами. Наиболее известным и широко применяемым является разнесенная коммутация, при которой из двух поступающих от приемных антенн сигналов детектируется только наиболее мощный. Этот способ позволяет увеличить процент успешно принятых сообщений, но на этом его преимущества и заканчиваются.

Разработчики вышеуказанных радиомодемов создали и запатентован более совершенный способ, позволяющий использовать одновременно оба принимаемых сигнала. Одновременное использование двух потоков данных позволяет почти в два раза (реально — в 1,91) увеличить чувствительность приемника независимо от влияния эффекта затухания сигнала. Эта технология и получила наименование «параллельное декодирование/интеллектуальное объединение».

В результате одновременного приёма сигнала на две антенны появляется возможность их использования в различных комбинациях, а не просто выбора наиболее мощного из них. Разработанная компанией технология интеллектуального объединения сигналов позволяет применять различные алгоритмы обработки в зависимости от относительной мощности и тренда (тенденции изменения) параллельно

принятых сигналов. Например, если более мощный сигнал имеет тенденцию к ослаблению, предпочтение отдается менее мощному сигналу достаточной для использования мощности, который имеет тенденцию к усилению.

Практические результаты оценки эффективности технологии параллельного декодирования/интеллектуального объединения сигналов представлены в Таблице 1. Эти данные демонстрируют преимущества рассматриваемой технологии при сравнении с работой аналогичной радиоприемной системы, использующей одну антенну, в различных условиях приёма. Сравнение производилось для условий успешного приёма 99% сообщений длиной 800 бит каждое.

Таблица 1

Модель затухания	Один приемник	Два приемника (PD)	Разница
Стационарный приём	-110,7 дБм	-113,5 дБм	2,8 дБ
Городская застройка	-98,7 дБм	-108,2 дБм	9,5 дБ
Сельская местность	-99,5 дБм	-109,5 дБм	10 дБ
Пересеченная местность	-99,3 дБм	-108,5 дБм	9,2 дБ

Как видно из таблицы, радиомодемы, использующие технологию параллельного декодирования/интеллектуального объединения сигналов, позволяют улучшить параметры принимаемого сигнала практически на 10 дБ, что соответствует увеличению мощности передатчика базовой станции в аналогичной по своим характеристикам радиосети в 10 раз. Это обеспечивает расширение зоны уверенного приёма радиосигнала без использования дополнительных базовых станций. В случае когда необходимость расширения зоны электромагнитной доступности отсутствует, рассматриваемая технология позволяет серьезно увеличить надёжность радиосети и ее живучесть, поскольку обеспечивает увеличение процента корректно принимаемых с первой попытки сообщений, в том числе, в сложной помеховой обстановке. Сокращение количества повторно передаваемых сообщений приводит к существенному росту пропускной способности и сокращению времени реакции системы.

Размер оперативной зоны и количество повторно передаваемых сообщений оказывают серьезное влияние на пропускную способность. В случае возникновения необходимости повторной передачи сообщений в радиосети обмена данными, работающей на скорости 19,2 кбит/с, ее пропускная способность для отдельных видов данных (коротких сообщений) может сократиться в 10 раз.

Другим фактором, влияющим на снижение пропускной способности, является избыточная информация, необходимая для реализации функции коррекции ошибок. Нельзя считать корректным утверждения типа: «наш протокол использует алгоритм коррекции ошибки, имеющий 25% избыточности, поэтому пропускная способность в нашей радиосети составляет  $19,2 \times 0,75 = 14,4$  кбит/с». Несмотря на то, что такое утверждение в принципе соответствует действительности, но только частично.

Простые расчеты, подобные приведенному выше, игнорируют многие важные факторы, которые должны учитываться при оценке пропускной способности. К ним, в частности, относятся адресация, порядковые номера пакетов данных, алгоритмы обнаружения ошибки и подтверждения приёма сообщений. Все данные, которые добавляются к информационному сообщению не пользователем, а средствами системы (а не только избыточные данные, необходимые для реализации функции коррекции ошибки), являются непроизводительными (служебными) и отражаются на ее пропускной способности.

Не менее серьезное влияние на пропускную способность оказывает время «атаки» передатчика (набора передатчиком мощности, необходимой для начала передачи данных, РТТ — power to transmit), и стабилизации по частоте. Этот важный компонент «накладных расходов» очень часто недооценивается, поскольку он не оказывает серьезного влияния на работу речевых каналов связи, где процесс нажатия тангенты радиостанции и начала передачи речевого сообщения занимает не менее четверти секунды. В случае с обменом данными все обстоит иначе.

Для иллюстрации этого положения были проведены сравнительные испытания радиомодема Gemini (время «атаки» — менее 10 мс) и другого радиомодема с аналогичными параметрами, подключенного к серийно выпускаемой современной мобильной радиостанции одного из ведущих производителей оборудования этого класса (время «атаки» передатчика — 80 мс). В обоих случаях передавались одинаковые сообщения. В результате модель Gemini затратила на передачу 52 мс, а ее оппонент — 87 мс или на 40% больше. При скорости обмена данными 19,2 кбит/с это соответствует дополнительной пропускной способности, равной 7680 бит/с.

### **ВЫВОДЫ:**

Таким образом, в настоящее время подвижная технологическая радиосеть обмена данными УКВ-диапазона обладает всем комплексом характеристик, обеспечивающих ее эффективное применение для обслуживания работы Автоматизированных систем оперативно-диспетчерского управления подвижными дежурными силами служб общественной безопасности. Она позволяет решать комплекс проблем, обусловленных необходимостью сохранения размеров зоны уверенного приёма и поддержанием высокой пропускной способности при сохранении присущего радиосети данного типа достаточно высокого уровня надёжности и живучести.

Архитектурно такая радиосеть представляет собой группу базовых станций, установленных таким образом, чтобы охватить всю оперативную зону в территориальном образовании с учетом плотности размещения пользователей в населенных пунктах и на междугородных магистралях. Каждая базовая станция обслуживает группу подвижных объектов в закрепленной зоне, обеспечивая двусторонний обмен данными. Все базовые станции сопряжены с центральным компьютером, который также выполняет функции коммутации сообщений, передаваемых в радиосети обмена данными, и обеспечивает их автоматическое доведение до заданных адресатов. Переход подвижных пользователей из зоны действия одной базовой станцией в соседнюю производится по эстафете в автоматическом режиме.

Работа в составе радиосети осуществляется по IP-протоколу, специально оптимизированному для обслуживания подразделений служб общественной безопасности и предусматривающему возможность автоматической передачи данных о местоположении подвижных объектов при каждом сеансе связи. Радиосеть обеспечивает двусторонний обмен данными между стационарными пунктами управления и подвижными объектами (одним, группой или одновременно всеми), что позволяет организовать надёжное автоматизированное управление с гарантированным доведением команд диспетчера до подвижных средств и докладов с подвижных средств до соответствующих должностных лиц. Каждое сообщение в системе отправляется строго по заданному адресу и не может быть получено и использовано абонентом, не имеющим соответствующего права доступа к нему.

Каждый подключенный к системе подвижный объект имеет возможность послать запрос в адрес диспетчера или в любую удаленную базу данных, сопряженную с информационной системой любой службы общественной безопасности, и получить ответ на запрос в виде сообщения различной длины. Весь обмен данными контролируется автоматически центром коммутации сообщений. Работа радиосети обмена данными имеет жесткое централизованное управление.

---

## Сноски

1. Вопросы противодействия профессиональным средствам радиоэлектронной борьбы и радиоэлектронного подавления в настоящей статье не рассматриваются. ↩
2. **Хáкер** (от [англ. hack](#) - разрубать) — особый тип компьютерных специалистов. Компьютерные взломщики т.е. осуществляющие неправомерный доступ к компьютерам и информации. ↩
3. **Крэкер** ([англ. cracker](#)) - тип [компьютерного взломщика](#): человек, взламывающий системы защит информационных систем или создающий программные средства для взлома систем защит. Вне профессиональной среды применяется общий термин «[компьютерный взломщик](#)» или чаще «[хакер](#)», что также часто не является правильным. В абсолютном большинстве случаев «крэкер» не располагает исходным кодом программы, поэтому программа изучается связкой [дизассемблера](#) и [отладчика](#) с применением специальных [утилит](#). ↩
4. Далее в расчетах принимается скорость обмена данными, равная 19200 бит/с, как минимально целесообразная для организации обмена данными по IP-протоколу. ↩