**ДИПЛОМНАЯ РАБОТА**

**Тема: "Анализ систем безопасности, использующих GSM каналы"**

Исполнитель:

Руководитель:

Рецензент:

Содержание

Введение

1. Современное состояние систем безопасности

1.1 Тенденции развития систем безопасности с точки зрения использования различных каналов связи

1.2 Использование беспроводных каналов в системах охраны

1.3 Обзор существующих систем безопасности, использующих gsm каналы

2. Построение систем безопасности, использующих gsm каналы

2.1 Построения gsm канала

2.2 Принцип шифрования gsm канала

2.3 Функции gsm каналов, используемые системами безопасности

3. Анализ функционирования систем безопасности, использующих gsm каналы

3.1 Анализ помехоустойчивости и помехозащищённости gsm канала

3.2 Исследование скорости передачи данных и пропускной способности gsm канала

3.3 Анализ модели gsm канала по обеспечению требуемой зоны покрытия

3.4 Разработка рекомендаций по улучшению технических характеристик систем безопасности, использующих gsm каналы

4. Вопросы безопасности проведения работ по эксплуатации систем безопасности, использующих gsm каналы

Заключение

Список использованных источников

УТВЕРЖДАЮ

Начальник кафедры ТСБС

к. т. н., доцент, полковник милиции

"\_\_\_\_\_" 2009 г.

Задание на дипломную работу слушателю

1. Тема: "Анализ систем безопасности, использующих GSM каналы".

Утверждена приказом начальника ВИ МВД РФ

№ \_\_\_ от "\_\_\_ " \_\_\_\_\_\_\_\_\_\_ 200 \_\_ г.

2. Цель дипломного проекта (работы): Анализ функционирования существующих систем безопасности, использующих GSM каналы, и разработка рекомендаций по улучшению технических характеристик систем.

3. Срок сдачи дипломного проекта (работы): "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 2009 г.

4. Исходные данные к проекту (работе):

4.1 Системы безопасности, использующих GSM каналы в диапазоне 890-960 МГц (GSM-900).

4.2 Ширина полосы канала связи - 200 кГц, частотное разделение дуплексных каналов FDD с расстоянием между дуплексными каналами 45 МГц.

4.3 Модуляция сигнала - двоичная гауссова с минимальным частотным сдвигом (GSMK).

4.4 Анализ модели GSM канала по методике EUROCOST (модель Хата).

5. Перечень подлежащих разработке вопросов:

5.1. Обзор существующих систем безопасности, использующих GSM каналы.

5.2. Анализ помехоустойчивости и помехозащищённости GSM канала.

5.3. Исследование скорости передачи данных и пропускной способности GSM канала.

5.4. Анализ модели GSM канала по обеспечению требуемой зоны покрытия.

5.5. Разработка рекомендаций по улучшению технических характеристик систем безопасности, использующих GSM каналы.

5.5. Рассмотрение вопросов безопасности жизнедеятельности функционирования

систем безопасности, использующих GSM каналы.

6. Перечень обязательного графического материала:

6.1. Название дипломной работы, цель, основные задачи.

6.2. Перечень систем безопасности, использующих GSM каналы, основные технические характеристики, алгоритм работы систем.

6.3. Результаты анализа помехоустойчивости, помехозащищённости, скорости передачи, пропускной способности систем безопасности.

6.4. Рекомендации, выводы о проделанной работе.

Дата выдачи задания: "\_\_\_\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2009 г.

Задание выдал:

Руководитель к. т. н., доцент, полковник милиции

(ученая степень, звание, специальное звание)

Бабкин А.Н.

(подпись) (фамилия, инициалы)

Задание получил:

Слушатель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Аврамчук А.И.

(подпись) (фамилия, инициалы)

Аннотация

В дипломной работе проводится сравнение различных беспроводных технологий, детально рассмотрен принцип построения GSM-канала в системах охраны, GSM сравнивается с другими беспроводными технологиями.

Проведен обзор нескольких основных беспроводных систем охраны, на их примере был проведен анализ его использования в различных системах охраны. Проведен анализ функционирования систем безопасности, использующих GSM каналы, рассмотрены принцип шифрования, помехоустойчивость и помехозащищенность в GSM-канале.

Сформулированы несколько основных принципов и рекомендаций по использованию GSM-канала в системах охраны. Обозначены основные пути развития сетей GSM.

Представлен один из возможных вариантов расчета зоны покрытия отдельно взятой базовой станции.

Реферат

Дипломная работа содержит 82 страницы, 8 рисунков, 4 таблицы, 27 источников.

Ключевые слова: GSM (Global System for Mobile Communications), DTMF (Dual-Tone Multi-Frequency), ContactID, GPRS (General Packet Radio Service), EDGE (Enhanced Data rates for GSM Evolution), SMS, Voice, LAN/WAN, MSC (Mobile Switching Centre) BSS (Base Station System) ОМС (Operations and Maintenance Centre) MS (Mobile Stations), TCP/IP-соединение, помехоустойчивость, помехозащищенность, TDMA (Time Division Multiple Access).

Объектом анализа является применение GSM-канала в системах охраны.

Цель дипломной работы: анализ использования GSM-канала, разработка рекомендаций по их применению.

В данной дипломной работе были рассмотрены преимущества и недостатки использования GSM-канала в системах безопасности, возможные пути развития GSM технологий, проведено сравнение с другими каналами связи, возможность их взаимодействия.

На основании проведённого анализа были сформулированы основные принципы использования и рекомендации по применению GSM-канала в системах безопасности.

## Введение

В настоящее время рынок услуг и оборудования охранно-пожарной сигнализации стремительно растет. Однако до недавнего времени основным недостатком систем охранной и пожарной сигнализации (ОПС) было использование проводных телефонных линий. К основным недостаткам данных систем можно отнести неустойчивую работу городских телефонных линий, низкую физическую защищенность, отсутствие возможности охраны нетелефонизированных объектов (дачи, коттеджи и т.д.). Поэтому в качестве надежной альтернативы "проводным охранным системам" появилось новое направление или "радиоканальные охранные системы".

Преимущества радиоканальных охранных систем очевидны:

отсутствие зависимости от телефонной линии и качества работы сети;

простота монтажа;

возможность охраны любого объекта (в пределах зоны действия радиоканальной сети).

универсальность - из простых элементов можно построить сколь угодно сложную систему: высокая скорость монтажа и запуска в эксплуатацию, возможность оперативного изменения конфигурации, мобильность охранного пульта, возможность сосуществования нескольких пультов. Нет принципиальных ограничений для подключения в случае необходимости к существующей системе охраны.

Первоначально беспроводные системы не получили широкого распространения из-за низкой надежности (проводная связь в этом плане еще лет пять на зад была надежнее). Но в настоящее время появился широкий спектр различных дополнительны устройств, активно используются новые поколения беспроводных систем связи.

Повсеместное использование сотовых систем связи не могло не сказаться на системах охраны. Возможности, предоставляемые операторами сотовой связи все активнее используются в системах охраны. Также можно видеть, что GSM каналы связи еще не исчерпали лимит своего развития. На сегодняшний день беспроводные охранные системы на базе GSM получили широкое распространение благодаря их относительно невысокой стоимости и простоте установки и эксплуатации. Сотовая сеть стандарта GSM-900/1800 обеспечивает лучшее качество связи и уже развернута в большинстве городов России и стран СНГ.

Системы, использующие GSM-связь, позволяют осуществить охрану любых объектов, в том числе и нетелефонизированных. Использование GSM избавляет от необходимости развертывать свою сеть ретрансляторов - используются ретрансляторы GSM-операторов. Вследствие этого можно брать под охрану объект везде, где уверенно работает сеть GSM-оператора.

И, конечно, очень перспективным представляется использование новых протоколов и сетей 3G, специально предназначенных для корпоративных клиентов - виртуальные корпоративные сети передачи данных с имитостойкостью и защитой информации.

Однако существенным недостатком подобных систем является низкая помехозащищенность. Не секрет, что GSM-канал легко подавить, "GSM глушилки" находятся сегодня в свободной продаже, да и работа сети GSM не всегда отличается высокой стабильностью и может отказать в самый неподходящий момент. Хотя последние разработки позволяют полностью контролировать GSM-канал, оперативно менять частоты, что заметно повышает помехозащищенность

Оптимально использовать GSM-канал в качестве дублирующего или дополнительного к проводным или другим радиоканальным системам. Огромный плюс GSM-систем - возможность самим клиентом контролировать состояние объекта и управлять его охраной.

## 1. Современное состояние систем безопасности

## 1.1 Тенденции развития систем безопасности с точки зрения использования различных каналов связи

Сегодня в мировой практике охранных услуг определилась устойчивая тенденция на усиление роли технических средств. Тенденция эта не случайна: многочисленные исследования в области личной и имущественной безопасности показали, что широкое использование технических средств позволяет исключить либо свести к минимуму негативное влияние самого ненадежного звена в системе охраны - человека, которому присущи утомляемость, невнимательность, халатность и т.п. При этом, организация охраны с помощью технических средств обходится потребителю значительно дешевле, а надежность ее выше. Более чем 50-летний опыт работы вневедомственной охраны МВД России в этой области показал, что наиболее эффективным и экономически выгодным видом является централизованная охрана. Суть ее в том, что информация от технических средств, установленных на территориально рассредоточенных объектах, поступает непосредственно на центральный пульт, где в автоматизированном режиме производится ее анализ, обобщение и выдача заявки на реагирование, в зависимости от ситуации, милицейскому наряду либо технической службе.

Техническую основу централизованной охраны составляют системы централизованного наблюдения (СЦН).

Наиболее широкое применение, как у нас, так и за рубежом нашли СЦН, использующие в качестве каналов связи телефонные линии. Это вполне объяснимо. Оборудование таких систем сравнительно дешево, а почти повсеместная телефонизация позволяет подключать к ним практически любые объекты. Учитывая, что практически с самого начала образования вневедомственная охрана России в рамках одной структуры обеспечивала одновременное решение трех основных функций: технической (охрана с помощью технических средств), милицейской (реагирование нарядами милиции) и страховой (возмещение материального ущерба), именно к технической составляющей всегда предъявлялись повышенные требования по надежности с целью снижения затрат по двум остальным.

В середине 90-х годов при создании СЦН основное внимание уделялось таким аспектам, как:

автоматизация, которая позволяет до минимума упростить процессы сдачи/взятия объектов под охрану, сократить дежурный персонал пультов централизованной охраны; существенно сократить количество ложных тревог из-за неправильных действий хозорганов;

контроль канала связи, обеспечивающий высокую достоверность передачи и исключающий потерю тревожной информации;

разработка широкой гаммы объектовых устройств с различными функциональными и сервисными возможностями, позволяющих удовлетворить потребности самых широких слоев населения.

С учетом этих требований были разработаны и внедрены такие системы, как "Ахтуба", "Юпитер", "Приток-А", "Фобос-А", "Фобос-3" и другие.

С точки зрения организации защиты объектов от несанкционированного проникновения (как по оборудованию техническими средствами охраны, так и по тактике действий дежурных служб) все перечисленные СЦН не имеют каких-либо существенных отличий, однако, каждая из них обладает своими достоинствами и недостатками, которые определяют и ограничивают область их применения.

Однако главным недостатком указанных систем является разнородность технических и конструктивных решений, а также закрытая архитектура построения, что не позволяет провести их объединение в единый универсальный комплекс технических средств централизованной охраны в пределах одного ПЦО. Это, в конечном, итоге приводит к возникновению определённых проблем для всех структур вневедомственной охраны во внедрении, эксплуатации, обслуживании и ремонте разнородных технических средств, в проведении единой технической политики, обеспечении должного уровня качества и надежности оборудования, а, следовательно, к дополнительным финансовым затратам и увеличению тарифов на охранные услуги.

Именно поэтому, наиболее актуальной остается на сегодняшний день проблема упорядочения парка эксплуатирующихся систем централизованного наблюдения, его обновления, замены устаревшего оборудования современным, более надежным. Именно поэтому, наиболее актуальной остается на сегодняшний день проблема упорядочения парка эксплуатирующихся систем централизованного наблюдения, его обновления, замены устаревшего оборудования современным, более надежным.

Поэтому в целях дальнейшего развития и совершенствования централизованной охраны к новым разработкам в последнее время предъявляются дополнительные требования:

имитостойкость и криптозащита, обеспечивающие устойчивость системы к несанкционированному "обходу" и обусловленные появлением "квалифицированных" краж;

высокая информативность, обеспечивающая разделение сигналов о проникновении и пожаре, аварии или изменении параметров линии связи и т.д.;

возможность сопряжения системы с оптоволоконными каналами связи, обусловленная внедрением предприятиями связи новых цифровых технологий передачи информации;

унификация создаваемых технических средств, т.е. возможность объединения различных устройств в единый программно-аппаратный комплекс централизованной охраны.

Приоритетной задачей технической политики в области развития централизованной охраны является разработка отсутствующих на сегодняшний день единых требований на системы централизованного наблюдения, что в условиях многообразия существующих и вновь появляющихся предприятий-разработчиков и производителей средств охранно-пожарной сигнализации позволит унифицировать стыки систем передачи извещений, как вновь разрабатываемых, так и уже находящихся в эксплуатации.

В последние годы особое внимание уделялось созданию и развитию радиосистем передачи извещений (РСПИ). внедрение охранных систем, использующих радиочастотные каналы связи, позволяет:

расширить сферу деятельности подразделений вневедомственной охраны путем организации охраны объектов, не имеющих линии телефонной связи;

повысить надежность систем охраны особо важных объектов за счет дублирования телефонных каналов связи;

обеспечить при необходимости срочную установку оборудования на объекте, нуждающемся в охране.

Деятельность НИЦ "Охрана" в данной области была направлена на удешевление оборудования радиосистем, с целью повышения его доступности для населения.

В тоже время качество систем, как в отношении потребительских свойств, так и в отношении надежности и защищенности передаваемой информации, должно постоянно повышаться.

С этой целью перспективным направлением является создание радиосистемы ближнего радиуса действия со сниженной стоимостью объектового оборудования и улучшенными тактико-техническими, стоимостными и эксплуатационными параметрами, позволяющей организовать охрану таких объектов как гаражные и дачные кооперативы, садоводческие товарищества и т.п.

Преимущества радиоканальных охранных систем очевидны:

отсутствие зависимости от телефонной линии и качества работы сети;

простота монтажа;

возможность охраны любого объекта (в пределах зоны действия радиоканальной сети).

На сегодняшний день все беспроводные системы можно разделить на четыре группы:

GSM системы;

радиканальные системы малого радиуса действия;

радиоканальные системы большого радиуса действия;

спутниковые системы.

GSM-системы получили широкое распространение в начале XXI века после бурного развития мобильной связи. Вначале в качестве каналообразующего оборудования использовались мобильные телефоны, которые подключались к охранным панелям через интерфейс RS-232 и управлялись AT-командами. Данное решение было очень ненадежным, так как телефоны могли зависнуть или просто отключиться, кроме того, условия эксплуатации мобильных телефонов не предусматривали работу в сырых и неотапливаемых помещениях, что существенно ограничивало область их применения. Сегодня, производители оборудования мобильной связи выпускают специализированные GSM-модемы (M2M-решения) для построения на их основе беспроводных систем безопасности. Данное решение существенно повысило надежность работы системы, а также предоставило разработчикам систем безопасности дополнительные возможности по работе с сервисами GSM. В качестве способа передачи информации в GSM-системах используются SMS-сообщения, модемное соединение (CSD), передача тоновых посылок (режим DTMF) и режим пакетной передачи сообщений GPRS. Появление режима GPRS позволило существенно снизить затраты на эксплуатацию систем радиоохраны. На сегодняшний день беспроводные охранные системы на базе GSM получили широкое распространение благодаря их относительно невысокой стоимости и простоте установки и эксплуатации. Однако существенным недостатком подобных систем является низкая помехозащищенность. Не секрет, что GSM-канал легко подавить, "GSM глушилки" находятся сегодня в свободной продаже, да и работа сети GSM не всегда отличается высокой стабильностью и может отказать в самый неподходящий момент. Указанные недостатки ограничивают применение оборудования подобного класса при построении систем безопасности. Данные системы в большей степени применяются в качестве резервных (дополнительных) каналов связи или для построения систем мониторинга удаленных объектов для сбора телеметрической информации.

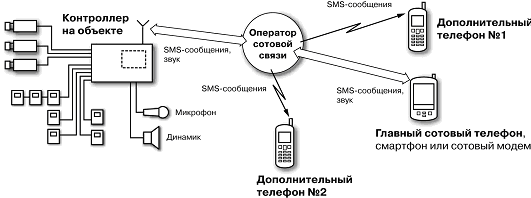


Рис.1 Схема передачи информации в GSM охранной системе при использовании функции SMS.

GSM охранная система может включать в себя один или несколько GSM контроллеров серии TSS-705, а также средства контроля и управления этими GSM контроллерами - сотовые телефоны и (или) компьютеры.

GSM контроллеры устанавливаются на удаленных объектах. К каждому из них можно подключать:

Различные дискретные и резистивные датчики. Например, контактные датчики, герконы, терморезисторы для контроля температуры, датчики охранной и пожарной сигнализации и т.п.;

Видеокамеры (до 3 цветных или черно-белых видеокамер (PAL или NTSC) на один контроллер);

Микрофон и звуковой динамик;

Исполнительные устройства (контроллер имеет 3 реле для управления такими устройствами);

Кнопки для установки датчиков на охрану непосредственно на объекте;

Кнопки и (или) считыватель кода различных идентификаторов (карт, брелоков) для снятия датчиков с охраны;

Примеры систем: РСПИ "Риф Стринг-202", "стрелец", "дельта".

К радиоканальным системам малого радиуса действия относятся беспроводные системы, работающие в частотном диапазоне (433 МГц и 2,4 ГГц) с малой выходной мощностью (10 мВт и 100 мВт соответственно).

В основном данные системы применяются для организации локальной беспроводной связи на территории крупных объектов. Радиус действия таких систем составляет обычно от нескольких сотен метров до нескольких километров в зависимости от условий распространения радиосигнала. При этом пункт централизованного наблюдения (ПЦН) обычно располагается на этом же объекте, либо организуется специальный выделенный канал связи для передачи информации на удаленный ПЦН. В настоящее время данные системы получили широкое распространения благодаря их относительно низкой стоимости и простоте монтажа. На сегодняшний день все больше и больше популярны приемопередатчики стандарта 2,4 ГГц, такие как ZigBee, NanoNet и др. Данные передатчики выпускаются в однокристальном исполнении с поддержкой стека высокоуровневых протоколов, что, безусловно, упрощает разработку систем беспроводной связи на их основе и дает разработчикам широкие возможности по реализации алгоритмов обмена данными. Недостатком данных систем являются их низкая помехозащищенность и малый радиус действия.

К радиоканальным системам большого радиуса действия. относятся системы, имеющие выделенный радиоканал и обеспечивающие радиус действия 20-100 км в условиях городской застройки. В состав данных систем входят абонентское оборудование, ретрансляторы (базовые станции) и пульт централизованного наблюдения. В большинстве своем системы данного класса используют частотный диапазон 146-174 МГц и выходную мощность 1-10 Вт. С точки зрения организации радиоинтерфейса системы можно разбить на две группы.

Системы, использующие стандартные УКВ-радиоинтерфейсы. Такие системы, как правило, используют частотную манипуляцию и ширину канала 12,5 или 25 кГц. Недостатком таких систем является низкая пропускная способность и невысокая помехозащищенность, так как сигнал с полосой 12,5 кГц легко подавить.

Системы, использующие специализированные радиоинтерфейсы используют радиоинтерфейсы, адаптированные под решение задач радиоохраны и обеспечивающие защиту информации и высокую помехозащищенность канала связи. Примером такой системы является радиоканальная система АРКАН, использующая для передачи узкополосные сигналы и алгоритм "прыгающих частот". Перестройка частоты происходит по случайному закону в широкой полосе (300-500 кГц). Данное решение обеспечивает высокую помехозащищенность и высокую емкость системы. К недостаткам радиоканальных систем большого радиуса действия можно отнести высокую стоимость инсталляции сети, однако при большом количестве абонентов эти затраты окупаемы. Данные системы широко применяются в средних и крупных городах на ПЦН с абонентской базой свыше 2000-3000 абонентов.

Спутниковые системы используют в качестве каналов связи спутниковую связь ("ГлобалСтар", "Инмарсат", "Турайя"). Подобные системы применятся для контроля/охраны удаленных объектов, в местах, где отсутствует мобильная и проводная связь. Главным недостатком этих систем является высокая стоимость как абонентского оборудования, так и затрат на эксплуатацию. С другой стороны, для решения задач охраны удаленных одиночных объектов данные системы не имеют другой альтернативы. С точки зрения вопросов сопряжения ОПС и каналообразующего оборудования существует три решения: ОПС со встроенным радиоканальным оборудованием Данное решение простое и недорогое, в одном корпусе вы получаете и охранную панель с источником бесперебойного питания, и радиоканал. Недостатком данного решения является небольшое количество охраняемых зон, как правило, их не большее 4-8. Но для небольших объектов это вполне приемлемое и очень экономичное решение.

ОПС с внешним радиоканальным оборудованием, подключаемым через специализированный интерфейс. Системы данного типа обычно предлагают производители, имеющие широкую линейку систем ОПС и различные типы каналообразующего оборудования. Поэтому пользователь может в зависимости от конкретной задачи определить для себя состав проектируемой системы ОПС и собрать "конструктор" из необходимых компонентов. Как привило, данные системы используют шинные интерфейсы связи между узлами (например, RS-485). Преимущество данного подхода заключается в гибкости проектирования ОПС. В зависимости от задачи вы можете выбирать контрольную панель с необходимым количеством охранных зон, использовать радиоканал или проводную связь, при этом все оборудование будет унифицировано, иметь единую логику работы и единые протоколы обмены. Недостатком данного решения является то, что вы не сможете использовать оборудование разных производителей, а это не всегда удобно, например, в случае если вы собираетесь использовать системы ОПС одного производителя и радиоканал другого.

ОПС с внешним радиоканальным оборудованием, подключаемым через стандартный интерфейс. Данный подход решает проблему, описанную выше. Используя стандартный интерфейс, можно использовать оборудование разных производителей. Однако на сегодняшний день производители оборудования не стремятся разработать единый стандарт, наоборот - используют свои закрытые протоколы. Единственным открытым стандартом сегодня является интерфейс Contact ID, разработанный компанией ADEMCO и предназначенный для передачи сообщений по телефонным линиям в режиме тоновых посылок DTMF. Большинство контрольных панелей имеют данный интерфейс. Поэтому единственным решением для производителей каналообразующего оборудования для охранных систем было реализовать внутри своих устройств декодер ContactID. Данные решения сегодня широко применяются и в GSM-модемах, и радиоканальных системах. Пользователь, в свою очередь, может выбирать, какой канал связи использовать: проводной или беспроводной, при этом оборудование ОПС перемонтировать и перенастраивать не нужно, просто выход ContactID подключается либо к телефонной линии, либо на вход радиопередатчика.

Одной из самых быстроразвивающихся беспроводных технологий является ZigBee, который изначально разрабатывалась как низкоскоростной канал связи для объединения в сеть различных датчиков. Применительно к безопасности это могут быть датчики охранной и пожарной сигнализации.

Возможно, причем в скором времени ZigBee потеснит многие из существующих сегодня радиоканальных ОПС. Ведь почти все они разработаны вне каких-либо стандартов. У каждого производителя - свои протоколы обмена, и заменить имеющиеся на объекте беспроводные датчики на оборудование другого производителя невозможно. Если стандарт ZigBee получит распространение, что вполне вероятно, то заказчик получит возможность использовать в системах ОПС практически любые датчики на выбор. Тем более что стандартные профили (спецификации наборов команд и протоколов обмена) для конкретных приложений в области автоматизации зданий и систем безопасности разработаны, опубликованы, и все это вместе взятое гарантирует совместимость оборудования разных производителей.

Этот стандарт, не побоюсь повториться, хорош для соединения центрального узла с периферией, которая размещается территориально распределенно, причем за счет включения в систему ретрансляторов территория покрытия может быть весьма большой. Теоретически можно использовать ZigBee и в СКУД. Но этот канал имеет небольшую скорость передачи данных и небольшую дальность. Согласитесь, нерационально строить длинную цепочку ретрансляторов ради соединения контроллера с компьютером. Есть много более простых, а главное, дешевых и надежных способов.

Можно сказать, что все перечисленные технологии на сегодняшний день активно развиваются и широко применяются для решения задач охраны стационарных объектов. Выбор той или иной беспроводной системы определяется в зависимости от типа объектов, их количества, требований к надежности доставки сообщений и удаленности объектов. В некоторых случаях для повышения надежности используется резервирование каналов связи. Можно сказать, что будущее за беспроводными технологиями и скоро они полностью вытеснят с рынка проводные охранные системы.

## 1.2 Использование беспроводных каналов в системах охраны

Системы видеонаблюдения.

Первыми в данной области появились электронные устройства, способные отдавать лишь текстовые SMS-сообщения с охраняемого объекта. Такое устройство состояло из электрического блока, к которому можно было подключить 1-4 внешних датчика или шлейф охранной сигнализации и обычного мобильного телефона. Устройство можно было установить на всяком объекте, имеющем устойчивый прием GSM-сети. Принцип работы устройства основан на оповещении пользователя с помощью текстового SMS-сообщения, которое передавалось на мобильный телефон пользователя чрез GSM-канал в случае срабатывания охранного датчика или нарушения целостности шлейфа охранной сигнализации. Подобные устройства спешно завоевали популярность посреди хозяев небольших загородных домов и коттеджей невысокой ценой и простотой установки. В качестве ответной меры владелец подобного устройства при получении SMS-сообщения несложно перезванивал на мобильный телефон соседа или местного сторожа, тот, что в свою очередность, шел к дому и выяснял причины срабатывания. При всем при том сходные устройства имели и существенные недостатки, не разрешено было отличить неправильное срабатывание от тревожного без участия человека, а при тревожном событии нередко не разрешено было его предотвратить, При этом, при сильной загрузке сотовой сети SMS-извещение могло быть доставлено с опозданием от нескольких минут до нескольких часов, что делало данную систему ненужной. Современные системы видеонаблюдения по GSM как правило выполняют следующие функции: взаимодействие пользователя с устройством для получения видеоизображения может производиться в всякое время; передача видеоизображения от 1-4 телекамер в реальном времени (задержка от начала события вплоть до отображения на приемном мониторе не более 1-2 сек); автоматический дозвон вплоть до пользователя по срабатыванию встроенного детектора движения и/или вешнего датчика; автоматическая запись фото и видеоинформации во встроенную память устройства; запись принимаемой фото и видеоинформации на жесткий диск компьютера; подключение внешнего охранного датчика или шлейфа к тревожному входу устройства; подключение исполнительного устройства к релейному выходу устройства и прямое управление им по каналу связи.

Применение систем удаленного видеонаблюдения по GSM вероятно на удаленных объектах, где отсутствуют проводные каналы связи: загородные дома, дачи, склады, автостоянки, гаражи, автозаправочные станции, железнодорожные переезды. Для удаленного видеоконтроля за коммуникациями: водо-, газо- и нефтепроводы, электростанции, раздельно стоящие подстанции, вышки и тому подобное. Несмотря на кажущуюся сложность устройств видеонаблюдения по GSM, они остаются просты в подключении и комфортны в эксплуатации. Уже не требуется использование на передающей стороне мобильного телефона, GSM-модуль встроен прямо в остов прибора. Электропитание осуществляется от источника постоянного тока с широким диапазоном напряжений 8-15В или от электросети 220В.

Альтернативой GSM-каналу являются беспроводные сети WLAN (Wireless Local Area Network - беспроводная локальная сеть). Сеть WLAN - вид локальной вычислительной сети (LAN), использующий для связи и передачи данных между узлами высокочастотные радиоволны, а не кабельные соединения.

Пользовательские устройства можно интегрировать в сеть, установив на них беспроводные сетевые адаптеры. Для обеспечения беспроводным пользователям доступа к уже существующей сети Ethernet нужно установить беспроводную точку доступа. Наиболее важный элемент беспроводных сетей - беспроводная точка доступа (англ. Wireless Access Point)

Точки доступа призваны выполнять самые разнообразные функции, как для подключения группы компьютеров (каждый с беспроводным сетевым адаптером) в самостоятельные сети, так и для выполнения функции моста между беспроводными и кабельными участками сети. Такие совмещённые сети называются Инфраструктурой (Infrastructure) и используются для доступа к центральным базам данных или беспроводного подключения мобильных пользователей.

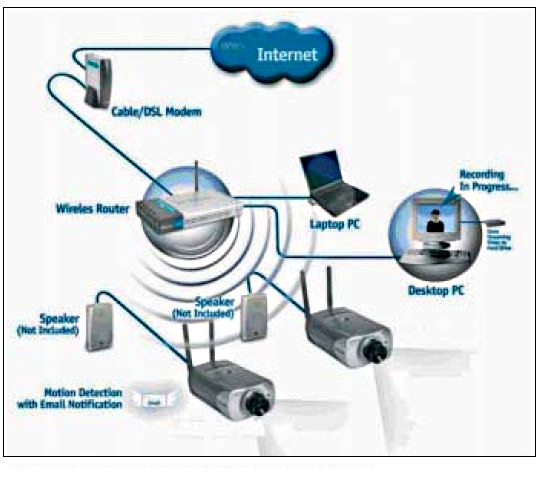


Рис.2. Схема построение видеосистемы на WI-FI

Cтандарт Wi-Fi (англ. Wireless Fidelity - "беспроводная точность", по аналогии с Hi-Fi - стандарт на оборудование Wireless LAN). При использовании современных потоковых алгоритмов сжатия скорости 0,5 Мбит/с этого вполне достаточно для передачи одного канала видео приличного качества. Также это расстояние можно увеличивать с помощью направленных антенн и промежуточных точек доступа.

Защита видеоинформации в беспроводных IР-системах видеонаблюдения достигается несколькими способами. Ключевыми среди них являются: применение брандмауэров, использование паролей и шифрование. Брандмауэр работает как электронные "ворота", пропускающие зарегистрированных пользователей и запрещающие доступ неавторизованным лицам. Применение паролей позволяет не только ограничить доступ к системе видеонаблюдения, но и распределить права доступа персонала к определенным видеокамерам. А при шифровании попытки перехвата зашифрованных данных в IP-системе охранного видеонаблюдения становятся бессмысленными, если злоумышленник не знает уникального кода для расшифровки потока данных. Код, в свою очередь, устанавливается системным администратором.

GPS мониторинг транспорта.

Спутниковый мониторинг транспорта - система спутникового мониторинга и управления подвижными объектами, построенная на основе использования современных систем спутниковой навигации (GPS/ГЛОНАСС), оборудования и технологий связи (GSM/УКВ), вычислительной техники и цифровых карт. GPS мониторинг транспорта - технология, применяемая в диспетчерских службах на транспорте, а также для решения задач транспортной логистики в системах управления перевозками (англ. TMS *-* Transportation management system) и автоматизированных системах управления автопарком (англ. FMS - Fleet Management System) для контроля фактических маршрутов транспортных средств при помощи системы GPS.

Автотрекер - прибор, устанавливаемый на автомобиль с целью отслеживания его дальнейшего перемещения и контроля его местоположения.

Обычно автотрекер определяет своё местоположение принимая сигналы ГЛОНАСС/GPS и отправляя их посредством мобильного интернет канала GPRS на сервер в интернете, на котором владелец прибора наблюдает его перемещения. Почти все современные (2008-2009 гг.) приборы, работающие на этом принципе, могут принимать входящие звонки.

Для решения задач мониторинга используются следующие компоненты системы:

спутниковые системы навигации (GPS - США, ГЛОНАСС - РФ),

приёмники GPS и/или ГЛОНАСС,

системы связи с центральным пунктом (космическая /GSM / УКВ) и/или система локального накопления данных.

Иногда дополнительно используются дополнительные датчики, установленные на самом техническом средстве: текущий запас топлива, факт открывания двери или капота, факт наличия пассажира (такси), температура в рефрижераторе, факт работы или простоя спецмеханизмов (поворот стрелы крана, работы бетоносмесителя), факт нажатия тревожной кнопки и т.п.

Полученные данные могут либо накапливаться в локальном устройстве и затем переноситься в центральную базу по возвращении в парк, либо передаваться на центральный сервер в режиме реального времени.

Системы GPS мониторинга транспорта решают следующие задачи:

мониторинг включает отслеживание текущих координат, направления и скорости движения транспортного средства в реальном времени для нужд диспетчерских служб. В некоторых системах также возможна установка дополнительных датчиков на открытие дверей, включение/выключение исполнительных механизмов спецтехники, топливных датчиков, датчиков для измерения температуры в рефрижераторе и пр. Некоторые системы допускают подключение к бортовому компьютеру автомобиля (через CAN-шину) и удалённое чтение параметров эксплуатации транспортного средства.

учёт пройденного километража и расхода топлива нужен для своевременного прохода ТО, обоснования списания ГСМ бухгалтерией и пр. В системах TMS с помощью GPS производится автоматический учёт доставки грузов в заданные точки.

контроль соответствия фактического маршрута автомобиля плановому позволяет повысить дисциплину водителей. В России, в отличие от развитых стран, эта функция крайне востребована для пресечения несанкционированного использования служебных транспортных средств наёмными водителями в целях личного обогащения, а также для пресечения несанкционированного слива топлива. По оценкам журнала "Логистика", только за счёт повышения дисциплины водителей в российских условиях системы GSM мониторинга окупаются за несколько месяцев.

безопасность: знание координат позволяет быстро найти угнанное либо попавшее в беду транспортное средство. Дополнительно автомобили могут оборудоваться скрытой кнопкой, нажатие либо ненажатие на которую отсылает тревожный сигнал в диспетчерский центр. Кроме этого, некоторые терминалы GPS мониторинга могут работать в режиме GSM-сигнализации, то есть звонить на заданный телефонный номер в случае срабатывания штатной сигнализации.

Типичная система GPS мониторинга состоит из трёх звеньев: терминалов, устанавливаемых на автомобили, сервера и клиентских рабочих мест. Терминалы представляют собой специализированные GPS-трекер, содержащие модуль собственно GPS и модуль сотовой связи (GSM или CDMA). Функции сервера может выполнять обычный ПК с установленным серверным ПО. В отличие от рабочих мест, сервер должен быть всегда включён, так как именно на нём накапливаются данные о маршрутах. Клиентское ПО в редких случаях может быть объединено в одну программу с серверной частью, но как правило допускается одновременное подключение нескольких рабочих мест к одному серверу.

В зависимости от применяемых технических решений можно выделить пять поколений систем GPS мониторинга транспорта:

самые первые системы были оффлайновыми, то есть не позволяли осуществлять мониторинг в реальном времени. GPS-трекер записывал все данные в память и передавал их на сервер по прибытии транспортного средства на базу через проводной или беспроводной интерфейс. Такая схема позволяла контролировать маршрут автомобиля только постфактум и не способна помочь, например, при угоне автомобиля.

во втором поколении для организации связи между GPS-терминалами и сервером использовались SMS либо механизм CSD. На сервер устанавливались один или несколько модулей сотовой связи, позволяющие принимать SMS или звонки с данными. Подобные системы отличались огромными платежами за мобильную связь и очень большим периодом времени между измерениями координат. С массовым распространением мобильного интернета системы второго поколения практически вымерли.

в третьем поколении в качестве транспортной сети используются GPRS или EV-DO, что позволяет на порядок снизить расходы на мобильную связь и резко улучшить точность прорисовки маршрутов. Сервер в таких системах устанавливается непосредственно у клиента и подключается к интернет и к локальной сети офиса. На сервер и на рабочие места пользователей устанавливается специализированное программное обеспечение. В некоторых системах допускается аренда портов сервера, предоставляемого поставщиком. На данный момент это самая распространённая схема мониторинга.

системы четвёртого поколения также использует один из механизмов мобильного интернет в качестве транспортной системы, но отличаются от третьего использованием веб-технологий. В этом случае сервер размещается у компании-поставщика, его мощности делятся между многими клиентами, а защищённый доступ к данным осуществляется через Web-страницу с любого компьютера, подключенного к интернет. Так как один сервер способен работать одновременно с тысячами трекеров, резко снижается стоимость внедрения и обслуживания системы. Одновременно возрастает надёжность хранения и доступность данных, так как компании-операторы способны содержать многократно резервированное качественное серверное оборудование и штат технических специалистов для его круглосуточного обслуживания. Потенциальным недостатком систем четвёртого поколения является полная централизация - вероятность сбоя или наступления форс-мажорных обстоятельств в таких системах крайне низка, зато последствия сбоя могут стать весьма дорогостоящими для компании-оператора.

системы мониторинга пятого поколения представляют из себя глобальное развитие и централизацию систем предыдущего поколения в единый, распределенный центр мониторинга. В таком варианте данные от устройств собираются одним или несколькими коммуникационными серверами, стекаются на один основной сервер базы данных и растекаются между подключенными промежуточными серверами, которые уже обеспечивают взаимодействие с пользователем (веб-мониторинг) или выполняют фоновые задачи. При таком построении системы пользователи с разных районов, стран и даже континентов работают с наиболее близко расположенным региональным веб-сервером с минимальной задержкой (пингом) до него.

На данный момент на российском рынке представлено порядка 20 различных систем GPS мониторинга, как импортных, так и отечественных. Импортные решения, как правило, отличаются расширенной функциональностью, зато в отечественных лучше реализованы функции контроля за несанкционированным использованием автомобиля, лучше решён вопрос карт, а формы отчётов соответствуют российскому законодательству. Немаловажным в российских условиях фактором является также защита терминалов от противодействия водителей: наличие резервного аккумулятора, пломбирование устройств и прочие.

В качестве основного канала связи в профессиональных СКУД могут использоваться только те беспроводные технологии, которые эквивалентны по функционалу, назначению и стоимости стандартной проводной компьютерной сети предприятия, - это Wi-Fi, Wi-Max и аналогичные беспроводные сети.

Технологии сенсорных сетей типа ZigBee, Z-Wawe и многие аналогичные должны использоваться по своему прямому назначению - для получения информации от различных датчиков без прокладки проводов на ограниченной (локальной) территории. Такая привлекательная сеть, как GSM, может использоваться либо в домашних системах, либо как дополнительный канал удаленного доступа к серверу СКУД для получения отчетов и аналогичных действий.

## 1.3 Обзор существующих систем безопасности, использующих gsm каналы

Радиосистема ""Стрелец".

Радиосистема "Стрелец" - одна из первых отечественных радиосистем, предназначена для организации охранно-пожарной и адресно-аналоговой пожарной сигнализации на объектах не только частного, но и общественного пользования, где по различным причинам (сохранение целостности интерьера, непрерывная эксплуатация помещений и т.д.) применение проводных систем невозможно или ограничено.

Особенности системы:

двухсторонний протокол обмена между всеми радиоустройствами Аргус-Диалог;

10 радиочастотных каналов передачи (с автоматическим и ручным выбором);

автоматический выбор резервного канала передачи (свободного от помех);

разнесенный радиоприем;

до 400 радиоустройств, находящихся в зоне взаимной радиовидимости на одном радиочастотном канале передачи.

возможность построения полноценной адресной пожарной радиосистемы.

программируемый период передачи контрольных радиосигналов от 12 с до 2 мин.

криптографическая защита сигналов с механизмом динамической аутентификации.

микросотовая топология системы.

Емкость системы:

до 16 радиорасширителей

до 512 радиоизвещателей (до 32 извещателей на каждый радиорасширитель)

до 256 радиоканальных исполнительных устройств, сирен, брелков и пультов управления (до 16 устройств на каждый радиорасширитель).

Дальность:

до 600 м в пределах микросоты

до 1000 м между микросотами

до 6000 м - 5 участков ретрансляции.

Продолжительность работы радиоизвещателей:

от основной батареи: от 3 (период передачи контрольных радиосигналов 12 с) до 7,5 лет (период передачи контрольных радиосигналов 2 мин);

от резервной батареи: не менее 2 месяцев.

Система имеет два диапазона рабочих частот: 433 МГц или 868 МГц

Предусмотрена интеграция радиосистемы СТРЕЛЕЦ® с беспроводной системой "Орфей-Р". Для построения полноценной системы охраны существует возможность интеграции радиосистемы Стрелец с известной системой видеонаблюдения "ВидеоИнтеллект" (ITV, Москва). Для передачи извещений с объектов на централизованные пульты охраны, в том числе и ЧОП, предусмотрена совместная работа радиосистемы Стрелец с популярными СПИ "Андромеда" ("Синорд", Санкт-Петербург), "Мираж" ("Стелс", Томск).

Также существует возможность интеграции радиосистемы СТРЕЛЕЦ® с системой контроля и управления доступом (СКУД)"Кронверк" ("СКД", Санкт-Петербург) и аппаратно-программным комплексом "Бастион" ("Электронные системы", Самара).

Микросотовая структура радиосистемы Стрелец позволяет связать в единую систему ОПС группу отдельно стоящих объектов, предоставив возможность как централизованного (с поста охраны), так и децентрализованного (на каждом объекте) контроля и управления системой. В сегодняшний день радиосистема Стрелец установлена и эксплуатируется в Государственном Музее "Эрмитаж", Государственной Третьяковской Галерее, Суздальском Музее деревянного зодчества, объектах Федеральной пограничной службы ФСБ, МВД и Министерства Обороны, а также во многих жилых, коммерческих и производственных помещениях РФ, стран Европы и СНГ.

Рассмотрим **РСПИ "Дельта".**

**РСПИ "Дельта" предназначена для обеспечения передачи информации с охраняемых удаленных объектов, их сбора, обработки и хранения на пультах централизованного наблюдения в масштабах предприятий, районов, городов, областей. Обеспечивается: пожарная, охранная, тревожная сигнализация, контроль доступа на охраняемые объекты, автоматический контроль состояния оборудования, контроль состояния и утечки химически опасных веществ, утечки воды, газа, телеметрия и т.д. Извещения, посылаемые объектовыми передатчиками, поступают на пульты централизованного наблюдения. Каждое принятое извещение декодируется и обрабатывается, после чего оператор может принять необходимые меры по привлечению сил быстрого реагирования. Предусмотрено дублирование по телефонным линиям и автоматическая отправка SMS сообщений.**

Принцип работы радиоканальной системы передачи извещений “Дельта" основан на использовании выделенного для этих целей радиочастотного ресурса для передачи сообщений с объектов, оборудованных радиопередатчиками, на пульт централизованного наблюдения, где происходит приeм сообщений, их обработка, отображение на мониторе диспетчера, который передает полученную информацию в соответствующие службы реагирования по специальным каналам связи.

Использование выделенного канала исключает зависимость системы от других операторов связи, а его эксплуатационная готовность обеспечивается государственной радиочастотной службой. К объектовому радиопередатчику может быть подключена любая периферия (охранная, тревожная, пожарная сигнализация, датчики утечки воды, газа, телеметрия и т.д.).

Конфигурация сети позволяет использовать информацию, необходимую для соответствующего реагирования таким структурам, как подразделения вневедомственной охраны МВД, ведомственная охрана, служба спасения, пожарная охрана, частные охранные предприятия, городские коммунальные службы, предприятия водоснабжения. электросети, теплосети и т.д.

**Основные характеристики:**

**Частотный диапазон 136-174 или 400-500 МГц.**

**Мощность передатчиков до 15Вт.**

**Дальность без ретрансляции 15 км.**

**До 30 ретрансляторов в системе.**

**Емкость системы 12000 объектов с использованием одной частот.**

**Состав системы:**

**пульты централизованного наблюдения, состоящие из: АФУ v антенно-фидерных устройств, базовых станций, ПК - персональных компьютеров с установленным ПО АРМ - программным обеспечением автоматизированного рабочего места операторов, оборудования энергонезависимого питания. Для автоматической отправки SMS сообщений используются специализированные GSM радиомодемы - "Дельта - GSM". Дублирование по телефонной линии обеспечивает "Дельта-Т".**

**объектовое оборудование состоящие из передатчиков с антеннами подключенных к извещателям непосредственно или к любым ПКП v приемно-контрольным приборам и оборудования энергонезависимого питания.**

**для расширения зоны радиоохраны могут использоваться ретрансляторы.**

**Основные отличительные особенности:**

**большая дальность обеспеченная высокой мощностью передатчиков - до 15 Вт и высокой чувствительностью приемного тракта - 0.25мкВ.**

**большая емкость, обеспеченная малой длительностью посылки - 0.125 секунды**

**передатчики выполняют функции объектовых ПКП.**

**применение высокоскоростного формата FSK передачи данных с проверкой контрольных сумм сообщений и алгоритм дублирования передаваемых сообщений с разнесенными по времени посылками в случайный временной интервал (5-8 секунд) придают системе высокую надежность при высокой емкости и информативности (до 256 параметров).**

**интервал тестовых сигналов может быть установлен от 1 минуты до 256 часов, что позволяет тестировать объекты с необходимым периодом в зависимости от емкости системы либо в зависимости от категории объектов.**

**одновременный мониторинг стационарных и мобильных объектов.**

**комплексное использование прямого радиоканала, телефонных каналов и GSM.**

**невысокая стоимость.**

**возможность построения системы от небольшого пульта с несколькими охраняемыми объектами до сети, включающей в себя большое количество центральных станций и ретрансляторов, в масштабах крупного города или области.**

Дельта" используют протоколы, подобные системе "PIMA" (Израиль) и "Informer 12000" (США), что позволило перенять более богатый опыт мировых лидеров и при этом иметь все преимущества отечественного производителя.

Рассмотрим в качестве примера "Орлан GSM 900/1800" ("Охрана и безопасность", Украина)

"Орлан" - комплекс технических средств и программного обеспечения для создания ПЦН за состоянием устройств пожарной и охранной сигнализации GSM с использованием сотовой сети GSM-900/1800 в голосовом режиме и режиме GPRS. Предназначен для приема кодированных сообщений, передаваемых радиокоммуникаторами серии "Лунь", и трансляции их на ПК для регистрации и обработки с помощью программного обеспечения "Феникс 2". Программное обеспечение поддерживает подключение к ПК цифровых приемников ПАКТ2 и DSC-SurGard для приема кодированных сообщений по телефонной линии от большинства охранно-пожарных панелей (Napco, Ademco, DSC и проч.). ПЦН "Орлан" обеспечивает прием сообщений от внешних устройств со звуковым и визуальным сопровождением, расшифровкой и обработкой, слежение и мгновенное изменение состояния объекта на ПЦН при приходе очередного сообщения. Предусмотрено до пяти функций удаленного управления объектовыми приборами операторами пульта, а также хранение и отображение информации в текстовом и графическом виде.

ПЦН ведет архивы принятых сообщений, поиск в архиве по различным критериям, печать и экспорт базы данных, архива событий. Имеется возможность разбивки объекта на группы и отслеживания информации отдельно по каждой группе, возможность задания расписания работы для каждой из групп. Резервное копирование и архивирование базы данных происходит автоматически. Дублирование. Все события с объекта дублируются на мобильный телефон хозяина в виде SMS (до 3 телефонов), на удаленный пульт "Феникс-мини" в виде SMS (до 3 пультов), а также по каналу GPRS. Имеется возможность перевода объекта, группы или отдельного шлейфа в режим постоянного или временного стенда. Проводятся анализ и построение графиков и отчетов о работе пульта за месяц. Информативность (виды извещений) - 256. Размер буфера памяти принятых событий - 32. Время готовности ПЦН к работе - не более 40 секунд. Время одного сеанса связи в голосовом режиме - не более 4 секунд. Время одного сеанса связи в в режиме GPRS - не более 1 секунды.

Централизованная база данных в формате Microsoft SQL Server 2000 с клиент-серверной архитектурой ПО, распределенный доступ к БД с различных ПК в сети. Протоколирование времени прибытия группы реагирования на объект. Индивидуальный интервал тестирования для каждого охранного прибора (от 15 мин). Регистрация операторов ПЦН.

Рассмотрим СПИ Андромеда.

СПИ Андромеда имеет пять каналов передачи информации: радио, телефонной линии, GSM (GPRS, SMS, Voice), LAN/WAN, возможность подключения до 8000 объектов, отображать на карте города объекты и группы быстрого реагирования в реальном времени. Множество полезных функций упрощают и автоматизируют работу операторов. Для работы по GSM-каналу применяется комплект объектовых устройств системы "Андромеда Hunter-Pro 96". Этот объектовый прибор имеет расширение до 96 зон и с возможностью передачи сигнала по всем каналам связи. Модуль сотовой связи GSM-200 обеспечивает передачу сообщений от контрольной панели на центральную станцию в голосовом канале и канале GPRS стандарта GSM.

В СПИ Андромеда решено взаимодействие с пультами производства компании "Альтоника" (системы LONTA®-202 и "Риф-Стринг"-200), а так же с пультами, имеющими на выходе открытые стандартные протоколы "Sur-Gard" (собственно пульты "Sur-Gard", пульт "Контакт-GSM", производства ООО "Ритм") и "Ademco 685" (например, LARS).

Для использования остальных современных каналов связи (Ethernet, GPRS) также вполне достаточно доработки используемого на ПЦН программного обеспечения.

В СПИ Андромеда также интегрирована система Стрелец при помощи преобразователя "СТЭЛС". Это самостоятельный прибор, обеспечивающий подключение до 16 РРОП, которые собирают информацию от датчиков и передают ее в центр мониторинга. Поскольку каждый РРОП может обслуживать до 32-х датчиков, получаем систему, которая позволяет передавать сообщения с объекта, оборудованного 512 различными беспроводными устройствами, входящими в состав системы Стрелец.

Станция мониторинга STAM-2 (Satel, Польша).

Станция мониторинга STAM-2 польской компании Satel состоит из программного обеспечения, основной платы для приема сообщений от ПКП и защитного аппаратного USB-ключа. При этом основную плату можно установить в любой свободный PCI-слот ПК, а c автономным источником питания возможна работа станции и без компьютера. Программа мониторинга существенно облегчает работу оператора системы ОПС, автоматически выбирая события, требующие его вмешательства, предоставляя список инструкций в каждой конкретной ситуации и напоминая о невыполненных задачах. STAM-2 может обслуживать более 50 000 абонентов, выводить на печать отчеты о действиях операторов системы ОПС, отчеты о системных событиях и автоматически отслеживать несанкционированное изменение системных файлов.

ПЦН STAM-2 поддерживает следующие способы обмена данными с ПКП: прием сигналов по телефонной линии, по IP-каналу, по сети GSM в виде SMS-сообщений и по радиоканалу при наличии радиостанции стандарта VISONIC. При этом подбор плат, устанавливаемых на ПК, зависит от выбранных способов передачи данных. В рамках одной станции мониторинга STAM-2 может работать до 16 соединенных между собой плат, что позволяет регулировать количество доступных телефонных линий и IP-адресов.

Система имеет модульный принцип построения. Один модуль "АРМ оператора ПЦН" позволяет подключить до 540 объектов. Можно организовать работу нескольких "АРМ оператора ПЦН". В качестве коммуникатора используются универсальный коммуникатор (GSM+ГТС) и IP-коммуникатор (IP-модем). По каналу GSM информация передается в цифровом формате DATA.

SMS-уведомление владельца объекта о доставке извещения на ПЦН и на сотовый телефон владельца. Альтернативный канал передачи извещений размыканием контактов реле ПЦН.

ПЦН представляет собой автоматизированное рабочее место на основе персонального компьютера с подключенными к нему концентраторами и установленным программным обеспечением интегрированной системы безопасности "Лавина".

Позволяет решать комплекс задач по мониторингу системы, подготовке и ведению базы данных по объектам, программированию ключей переноса данных для объектовых приборов.

Возможно выполнение адаптивного конфигурирования и настройка системы, программирование объектовых приборов, получение различной справочной и отчетной информации.

Программное обеспечение состоит из нескольких модулей, которые обеспечивают прием и декодирование информации, отображение состояния всех объектов, подключенных к системе, выдачу тревожных извещений, фиксацию действий операторов при поступлении тревожных сообщений, детальное представление каждого объекта; отображение журнала событий, контроль работоспособности модулей связи с концентратором.

Соответствующие модули ПО решают задачи по подготовке и ведению базы данных по объектам, программированию ключей переноса данных для объектовых приборов, обеспечивают формирование отчетов по объектам и системе в целом.

Программируемая беспроводная сигнализация ABAX.

Система ABAX включает в себя беспроводные контроллеры, охранные датчики, оповещатели и другие устройства ОПС фирмы Satel, на базе которых строится система беспроводной сигнализация офиса, магазина или квартиры. Эта система позволяет расширить беспроводными устройствами любую проводную ОПС. Важной особенностью ABAX является наличие двусторонней радиосвязи между контроллером и устройством с шифрованием данных, что обеспечивает высокую степень защиты системы ОПС от взлома и саботажа.

ABAX моментально реагирует на тревожные события и передает тревогу на ПКП системы. При этом она обеспечивает работу системы сигнализации в энергосберегающем режиме и позволяет дистанционно конфигурировать беспроводные устройства при помощи русифицированного ПО. Работает ABAX в полосе частот 868,0…868,6 Гц с модуляцией FSK.

В качестве базового устройства сигнализации ABAX используется контроллер ACU-100 фирмы Satel, который может обслуживать одновременно до 48 охранных устройств, и работает совместно с любыми приемно-контрольными приборами (ПКП). ABAX организует двустороннюю связь между беспроводными устройствами, поэтому прием сообщений от датчиков сигнализации всегда подтверждается. В то же время ACU-100 проводит в режиме on-line опрос беспроводных датчиков сигнализации, определяя присутствие в системе каждого устройства.

Система мониторинга подвижных объектов "Алмаз".

Предназначена для защиты и мониторинга мобильных, а так же стационарных объектов с использованием технологии ГЛОНАСС/GPS/GSM. Отличительная особенность системы - наличие второго (резервного) канала связи, который организовывается на базе УКВ-связи или спутникового телефона.

Система мониторинга подвижных объектов "Алмаз" служит для организации централизованной охраны и мониторинга подвижных (стационарных) объектов на базе технологий GPS/GSM, а также повышения оперативности управления группами задержания подразделений вневедомственной охраны.

В соответствии с назначением в числе основных функций системы:

слежение за местоположением контролируемых подвижных объектов с использованием электронной карты местности;

контроль, диспетчеризация и охрана автотранспорта и других подвижных объектов;

контроль состояния датчиков объекта, подключенных к терминальным устройствам, и ситуаций на объектах;

фиксация внештатных ситуаций на контролируемых объектах;

управление исполнительными устройствами объектов при возникновении нештатных ситуаций;

документирование и архивирование информации, поступающей от объектов контроля и диспетчерского центра;

организация надежных каналов связи между диспетчерским центром и объектами контроля.

Принцип действия системы основан на комплексном использовании каналов системы сотовой связи стандарта GSM 900/DCS 1800 или радиоканалов УКВ в качестве средств обмена информацией между абонентами системы и диспетчерским центром (ДЦ), а также глобальной системы позиционирования GPS для получения информации (определения координат) о текущем местоположении подвижных абонентов системы. Информация от удаленных терминалов поступает в ДЦ для отображения, накопления и последующей обработки по каналам связи стандарта GSM 900/DCS 1 800 (с применением услуг SMS или GPRS) и УКВ радиоканалам.

Система "Алмаз" представляет собой совокупность сети терминальных устройств (ТУС), расположенных на подвижных и стационарных объектах, и диспетчерского центра мониторинга.

В состав терминальных устройств, устанавливаемых на борту автотранспортных средств ("Топаз-201"), входит приемник сигналов глобальной сети позиционирования. Используемая в системе "Алмаз" технология обработки и передачи сигналов позиционирования подвижных объектов позволяет из единого диспетчерского центра осуществлять мониторинг и управление объектами, отображать их местоположение на карте местности с точностью до 5 м.

Система "Алмаз" обеспечивает решение следующих задач:

контроль технологических параметров мобильных (стационарных) объектов и управление исполнительными устройствами этих объектов;

управление парком транспортных средств;

охрану, управление и контроль сетей торговых автоматов или банкоматов;

охрану объектов (жилых или служебных помещений, газопроводов, объектов энергосетей, автотранспорта и перевозимых грузов).

## 2. Построение систем безопасности, использующих gsm каналы

## 2.1 Построения gsm канала

Стандарт GSM был разработан Европейским институтом телекоммуникационных стандартов (ETSI) и признан наиболее надежным и массовым по использованию в средствах телекоммуникации и связи. По очень приблизительным подсчетам, число абонентов данного вида связи в Евразии составляет 100 млн.

Функциональное построение и интерфейсы, принятые в стандарте GSM, иллюстрируются структурной схемой, на которой MSC (Mobile Switching Centre) - центр коммутации подвижной связи; BSS (Base Station System) - оборудование базовой станции (БС); ОМС (Operations and Maintenance Centre) - центр управления и обслуживания; MS (Mobile Stations) - подвижные станции (МС).

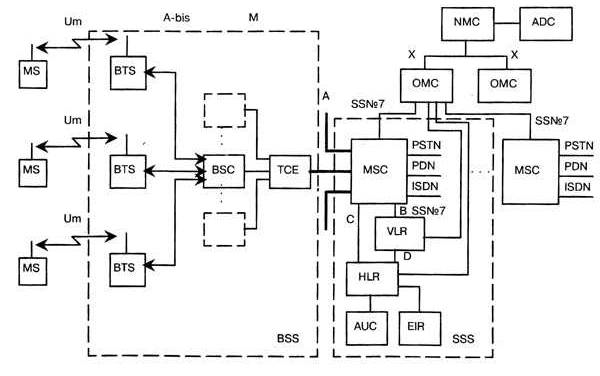


Рис.3. Функциональное построение и интерфейсы стандарта GSM

Функциональное сопряжение элементов системы осуществляется рядом интерфейсов. Все сетевые функциональные компоненты в стандарте GSM взаимодействуют в соответствии с системой сигнализации МСЭ-Т (ранее МККТТ) SS N 7 (CCITT SS. N 7)).

Центр коммутации подвижной связи обслуживает группу сот и обеспечивает все виды соединений, в которых нуждается в процессе работы МС. MSC аналогичен коммутационной станции ISDN и представляет собой интерфейс между фиксированными сетями (PSTN, PDN, ISDN и т.д.) и сетью подвижной связи. Он обеспечивает маршрутизацию вызовов и функции управления вызовами. Кроме выполнения функций обычной коммутационной станции ISDN, на MSC возлагаются функции коммутации радиоканалов. К ним относятся "эстафетная передача", в процессе которой достигается непрерывность связи при перемещении подвижной станции из соты в соту, и переключение рабочих каналов в соте при появлении помех или неисправностях.

Каждый MSC обеспечивает обслуживание подвижных абонентов, расположенных в пределах определенной географической зоны (например, Москва и область). MSC управляет процедурами установления вызова и маршрутизации. Для телефонной сети общего пользования (PSTN) MSC обеспечивает функции сигнализации по протоколу SS N 7, передачи вызова или другие виды интерфейсов в соответствии с требованиями конкретного проекта. MSC формирует данные, необходимые для выписки счетов за предоставленные сетью услуги связи, накапливает данные по состоявшимся разговорам и передает их в центр расчетов (биллинг-центр). MSC составляет также статистические данные, необходимые для контроля работы и оптимизации сети. MSC поддерживает также процедуры безопасности, применяемые для управления доступами к радиоканалам.

Практически HLR представляет собой справочную базу данных о постоянно прописанных в сети абонентах. В ней содержатся опознавательные номера и адреса, а также параметры подлинности абонентов, состав услуг связи, специальная информация о маршрутизации. Ведется регистрация данных о роуминге (блуждании) абонента, включая данные о временном идентификационном номере подвижного абонента (TMSI) и соответствующем VLR. К данным, содержащимся в HLR, имеют дистанционный доступ все MSC и VLR сети и, если в сети имеются несколько HLR, в базе данных содержится только одна запись об абоненте, поэтому каждый HLR представляет собой определенную часть общей базы данных сети об абонентах. Доступ к базе данных об абонентах осуществляется по номеру IMSI или MSISDN (номеру подвижного абонента в сети ISDN). К базе данных могут получить доступ MSC или VLR, относящиеся к другим сетям, в рамках обеспечения межсетевого роуминга абонентов.

VLR содержит такие же данные, как и HLR, однако эти данные содержатся в VLR только до тех пор, пока абонент находится в зоне, контролируемой VLR. В сети подвижной связи GSM соты группируются в географические зоны (LA), которым присваивается свой идентификационный номер (LAC). Каждый VLR содержит данные об абонентах нескольких LA. Когда подвижный абонент перемещается из одной LA в другую, данные о его местоположении автоматически обновляются в VLR. Если старая и новая LA находятся под управлением различных VLR, то данные на старом VLR стираются после их копирования в новый VLR. Текущий адрес VLR абонента, содержащийся в HLR, также обновляется.

EIR - регистр идентификации оборудования, содержит централизованную базу данных для подтверждения подлинности международного идентификационного номера оборудования подвижной станции (IМЕI). Эта база данных относится исключительно к оборудованию подвижной станции. База данных EIR состоит из списков номеров IМЕI, организованных следующим образом: БЕЛЫЙ СПИСОК - содержит номера IМЕI, о которых есть сведения, что они закреплены за санкционированными подвижными станциями. ЧЕРНЫЙ СПИСОК - содержит номера IМЕI подвижных станций, которые украдены или которым отказано в обслуживании по другой причине. СЕРЫЙ СПИСОК - содержит номера IМЕI подвижных станций, у которых существуют проблемы, выявленные по данным программного обеспечения, что не является основанием для внесения в "черный список". К базе данных EIR получают дистанционный доступ MSC данной сети, а также MSC других подвижных сетей.

ОМС - центр эксплуатации и технического обслуживания, является центральным элементом сети GSM, который обеспечивает контроль и управление другими компонентами сети и контроль качества ее работы. ОМС соединяется с другими компонентами сети GSM по каналам пакетной передачи протокола Х.25. ОМС обеспечивает функции обработки аварийных сигналов, предназначенных для оповещения обслуживающего персонала, и регистрирует сведения об аварийных ситуациях в других компонентах сети. В зависимости от характера неисправности ОМС позволяет обеспечить ее устранение автоматически или при активном вмешательстве персонала. ОМС может обеспечить проверку состояния оборудования сети и прохождения вызова подвижной станции. ОМС позволяет производить управление нагрузкой в сети. Функция эффективного управления включает сбор статистических данных о нагрузке от компонентов сети GSM, записи их в дисковые файлы и вывод на дисплей для визуального анализа. ОМС обеспечивает управление изменениями программного обеспечения и базами данных о конфигурации элементов сети. Загрузка программного обеспечения в память может производиться из ОМС в другие элементы сети или из них в ОМС.

NMC - центр управления сетью, позволяет обеспечивать рациональное иерархическое управление сетью GSM. Он обеспечивает эксплуатацию и техническое обслуживание на уровне всей сети, поддерживаемой центрами ОМС, которые отвечают за управление региональными сетями. NMC обеспечивает управление графиком во всей сети и обеспечивает диспетчерское управление сетью при сложных аварийных ситуациях, как например, выход из строя или перегрузка узлов. Кроме того, он контролирует состояние устройств автоматического управления, задействованных в оборудовании сети, и отражает на дисплее состояние сети для операторов NMC. Это позволяет операторам контролировать региональные проблемы и, при необходимости, оказывать помощь ОМС, ответственному за конкретный регион. Таким образом, персонал NMC знает состояние всей сети и может дать указание персоналу ОМС изменить стратегию решения региональной проблемы.

BSS - оборудование базовой станции, состоит из контроллера базовой станции (BSC) и приемопередающих базовых станций (BTS). Контроллер базовой станции может управлять несколькими приемо-передающими блоками. BSS управляет распределением радиоканалов, контролирует соединения, регулирует их очередность, обеспечивает режим работы с прыгающей частотой, модуляцию и демодуляцию сигналов, кодирование и декодирование сообщений, кодирование речи, адаптацию скорости передачи для речи, данных и вызова, определяет очередность передачи сообщений персонального вызова.

## 2.2 Принцип шифрования gsm канала

Использование пароля (или кода PIN - персонального идентификационного цифрового кода) - один из простых методов аутентификации. Он дает очень низкий уровень защиты в условиях использования радиосвязи. Достаточно услышать этот персональный код всего лишь один раз, чтобы обойти средства защиты. В действительности GSM использует PIN-КОД в сочетании с SIM (Subscriber Identify Module): данный PIN-КОД проверяется на месте самим SIM без передачи в эфир.

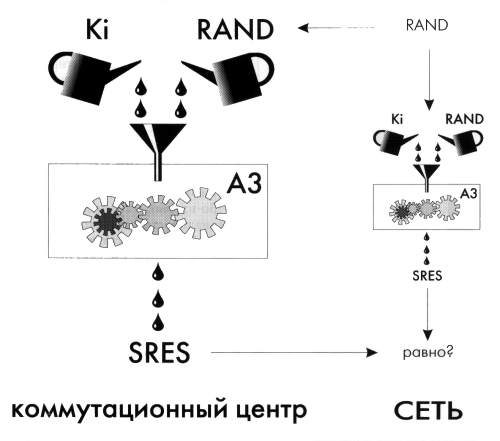


Рис.4. Вычисление аутентификации

Помимо него, GSM использует более сложный метод, который состоит в использовании случайного числа (от О до 2^128-1), на которое может ответить только соответствующее абонентское оборудование (в данном случае - SIM). Суть этого метода в том, что существует огромное множество подобных чисел и поэтому маловероятно, что оно будет использовано дважды.

Аутентификация производится путем требования дать правильный ответ на следующую головоломку: какой ответ SRES абонент может вывести из поступившего RAND, применяя алгоритм A3 с личным (секретным) ключом Ki?

Ответ, который называется SRES (Signed RESult - подписанный результат), получают в форме итога вычисления, включающего секретный параметр, принадлежащий данному пользователю, который называется Ki (рис.1). Секретность Ki является краеугольным камнем, положенным в основу всех механизмов безопасности - свой собственный Ki не может знать даже абонент. Алгоритм, описывающий порядок вычисления, называется алгоритмом A3. Как правило, такой алгоритм хранится в секрете (лишние меры предосторожности никогда не помешают!).

Для того чтобы достигнуть требуемого уровня безопасности, алгоритм A3 должен быть однонаправленной функцией, как ее называют эксперты криптографы. Это означает, что вычисление SRES при известных Ki и RAND должно быть простым, а обратное действие - вычисление Ki при известных RAND и SRES - должно быть максимально затруднено. Безусловно, именно это и определяет в конечном итоге уровень безопасности. Значение, вычисляемое по алгоритму A3, должно иметь длину 32 бита. Ki может иметь любой формат и длину. Криптографические методы дают возможность с помощью относительно простых средств добиться высокого уровня безопасности. В GSM используются единые методы для защиты всех данных, будь то пользовательская информация, передача сигналов, связанных с пользователем (например, сообщений, в которых содержатся номера вызываемых телефонов), или даже передача системных сигналов (например, сообщений, содержащих результаты радиоизмерений для подготовки к передаче). Необходимо проводить различие только между двумя случаями: либо связь оказывается защищенной (тогда всю информацию можно отправлять в зашифрованном виде), либо связь является незащищенной (тогда вся информация отправляется в виде незашифрованной цифровой последовательности).



Рис.5. Шифрование и расшифровка

Алгоритм А5 выводит последовательность шифрования из 1 14 бит для каждого пакета отдельно, с учетом номера кадра и шифровального ключа Кс.

Как шифрование, так и расшифровка производятся с применением операции "исключающее или" к 114 "кодированным" битам радиопакета и 114-битовой последовательности шифрования, генерируемой специальным алгоритмом, который называется А5. Для того чтобы получить последовательность шифрования для каждого пакета, алгоритм А5 производит вычисление, используя два ввода: одним из них является номер кадра, а другим является ключ (который называется Кс), известный только мобильной станции и сети (рис.2), В обоих направлениях соединения используются две разные последовательности: в каждом пакете одна последовательность используется для шифрования в мобильной станции и для расшифровки на BTS, в то время как другая последовательность используется для шифрования в BTS и расшифровки в мобильной станции.

Номер кадра меняется от пакета к пакету для всех типов радиоканалов. Ключ Кс контролируется средствами передачи сигналов и изменяется, как правило, при каждом сообщении. Этот ключ не предается гласности, но поскольку он часто меняется, то не нуждается в столь сильных средствах защиты, как ключ Ki; например, Кс можно свободно прочитать в SIM.

Алгоритм А5 необходимо устанавливать на международном уровне, поскольку для обеспечения MS-роуминга он должен быть реализован в рамках каждой базовой станции (равно как и в любом мобильном оборудовании). На данный момент один-единственный алгоритм А5 установлен для использования во всех странах. В настоящее время базовые станции могут поддерживать три основных варианта алгоритма А5: А5/1 - наиболее стойкий алгоритм, применяемый в большинстве стран; А5/2 - менее стойкий алгоритм, внедряемый в странах, в которых использование сильной криптографии нежелательно; А5/3 - отсутствует шифрования. В России применяется алгоритм А5/1. По соображениям безопасности его описание не публикуется. Этот алгоритм является собственностью организации GSM MoU. Тем не менее, его внешние спецификации обнародованы, и его можно представить как "черный ящик", принимающий параметр длиной 22 бита и параметр длиной 64 бита для того, чтобы создавать последовательности длиной 114 битов. Как и в случае с алгоритмом аутентификации A3, уровень защиты, предлагаемой алгоритмом А5, определяется сложностью обратного вычисления, то есть вычисления Кс при известных двух 114-битовых последовательностях шифрования и номера кадра.

Ключ Кс до начала шифрования должен быть согласован мобильной станцией и сетью. Особенность стандарта GSM заключается в том, что ключ Кс вычисляется до начала шифрования во время процесса аутентификации. Затем Кс вводится в энергонезависимую память внутри SIM с тем, чтобы он хранился там даже после окончания сеанса связи. Этот ключ также хранится в сети и используется для шифрования.

Всякий раз, когда какая-либо мобильная станция проходит процесс аутентификации, данная мобильная станция и сеть также вычисляют ключ шифрования Кс, используя алгоритм А8 с теми же самыми вводными данными RAND и Ki, которые используются для вычисления SRES посредством алгоритма A3.

Алгоритм А8 используется для вычисления Кс из RAND и Ki (рис.3). Фактически, алгоритмы A3 и А8 можно было бы реализовать в форме одного-единственного вычисления. Например, в виде единого алгоритма, выходные данные которого состоят из 96 бит: 32 бита для образования SRES и 64 бита для образования Кс.

Следует также отметить, что длина значимой части ключа Кс, выданная алгоритмом А8, устанавливается группой подписей GSM MoU и может быть меньше 64 битов. В этом случае значимые биты дополняются нулями для того, чтобы в этом формате всегда были использованы все 64 бита.

Шифрование оказывается весьма эффективным для защиты конфиденциальности, но для защиты каждого отдельно взятого обмена информацией по радиоканалу не может использоваться. Шифрование с помощью Кс применяется только в тех случаях, когда сети известна личность абонента, с которым идет разговор. Понятно, что шифрование не может применяться для общих каналов, таких как ВССН, который принимается одновременно всеми мобильными станциями в данной сотовой ячейке и в соседних сотовых ячейках (иначе говоря, оно может применяться с использованием ключа, известного всем мобильным станциям, что абсолютно лишает его смысла как механизм безопасности). При перемещении мобильной станции на какой-либо специальный канал некоторое время происходит "начальная загрузка", в течение которой сеть еще не знает личность абонента, скажем, Владимира, и, следовательно, шифрование его сообщения невозможно. Поэтому весь обмен сигнальными сообщениями, несущий сведения о личности неопределенного абонента, должен происходить в незашифрованном виде. Какая-либо третья сторона на данной стадии может подслушать информацию об этой личности. Считается, что это ущемляет право Владимира на секретность, поэтому в GSM введена специальная функция, позволяющая обеспечить такого рода конфиденциальность.

Защита также обеспечивается путем использования идентификационного псевдонима, или TMSI (Временный идентификатор мобильного абонента), которое используется вместо идентификатора абонента IMSI (Международный идентификатор мобильного абонента) в тех случаях, когда это возможно. Этот псевдоним должен быть согласован заранее между мобильной станцией и сетью.

Особенно стоит отметить, что в наземном канале передачи данные передаются по проводам в незашифрованном виде, и перехват информации идет именно с них.

## 2.3 Функции gsm каналов, используемые системами безопасности

SMS канал.

Довольно сильно распространен на рынке систем безопасности в нашей стране тип сигнализаций использующий функцию SMS сообщений. Такая популярность обуславливается низкой стоимостью (самой сигнализации так и абонентской платы) и простотой использования данных GSM-сигнализаций. В профессиональных охранных системах данный тип передачи извещений используется в основном как сервисный канал. Оповещение о чрезвычайной ситуации или о проникновении на объект является обязательным атрибутом систем охраны и с точки зрения технической реализации может быть исполнено в такой форме как предупреждение голосом (звонком на телефон), DTMF (Dual Tone Multi-Frequency - термин для обозначения тонального набора) кодом, в любом цифровом виде, а также передачей SMS сообщения собственнику.

Для передачи извещений по средством SMS сообщений используется самый известный GSM-сервис мобильных операторов. И одновременно самый простой в реализации метод. GSM модемы с SMS-передатчиком имеют доступную цену, в тоже время просты в настройке, а пультовым приемным устройством может являться любой сотовый телефон.

SMS (англ. Short Message Service - служба коротких сообщений) - система, позволяющая посылать и принимать сообщения в виде текста при помощи мобильного телефона.

Текст может состоять из алфавитно-цифровых символов. Максимальный размер сообщения в стандарте GSM - 140 байт. Таким образом, при использовании 7-битной кодировки (латинский алфавит и цифры) можно отправлять сообщения длиной до 160 символов. При использовании 8-битной кодировки (немецкий, французский язык) можно отправлять сообщения длиной до 140 символов. Для поддержки других национальных алфавитов (китайского, арабского, русского и др.) используется 2-байтная кодировка UTF-16 (Unicode). Таким образом, SMS-сообщение, написанное кириллицей, не может превышать 70 знаков. Что весьма ограничивает использование данного сервиса в охранном оборудование.

В стандарте также предусмотрена возможность отправлять сегментированные сообщения. В таких сообщения в заголовке пользовательских данных (UDH) помещается информация о номере сегмента сообщения и общем количестве сегментов. Эту возможность поддерживают не все GSM-модемы, а те, которые поддерживают, зачастую накладывают ограничение на количество сегментов в сообщении (3 или 5). Модем, который не поддерживает сегментирование, отображает каждый сегмент как отдельное сообщение. Как правило, каждый сегмент тарифицируется как отдельное сообщение.

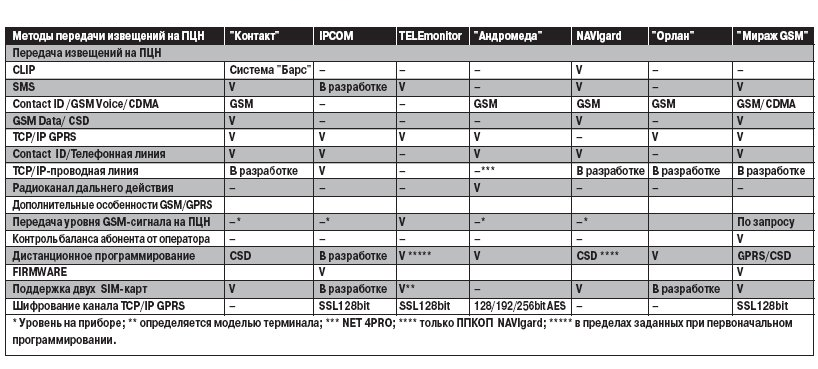
Технология SMS поддерживается основными сотовыми сетями (GSM, NMT, D-AMPS, CDMA). Также SMS-сообщения на телефоны можно отправлять из интернета и других сетей, используя специальные программы, а также непосредственно шлюзы мобильных операторов.

В своей работе GSM-сигнализации, использующих SMS сообщения для передачи тревожных сообщений полностью идентичны своим аналогам, которые используют другие каналы передачи данных. В данных сигнализациях используются все те же GSM-модемы. На объекте устанавливается контрольная панель с GSM-модулем. В зависимости от типа связи с датчиками (проводные и беспроводные охранные датчики) подключаются охранно-пожарные датчики. В случае срабатывания одного из датчиков, на панель поступает сигнал. В свою очередь в случае замыкания одной из зон, контроллер дает команду GSM-модему отправить SMS сообщение по одному или нескольким номеров из памяти.

Широкое распространение получил так называемые дачные охранные сигнализации. Данный тип GSM-сигнализаций почти всегда сочетает в себе охранные функции и функции дистанционного управления исполнительными устройствами. В профессиональной охране данный тип связи применяется ограниченно, в основном как сервисный канал, например для подтверждения взятия объекта под охрану или контроль напряжения сети на объекте. Так же данный канал используется как последний резервный канал в профессиональных охранных системах.

Слабое место данных охранных систем всем хорошо известно: SMS-сообщения могут задерживаться в SMS-сервере на неопределенное время, а иногда просто теряются. Т.к. данный канал связи не является приоритетным. В случае загруженности GSM канала SMS сообщения отправляются в последнюю очередь (чего не скажешь о голосовых вызовах). Неопределенность времени доставки SMS сообщений делают этот метод недопустимым для профессиональной охраны.

Таблица 1. Поддержка способов передачи извещений на ПЦН.

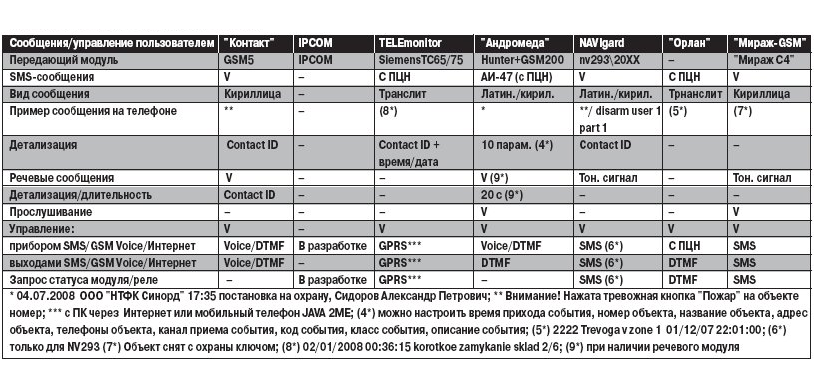


Voice канал.

Voice (речевой) канал условно делиться на DTMF сигнал и речевое оповещение. Данный канал очень популярен среди пультовых охранных систем. У данного канала GSM сети есть свои плюсы и минусы. Из плюсов можно выделить простота перехода с проводной охранно-пожарной сигнализации на GSM-сигнализацию. Минусы это забивание канала в случае неисправности или плохого сигнала. Voice канал - cамый распространенный канал передачи данных в охранных системах использующий GSM технологии передачи данных. Voice канал - это голосовой тракт использующий речевое оповещение (обычно в частных охранных системах) и DTMF-код (оборудование для пультов централизованного наблюдения). Про речевом оповещении в случае тревоги GSM-сигнализация звонит на телефон и проговаривает в заранее записанное сообщение. С DTMF немного сложнее. В DTMF при нажатии на клавишу кнопочного телефона раздается звук (тон), который является комбинацией двух тонов, высоко - и низкочастотного.

Система сигналов DTMF включает восемь тонов, которые были специально подобраны таким образом, чтобы передаваться через телефонную сеть без затухания и с минимальным воздействием друг на друга. Поскольку эти звуковые сигналы попадают в частотный диапазон человеческого голоса, были дополнительно введены меры для того, чтобы голос не воспринимался как набор. Одна из таких мер - деление тонов на две группы, высоко - и низкочастотную.

Таблица 2. Возможности, представляемые различными системами охраны.



Обычно в GSM-сигнализациях для пультов централизованного наблюдения (ПЦН) используются стандартные форматы, например протокол Contact ID. На данный момент DTMF - самый распространенный канал передачи данных, поскольку форматы данных, принцип передачи, приемное оборудование - полностью заимствовано у проводного мониторинга. Например, если охранное предприятие уже имеет станцию централизованного мониторинга, то применение GSM-сигнализаций не вызывает лишних затрат, т.к не требуется заменять оборудование на станции мониторинга. Использование DTMF форматов предъявляет дополнительные требования к проработке звукового тракта GSM-модема. Аналого-цифровые преобразования влекут за собой искажения при передаче сигнала. Из-за этого могут происходить сбои при приеме отчетов от объектового оборудования. Данная проблема довольно часто встречается у отечественного оборудования. И хотя сигнал не потеряется в сети (большинство систем контролируют передачу данных, запрашивая подтверждение приема), но значительно увеличится время прохождения сигнала. Причем увеличение времени прохождения сигнала может быть фатальным. Представьте себе ситуацию, когда на объект установлено оборудование использующее передачу данных в формате DTMF кодов. Из-за неисправности оборудования или плохого качества сигнала, объектовый прибор не сможет передать сообщение на пульт. И, как следствие, не получит подтверждения о приеме. Не получив сообщение о приеме прибор начнет повторный набор, с попыткой передать сообщение. Но в итоге, не получив ничего, начинается цикл дозвонов. Этот цикл полностью займет весь канал, что не позволит передать сообщение другим объектовым приборам, т.е. будет потеряна связь с объектами. Не будет сообщений о тревоге, не будет сообщений о постановке и снятия с охраны и т.д. И как следствие полностью нерабочий пульт централизованного наблюдения.

CLIP (Calling Line Identification Presentation).

Данный метод основан на сервисе оператора мобильной связи по предоставлению информации о номере абонента, совершающего звонок. Принцип систем, использующих CLIP, очень прост. Объектовый ППКОП в случае системного события совершает звонок по сети сотовой связи на приемное устройство, в качестве которого может выступать GSM-модем или обычный мобильный телефон. Приемное устройство считывает номер вызывающего абонента и отклоняет вызов. Сам факт звонка от известного в системе абонента и является основанием для регистрации тревожного события. Достоинство метода очевидно - отсутствует плата за исходящий вызов, ведь никакого соединения не происходит. Однако информативность такого сообщения очень мала.

Правда, этот способ можно видоизменить для повышения информативности. Например, установить на ПЦН несколько GSM-модемов. Передающее устройство программируют таким образом, чтобы по одной группе событий модем делал вызов на первый модем (тревоги), по другой группе - на второй и т.д. Следует отметить, что данный способ не нашел существенного распространения из-за малой информативности.

GSM DATA/CSD (Circuit Switch Data).

Цифровой канал передачи данных на скорости 9,6 кбит/с. Этот метод характеризуется практически 100% -ной вероятностью доставки сообщения. Время установления соединения около 20 с. Тарификация CSD поминутная, как и для голосового канала GSM. В отличие от передачи сообщения в стандартном формате Contact ID в голосовом канале, протокол передачи в CSD не стандартизирован (хотя может быть максимально приближен к CID).

Это не позволяет использовать передатчики одного производителя в системе другого производителя (конечно, если они не договорились и не предприняли специальных мер по сопряжению своих систем).

Возможна установка в "прозрачном" (transparent) и "непрозрачном" (non-transperent) режимах. Отличительная особенность передачи данных с использованием "непрозрачного" режима большая помехозащищенность, достигаемая за счет введения алгоритма коррекции ошибок, а также наличия подтверждения успешной (без искажений) доставки передаваемой информации. Таким образом, использование "непрозрачного" CSD-соединения представляется предпочтительным при низком соотношении сигнал/шум. Однако длительность времени установления соединения в "непрозрачном" режиме больше, чем в "прозрачном". В режиме CSD также реализована процедура подтверждения принятых извещений на ПЦН.

TCP/IP GPRS (General Packet Radio Service).

Как известно, технология пакетной передачи GPRS использует в качестве механизма доставки пакетов данных протоколы TCP/IP, в случае применения которых каждому из устройств сети присваивается уникальный IP-адрес. Существует два вида IP-адресов: статические и динамические. Статические IP-адреса могут предоставляться либо Интернет-провайдерами, либо операторами сотовых сетей.

Динамические IP-адреса выдает оператор при подсоединении к сети GPRS и только на время сеанса связи. Если по каким-либо причинам сеанс прервался, то при повторном подсоединении устройство, не имеющее статического IP-адреса, получит новый динамический, отличный от предыдущего. Необходимо упомянуть тот факт, что если устройство, в том числе модем GSM/GPRS, авторизовалось в сети и получило динамический IP-адрес, то для поддержания виртуального GPRS-канала в активном состоянии нужно через определенные временные интервалы передавать сигнальные пакеты на любой известный IP-адрес, иначе оператор разъединит соединение с сетью.

Возможны разные варианты выделения IP-адресов ЦПО и концентраторам сетей счетчиков. Наиболее часто встречающийся вариант - наличие у ЦПО статического IP-адреса, а у абонентов - динамических. Причем статический IP-адрес выделяет ЦПО не сотовый оператор, а Интернет-провайдер при подключении ЦПО к Интернету по выделенному каналу доступа (образованному с помощью технологий ЛВС, ADSL или др.).

При такой организации системы возможны два сценария установления соединения между устройствами в целях передачи данных. Если инициирующим соединение устройством является концентратор, он организует GPRS-сеанс с инфраструктурой сотового оператора, получает от него динамический IP-адрес и устанавливает TCP/IP-соединение с ЦПО (если “знает” его статический IP-адрес). Последний (ЦПО) должен быть сконфигурирован на прием (и обработку) запросов на соединение по выделенному каналу доступа в Интернет. При поступлении запроса на соединение от концентратора его динамический IP-адрес станет “известен" ЦПО (в IP-заголовке пакета содержится информация об адресе отправителя), что сделает возможным двухсторонний обмен информацией.

Если же инициатором связи является ЦПО, то он дозванивается до удаленного модема по голосовому каналу GSM или посылает SMS-сообщение на его номер. Концентратор воспринимает входящий звонок (или поступившее SMS-сообщение) с известного номера как команду на установление соединения с ЦПО и далее действует так, как было описано ранее. Минимальным требованием при организации соединения с ЦПО является “знание" концентратором статического IP-адреса ЦПО. Если же концентратор не “знает” этот адрес, то его можно сообщить концентратору по голосовому каналу GSM или посредством службы SMS.

При необходимости организовать связь с концентратором, имеющим статический IP-адрес, ЦПО обращается к нему по этому адресу, устанавливая GPRS-соединение. Для этого модем GSM/GPRS концентратора должен быть сконфигурирован на прием (и обработку) запросов на соединение по каналу TCP/IP. Такой способ организации канала передачи данных возможен, однако на практике почти не встречается из-за сложности получения статических IP-адресов у сотовых операторов для всех удаленных устройств системы.

Актуален и такой вариант: концентраторы и ЦПО имеют динамические IP-адреса. Это возможно, когда ЦПО не оснащен выделенным каналом доступа в Интернет, но расположен в зоне действия одного из операторов сотовой связи. В этом случае уже не важно кто является инициатором связи - концентратор или ЦПО, действия по реализации канала передачи данных всегда будут одни и те же.

Инициирующее связь устройство (например, ЦПО) организует GPRS-сеанс с инфраструктурой сотового оператора и получает от него динамический IP-адрес. Затем оно сообщает (например, с помощью службы SMS) полученный адрес другому устройству (концентратору) и передает ему команду соединиться по этому адресу. Вызываемое устройство, организовав GPRS-сеанс и получив динамический IP-адрес, устанавливает TCP/IP-соединение с вызывающим устройством.

## 3. Анализ функционирования систем безопасности, использующих gsm каналы

## 3.1 Анализ помехоустойчивости и помехозащищённости gsm канала

Помехи в радиоканале создаются как за счет искажений сигнала при его распространении, так и в результате воздействия внешних источников. Первый тип искажений сравнительно легко устраним, в то же время с помехами от внешних источников борются при помощи расширения спектра передаваемого сигнала. Теоретически, увеличение базы сигнала (произведение эффективного значения длительности сигнала и эффективного значения ширины его спектра) позволяет уменьшить помеху до сколь угодно малого уровня.

Основная сложность при построении GSM канала связана с невозможностью обеспечить непрерывность GSM/GPRS-связи с оператором из-за перебоев в сети, которые приводят к прерыванию передачи данных, но и к зависанию модема. Практика показывает, что ни один GSM-оператор на сегодняшний день не обеспечивает предоставление гарантированного GPRS-канала связи. В попытках реализации непрерывности подключения разработчики вынуждены дополнительно оснащать традиционные (простые) GSM-модемы дополнительными устройствами - внешними контроллерами, сторожевыми таймерами, осуществляющими перезагрузку модема при зависании. К сожалению, подобные решения хоть и являются обычно "экономичными", но по-прежнему не гарантируют непрерывного и бесперебойного процесса передачи данных, а также ведут к усложнению системы в целом и, как следствие, к снижению ее надежности.

Дополнительно к перечисленным методам, для повышения помехоустойчивости РЭС, использующих узкополосные сигналы, применяют многократное дублирование фрагментов передаваемых сообщений в частотной или временной области. Например, модемы для передачи данных в коротковолновом диапазоне частот используют для одновременной передачи информации до 50 несущих частот используются медленные скачки по частоте SFH (Slow Frequency Hopping) или иначе - медленная псевдослучайная или программная перестройка радиочастот (ППРЧ). Использование ППРЧ совместно с помехоустойчивым кодированием и перемежением позволяет в условиях узкополосных помех в каналах с замираниями повысить помехоустойчивость на приеме на 9-11дБ, в то время, как без ППРЧ эта цифра колеблется в пределах 4-6дБ.

Помехоустойчивость, по мнению целого ряда специалистов в области радиоканальных пожарных и охранных систем, определяется следующим:

количеством частотных диапазонов, в которых может работать радиосистема;

количеством частотных каналов в каждом диапазоне;

возможностью автоматического выбора резервных каналов;

наличием автоматической регулировки мощности излучения.

В соответствии с европейской классификацией (в России данная классификация по РД 78.36.003-2002 несколько иная - имеются две категории объектов, в каждой из которых две подкатегории) существует три класса пожарных и охранных проводных и радиоканальных систем, отличающихся между собой, прежде всего, по степени риска технически подготовленного взлома (ЕМ 50131-1):

класс А: низкая степень риска - объекты частного пользования (загородные дома, квартиры);

класс В: средняя степень риска - объекты общественного пользования (магазины, учебные заведения);

класс С: высокая степень риска - объекты государственной важности (музеи, исторические памятники).

Представим себе типичную ситуацию на объекте, находящемся под охраной радиосистемы. Время от времени пропадает связь с тем или иным радиоустройством. Скорее всего, причиной является не преднамеренное саботирование работы системы, а работа других приборов и систем на выбранном при установке системы канале связи (литере). Напомним, что диапазон частот 433 и 868 МГц является нелицензируемым, и его используют не только пожарные и охранные радиосистемы, но и бытовые устройства: переносные радиостанции, игрушки, шлагбаумы и т.д. В зависимости от класса радиосистемы должны реагировать по-разному:

класс А: индикация о временной потере связи с радиоустройством системы отсутствует;

классы В и С: радиосистема обязана максимально использовать все возможные способы доставки сигнала и только после этого передать сигнал "Тревога". Например, извещатель, не получив квитанцию от приемно-контрольного прибора после передачи тестового сигнала (что возможно только в системе с двусторонним протоколом), немедленно меняет частотный канал, мощность излучения, периодичность выхода в эфир и т.д. Если связь не может быть восстановлена даже после всех упомянутых действий, то в данном случае имеет место преднамеренное саботирование работы системы.

Способность радиолинии работать в условиях воздействия организованных помех называется помехозащищенностью.

Помехозащита разделяется на два класса:

1) пространственная помехозащита (за счет низкого уровня боковых лепестков приемной антенны, по которым действует помеха, формирование "нулей" диаграммы направленности приемной антенны в направлении на источник помех);

2) сигнальная помехозащита за счет широкополосных методов модуляции.

Принцип подавления основан на постановке узкополосной помехи приемному каналу GSM-устройства. На сегодняшний день подавителей GSM-устройств большое множество и основное их использование заглушать мобильные телефоны на совещаниях, конференциях, библиотеках, театрах и т.п. Однако это не мешает применять их и для негативных целей. Их применение не останется не замеченным для операторов мобильной связи.

Известны несколько типов устройств, применяемых для глушения спутниковых охранных систем:

1. Широкополосная глушилка. Постоянно излучает мощный шум на всех рабочих частотах GSM. Тем самым GSM-модулю перестает видеть как спутники GPS, передающие текущие координаты автомобиля, так и БС оператора GSM.

2. Перебирающая частоты --этот тип глушилок работает также как первый тип, отличие в том, что шумоподобная помеха ставится последовательно по всем частотам канала GSM, не позволяя GSM-модулю передавать сигнал. Размером она достаточно компактная и питается от обычных батареек. Действует в радиусе 5-15 метров.

3. "Умная" - - это глушилка, которая выдает себя за базовую станцию оператора GSM. При ее включении, GSM-модуль будет работать без сбоев и считать, что все хорошо. Глушилка требует серьезного источника питания.

На сегодня существует два способа борьбы с глушением:

определение факта глушения на стороне GSM-модуля. Если модуль видит, что в эфире на рабочих частотах появился сигнал (шум), он пытается успеть произвести оповещение. Но это маловероятно, ведь отправить SMS или голосовое сообщение вряд ли получится, т.к передатчик уже заглушен.

определение факта глушения извне. Для этого организуется постоянная проверка связи между GSM-модулем и специально выделенным сервером -контроль канала. Таким образом, на стороне сервера можно гарантированно определить пропажу связи с автомобилем. В случае пропажи GSM-сигнала, сервер оповещает владельца SMS-сообщением, по e-mail, или звонком.

Для снижения глушения сигнала нужно:

иметь дублирующий канал для обмена важной информацией;

использовать периодический тест с объекта;

применение выносных антенн.

## 3.2 Исследование скорости передачи данных и пропускной способности gsm канала

Максимальная скорость передачи данных по одному голосовому каналу GSM (режим CSD) составляет 9600 Кбит/с, а многоканальный режим HSCSD обеспечивает передачу данных на скорости 19 200 Кбит/с и выше

Таблица 3. Перечень услуг и качество работы приложений на различных скоростях передачи

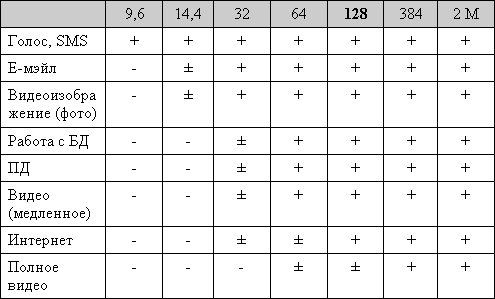
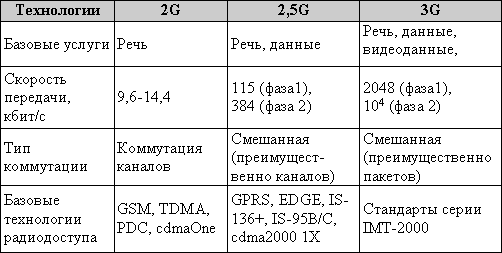


Таблица 4. Характеристики поколений GSM



К недостаткам использования голосового канала GSM можно отнести значительную стоимость пересылки килобайта информации и существенное негативное влияние (на экономические показатели системы) времени организации сеанса связи между модемами при передаче малых объемов данных. Например, время передачи 20 Кбит информации равно примерно 2 с, а время организации сеанса может варьироваться от 2 до 16 с, в зависимости от режима работы модемов.

Максимально возможная скорость обмена данными с помощью технологии GPRS теоретически может достигать 170 Кбит/с.

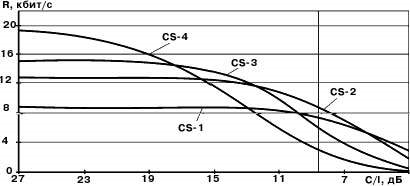


Рис.6. Зависимоть пропускной способности от схемы кодирования.

В технологии GPRS была предложена новая структура пакета размером 456 бит (четыре информационных блока по 114 бит), которая обеспечивает общую скорость передачи по каналу 22,8 кбит/с

В целях повышения гибкости передачи и пропускной способности в системе GPRS могут использоваться четыре схемы кодирования данных: от CS1 до CS4. Для управления работой радиолинии в режиме пакетной передачи разработан специальный протокол RLC (Radio Link Control), который обеспечивает ее адаптивную настройку, программную перестройку частоты и управление мощностью. Адаптация радиолинии включает выбор той или иной схемы кодирования (CS1 - CS4) в зависимости от вида передаваемой информации, характеристик радиоканала и уровня помех.

Таким образом, в режиме GPRS каждому абоненту предоставляется от 1 до 8 канальных интервалов. Во время пакетной передачи ресурсы линий связи "вверх" и "вниз" могут выделяться независимо друг от друга, т.е. в системе допускается реализация асимметричного режима передачи. Сегодня при использовании схемы кодирования CS2 скорость передачи данных в GPRS-системе составляет 115,2 (8х14,4) кбит/с, однако теоретически она может быть увеличена до 171,2 (8х21,4) кбит/с - если применить схему кодирования CS4.

Проведенные в октябре 2008 года исследования скорости мобильного соединения показали, что реально средняя скорость составляет входящего соединения 130 Кбит/c, исходящего - 57 кбит/c. Ни один из операторов мобильного Интернета не показал максимально возможную для используемого им стандарта скорость (474 Кбит/c для EDGE у GSM).

Отдельно стоит упомянуть, что скорость передачи значительно возрастает при использовании технологии EDGE.

EDGE (англ. Enhanced Data rates for GSM Evolution) - цифровая технология для мобильной связи, которая функционирует как надстройка над 2G и 2.5G (GPRS) - сетями. Для поддержки EDGE в сети GSM требуются определённые модификации и усовершенствования. На основе EDGE могут работать: ECSD - ускоренный доступ в Интернет по каналу CSD, EHSCSD - по каналу HSCSD, и EGPRS - по каналу GPRS. EDGE был впервые представлен в 2003 году в Северной Америке.

Несмотря на то, что EDGE не требует аппаратных изменений в NSS-части сети GSM, модернизации должна быть подвергнута подсистема базовых станций (BSS). Необходимо установить трансиверы, поддерживающие EDGE (8PSK модуляцию) и обновить программное обеспечение. Также требуются телефоны, обеспечивающие аппаратную и программную поддержку модуляции и кодовых схем, используемых в EDGE.

В настоящее время около шестнадцати отечественных оператора используют технологию EDGE, в том числе и "большая тройка" - МТС, Билайн, Мегафон.

## 3.3 Анализ модели gsm канала по обеспечению требуемой зоны покрытия

На дальность радиосвязи влияют следующие факторы:

1. Местоположение BS и MS и рельеф местности.

2. Мощность и чувствительность MS.

3. Мощность и чувствительность BS.

4. Используемые на MS и BS антенны.

5. Воля Господа Бога (опытные связисты шутят, что это - главное).

Обычно базовые станции имеют мощность 20 - 30 Вт. Антенны применяются либо штыревые, либо направленные. Чувствительность базовых станций составляет - 100 дБ - 115 дБ. Изменить или повлиять на все эти параметры пользователь, конечно, не может. Большинство операторов используют ограничение дальности работы мобильного телефона от базовой станции - 35 км (для GSM-900, для GSM-1800 - порядка 10), что обусловлено особенностями стандарта. Однако в GSM предусмотрена также нестандартная конфигурация соты, при которой дальность связи увеличивается на 70 - 100 км (конфигурация Extended Cell). К сожалению, при такой конфигурации количество разговорных каналов уменьшается до 2 - 3, что уменьшает емкость сети. Использовать такой режим в городе и около оператору не выгодно. Иногда этот режим используется на морском побережье для создания прибрежной зоны покрытия.

Железобетонные строения способны ослаблять сигналы, проходящие через них (при внутреннем покрытии), в 100-1000 раз (то есть на 20-30 дБ). К числу препятствий можно также отнести кузова автомобилей, кроны деревьев и т.д. Влияние могут оказать и атмосферные осадки.

При расчете зоны покрытия применяется модель Хата, так как она рекомендована Международным Консультативным Комитетом по Радиосвязи (МККР) и довольно проста в применении. Эта модель позволяет вычислить потери на радиотрассе для конкретной местности и параметров базовой станции.

Средний уровень потерь на радиотрассе, следуя эмпирической модели Хата, определяется следующим образом:

(дБ).



Где частота, (МГц); высота базовой станции, (м); расстояние между базовой станцией и абонентской станцией, (км); высота абонентской станции, (м);



коэффициент, учитывающий высоту антенны абонентской станции ( для небольшого или среднего города, для большого города),



коэффициент, учитывающий характер местности ( для сельской местности, для пригорода, для города),



коэффициент, отражающий влияние плотности застройки, (%) - плотность застройки;



коэффициент, учитывающий сферичность Земли (вводится, если 0,2R0 < r ≤ 0,8R0, где R0 - расстояние прямой видимости).

Пример расчета:

Необходимо рассчитать зону покрытия БС стандарта GSM-900 в большом городе с плотностью застройки 35%, исходя из требования обеспечения надлежащего качества сигнала.

МГц;



м;



м.



Решение



для города ().



Средний уровень потерь на радиотрассе:



(дБ);



(дБ).



Теперь, исходя из выходной мощности передатчика *P* (дБ), запаса по замираниям *S (*дБ) и требуемого уровня сигнала на входе приемника *Q* (дБ) (), запишем уравнение для нахождения *R* - максимального расстояния от БС, на котором достигается требуемое качество связи:



Задавая соответствующие параметры *P* (дБ), *S* (дБ) (обычно берется равным 20 дБ), *Q* (дБ) (для МС берется - 110 дБ), можно вычислить расстояние уверенной связи *R*; на основании этих данных строится зона покрытия БС с точки зрения качества сигнала (без учета нагрузки на соту и возможностей БС по пропускной способности).

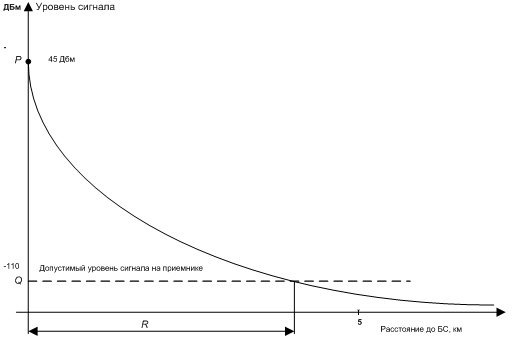


Рис.7. Зависимость уровня сигнала от расстояния между БС и абонентом.

На рисунке выше показан характерный вид функции уровня сигнала в зависимости от расстояния между БС и абонентом. Пересечение этой функции с прямой *Q* дает значение максимального значения радиуса зоны обслуживания, при котором еще предоставляются услуги требуемого качество. Для стандарта GSM-900 *R*~3-10 км (в отдельных случаях до 30 км).

Потому и приходится сужать зону покрытия и увеличивать количество БС, исходя из прогнозов абонентской нагрузки на соту. При расчете абонентской нагрузки и, следовательно, емкости соты часто пользуются моделью. Эрланга для систем с отказом (модель Эрланга В).

В этом случае вероятность отказа в обслуживании (вероятность поступления вызова в момент занятости всех каналов) вычисляется как:



где А=λT - нагрузка (в данной формуле), n - общее число каналов.

Рассчитаем нагрузку на БС, обслуживающую поселок на 50 коттеджей, оборудованных охранной системой, использующих Voice-канал передачи сообщений.

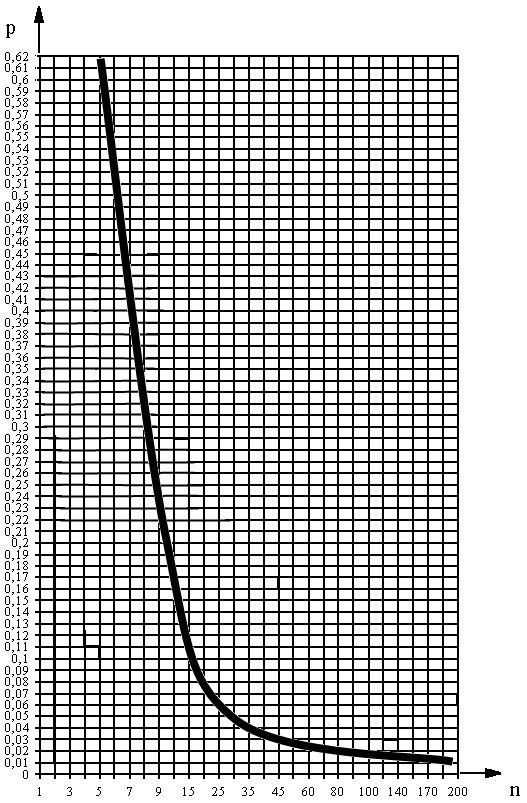


Рис.8. Вероятность отказа в обслуживании от числа каналов

Нагрузка на БС складывается из системных звонков (раз в 5 минут продолжительность - 5 секунд, т.к первые 5 секунд бесплатны) и звонков, осуществляемых гражданскими абонентами. Приблизительно такая нагрузка будет равна A=1. Вероятность отказа в обслуживании (вероятность поступления вызова в момент занятости всех каналов) вычисляется как:



Тогда зависимость вероятности отказа от количества каналов будет представлена на рис.8.

## 3.4 Разработка рекомендаций по улучшению технических характеристик систем безопасности, использующих gsm каналы

Охранные системы на основе GSM можно использовать, как для личных целей, так и в комплексных централизованных системах охраны и мониторинга. Очень выгодно, а иногда единственно приемлемо, использование GSM сигнализации на объектах, где затруднена прокладка кабельных и телефонных сетей.

GSM-сигнализация повышает защищенность объекта собственности благодаря следующим факторам:

факт наличия сигнализации вынудит не опытных преступников отказаться от своих преступных намерений;

оперативная передача тревожного сообщения на телефон собственника или на ПЦН, а так же срабатывание сирены, приведут, в конечном счете, к прибытию на место группы быстрого реагирования или наряда милиции, что в свою очередь приведет к задержанию преступников.

Первое, и очень важное условие: сигнализация должна быть вандалоустойчивой, т.е. находиться в металлическом боксе, где установлены все элементы, в т. ч. - GSM-терминал, колодки подключения шлейфов, блок питания. Это необходимо для выполнения главных ее функций - передачи тревожного сообщения и включения других устройств.

Второе - прибор должен иметь не менее 4 разъемов для подключения различных датчиков. Желательно, чтобы эти зоны были программируемыми - например, к первому разъему - цепочку датчиков движения, ко второму - цепочку дымных датчиков, к третьему - геркон на входной двери, к четвертому - цепочка датчиков удара. Также не помешает 2 выхода на исполнительные устройства (например, световую и звуковую сигнализацию).

Третье - особое внимание необходимо уделить наличию и качеству встроенного источника питания. Источник бесперебойного питания и батарея должны обеспечивать надежную работу централи и подключенных к ней датчиков при отключении питания в течение как минимум суток. Блок питания должен защищать аккумуляторную батарею от глубокого разряда и выдерживать короткое замыкание выходов питания 12 В.

Четвертое - желательно, чтобы имелась выносная светодиодная индикация, которая позволяет визуально контролировать состояние прибора. Это важно при использовании электронных ключей типа Touch Memory, радиобрелоков и карт для дистанционной постановки и снятия прибора с охраны.

Пятое - хорошо, чтобы система могла в одном сообщении полностью описывать состояние всей системы: тревоги с указанием зоны, состояния системы, описывать, какие реле включены, сколько осталось заряда в батарее, каково состояние телефонной линии (если она есть). Имеются и опциональные параметры - к примеру, в зависимости от своего "интеллекта", системы GSM-охраны могут не только сообщать владельцу о проблемах, но и самостоятельно реагировать на такие раздражители. Злоумышленники могут и блокировать сотовую сеть в округе с помощью банальной сотовой "глушилки", поэтому важно, чтобы в ответ, скажем, на вторжение система не тупо перебирала номера для сообщения столь "радостной" новости, а сразу открывала клетки с собаками-телохранителями, зажигала свет, включала сирену или пускала слезоточивый газ.

Шестое - очень важно, чтобы сигнализация умела контролировать наличие или отсутствие сигнала базовой станции. Практически для всех моделей GSM-сигнализаций применение злоумышленником устройств подавления сигнала или создания помех является неразрешимой проблемой. Система должна подавать сигнал предварительной тревоги владельцу здания при ухудшении качества сигнала от базовой станции. Важно если GSM панель передает сообщения одновременно нескольким пользователями и пультам централизованного наблюдения. Сообщения для ПЦН должны передаваться в шифрованном виде (это повышает надежность охранного комплекса). Сообщения для пользователя должны легко читаться и быть максимально информативными. Хорошо когда в одном сообщении полностью описывается состояние всей системы. Тревога с указанием зоны, состояние централи, какие реле включены, есть ли сеть 220, заряд АКБ, состояние телефонной линии (если она есть).

С точки зрения поддержания стабильной радиосвязи необходимо использование таких элементов как выносные антенны. Существуют три ситуации, в которых стационарные направленные пассивные антенны могут помочь:

неустойчивая связь на границе зоны покрытия из предельной удаленности от ближайшей базовой станции (БС)

работа внутри зоны покрытия, но в местах радиотени (складки рельефа, экранировка крупными естественными и искусственными сооружениями)

связь внутри помещения с высокой степенью ослабления сигнала (подвалы и полуподвалы, металлические сооружения, здания, обшитые металлом и т.д.).

Реальное расширение зоны покрытия за счет применения выносной антенны может быть осуществлено, но весьма в скромных пределах. Причем это увеличение сильно зависит от используемого стандарта.

Достаточно сильный эффект дает использование GSM-репитеров, но из-за высокой стоимости применять их рационально на крупных объектах.

Серьезную проблему составляет перегруженность линий связи в крупные праздники. Решением проблемы является установка объектового прибора с sim-картами двух различных сотовых операторов связи.

Оптимальным для GSМ-сигнализаций является комбинирование различных функций (SMS, Voice). Также эффективно использование GSM как дублирующий или дополнительный канал проводным и иным радиоканальным системам передачи извещения.

С точки зрения пропускной способности канала оправдано использование технологии EDGE. Правда, эта технология (как и 3G) не получила еще повсеместного распространения.

## 4. Вопросы безопасности проведения работ по эксплуатации систем безопасности, использующих gsm каналы

Базовые станции в городах, как правило, устанавливаются на административных зданиях, гораздо реже - на жилых. Используются производственные и технические сооружения (трубы заводов или ТЭЦ). Здание должно быть достаточно высоким, чтобы обеспечить максимально широкую зону радиопокрытия. Для обеспечения требуемой высоты установки Операторы часто используют специальные мачты, чтобы обеспечить требуемую высоту установки.

В России действует СанПиН 2.2.4 1191-03 Электромагнитные поля в производственных условиях, на рабочих местах. Санитарно-эпидемиологические правила и нормативы, а также гигиенические нормативы ГДР (ПДУ) 5803-91 (ДНАОП 0.03-3.22-91) Предельно допустимые уровни (ПДУ) воздействия электромагнитных полей (ЭМП) диапазона частот 10-60 кГц Промышленное электроснабжение 50 Гц.

Уровень поверхностной плотности потока мощности в диапазоне частот, в котором работает оборудование сотовых операторов, проверяется специальной аппаратурой: и во многих случаях излучение от БС не фиксируется приборами вообще, так как оно ниже принятых во всем мире стандартов (10 микроватт на кв. см - такова допустимая норма электромагнитного излучения). Следят за этим органы государственного санитарного надзора - именно они выдают соответствующие разрешения.

Даже в самой "опасной" зоне - при нахождении с базовой станцией примерно на одном уровне горизонтально - опасная зона составляет не более 30 метров. Излучение имеет свойство угасать пропорционально квадрату расстояния (если расстояние от источника излучения увеличилось в 2 раза, излучение ослабилось в 4 раза и т.д.). Таким образом, несколько десятков метров удаления от базовой станции - это практически 100-процентная гарантия отсутствия какого-либо излучения, способного влиять на здоровье.

В современных аппаратах мощность излучения может автоматически варьироваться в зависимости от удаленности от передающей станции и прочих условий приема в пределах от 0,2 Ватта до 2 Ватт, т.е. в десять раз. Поскольку организм человека управляется электрическими импульсами слабой мощности, то источник электромагнитного излучения мощностью до 2 Ватт не может не оказывать патогенного воздействия, на нервную систему человека. Мощность однократного воздействия не столь опасна, как его продолжительность, что является еще одной причиной использования выносных антенн.

## Заключение

В данной работе я рассмотрел тенденции развития GSM-систем охраны, основные технические характеристики сотовых сетей применительно к системам охраны. Мною били сделаны технически обоснованные выводы о том, что GSM-системы в настоящее время являются наиболее оптимальными среди других радиоканальных систем для использования. С развитием систем передачи информации по сотовым сетям преимуществ станет больше, и охранные GSM-комплексы выйдут на новый уровень качества, надежности и доступности для пользователей. Я сделал вывод, что крайне эффективным является использование GSM-канала в сочетании с другими каналами передачи извещений (что на данный момент реализуется повсеместно). GSM-системы имеют ряд неоспоримых преимуществ:

возможность использования сервисов оператора сотовой связи для предоставления услуг охраны;

простоту и удобство применения;

доступность сотовой связи подавляющему большинству граждан;

отсутствие необходимости приобретать ретрансляторы для работы системы.

Уже сейчас использование сетей третьего поколения открывает множество дополнительных возможностей, значительно повышая функциональность GSM-систем охраны.

Мною был проведен анализ основных функций GSM-сетей, их использование в системах охраны. Было проведено исследование скорости передачи данных и пропускной способности GSM канала.

Я рассчитал среднюю зону покрытия базовой станции GSM-900 и рассчитал нагрузку на соту, на основании чего сделал вывод о достаточно высокой надежности для охраны дачного поселка.

В своей работе я рассмотрел механизм построения GSM-канала, его основные технические характеристики. До сих пор одним из основных недостатков GSM-канала является его слабая помехозащищенность (вместе с доступностью устройств для глушения сигнала), что делает неэффективным его одиночное применение.

На основании дипломной работы я сформулировал ряд рекомендаций по улучшению технических характеристик систем безопасности, использующих GSM-каналы. На их основании я пришел к логическим выводам о возможных путях развития беспроводных систем охраны.

## Список использованных источников

1. Основыпостроения телекоммуникационных систем и сетей: учебник для вузов / В.В. Крухмалёв, Н.В. Гордиенко, А.Д. Моченов и др.; под. ред. В.Н. Гордиенко и В.В. Крухмалёва. - М.: Горячая линия - Телеком, 2004. - 510 с.: ил.
2. Анин Б.Ю. Защита компьютерной информации / Б.Ю. Анин. - СПб.: BHV - Санкт-Петербург, 2000.
3. Карташевский В.Г. Сети подвижной связи / В.Г. Карташевский, С.Н. Семенов, Т.В. Фирстова. - М.: Эко-Трендз, 2001.
4. Системы мобильной связи: учебное пособие для вузов / В.П. Ипатов, В.К. Орлов, И.М. Самойлов, В.Н. Смирнов; под ред.В.П. Ипатова. - М.: Горячая линия - Телеком, 2003. - 272 с., ил.
5. Кирилов В.И. Многоканальные системы передачи: учебник / В.И. Кирилов. - 2-е изд. - М.: Новое знание, 2003. - 751 с.: ил.
6. Антенно**-**фидерные устройства и распространение радиоволн: учебник для вузов / Г.А. Ерохин, О.В. Чернышов, Н.Д. Козырев, В.Г. Кочержевский; под. ред. Г.А. Ерохина. - 2-е изд., испр. - М.: Горячая линия - Телеком, 2004. - 491 с.: ил.
7. Ксенофонтов С.Н. Направляющие системы электросвязи: учебное пособие для вузов / С.Н. Ксенофонтов, Э.Л. Портнов. - М.: Горячая линия - Телеком, 2004, - 268 с.: ил.
8. Тепляков И.М. Основыпостроения телекоммуникационных систем и сетей: учебное пособие / И.М. Тепляков. - М.: Радио и связь, 2004. - 328 с.: ил.
9. Адрианов В.И. Сотовые, пейджинговые и спутниковые средства связи / В.И. Адрианов, А.В. Соколов. - СПб.: BHV - Санкт-Петербург; Арлит, 2001.
10. Громаков, Ю.А. Стандарты и системы подвижной радиосвязи / Ю.А. Громаков. - М.: Эко-Трендз, 1998.
11. Урядников Ф.Ю. Сверхширокополосная связь. Теория и применение / Ф.Ю. Урядников С.С. Аджемов. - М.: СОЛОН-Пресс, 2005. - 368 с. - (Серия "Библиотека студента")
12. Адрианов В.И. Средства мобильной связи / В.И. Адрианов, А.В. Соколов. - СПб.: BHV - Санкт-Петербург, 1998.
13. Ратынский М.В. Основы сотовой связи / М.В. Ратынский. - М.: Радио и связь, 1998.
14. **Федеральный закон Российской Федерации от 7.07.2003 г. "О связи".**
15. Билинкис В.Д. Методы оценки технического уровня и конкурентоспособности продукции: Учебное пособие - Воронеж: ВГТУ, - 2002. - 118 с.
16. . Системы цифровой радиосвязи: базовые методы и характеристики: Учеб. пособие Волков Л.Н., Немировский М.С., Шинаков Ю.С. (2009 г)
17. Красс М.С. Математика для экономических специальностей: Учебник. - 4 - е изд., испр. - М.: Дело, 2003. - 704 с.
18. Системы и сети передачи информации: Учеб. пособие для вузов / М.В. Гаранин, В.И. Журавлев, С.В. Кунегин. - М.: Радио и связь, 2001. - 336 с.
19. http://ru. wikipedia.org/
20. http://pbsecurity.ru/
21. http://tzmagazine.ru/
22. http://www.secuteck.ru/
23. http://www.akvilona.ru/
24. http://bash.org.ru/
25. http://www.ohrana-gsm.ru/
26. http://www.alarm-gsm.ru/
27. http://www.edgemodem.ru/