

# СИСТЕМА ОХРАННОЙ СИГНАЛИЗАЦИИ МНОГОАБОНЕНТНЫХ НЕТЕЛЕФОНИЗИРОВАННЫХ ОБЪЕКТОВ

**То, что кражи наносят огромный материальный ущерб промышленности и частным лицам, очевидно. А постоянные переживания и страх за сохранность имущества могут вредно повлиять на психику людей. Поэтому в планы важнейших мероприятий ГУВО МВД России 2000 года (в соответствии с приказом МВД России №608-99) и было включено внедрение современных систем безопасности. Они должны обеспечить сохранность имущества и защищенность людей на качественно новом уровне, увеличить число объектов, охраняемых подразделениями вневедомственной охраны, расширить сферу услуг, решить проблемы охраны и жизнеобеспечения объектов особой важности и повышенной опасности. К таким системам безопасности с полным правом можно отнести систему "Рост", разработанную в ООО "Медэл" (г.Рязань).**



М.Даниченко,  
В.Макаров,  
В.Соломаха

- средствами автоматизированного сбора информации о состоянии защищаемых объектов и передачи ее по каналам связи на соответствующий центр для обработки;
- программным обеспечением, реализующим высокоэффективные и надежные коммуникационные, информационные и организационные технологии;
- возможностью конфигурирования под конкретный объект;
- способностью координировать взаимодействие оперативно-технических служб объекта и МВД.

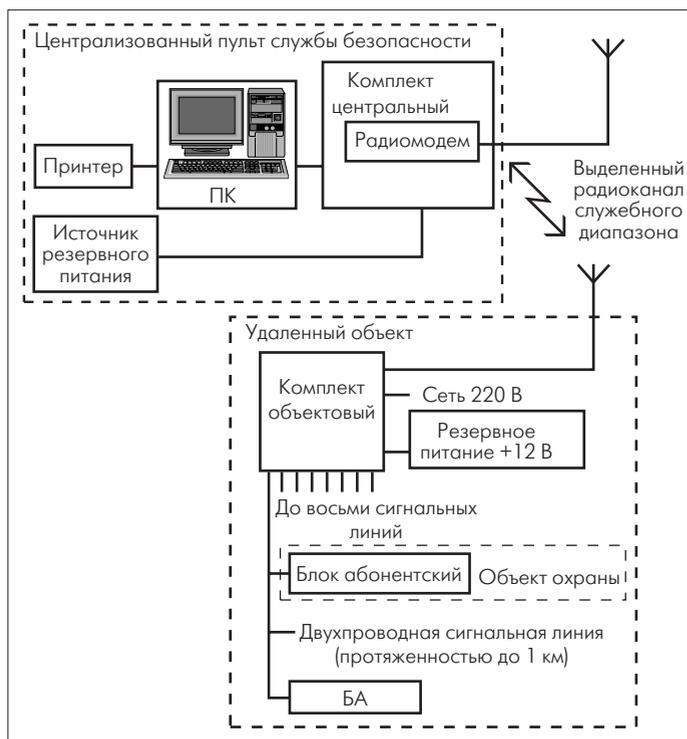
Всем этим требованиям в полной мере соответствует система передачи данных "Рост", опытный образец которой разработан и изготовлен ООО "Медэл" (г.Рязань). В ее функции входит – осуществлять сбор, обработку и передачу данных о состоянии объектов на пульт локальной службы безопасности (при реализации автономного режима охраны) и (или) на пульт централизованного наблюдения, в том числе и вневедомственной охраны МВД. Система предназначена для организации охраны стационарных многоабонентных объектов (многоквартирных домов, гостиниц, гаражных и дачных кооперативов, коттеджных поселков, торговых павильонов, производственных помещений). При доработке программного обеспечения можно использовать ее для экстренного вызова медицинского персонала и телеметрических передач в больницах и клиниках, контроля предельных параметров окружающей среды или технологических процессов на промышленных предприятиях.

В систему, предназначенную для контроля за состоянием удаленных объектов, входит центральный комплект, который совместно с персональным компьютером образует автоматизированное рабочее место оператора наблюдения (пульт службы безопасности), и объектовый комплект, устанавливаемый на удаленном охраняемом многоабонентном стационарном объекте (рис.1). Связь между комплектами осуществляется по радиоканалу с помощью встроенных радиомодемов в служебном диапазоне частот 140–170 МГц со скоростью обмена не менее 1800 бит/с (по желанию заказчика возможно использование любого диапазона частот). При расположении пульта службы наблюдения непосредственно на охраняемом объекте связь персонального компьютера с объектовым комплектом осуществляется по интерфейсу RS-232. В состав системы может входить до 32 объектовых комплектов. Дальность до объекта определяется временем подъезда оперативных групп.

Если число абонентов превышает возможности одного объектового комплекта, связь его с пультом наблюдения происходит по двухпроводному интерфейсу RS-485 (рис.2).

*Автоматизированное рабочее место оператора наблюдения* обеспечивает обмен информацией с объектовыми комплектами, обработку, отображение и хранение данных о состоянии охраняемых объектов. Программное обеспечение, управляемое ОС

На сегодняшний день наиболее перспективными средствами обеспечения комплексной безопасности объектов признаны интегрированные системы [1]. Некоторые из них (в том числе "Рубеж-07-3" и "Дозор") уже включены в Перечень технических средств вневедомственной охраны и разрешены к применению. Каждая из систем предназначена для обеспечения безопасности средних и больших объектов и представляет собой мощный аппаратно-программный комплекс, объединяющий подсистемы охранной и пожарной сигнализации, контроля и управления доступом, систему телевизионного наблюдения и сеть автоматизированных рабочих мест. Однако глобальность задач интегрированных систем требует больших затрат на собственно аппаратуру, программное обеспечение, монтаж и обслуживание, что сдерживает широкое их применение. Распространение и живучесть той или иной системы во многом определяются ее удельной стоимостью, приведенной к одному объекту охраны. Так что рынок недорогих систем безопасности многоабонентных объектов по-прежнему открыт и свободен. Для предотвращения и ликвидации угроз эти системы должны обладать [2]:



**Рис. 1. Структура системы "Рост" для удаленных объектов**

Windows 95, включает в себя подсистемы конфигурирования объектов, оперативного контроля и управления, протоколирования событий. На мониторе пульта наблюдения отображаются текущее состояние объектов охраны и тревожные сообщения в виде мнемонической схемы и таблиц. Ведется постоянный автоматический контроль работы оператора системы, все его действия в требуемый момент времени заносятся в протокол системы. Осуществляется диспетчеризация оперативно-технических групп реагирования.

*Объектовый комплект* выполняет функции концентратора, осуществляя сбор информации о состоянии индивидуальных охраняемых объектов, число которых достигает 288 (8 сигнальных линий по 36 объектов). В комплекте предусмотрены переход на резервное питание (аккумуляторные батареи +12 В) при пропадании сети 220 В, защита от короткого замыкания и обрыва сигнальной линии связи с абонентскими блоками с определением места нарушения, формирование сигнала при несанкционированном проникновении в аппаратуру комплекта.

*Абонентский блок* установлен на каждом индивидуальном объекте, например в квартире, гаражном боксе, садовом домике, гостиничном номере, торговой палатке и т.п. По двухпроводной сигнальной линии (общей для всех абонентских блоков) он связан с объектовым комплектом. По этой линии на абонентские блоки одновременно поступают информация и электропитание (постоянное напряжение 24 В). Топология линии протяженностью до 1 км при этом может быть различной: звездообразной, древовидной, кольцевой. Полярность включения и распределение абонентских блоков на линии – произвольны (работоспособность сохраняется при подключении всех 36 блоков на конце линии).

Сам абонентский блок представляет собой трехшлейфовое приемно-контрольное устройство, осуществляющее сбор первичной информации о состоянии объекта. Он обеспечивает независимое управление режимами охраны объекта:

- "Контроль" – взятие под охрану объекта соответствующими службами;

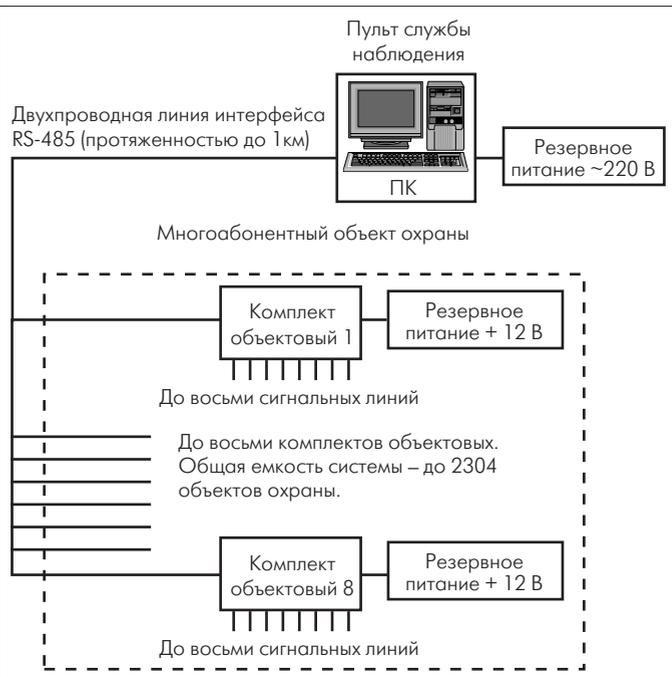
- "Доступ" – санкционированное проникновение на объект и снятие объекта с охраны.

Смена режимов охраны происходит с помощью кодового механического ключа или брелоков дистанционного ИК-управления, которые имеют кнопки для снятия и постановки на охрану. Индикация режимов – звуковая, от встроенного пьезоэлектрического излучателя. Для внешних маломощных (36 В, 0,25 А) световых или звуковых сигнализаторов предусмотрен релейный выход.

Блок оснащен двумя шлейфами охранной сигнализации. Первый контролирует входной шлюз (дверь квартиры, калитку гаражных ворот и т.д.). Второй образует основной контур сигнализации по всему помещению. Шлейфы обладают повышенной имитостойкостью за счет контроля их сопротивления в пределах  $\pm 10\%$  и могут работать с любыми датчиками, имеющими нормально замкнутые выходные контакты. Кроме того, блок содержит шлейф аварийных сигнализаторов, предназначенных для включения датчиков предупреждения различных видов угроз (пожар, утечка газа, топлива и воды) и контроля предельных параметров окружающей среды.

Каждый абонентский блок оборудован кнопочным выключателем "Нападение" для экстренного формирования сигналов при открытой угрозе или нападении на хозяина объекта (предусмотрена возможность для монтажа выносного кнопочного выключателя). Корпус блока защищен датчиком несанкционированного проникновения в его аппаратуру. На лицевой панели блока установлены светодиодные индикаторы работоспособности системы и исправности охраняемых шлейфов. Это позволяет пользователям объекта контролировать целостность шлейфов при постановке на охрану (не полное закрытие окон, нарушение проводки шлейфов при ремонте и т.п.)

Достоинство системы "Рост" – специально разработанный ООО "Медэл" способ обмена информацией, обеспечивающий высокий уровень помехозащищенности при передаче данных от источника первичной информации до пульта наблюдения [3]. Особое внимание уделено защите действующих абонентских блоков от умышленного их изъятия и введения в работу ложных. Каждый абонентский блок имеет серийный номер (32 бита), который записывается в ПЗУ микроконтроллера. При инициализации системы этот номер заносится



**Рис. 2. Структура системы "Рост" для объекта с большим числом абонентов**

сится в базу данных компьютера автоматизированного рабочего места оператора наблюдения. Однако использовать полный адрес в сеансе не представляется возможным из-за возникающего резкого снижения скорости передачи в линии. Поэтому для осуществления адресного сеанса запроса-ответа каждому блоку присваивается еще и индивидуальный номер в линии (6 бит), по которому производится обращение.

Защита от дубликата, сознательно введенного вместо рабочего абонентского блока, например краденого из другой системы и имеющего аналогичный номер в линии, заключается в установке блоком в ответном сигнале бита рестарта, который в соответствии с алгоритмом формируется при включении питания и не может быть снят блоком иначе как по сигналу подтверждения приема объектовым комплектом. В свою очередь, на поступление бита рестарта объектовый комплект выдает команду на идентификацию блоков по серийным номерам (рис.3). Подлог незамедлительно фиксируется. Аналогично выявляется и подмена при внедрении “двойника” абонентского блока в обесточенную сигнальную линию, например в момент ремонтно-профилактических мероприятий.

Объектовый комплект и абонентский блок разрабатывались для эксплуатации в условиях значительных перепадов температуры, влажности, сильных электрических помех и наводок. Это потребовало использования дополнительных приемов по повышению устойчивости и достоверности передаваемой информации. Один из них – передача синхросигнала (см.рис.3), например 10 импульсов с фиксированным периодом  $t_1$ , предваряющего каждый пакет запроса и ответа. Это дает возможность принимающей стороне сформировать свой эталон длительности, который потом будет использован в идентификации информационных битов. По усредненной за 10 импульсов оценке периода  $t_1$  корректируется значение ожидаемых на приеме и жестко связанных с ним периодов информационных битов от источника информации. Такая последовательность импульсов будет уникальной в пакете данных, а также в линии вообще, поэтому на приемной стороне она не может быть спутана с

другой частью информационного пакета. Подобная корректировка позволяет обойтись в удаленных блоках без дорогостоящих мер по температурной стабилизации частоты тактовых генераторов. При этом скорость передачи в линии и достоверность передаваемой информации не снижаются.

Другой прием – передача объектовым комплектом абонентскому блоку бита подтверждения приема данных в составе сигнала запроса для следующего (по номеру в линии) абонентского блока. Такой прием подтверждения позволяет отказаться от дополнительного информационного пакета и, следовательно, от увеличения общего цикла опроса удаленных блоков. Это, с одной стороны, ведет к высокой скорости обновления информации от удаленных датчиков, а с другой – позволяет вести работу в условиях помех благодаря дополнительным сеансам обмена в линии взамен несостоявшихся.

Еще один прием по повышению помехоустойчивости передачи данных – механизм контроля достоверности информации (контроля достоверности сеанса связи в условиях помех) с помощью передачи данных сначала в прямой, а затем в инверсной форме. Он существенно повышает надежность контроля по сравнению с контролем одним только битом паритета (четности). А в случае непрохождения всего сообщения дает возможность использовать информацию в одной из половин пакета (прямой или инверсной), в которой бит паритета является истинным. В предлагаемом способе полная длительность информационного пакета всегда будет одинакова, так как число периодов информационных битов при любом значении данных будет неизменным (суммарное число нулей в прямой и инверсной форме всегда равно суммарному числу единиц). Поэтому на приемной стороне заранее известна длина пакета, и на ее ожидание всегда отводится одинаковый (постоянный) тайм-аут, что позволяет контролировать достоверность выполняемого в линии обмена также и по временным параметрам.

Объектовый комплект контролирует не только состояние датчиков удаленных блоков, но и наличие, исправность самих удаленных блоков и исправность двухпроводной линии связи по проценту корректных сеансов связи с удаленными блоками (заданному для данной системы). Поэтому такой алгоритм запоминания тревожных изменений, как совокупность механизмов подтверждения приема данных объектовым комплектом и контроля абонентским блоком собственного старта, рестарта и целостности блока, гарантирует обнаружение любых, в том числе и кратковременных, тревожных изменений или нештатных ситуаций в системе. Это возможно и при действии в линии помех, возникающих как из-за условий эксплуатации, так и преднамеренно.

При организации радиоканала передачи данных требовалось решить проблему, связанную с жестким ограничением задержки поступления тревожного сообщения о нападении на объект охраны, которое не должно превышать 2 с. Это предполагает получение и подтверждение приема информации от всех 32 объектовых комплектов в данном интервале времени. Проблема устранена двумя путями. Во-первых, использованием в радиомодемах специализированных радиостанций для систем телеметрии с временем переключения прием-передача не более 50 мс и, во-вторых, применением метода сжатия данных.

Коммерческий успех, а также технический, экономический и социальный эффект системы “Рост” могут обеспечить ее основные отличительные особенности:

- любое территориальное расположение объектов охраны по городу и пригородам (дальность до объекта охраны полностью определяется временем реакции соответствующих служб);
- число объектов охраны – до 9216;

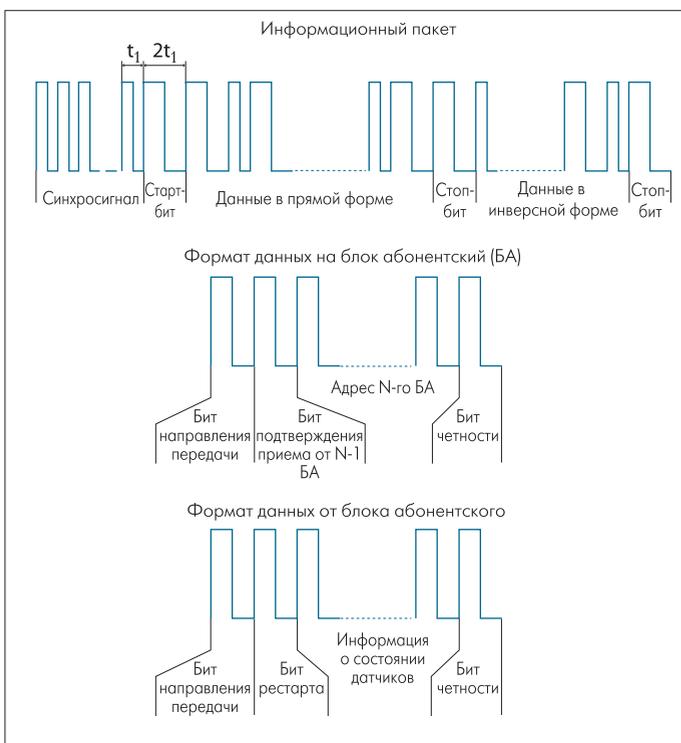


Рис.3. Упрощенная структура информационных пакетов данных в сигнальной линии



- независимые постановка и снятие с охраны каждого объекта охраны;
- полная независимость абонентского блока от системы электропитания объекта и резервное питание при пропадании сети 220 В;
- малое время и небольшие затраты на монтаж объектового комплекта;
- модульная структура системы, гибкость программного обеспечения, широкая номенклатура датчиков, позволяющие выполнять практически любые индивидуальные требования по организации охраны объектов, наращивать мощность системы и оперативно менять конфигурацию;
- наглядный графический интерфейс, обеспечивающий простоту и удобство в работе, в результате чего обслуживание системы не требует высокой квалификации оператора;
- полная персонализация пользователей с указанием путей оповещения хозяев объекта при тревожных сообщениях;
- ведение системного протокола, в который заносятся все события, включая действия обслуживающего персонала и пользователей;
- возможность просмотра и распечатки протокола наблюдения в целом или его фрагментов, выбранных по определен-

ным критериям (дате, месту, конкретному лицу, типу сообщений или их комбинаций).

Сегодня проводится работа по наращиванию функций системы, а именно введение режима аудиодомофона с возможностью управления дверным шлюзом и обмена данными между объектовым и центральным комплектом по телефонному каналу.

#### ЛИТЕРАТУРА

1. Козьминых С., Крахмалёв А. Интегрированные системы – перспективы развития средств обеспечения безопасности. – Техника охраны, 2000, №1.
2. Мотин Л. Роботы для противопожарной защиты в интегрированных системах безопасности. – ЭЛЕКТРОНИКА: НТБ, 2000, №2 с. 44–46.
3. Пат. 2155383 РФ. Способ обмена информацией в системе тревожной сигнализации/ Даниченко М., Дронников А., Соломаха В., Тюремов Н. Оpubл. 27.08.2000. Бюл. №24.

Редакция журнала приносит свои извинения фирме National Instruments за досадную ошибку, допущенную в № 1/2001 г. в адресе сайта. Правильное название: [www.ni.com/russia](http://www.ni.com/russia)

## Угроза кибертерроризма гражданской авиации

Безопасность гражданской авиации – одна из наиболее важных проблем международной безопасности ближайших лет. Теперь к шести главным категориям угроз гражданской авиации, определенным Международной организацией гражданской авиации (ICAO), – незаконному захвату и саботажу, включая террористические акты; несанкционированной перевозке опасных предметов; присутствию буйных пассажиров в салоне; зенитным управляемым ракетами; трафику в ядерных и других расщепляемых материалах; саботажу, подстрекаемому экономической конкуренцией, прибавилась седьмая – кибертерроризм.

ICAO давно начала проводить анализ и формирование противодействия в отношении угроз всех этих категорий, за исключением кибертерроризма, являющегося новейшей и наиболее неуловимой угрозой гражданской авиации в XXI веке. Кибертерроризм может проявляться в различных формах. В простейшем виде – это средство дезинформации или психологическое оружие. В большинстве форм кибертерроризм способен привести к пагубным последствиям – повреждениям и большим разрушениям в аэропортах и на самолетах.

Подобно всем другим аспектам международной гражданской авиации, безопасность – глобальная проблема, которая и решаться должна глобально. Некоторые национальные и международные организации уже создали командные центры для выработки способов защиты от кибератак на критические коммуникационные инфраструктуры. США обнародовали в 2000 г. свой план по объединению усилий мер безопасности существующих федеральных компьютеров. Отдел антитерроризма Интерпола установил постоянный мониторинг открытого использования агитационных вебсайтов известными международными транснациональными террористическими и мятежными группировками.

На недавнем совещании исследовательской группы ICAO было решено, что эта организация должна изучать возможные средства защиты от разного рода кибератак, которые могут существовать в системах CNS/ATM. Одним из решений может быть применение различных видов шифрованного противодействия.

ICAO Journal, 2000, June, p.18–19,26