УДК 621.396.6.001.63

СХЕМОТЕХНИЧЕСКИЕ ОСОБЕННОСТИ СИСТЕМ СИГНАЛИЗАЦИИ

А.С. ЛЕПОТЕНКО
(Представлено: канд. техн. наук, доц. Д.А. ДОВГЯЛО)

Рассмотрен принцип работы автоматизированной охранной системы. Определены основные задачи при проектировании охранных систем сигнализации. Приведены возможности модернизации охранной системы А6-04.

В настоящее время большое распространение получили системы охраны и пожарной безопасности. С каждым годом благосостояние человека увеличивается, что требует дополнительных устройств для защиты от посягательств. Для этого и разрабатываются охранные системы. Самые первые системы охраны зародились еще в Древних Египте и Японии и не имели ничего общего с нынешними системами безопасности [1]. Современные системы сигнализации представляют собой очень мощные устройства, способные не только обнаруживать и информировать, а так же, в случае необходимости, обезвреживать источник нарушения. Фундаментальным открытием, ставшим залогом всех будущих систем охраны, стал переход к цифровой обработке информации. Это дало возможность повысить быстродействию систем и увеличить защищенность от помех. Открытие фотоэлемента позволило автоматизировать систему сигнализации – стать ее “глазами“. Немаловажную роль в развитии систем охраны сыграла разработка датчиков различных физических величин, которые непосредственно встраиваются в системы охраны и расширяют их функциональные возможности. Основными датчиками, которые входят в типовую охранную систему можно считать следующие[2]:

– датчик движения, который может быть реализован на различных принципах преобразования (ИК-датчик, определяющий нарушение неприкосновенности объекта по излучаемому тепловому потоку; УЗ-датчик, определяющий время необходимое ультразвуковой волне для движения от датчика до объекта и назад; микроволновый датчик);

– датчик разбития стекла, как правило, акустический;

– датчик открытия и закрытия дверей, реализуемый бесконтактно, т.е. с использованием гальваномагнитных преобразователей или герконов;

– датчик дыма.

В настоящее время развитие систем сигнализации не стоит на месте. Для управления системами охраны подключают удобные пульты управления, через которые можно перепрограммировать данные устройства на определенные области защиты.

В последние годы появились множество систем охраны, которые устанавливают в жилых домах, их называют системами «умный дом». Эти системы могут управляться со смартфона хозяина через канал Wi-Fi. Передачу данных о нарушениях защищаемой области можно передавать по каналам GSM или GPRS.

Рассмотрим схемотехнические особенности систем сигнализации. Проанализируем их работу на примере весьма распространенной системы охраны А6-04 компании “АЛАРМ”. На рис. 1 показана обобщенная структурная схема А6-04.

Подобные структурные схемы реализованы и в других системах охраны. На схеме можно выделить следующие блоки и модули: модуль обмена информацией между терминалами (интерфейсы), блок управления - обработки информации, блок питания с системой защиты по питанию, блок управления шлейфами или зонами охраны (блок контроля датчиков), модуль формирования извещений на различные внешние устройства. Рассмотрим специфику этих устройств.

Для повышения быстродействия в блоке обработки информации применен микроконтроллер семейства ATmega 8, отличающийся своей функциональностью, гибкостью и удобством в обращении. Для «облегчения» процесса обработки и связи с другими устройствами к микроконтроллеру подключена пара регистров. Так же присутствует отдельная микросхема памяти для хранения основных команд, которые могут поступать из различных источников, например, программирование можно осуществлять с помощью пульта ПР-1, командно-управляемой панели или специализированных программаторов[3]. За счет применения в системе микроконтроллера ATmega 8 уменьшена задержка на обработку сигналов. Однако повышение скорости обработки сигнала зависит не только от аппаратной части блока обработки, но и от его программной части.

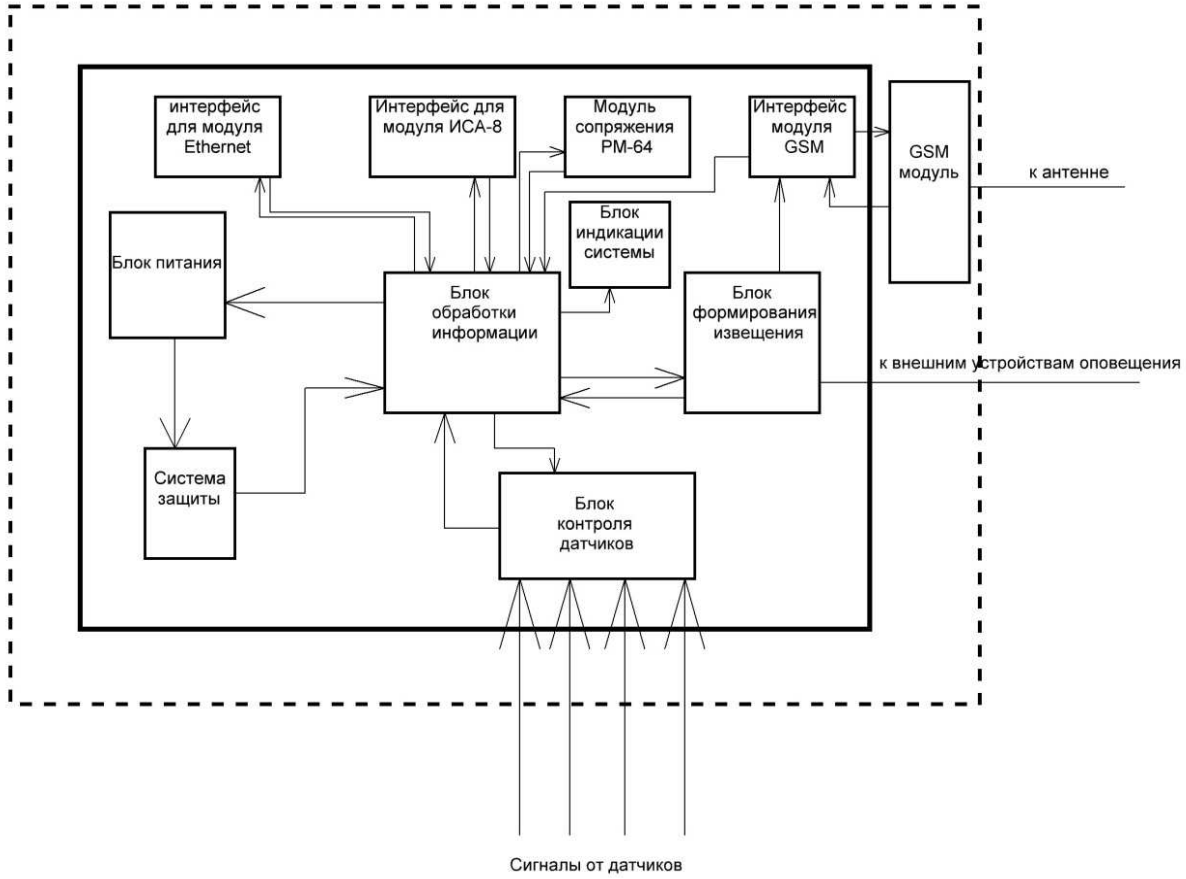

Рис. 1. Структурная схема системы сигнализации А6-04

Блок питания представляет собой источник, который формирует определенные питающие напряжения на все узлы охранной системы. Весьма важным является поддержание необходимого уровня питающих напряжений при скачках напряжения в сети или при его отсутствии. Для этих целей вводят специальные высокоточные каскады стабилизаторов напряжения, используют бестрансформаторные блоки питания, что позволяет значительно сократить габаритные размеры центрального модуля системы сигнализации. Для подавления высокочастотной составляющей в блок питания включают LC-фильтр. Так же в блок питания входит система защиты от высокого напряжения и тока – наборы специально подобранных плавких предохранителей.

Часто бывает, что в сети пропадает питающее напряжение, в результате чего охраняемая зона может быть подвержена атакам. Поэтому к системе подключают опорный источник питания, представляющий собой аккумулятор. Емкость аккумулятора составляет обычно 7000 мА/ч, чего хватает для обеспечения непрерывной работы в течении нескольких часов.

Важной частью системы сигнализации являются каналы оповещения. К ним относятся звуковые, световые и информационные системы. В последнее время весьма популярной среди информационных систем оповещения является GSM-система. Основная особенность GSM-модуля – возможность управления и получения информации от охранной сигнализации по каналу GSM-связи сотового оператора.

Главным управляющим элементом устройства является микроконтроллер ATmega 168 компании Atmel. С блока формирования извещения на GSM-модуль поступает сигнал о нарушении режима безопасности (нарушения периметра охраняемой зоны). Дальнейшие действия связаны с отсылкой SMS-сообщения, данное действие производится модулем SIM900[4]. В схеме используется несколько контрольных светодиодов: LED1 – контроль работы модуля GSM (при наличии связи и работы модуля моргает с частотой одна вспышка в течении 2-3 секунд, в остальных случаях имеются проблемы со связью или с самим модулем); LED2 – контроль работы системы (в рабочих режимах моргает с частотой 3 – 5 раз в секунду, в режиме программирования горит постоянным светом)[5]. Программирование GSM-модуля может осуществляться непосредственно сотовым телефоном посредством набора специальных команд, которые записывают в память sim-карты и впоследствии используют для управления системой охраны.

Как бы не были совершены современные GSM-модули, но и у них есть ряд недостатков, основным из которых является обеспечение защиты информации. Сегмент передачи данных от GSM-модуля к базовой станции имеет следующие слабые стороны:

– активные атаки (GSM-оборудование может подвергаться атакам устройств, имитирующих работу базовых станций);

– невозможность определения достоверности данных;

– слабые алгоритмы шифрования.

Таким образом, локальный интерфейс GSM-модуля и область передачи данных до базовой станции нельзя считать полностью защищенными.

Одним из самых распространенных методов повышения защиты является использование SSL-протокола [6]. SSL-протокол - криптографический протокол, обеспечивающий безопасную передачу данных по сети. Создаются определенные SSL-туннели, которые обеспечивают защиту от посягательств - рис. 2.

Рис. 2. Структурная схема передачи данных с SSL-шифрованием

С учетом этого, незащищенным остается только канал связи от базовой станции к клиенту. Однако SSL-шифрование можно использовать и в данном канале, но для этого необходимо обращаться к оператору сотовой связи и договариваться о подключении данной функции.

GSM-модули постоянно улучшаются и их функциональные возможности также расширяются. Одной из очень удобных функций является управление всей системой безопасности по GSM-каналу. В результате получается двунаправленный канал передачи и приема информации. Следует отметить, что для включения данной функции необходимо привлекать дополнительные как программные, так и аппаратурные средства, что значительно повышает функциональную сложность устройства и его стоимость.

Для повышения функциональных возможностей системы сигнализации А6-04 используют в основном программные методы, например, улучшение алгоритма прошивки. В последнее время очень широкое распространение получило использование определенных платформ, которые за счет реализации алгоритма своего функционирования повышают быстродействие системы и ее стабильность. Одной из веток развития GSM-модулей являются GSM-модули на J2ME. Java ME (J2ME) - это мощная встраиваемая платформа, предназначенная для мобильных устройств и систем безопасности. Она позволяет расширить функциональные возможности GSM-модулей. К основным ее преимуществам можно отнести:

– высокий уровень безопасности и защищенности системы в соответствии с сертификатами X.509;

– наличие встроенных средств отладки;

– высокую стабильность, отсутствие перезагрузок системы;

– внедрено средство затруднения восприятия кода.

Однако остаются несколько проблемных вопросов, требующих решения. Во-первых, для функционирования JAVA платформы необходим высокопроизводительный аппаратный комплекс, который сочетал бы в себе миникомпьютер. На рынке имеется множество вариантов одноплатных компьютеров, которые миниатюрны и при этом практически не теряют своей функциональности, например PC-G03 компании Intel. Вторым немаловажным аспектом является обеспечение связи модуля А6-04 и миникомпьютера. Этот нюанс решается достаточно легко, т.к. у модуля охранной системы есть большое количество интерфейсов, которые поддерживают персональные компьютеры, например Ethernet, RS-485 и многие другие [7].

Таким образом, можно считать, что, владея определенным уровнем знаний языка программирования можно проектировать и реализовать свои собственные программы для охранных систем.

ЛИТЕРАТУРА

1. Коверзин, Д. Особенности охранных систем [Электронный ресурс] / Д. Коверзин. – Режим доступа: http://sigadoma.ru/oxrannaya-signalizaciya/istoriya-razvitiya-oxrannoj-signalizacii.html. – Дата доступа: 10.03.2015.
2. Охранные системы [Электронный ресурс]. – Режим доступа: http://www.sob.by/safe.php. – Дата доступа: 12.04.2015.
3. ОАО ”АЛАРМ”, a6_operating_manual_part 1/ОАО”АЛАРМ” [Электронный ресурс]. – Минск, 2012. – Режим доступа: http://www.rovalant.com/download/a6_operating_manual_part1.pdf-c.19-25, 39-45.
4. SimCom, datasheet Sim 900 [Electronic resource]. – 2012. – Mode of access : http://amigalounge.com/files/SIM900_HD_V1.01(091226).pdf. – Date of access : 04.05.2015.
5. Дмитренко, Д. Прибор сигнализации GSM на основе модуля SIM900 [Электронный ресурс] / Д. Дмитренко. – 2009. – http://ddn.radioliga.com/cnt/11.htm. – Дата доступа: 03.03.2015.
6. Нестеров, В. Вопросы безопасности передачи данных [Электронный ресурс] / В. Нестеров, О. Пушкарев. – 2010. – Режим доступа: http://www.wireless-e.ru/assets/files/pdf/2008_4_32.pdf. – Дата доступа: 19.03.2015.
7. Робль, Р. Прогрессивные GSM-модули на J2ME [Электронный ресурс] / Р. Робль, З. Марич. – 2013. –Режим доступа: http://www.wireless-e.ru/assets/files/pdf/2010_02_12.pdf. – Дата доступа: 25.03.2015.

УДК 004.051

УВЕЛИЧЕНИЕ СКОРОСТИ ЗАГРУЗКИ ВЕБ-САЙТОВ

Ю.В. ЛАПТЕВ
(Представлено: канд. техн. наук, доц. Р.П. БОГУШ)

Рассматриваются наиболее полезные советы по оптимизации скорости загрузки веб-сайтов на стороне клиента.

С каждым годом Интернет растет очень быстро. Увеличивается пропускная способность каналов, а вместе с ними и количество передаваемого трафика. Сайты становятся больше по размеру и сложнее во взаимодействии. Размеры загружаемых файлов увеличиваются многократно, а время ожидания пользователей не уменьшается. За последние 5 лет средний размер веб-страниц вырос в 5 раз, а за последний год – в два раза. При этом каждая страница использует много различных объектов, что негативно сказывается на общем времени загрузки. Только около 5-10% от общего времени загрузки приходится на серверную часть. Все остальное составляет именно клиентская архитектура. Что обычно видит пользователь, заходя на сайт, и как долго он это видит? 70% посетителей уйдут после 10 секунд пребывания на сайте. При этом наиболее характерным временем ожидания будет 4 секунды: если за это время сайт загружается у 90% пользователей, то это считается быстрым веб-ресурсом. Однако многие компании пытаются выжать из своего сайта максимум по скорости работы. Недаром высоконагруженные проекты типа Google, Amazon, Вконтакте, Facebook и Одноклассники очень серьезно подходят к вопросу скорости загрузки своих сайтов. За каждым потерянным моментом времени кроется определенная сумма денег [1].

При помощи различных способов оптимизации загрузки веб-страниц удастся в разы уменьшить время ожидания полной загрузки страницы, а также сохранить больше активных пользователей, особенно среди тех, кто испытывает различные проблемы сетевого соединения.

Основной раздел. Клиентская оптимизация — это оптимизация процесса загрузки клиентским приложением содержимого веб-страниц. Основная цель такого процесса — достижение максимальной скорости загрузки страниц сайта браузером клиента. При построении высокопроизводительных сайтов должен присутствовать и серверный, и клиентский подход, они много в чем дополняют друг друга. Главное отличие клиентского подхода состоит в том, что в качестве объекта оптимизации рассматриваются страницы сайта, состоящие из HTML-документа, содержащего вызовы внешних объектов, а также сами внешние объекты (чаще всего это файлы стилей, скрипты и изображения). Различные технологические решения клиентской области сайта при одинаковой нагрузке на сервер могут обеспечивать совершенно разные характеристики клиентского быстродействия. При исключении из рассмотрения всех факторов, относящихся к серверному программному обеспечению и каналу передачи данных, можно заключить, что увеличение скорости загрузки страницы на различных стадиях загрузки принципиально возможно за счет ограниченного количества методов. Об этих методах и пойдет речь далее[1].

Одним из основных способов по увеличении скорости загрузки является уменьшение количества HTTP-запросов. Около 80% загрузки страницы ориентировано на загрузку компонентов страницы: скриптов, изображений, стилей, flash. Спецификация HTTP/1.1 советует, чтобы браузеры параллельно загружали не более 2-х компонентов веб-страницы с одного хоста. Уменьшив количество этих компонентов мы уменьшаем количество HTTP-запросов к серверу и как результат увеличиваем скорость за-