При использовании материалов статьи необходимо использовать данную ссылку:
Шведенко В.Н., Щекочихин О.В., Сизов В.Я. Защита информации в канале связи на основе формирования в нем противофазного сигнала // Информационно-экономические аспекты стандартизации и технического регулирования. 2019. № 5. (51). С. 14-17.

УДК 004.42

ЗАЩИТА ИНФОРМАЦИИ В КАНАЛЕ СВЯЗИ НА ОСНОВЕ ФОРМИРОВАНИЯ В НЕМ ПРОТИВОФАЗНОГО СИГНАЛА

Шведенко В.Н., Щекочихин О.В., Сизов В.Я.

Предлагается принципиальная схема программно-аппаратного комплекса защиты информации от утечек посредством акустоэлектрическим преобразованиям путем формирования разрушающего сигнала, который передается по параллельной линии защищаемого канал связи. Сформулированы требования к аппаратной части предложенного комплекса.

Ключевые слова: защита информации, разрушение информативного сигнала, акустоэлектрические преобразования

В современном мире вопрос защиты информации крайне актуален. В основном защищают программные средства от несанкционированного доступа, взлома и хищения информации. Над вопросом защиты информации от её утечки по техническим каналам путём разрушения информативных сигналов от технических средств проведен ряд исследований, среди которых можно выделить [1-5]. Предлагается разрушение информативного сигнала путём объединения двух каналов. Один с защищаемого прибора, подверженного акустоэлектрическим преобразованиям, по кабелю которого передаются данные. Ко второму каналу подключено специально спроектированное устройство, которое будет анализировать окружающий провод аудиофон в определённом диапозоне частот и соотносить с генерируемыми преобразованиями в кабеле, а также генерировать сигнал, находящийся в противофазе с зафиксированными акустоэлектрическими преобразованиями. (Рисунок 1).

Также необходимо учитывать, что нам необходимо не только вовремя подать разрушающий сигнал нужной частоты в канал связи, чтобы попасть в противофазу (Рисунок 3), но и генерировать сигналы определённой амплитуды (Рисунок 4), чтобы происходило именно разрушение, а не ослабление.

Как видно из рисунка 3 несовпадение частот разрушит только часть информации, но основную массу информативной составляющей всё равно можно будет зарегистрировать и в дальнейшем восстановить.

В СОВРЕМЕННОМ МИРЕ ВОПРОС ЗАЩИТЫ ИНФОРМАЦИИ КРАЙНЕ АКТУАЛЕН. В ОСНОВНОМ ЗАЩИЩАЮТ ПРОГРАММНЫЕ СРЕДСТВА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА, ВЗЛОМА И ХИЩЕНИЯ ИНФОРМАЦИИ. НАД ВОПРОСОМ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ЕЁ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ ПУТЁМ РАЗРУШЕНИЯ ИНФОРМАТИВНЫХ СИГНАЛОВ ОТ ТЕХНИЧЕСКИХ СРЕДСТВ ПРОВЕДЕН РЯД ИССЛЕДОВАНИЙ

Шведенко Владимир Николаевич, д.т.н., профессор, ведущий научный сотрудник ФГБУН ВИНИТИ РАН, г. Москва
Щекочихин Олег Владимирович, к.т.н., доцент, инженер информационной безопасности ООО «ММТР технологии», г. Кострома
Сизов Владислав Ярославович, аспирант ФГБУН ВИНИТИ РАН, г. Москва

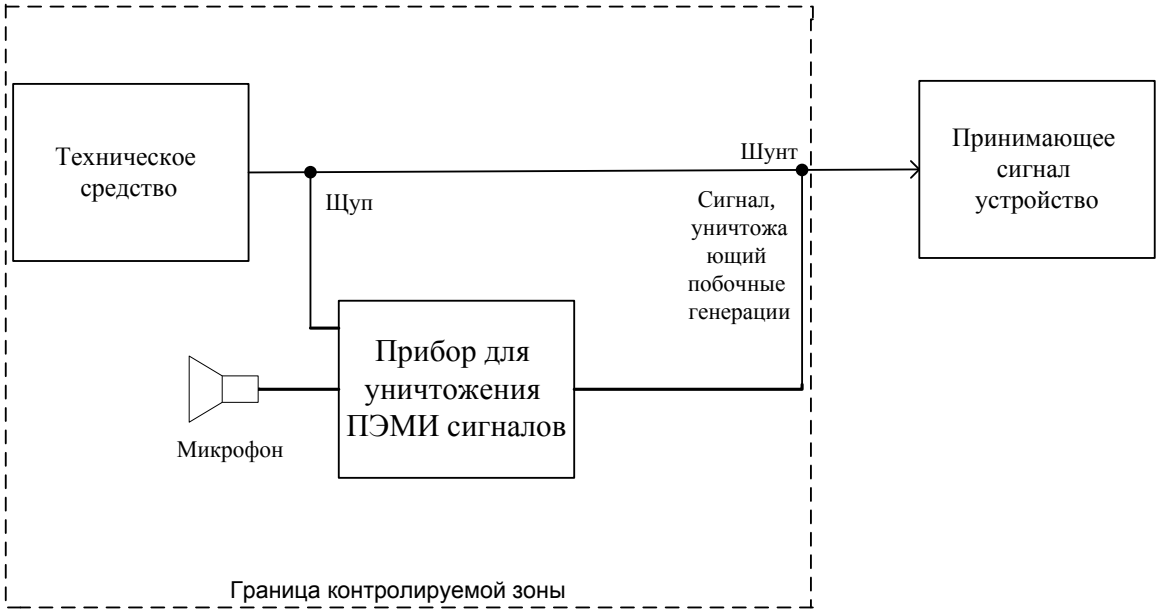

Рисунок 1. Схема подключения прибора к кабелю передачи информации

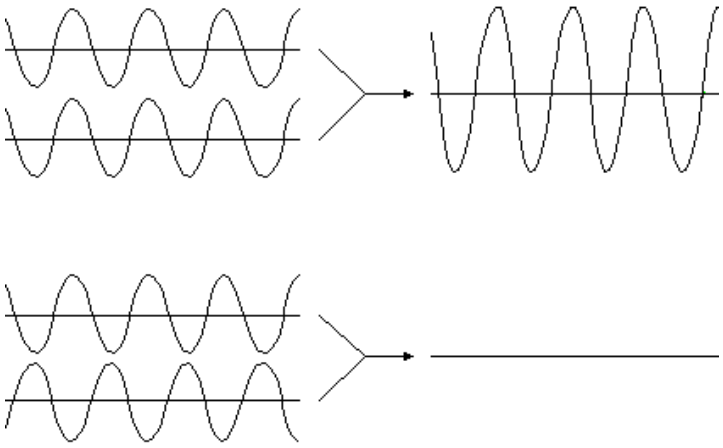

Рисунок 2. Волны, находящиеся в резонансе и волны в противофазе.

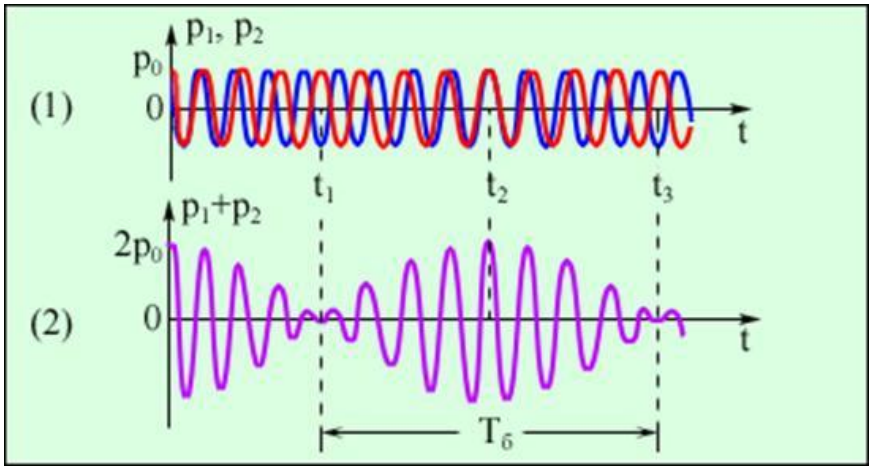

Рисунок 3. Несовпадение частот информативного и генерируемого прибором сигналов.

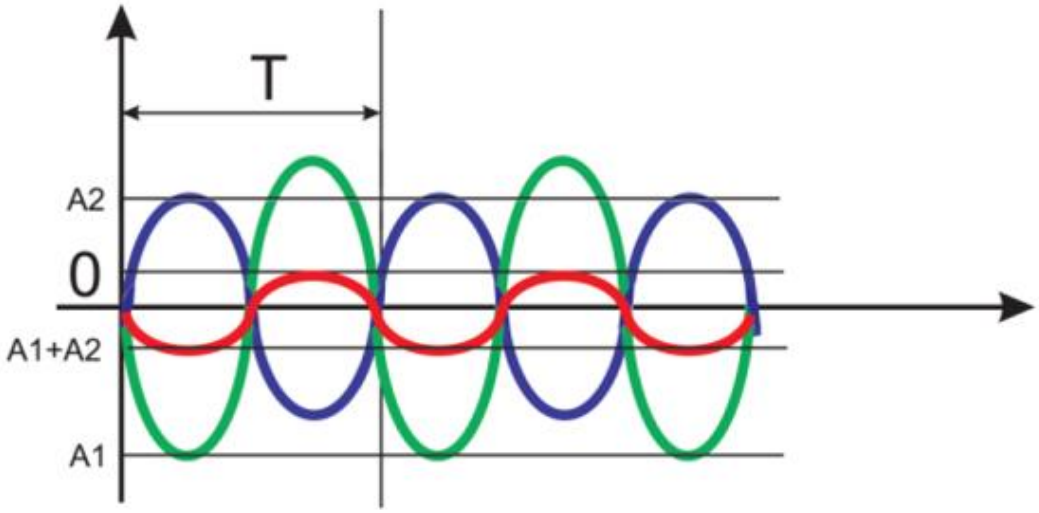

Рисунок 4. Ослабление сигнала.

После ослабления сигнал может быть принят разведывательная аппаратура.

Модуляция акустического сигнал может кодироваться следующими способами: амплитудный метод, частотный метод.

Прибор по уничтожению информативного сигнала должен быть способен успевать перестраивать разрушающий сигнал независимо от законов его формирования. Для решения этой задачи предлагается программно-аппаратный комплекс. Аппаратная часть комплекса основывается на специальных цифровых сигнальных процессорах (ЦСП) обработки данных, которые будут способны в реальном времени успевать попадать в фазу информативного сигнала.

Выбор цифровых сигнальных процессоров обусловлен тем, что они строятся по модифицированной гарвардской архитектуре. Для уменьшения задержки и обработки данных в реальном времени ЦСП использую принципы разделения шины команд и данных, а также дополнительные методы оптимизации, что позволяет выполнять бинарные операции в один цикл работы процессора вместо трех как в принстонской архитектуре.

Одним из условий создания программно-аппаратного комплекса является минимизация обращений к внешней памяти, что как правило приводит к увеличению времени обработки данных.

Программно-аппаратный комплекс разрушающий побочные преобразования сканирует микрофоном окружающий защищаемое устройство акустический фон. Затем программная часть комплекса сравнивает полученные результаты с показаниями напряжения в канале связи. После чего генерируется инвертированная фаза информативного побочного сигнала, и передается по параллельной линии защищаемого канала связи.

Прибор для защиты регистрирует звуки слышимого диапазона частот, а именно от 20 Гц до 20 кГц. Побочный сигнал в кабеле связи будет генерироваться на частотах близких к частотам звука, породившего генерацию.

Щуп необходимо располагать максимально близко к защищаемому прибору для ускорения получения данных о побочных генерациях. Шунт должен располагаться у самого края защищаемого помещения для минимизации воздействия акустического сигнала на канал связи защищаемого технического средства и принимающего оборудования.

Таким образом предложена принципиальная схема защиты канала связи от утечек информации за счет акустоэлектрических преобразований путем подачи инвертированного сигнала на параллельную линию или дополнительный проводник для разрушения информативного сигнала акустоэлектрических преобразований. iea

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ:

1. Uberkoppeln auf Leitungen [Cross-talk on cables]. BSI-Kurzinformationen, German Information Security Agency, Bonn, 2001. Электронный ресурс. URL: http://www.bsi.de/literat/faltbl/uebkopl.htm;
2. Schutzmaßnahmen gegen illegales Abh¨oren [Protection measures against illegal eavesdropping]. BSI-Kurzinformationen, German Information Security Agency, Bonn, 2003. Электронный ресурс. URL: http://www.bsi.de/literat/faltbl/f25schutz.htm;
3. Sergei Skorobogatov: Low temperature data remanence in static RAM. Technical Report UCAM-CL-TR-536, University of Cambridge, Computer Laboratory, June 2002.
4. K. Gandolfi, C. Mourtel, F. Olivier: Electromagnetic Analysis: Concrete Results. Cryptographic Hardware and Embedded Systems – CHES 2001, LNCS 2162, Springer, 2001, pp. 251–261.
5. Dakshi Agrawal, Josyula R. Rao, Pankaj Rohatgi: Multi-channel Attacks. 5th International Workshop on Cryptographic Hardware and Embedded Systems, LNCS 2779, Springer, 2003, pp. 2–16.

PROTECTION OF INFORMATION IN THE COMMUNICATION CHANNEL ON THE BASIS OF FORMING AN ANPHASE SIGNAL IN IT

Shvedenko Vladimir N., doctor of technical sciences, professor, leading researcher, FSBI VINITI RAS, Moscow
Shchekochikhin Oleg V., Ph.D., associate professor, information security engineer, MMTR Technologies LLC, Kostroma
Sizov Vladislav Y., graduate student, FSBI VINITI RAS, Moscow

A schematic diagram of a hardware-software complex for protecting information from leakage by means of acoustoelectric transformations with the formation of a destructive signal, which is transmitted along a parallel line of a secure communication channel, is proposed. The requirements for the hardware of the proposed complex are formulated.

Keywords: information protection, destruction of an informative signal, acoustoelectric transformations

REFERENCES:

1. Uberkoppeln auf Leitungen [Cross-talk on cables]. BSI-Kurzinformationen, German Information Security Agency, Bonn, 2001. Электронный ресурс. URL: http://www.bsi.de/literat/faltbl/uebkopl.htm;
2. Schutzmaßnahmen gegen illegales Abh¨oren [Protection measures against illegal eavesdropping]. BSI-Kurzinformationen, German Information Security Agency, Bonn, 2003. Электронный ресурс. URL: http://www.bsi.de/literat/faltbl/f25schutz.htm;
3. Sergei Skorobogatov: Low temperature data remanence in static RAM. Technical Report UCAM-CL-TR-536, University of Cambridge, Computer Laboratory, June 2002.
4. K. Gandolfi, C. Mourtel, F. Olivier: Electromagnetic Analysis: Concrete Results. Cryptographic Hardware and Embedded Systems – CHES 2001, LNCS 2162, Springer, 2001, pp. 251–261.
5. Dakshi Agrawal, Josyula R. Rao, Pankaj Rohatgi: Multi-channel Attacks. 5th International Workshop on Cryptographic Hardware and Embedded Systems, LNCS 2779, Springer, 2003, pp. 2–16.