

УСОВЕРШЕНСТВОВАНИЕ СИСТЕМ СИГНАЛИЗАЦИИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ GSM-КАНАЛА

Пирогов С. Н.

Научный руководитель – д. т. н., проф. Коваль Ю. А.

Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Ленина, 14, каф. Основ радиотехники (ОРТ),
тел. (057)7021430

The report covers the GSM signaling. The main methods of improving systems to ensure the safety of any complexity. The results of studies and analysis of the prospects of development of systems of this type.

В настоящее время безопасность материальных ценностей, движимого и недвижимого имущества практически не обеспечена без применения надежной и высококачественной охраны. Но высокопрофессиональная охрана на сегодняшний день невообразима без применения разнообразных технических разработок, которые дают возможность проводить круглосуточные охранные мероприятия, предельно минимизировав так называемый «человеческий фактор», уменьшить затраты на ее обслуживание и качественно поднять уровень надежности.

Среди таких технических разработок можно отметить высокотехнологичные и прогрессирующие тенденции в развитии и улучшении различных систем безопасности, основанных на, так называемой, GSM-сигнализации.

Основой систем GSM-сигнализации является приёмо-передающий комплекс (ППК), который обрабатывает сигналы от датчиков и передает сигнал тревоги и другие информационные сигналы по GSM-каналу на пульт центрального наблюдения либо телефон пользователя (рис. 1).

Системы GSM-сигнализации имеют ряд преимуществ (мобильность, надежность, простота инсталляции), которые позволяют им выходить на лидирующие позиции при охране различных объектов, таких как, квартиры, дачи, магазины, склады, заводские цеха и др [1].



Рисунок 1 – Структура типовой системы GSM-сигнализации

Среди наиболее распространенных отечественных систем можно выделить «Лунь-9Т», «Дунай», «Грифон».

По принципу подключения охранных датчиков к ППК делятся на беспроводные, проводные и комбинированные.

В системах GSM-сигнализации используются два типа извещения – при помощи SMS и с использованием пакетной передачи данных (GPRS, EDGE)[2].

В докладе анализируются недостатки систем сигнализации и рассматриваются возможные пути их совершенствования.

Основной уязвимостью систем GSM-сигнализации является доступ сторонних лиц к SIM-карте. Скопировав данные карты и зная тип передающего устройства, злоумышленник может отключить либо модифицировать систему. Правильная организация и расположение ППК делает такое действие практически неосуществимым [2].

Вторым существенным недостатком является подавление сигнала. Это наиболее популярный и действенный способ борьбы со средствами GSM-сигнализации. При помощи «джамера-глушилки» генерируются помехи. При этом уровень полезного сигнала падает ниже критического и связь ППК с базовыми станциями оператора прерывается. Если в этот момент сработает датчик, то сигнал тревоги будет сгенерирован, но передать его удастся, лишь в момент восстановления связи.

Для повышения помехозащищенности предлагается ряд методов. Для определения места уверенного приёма GSM-сигнала рекомендуется проводить радиомониторинг. Установка направленной антенны, ориентированной на базовую станцию, существенно повышает помехозащищенность. Рекомендуется также применение разветвленной системы, когда местонахождение ППК является скрытным.

Для повышения надежности предлагается режим «запрос-ответ», при котором и самая надежная система, когда центральный пункт связывается с ППК, проверяя наличие связи. Предлагаемые методы можно применять комплексно[3].

Весьма перспективным представляется использование новых протоколов и сетей 3G, специально предназначенных для корпоративных клиентов – виртуальные корпоративные сети передачи данных с имитостойкостью и защитой информации. Такие системы будут иметь существенно большие информационные возможности и быть более защищенными.

Список литературы:

1. <http://www.tzmagazine.ru/jpage.php?uid1=378&uid2=379&uid3=395>.
2. Тепляков И.М. Основы построения телекоммуникационных систем и сетей: учебное пособие / И.М. Тепляков. – М.: Радио и связь, 2004. - 328 с.: ил.
3. <http://www.secnews.ru/articles/>.