А. В. Мамаев

ИСПОЛЬЗОВАНИЕ НИЗКОЧАСТОТНОГО АКТИВНОГО КАНАЛА ПЕРЕДАЧИ СИГНАЛОВ В СИСТЕМАХ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧЕК

Проблема утечки информации по-прежнему остается очень острой. Результаты исследования [1] показывают, что доля умышленных утечек растет, несмотря на активное внедрение систем комплексной защиты информации от утечек. И это объяснимо. Ранее уже проводился анализ систем такого класса, и были сделаны соответствующие выводы [2]. Для решения проблемы предлагается использовать специально разработанный канал передачи сигналов оповещения.

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

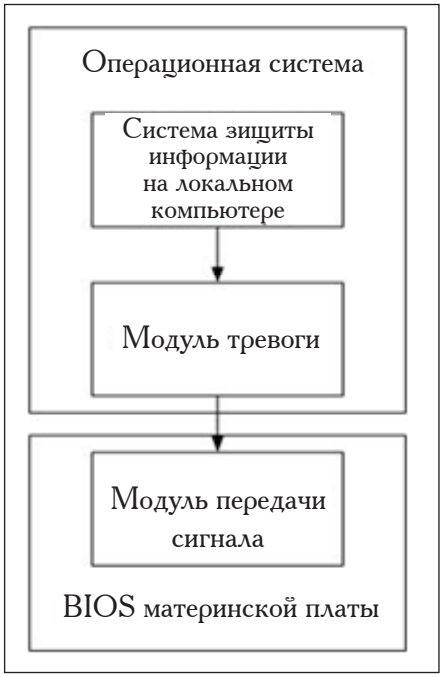

Рис. 1. Принципиальная схема измененной системы защиты

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». Таким образом 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 там «Модуль тревоги» посылает специальный сигнал и сбрасывает таймер, в противном случае «Модуль передачи сигнала» посылает соответствующий сигнал 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.

Для защиты от загрузки операционной системы с внешних носителей было решено разместить часть элементов низкочастотного активного канала передачи сигналов в BIOS материнской платы. Далее будут детально описаны механизм построения низкочастотного активного канала передачи сигналов, процедура работы с BIOS материнской платы и их взаимодействие.

Модель рассматриваемого нами канала представлена на рис. 2.

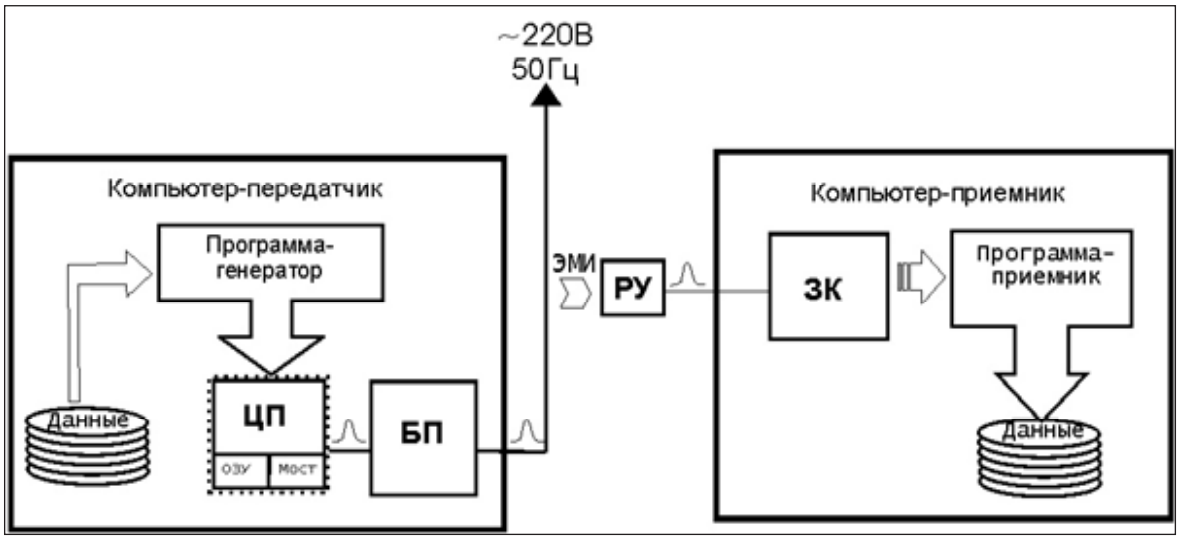

Рис. 2. Наглядная модель канала

В компьютере-передатчике запущена программа-передатчик, которая считывает данные с устройств, кодирует их в соответствии с протоколом передачи и, манипулируя током потребления центрального процессора (ЦП), осуществляет их трансляцию. В результате через блок питания (БП) изменяется потребляемый ток всего компьютера.

Изменение потребляемого тока в сети электропитания отслеживается регистрирующим устройством (РУ) компьютера-приемника. Регистрирующее устройство представляет собой магнитную антенну и преобразует магнитную составляющую низкочастотного электромагнитного излучения в электродвижущую силу (ЭДС) индукции, пропорциональную току потребления и являющуюся полезным сигналом. Это напряжение поступает на вход звуковой карты (ЗК) компьютера-приемника. Там оно оцифровывается и обрабатывается программой-приемником. Программа-приемник осуществляет декодирование поступающих от звуковой карты данных в исходные.

Рассмотрим структуру канала передачи сигнала (рис. 3).

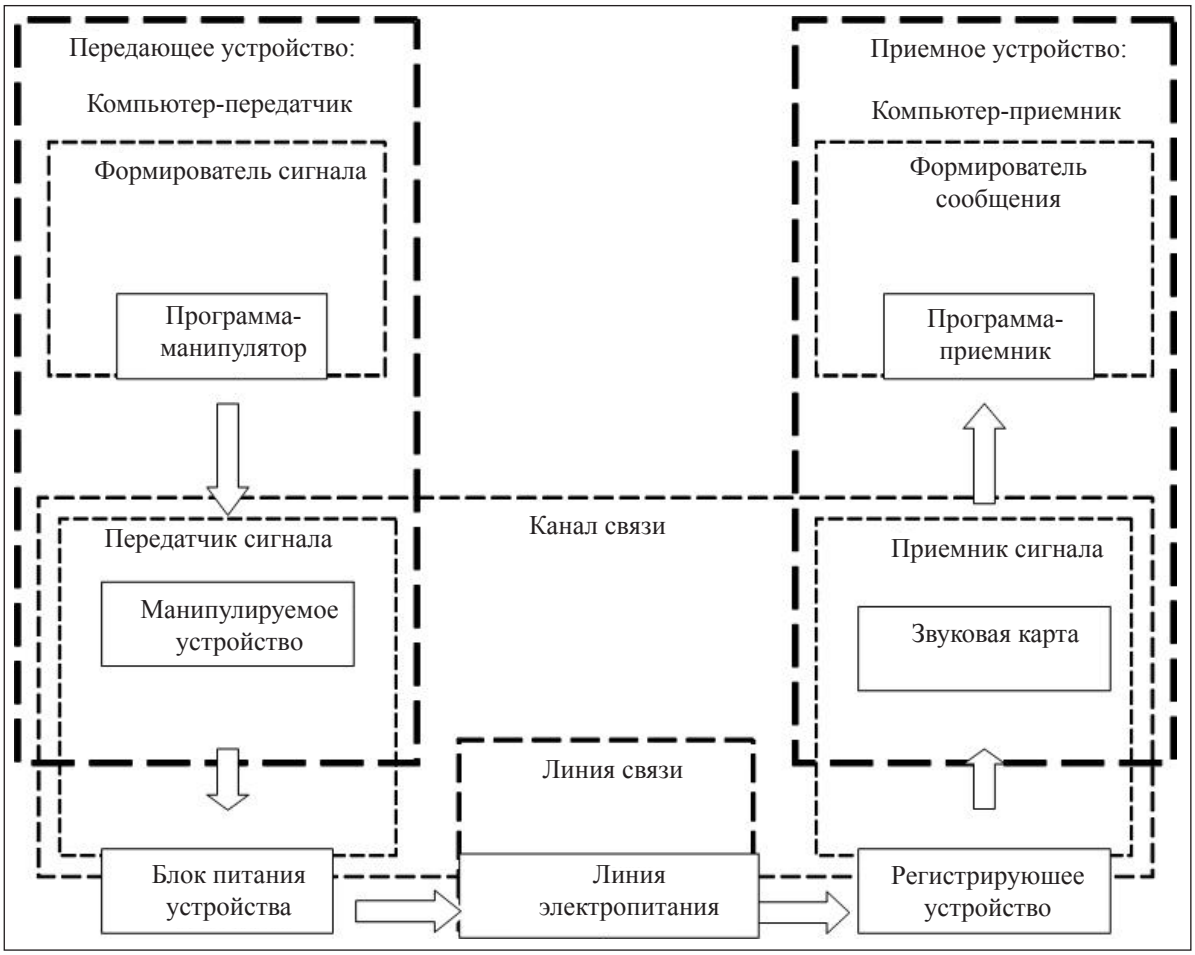

Рис. 3. Структурная схема канала передачи сигнала

Как видно из рисунка, структура канала функционально делится на семь частей:

- программа-манипулятор;
- манипулируемое устройство;
- блок питания;
- линия электропитания;
- регистрирующее устройство;
- звуковая карта;
- программа-приемник.

Опишем эти части.

Программа-манипулятор

Программа-манипулятор является собственно формирователем сигнала и отвечает за кодирование сообщения (данных) в двоичный код. Второй обязательной функцией программы является командная манипуляция передатчиком сигнала, вследствие чего происходит изменение потребляемого компьютером тока по закону изменения информационного сигнала в сообщении.

Манипулируемое устройство

Манипулируемое устройство является частью передатчика сигнала, и его основная функция — преобразование полученного первичного сигнала во вторичный сигнал, пригодный для передачи по линии связи. Осуществляется это путем модулирования первичного сигнала, полученного от программы-манипулятора, с несущим сигналом. Само манипулируемое устройство осуществляет преобразование команд от программы-манипулятора в изменение потребляемого тока в цепи питания.

В ходе выполнения работы было выявлено, что наиболее эффективным устройством является центральный процессор. Манипулирование этим устройством позволяет добиться изменения потребляемого компьютером тока не менее чем на 20 % (для процессоров Intel Pentium IV). Быстродействующий центральный процессор является практически неинерционным устройством и поэтому не ограничивает сверху полосу пропускания канала. А методы его манипулирования обеспечивают высокую степень скрытности факта передачи информации. К тому же центральный процессор является необходимой деталью любого персонального компьютера, из-за чего можно говорить об универсальности канала.

Однако отметим, что для достижения более эффективного манипулирования током потребления целесообразно использовать не одно, а целый комплекс устройств и методов управления ими. Разработчиками аппаратного обеспечения уже давно ведется работа по внедрению в них средств программного управления энергопотреблением. Поэтому воздействие передатчика сигнала на уровень потребляемого тока может быть двух видов:

- непосредственное — с помощью функций энергосбережения;
- косвенное — с помощью функций, не связанных напрямую с энергопотреблением, но существенно на него влияющих.

К первому виду относятся функции расширенного управления энергопотреблением (APM) и функции интерфейса расширенного контроля и управления питанием (ACPI). Ко второму виду можно отнести найденные экспериментально недокументированные функции центрального процессора.

Блок питания

Блок питания является необходимым звеном в цепи связи между манипулируемым устройством и линией электропитания. Именно в нем происходит модуляция тока сети электропитания внутренним током компьютера, который, в свою очередь, манипулируется программно. Так как воздействие на ток сети электропитания происходит по амплитуде, то осуществляемая здесь модуляция будет амплитудной.

К тому же блок питания, как и манипулируемое устройство, активно участвует в формировании импульсов тока, так как связан с нагрузкой обратной связью стабилизации. Из-за этого увеличение тока нагрузки, которая питается стабилизируемым напряжением (5 В), приводит к возрастанию нестабилизируемого напряжения (12 В) и, как следствие, к возрастанию потребляемой мощности устройств, питающихся этим напряжением, и всего компьютера [3]. Это явление заметно, например, на работе охлаждающих вентиляторов: при увеличении загруженности процессора сразу возрастает частота вращения вентиляторов.

Блок питания любого персонального компьютера является импульсным. Его основная задача — понижение напряжения электросети до уровня, необходимого для питания узлов компьютера. Изменение потребляемого тока различными узлами приводит к изменению общего тока потребления компьютера по закону передачи мощности:

$$\Delta P_{вх} = \frac{\Delta P_{вых}}{\eta} \cdot 100\%, \qquad (1)$$

где $\Delta P_{вх}$ — изменение потребляемой мощности на входе блока питания, $\Delta P_{вых}$ — изменение потребляемой мощности на его выходе и η — коэффициент полезного действия (КПД) блока питания. КПД современных блоков питания близок к 100 %, поэтому для упрощения его можно не учитывать. Получается, что изменение мощности потребления электроэнергии на выходе блока питания приводит к практически такому же изменению потребляемой мощности на его входе. Из этого величина изменения общего тока может быть вычислена по формуле:

$$\Delta I = \left(\Delta I_1 \cdot U_1 + \Delta I_2 \cdot U_2 + \ldots + \Delta I_n \cdot U_n\right) / U, \qquad (2)$$

где ΔI_i — изменение тока потребления i-го устройства компьютера, а U_i — напряжение питания i-го устройства, ΔI — изменение общего тока потребления компьютером, U — напряжение питания компьютера. Изменение общего тока равно отношению суммы изменений мощностей потребления каждым устройством к напряжению электросети. Если манипуляция осуществляется одним устройством, то формула упростится и примет вид:

$$\Delta I = \Delta I_1 \frac{U_1}{U}. \quad (3)$$

Центральные процессоры современных персональных компьютеров потребляют мощность до 130 Вт, при построении стенда использовался процессор с потребляемой мощностью 68 Вт. Как уже отмечалось, манипуляцией этих устройств можно добиться не менее чем 20-процентного перепада тока в сети питания, из чего следует, что более половины мощности этого устройства управляется программно.

Линия электропитания

В качестве линии связи в рассматриваемом канале используется линия электропитания с напряжением 110 или 220 В и частотой 50—60 Гц. Передающим устройством, т. е. компьютером-передатчиком, осуществляется амплитудная модуляция тока сети электропитания. Несущим сигналом здесь выступает электрический ток с частотой, равной частоте сети электропитания.

Как известно, к блоку питания персонального компьютера подходят три провода электросети: «фаза», «ноль» и «земля». Провод заземления никак не используется в передаче сигнала по каналу, так как величина проходящего по нему тока слабо зависит от меняющегося общего тока компьютера. К тому же этот провод является необязательным для работы компьютера и может отсутствовать.

Обычно на пути от передающего компьютера к принимающему в линии электросети могут встретиться различные устройства, например: сетевые фильтры, блоки бесперебойного питания, силовые трехфазные трансформаторы, «рубильники», различные устройства вычислительной техники и т. д. Анализ влияния этих устройств на передаваемый сигнал приведен ниже.

Регистрирующее устройство

Регистрирующее устройство является частью приемника сигнала, основная задача которого — преобразование сигнала из вторичного в первичный, пригодный для его обработки приемником сигнала (программой-приемником), т. е. осуществление демодуляции сигнала.

Подключение регистрирующего устройства к линии электросети может быть как контактным, так и бесконтактным. При контактном подключении РУ включается в разрыв провода электросети, а при бесконтактном, индуктивно, — между проводами или около одного из них. Бесконтактное подключение возможно за счет того, что при протекании по проводнику электрического тока вокруг него образуется магнитное поле, напряженность которого изменяется при изменении величины тока. Для регистрации напряженности этого поля регистрирующее устройство должно представлять собой магнитную антенну, преобразующую изменение величины напряженности в ЭДС индукции. Такими же свойствами обладают токовые клещи, широко используемые электриками для измерения величины тока в проводке без какого-либо контактного подключения.

Так как из элементарных законов электротехники следует, что измерить величину тока можно лишь устройством, подключенным последовательно с устройством, потребляющим этот ток, то получается, что необходимым условием возможности считывания сигнала регистрирующим устройством является установка его последовательно с компьютером-передатчиком, т. е. между источником электропитания и передатчиком сигнала, как показано на рис. 4:

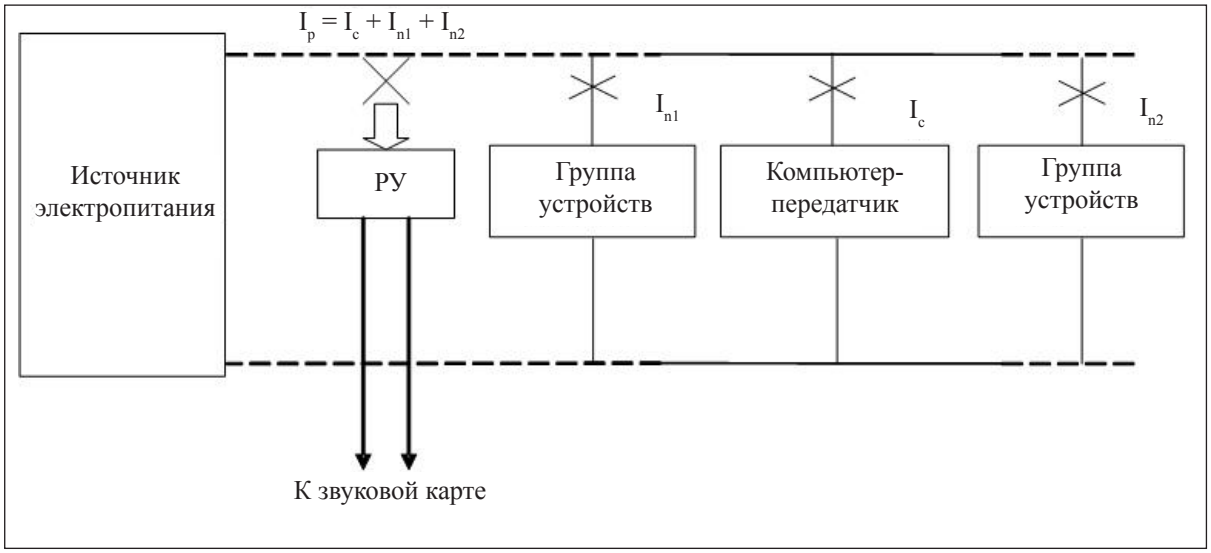

Рис. 4. Правильная установка регистрирующего устройства

На рисунке видно, что в зависимости от установки регистрирующего устройства регистрируемый им сигнал $I_р$ будет сильно меняться, так как он помимо сигнала от передающего устройства $I_С$ включает в себя и сигналы от других параллельно работающих устройств, являющихся помехой ($I_{П1}$ и $I_{П2}$). Поэтому РУ целесообразно подключать так, чтобы между ним и компьютером-передатчиком было как можно меньше параллельно работающих устройств, чтобы исключить воздействие токов помех $I_{П1}$. Полностью же исключить токи помех ($I_{П1}$ и $I_{П2}$) можно только при подключении РУ на участке между компьютером-передатчиком и общей проводкой сети электропитания ($I_С$).

В качестве РУ на практике использовалось электромагнитное реле РПВ2. Такое нестандартное использование реле стало возможным благодаря его конструкции. Металлический корпус реле не пропускает высокочастотное электромагнитное излучение и служит экраном, а внутренняя обмотка служит для преобразования изменения регистрируемого магнитного поля в ЭДС индукции. К тому же сплошной сердечник реле выполняет низкочастотную фильтрацию сигнала, благодаря тому что токи Фуко в нем пропорциональны частоте сигнала.

Звуковая карта

Звуковая карта является вторым устройством приемного устройства, и поэтому ее основная задача также заключается в подготовке сигнала для обработки программой-приемником. Звуковая карта оказалась вполне пригодной для выполнения этой функции. Сигнал частотой 50 Гц находится в полосе пропускания звуковой карты и практически без искажений может быть ею обработан.

В состав звуковой карты, как известно, входит аналогово-цифровой преобразователь, поэтому она может предоставить для программы-приемника оцифрованный вид сигнала. ЗК является практически обязательным устройством любого персонального компьютера, а использование ее для оцифровки обычного сигнала звукового диапазона не накладывает на ее тип каких-либо ограничений. Чувствительности микрофонного входа вполне достаточно для подключения к нему регистрирующего устройства без каких-либо дополнительных усилителей. Для меньшего затухания сигнала необходимо, чтобы внутреннее сопротивление РУ было много меньше входного сопротивления ЗК. Однако опыт показал, что сигнал с регистрирующего устройства был такой величины, что можно было пренебречь согласованием внутреннего сопротивления источника сигнала с входным сопротивлением ЗК.

Программа-приемник

Программа-приемник является формирователем сообщения и заключительным звеном в схеме канала передачи сигнала. По определению формирователь сообщения должен обеспечить декодирование принятого сигнала обратно в сообщение. Однако в результате различных искажений

и воздействия помех пришедший сигнал может существенно отличаться от переданного. Поэтому всегда можно высказать ряд предположений (гипотез) о том, какое сообщение передавалось. Задачей приемного устройства является принятие решения о том, какое из возможных сообщений действительно передавалось источником. Та часть приемного устройства, которая осуществляет анализ приходящего сигнала и принимает решение о переданном сообщении, называется решающей схемой. Эту задачу и должна выполнять программа-приемник.

Программа может считывать сигнал через интерфейс звуковой карты в виде данных импульсно-кодовой модуляции. Так как сигнал представляет собой амплитудно-модулированный сигнал удвоенной частоты электросети (100 Гц), то данные считываются блоками по

$$N = \frac{F}{f} \cdot n \qquad (4)$$

байт, где F — частота дискретизации сигнала (на практике: 44100 Гц), f — частота несущей сигнала (100 Гц), а n — число байт, отводимых под один отсчет и зависящих от степени квантования (n = 2). Получается поток блоков по 882 байта со скоростью f = 100 блоков в секунду.

Для подавления случайных всплесков сигнала этот поток можно подвергнуть медианной фильтрации [4]. Затем, чтобы обеспечить спектральный анализ сигнала, он может быть подвергнут цифровой фильтрации с помощью быстрого преобразования Фурье [5, 6]. Далее программа должна реализовать первую решающую схему: является ли обрабатываемый блок логическим «0» или «1». Затем, анализируя принятую логическую последовательность, программа должна определить начало сеанса передачи и тем самым реализовать вторую решающую схему. Если программа находит признак начала передачи, то получаемые логические данные декодируются в байты передаваемых данных. В условиях односторонней связи для синхронизации потока данных между передатчиком и приемником в программе может быть реализована манчестерская система кодирования, используемая в компьютерных сетях [7], которая обладает свойством самосинхронизации. К тому же специально для данного вида связи можно разработать дополнительную систему кодирования, которая ведет контроль над ошибками и осуществляет коррекцию спорных данных.

СПИСОК ЛИТЕРАТУРЫ:

1. Глобальное исследование утечек за 2009 год. URL: www.infowatch.ru.
2. *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.
3. *Гук М.* Аппаратные средства IBM PC. Энциклопедия. 2-е изд. СПб.: Питер 2003. – 928 с.
4. *Васильев В. Н., Гуров И. Л.* Компьютерная обработка сигналов в приложении к интерферометрическим системам. СПб.: БХВ – Санкт-Петербург, 1998. – 240 с., ил.
5. *Секунов Н. Ю.* Обработка звука на PC. СПб.: БХВ-Петербург, 2001. – 1248 с.: ил.
6. *Сергиенко А. Б.* Цифровая обработка сигналов. СПб.: Питер, 2003. – 604 с.
7. *Закер К.* Компьютерные сети. Модернизация и поиск неисправностей. Пер. с англ. СПб.: БХВ-Петербург, 2003. – 1008 с.