А. В. Мамаев

ПРОГРАММНО-АППАРАТНАЯ РЕАЛИЗАЦИЯ НИЗКОЧАСТОТНОГО АКТИВНОГО КАНАЛА ПЕРЕДАЧИ СИГНАЛОВ В СИСТЕМАХ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧЕК

В рамках проводимых исследований систем защиты информации от утечек была показана необходимость создания резервного канала передачи данных, сигналов тревоги для подсистемы мониторинга за рабочими станциями [1]. Решение этой проблемы, предложенное в предыдущей работе [2], не позволяло обеспечивать должный уровень защищенности. Главным минусом оказалось низкое соотношение сигнал/шум, что приводило к невозможности корректной передачи сообщений в условиях большого числа потребителей электроэнергии.

В данной работе предлагается осуществлять передачу сигналов по сети электропитания ЭВМ другим способом. Суть метода заключается в том, что генерация скачка напряжения производится на фазе сети электропитания в моменты, когда значение напряжения в сети близко к нулю [3]. Это обусловлено тем, что на этой фазе волны ни одно из устройств, питаемых из сети, не потребляет ток! А потребление тока внешними по отношению к системе устройствами является главным источником шума для передаваемого сигнала. В результате становится возможным создание кратковременных высокоамплитудных импульсов напряжения при значении напряжения несущей волны, близком к нулю. Это обеспечивает высокое отношение сигнал/шум.

Для реализации данной схемы канала передачи информации необходимо аппаратное дополнение компьютера передатчика. Специально сделанная плата устанавливается в блок питания (БП) компьютера. Провод питания номиналом минус 5В в современных материнских платах не используется, что позволяет нам применить его для соединения COM-порта материнской платы с БП компьютера. Установленная в БП плата с двумя электролитическими конденсаторами и двумя ключами-транзисторами позволяет сдвинуть во времени момент передачи сигналов и передавать сигнал, когда значение напряжения в сети близко к нулю [4].

Принципиальная схема системы защиты информации от внутреннего нарушителя, дополненная системой передачи по сети электропитания электронно-вычислительной машины (ЭВМ) сигналов оповещения, представленная на рис. 1, не изменилась.

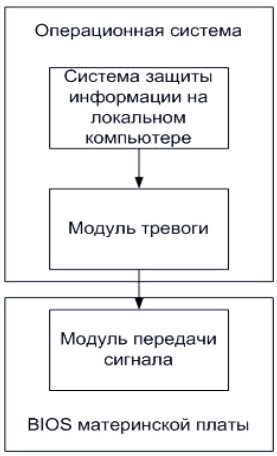

Рис. 1. Принципиальная схема измененной системы защиты

В случае нарушения политики безопасности используемая на локальном компьютере система защиты выдает соответствующий сигнал тревоги. Далее сигнал тревоги поступает в наш

«Модуль тревоги». Данный модуль выполняет очень важную роль — осуществляет доступ к BIOS локальной машины. Таким образом, он выполняет функции драйвера, дающего возможность работать в режиме ядра и обращаться напрямую к аппаратным ресурсам, и функции приложения, работающего в пользовательском режиме и осуществляющего отслеживание и дальнейшую передачу сигналов тревоги.

Сигнал тревоги формирует вызов из BIOS программы «Модуль передачи сигнала». Сигнал, попавший в BIOS локальной машины, отправляется дальше по созданному каналу связи, где далее будет зарегистрирован специальным регистрирующим устройством компьютера-приемника.

Данная схема позволяет защитить атакуемый компьютер от угроз типа:

- нарушение работоспособности локально-вычислительной сети;
- навязывание ложной информации.

Для защиты от загрузки операционной системы с внешних носителей предлагается встроить в «Модуль передачи сигнала» функцию таймера, сброс таймера производится специальным сигналом от «Модуля тревоги». При включении компьютера запускается минутный таймер, если загружается штатная операционная система, то установленный в ней «Модуль тревоги» посылает специальный сигнал и сбрасывает таймер, в противном случае «Модуль передачи сигнала» посылает соответствующее сообщение в службу безопасности. Время таймера может быть изменено исходя из среднего времени загрузки операционной системы на компьютерах схожей конфигурации.

Как уже отмечалось ранее, система передачи по сети электропитания ЭВМ сигналов оповещения состоит из нескольких частей:

- низкочастотный активный канал передачи сигналов;
- «модуль тревоги», генерирующий тревожный сигнал.

Новая модель предлагаемого канала представлена на рис. 2.

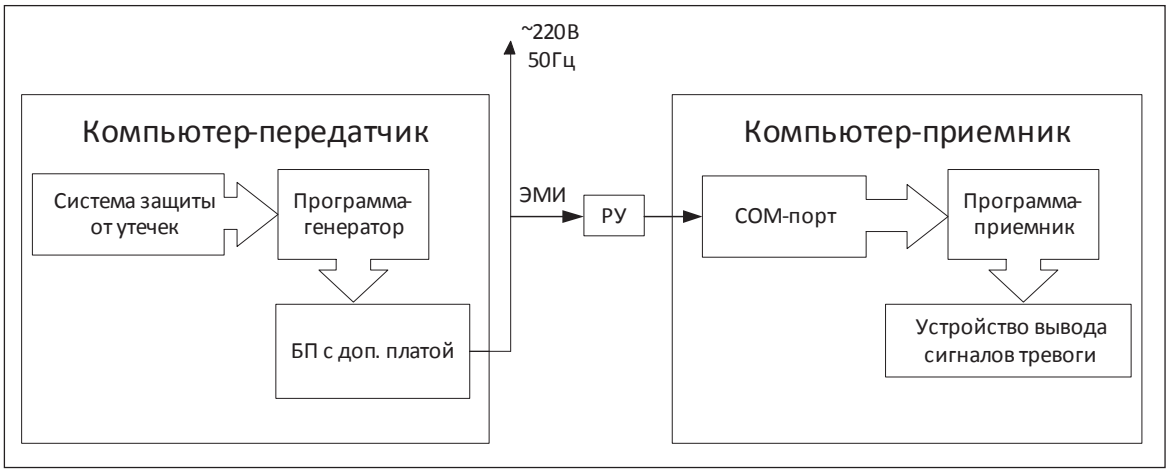

Рис. 2. Наглядная модель канала

Общий алгоритм работы системы заключается в следующем: в компьютере-передатчике система защиты информации генерирует сигнал тревоги и передает его программе-манипулятору, которая кодирует его в двоичный код и, манипулируя тактами разрядки конденсаторов БП, создает в сети электропитания кратковременные скачки тока. Эти скачки отслеживаются регистрирующим устройством (РУ) компьютера-приемника. РУ преобразует магнитную составляющую низкочастотного электромагнитного излучения в ЭДС индукции, пропорциональную току в сети электропитания. Это напряжение подается на интерфейс RS-232C.

Следует отметить одно свойство рассматриваемого канала передачи: частота генерации импульсов напряжения равна частоте несущего сигнала и составляет 50 Гц. Анализ средств защиты от утечек по сети электропитания и фильтрующих устройств показал, что импульсы столь низкой частоты будут беспрепятственно их обходить.

Для программирования интерфейса RS-232C был выбран язык ассемблер. Это объясняется его скоростными показателями и низким объемом машинного кода после компиляции. Программный модуль передачи данных по COM-порту будет находиться в ПЗУ BIOS. В большинстве компьютеров имеются два последовательных порта с интерфейсом RS-232C: COM1 и COM2, реже встречаются компьютеры с четырьмя портами. Базовые адреса портов следующие: COM1 — 3f8h, COM2 — 2f8h, COM3 — 3e8h, COM4 — 2e8h. В работе использовался порт COM1, занимающий адресное пространство от 3f8h до 3ffh. Наиболее просто реализовать передачу и получение данных по COM-порту можно при помощи регистра данных COM1, расположенного по адресу 3f8h. Он используется для двух целей: ввод/вывод из порта данных; установка скорости обмена по интерфейсу RS-232C.

Сигнал, зафиксированный РУ, подается на вход COM-порта RxD, обладающий гистерезисом. Тем самым входные импульсы формируют перепады напряжения. Положительный импульс сформирует отрицательную ступеньку, которая изменит знак потенциала только после прихода на RxD положительного импульса, что позволяет сформировать сигнал, воспринимаемый стандартным COM-портом и имеющий частоту 50 Гц.

Манипуляция током сводится к задаче разрядки конденсаторов БП компьютера. Получается, что в канале можно сформировать два типа спровоцированных колебаний: на спаде полуволны и на ее подъеме. Это дает возможность организовать двоичную последовательность, например, импульсу на спаде несущего сигнала будет соответствовать «1», а импульсу на подъеме «0».

Передача данных в рассматриваемом канале является односторонней. Следовательно, компьютер-приемник должен обладать самосинхронизацией, сам определять начало и конец передачи данных, а также выявлять ошибки передачи. Задача самосинхронизации решается использованием RS-232C в качестве протокола передачи данных.

Стандарт RS-232C описывает несимметричные передатчики и приемники: сигнал передается относительно общего провода — схемной «земли» [5]. Подмножество сигналов RS-232C, относящихся к асинхронному режиму, рассмотрим с точки зрения COM-портов ЭВМ.

При асинхронной передаче каждому байту предшествует старт-бит, который сигнализирует приемнику о начале посылки, за ним следуют биты данных и бит четности. Завершает посылку стоп-бит, гарантирующий паузу между посылками. Старт-бит следующего байта посылается в любой момент после стоп-бита, т. е. между передачами возможна пауза произвольной длительности. Старт-бит, имеющий всегда строго определенное значение (логический 0), обеспечивает простой механизм синхронизации приемника по сигналу от передатчика. Подразумевается, что приемник и передатчик работают на одной скорости обмена. Формат асинхронной посылки позволяет выявлять возможные ошибки передачи: ложный старт-бит, потерянный стоп-бит, ошибку паритета. Контроль формата позволяет обнаруживать обрыв линии: при этом принимаются логический ноль, который сначала трактуется как старт-бит, и нулевые биты данных. Потом срабатывает контроль стоп-бита.

Для управления потоком данных могут использоваться два варианта протокола — аппаратный RTS/CTS и программный XON/XOFF. Аппаратный протокол обеспечивает самую быструю реакцию передатчика на состояние приемника.

СПИСОК ЛИТЕРАТУРЫ:

1. *Лаврентьев Н. П., Мамаев А. В.* Анализ систем комплексной защиты информации от утечек с целью закрытия возможных уязвимостей // Безопасность информационных технологий. 2009. № 4. С. 117–119.
2. *Мамаев А. В.* Использование низкочастотного активного канала передачи сигналов в системах комплексной защиты информации от утечек // Безопасность информационных технологий. 2011. № 2. С. 83–89.
3. *Бессонов Л. А.* Теоретические основы электротехники. Электрические цепи. М.: Гардарика, 2002. – 638 с.
4. *Хоровиц П., Хилл У.* Искусство схемотехники: В 3-х томах. Cambridge University Press, 1980, 1989 / Пер. с англ.: Б. Н. Бронина, И. И. Короткевич, А. И. Коротова, М. Н. Микшиса, Л. В. Поспелова, О. А. Соболевой, К. Г. Финогенова, Ю. В. Чечёткина, М. П. Шарапова. Изд. 4-е, переработанное и дополненное. М.: Мир, 1993.
5. *Яшкардин В. Л.* RS-232. Рекомендованный стандарт для последовательной передачи данных. SoftElectro (2009). URL: http://www.softelectro.ru/rs232.html.