УДК 004.056.53

МОНИТОРИНГ НАЛИЧИЯ ЭЛЕКТРОМАГНИТНЫХ СИГНАЛОВ В БЛИЖНЕЙ ЗОНЕ

Г.В. Давыдов, В.А. Попов, А.В. Потапович
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Приведены исследования по выявлению каналов утечки информации за счет двойного использования отдельных элементов и устройств, в средствах вычислительной техники. С одной стороны, эти элементы и устройства выполняют основную функцию в изделии и дополнительно могут использоваться для выполнения функций, не оговоренных их основным назначением. Рассмотрены два метода мониторинга каналов утечки информации. Предложенный алгоритм и методика обнаружения синхронизированных с провоцирующим воздействием аномалий в тепловых полях проверяемого изделия является необходимым условием выявления аппаратных средств недекларированных возможностей образования канала утечки информации.
Ключевые слова: риск безопасности, защищенность информации, электромагнитный сигнал, радиоканал утечки информации.

MONITORING THE PRESENCE OF ELECTROMAGNETIC SIGNALS IN THE NEAR ZONE

H.V. Davydau, V.A. Papou, A.V. Patapovich
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The article presents studies on identifying information leakage channels due to dual use of individual elements and devices in computing equipment. On the one hand, these elements and devices perform the main function in the product and can additionally be used to perform functions not specified by their main purpose. Two methods of monitoring information leakage channels are considered. The proposed algorithm and method for detecting anomalies in thermal fields of the product being tested that are synchronized with the provoking effect are a necessary condition for identifying hardware with undeclared capabilities for forming an information leakage channel.
Keywords: security risk, information security, electromagnetic signal, radio channel of information leakage.

Защита информации, циркулирующей в средствах вычислительной техники, включает как организационные мероприятия, так и технические мероприятия защиты линий связи и питания от утечки информации. В месте, с тем существует опасность утечки информации по радиоканалу, организуемому на короткий промежуток времени от средств вычислительной техники. Такие каналы утечки информации могут образовываться как с использованием радиомодулей, интегрированных в центральный процессор, так и с использованием дополнительных функциональных возможностей элементов вычислительной техники (недекларированных возможностей) [1]. В работе в качестве примера образования канала утечки информации рассматривается использование радиомодуля RFID, внедренного в серверные центральные процессоры Xeon W-2255 компании Intel. Обнаружение встроенных в процессоры модулей или использование дополнительных функциональных возможностей элементов устройств вычислительной техники для образования недекларированных радиоканалов передачи информации рассматривается в работе. Обнаружение осуществляется по изменению теплового поля материнской платы вычислительного устройства при провоцирующем акустическом и электромагнитном воздействиях.

Структурная схема комплекса проверки вычислительной техники на наличие аппаратных средств недекларированных возможностей (НДВ) представлена на рис. 1.

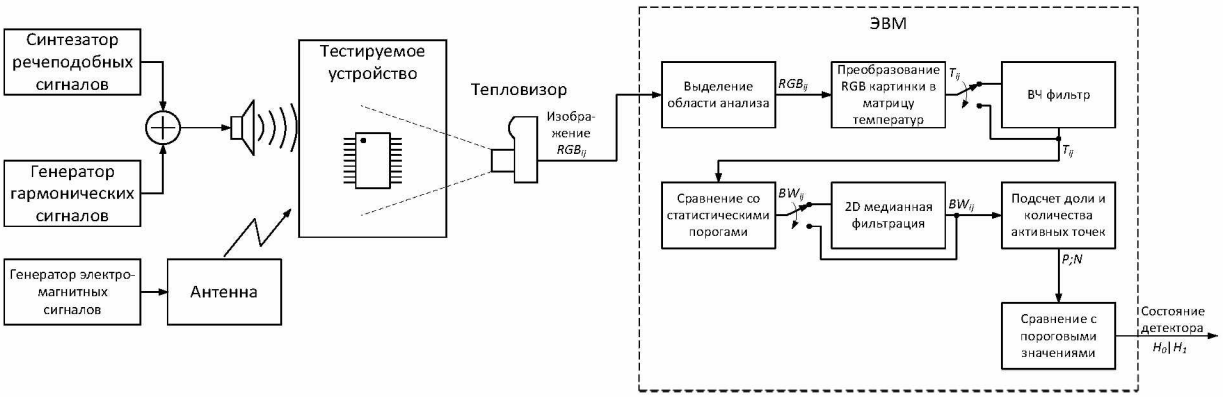

Рис. 1. Структурная схема комплекса проверки вычислительной техники на наличие аппаратных средств НДВ
Fig. 1. Structural diagram of the complex for checking computing equipment for the presence of NDV hardware

Для корректного проведения проверки вычислительной техники необходимы следующие ограничения и технические решения. Помещение для проведения проверки должно состоять из двух комнат. В одной комнате размещается испытуемый объект, тепловизор, акустические преобразователи для создания провоцирующих акустических полей и антенны, предназначенные для создания провоцирующих электромагнитных полей. В другой комнате, совмещенной с первой, располагаются операторы, управляющий компьютер, генератор провоцирующих акустических воздействий и генератор провоцирующих электромагнитных воздействий. Экспериментальные исследования показали, что на результаты проверки вычислительной техники на наличие аппаратных средств НДВ могут оказывать вибрации испытуемого объекта или тепловизора. Для исключения влияния этого фактора на результаты проверки была изменена конструкция крепления тепловизора к штативу, что позволило снизить вибрации тепловизора, вызываемые акустическим провоцирующим воздействием.

Для проведения проверки вычислительной техники на наличие аппаратных средств НДВ необходимо экранировать объект проверки и тепловизор от тепловых фоновых шумов. Тепловые фоновые шумы включают тепловое поле оператора, световое излучение, поступающее в помещение через окна, конвекционные тепловые потоки. Влияние теплового поля оператора на результаты проверки необходимо исключить путем организации его рабочего места в рядом расположенной комнате. На результаты проверки могут оказывать негативное влияние и конвекционные потоки и сквозняки. Поэтому при проведении проверки необходимо плотно закрывать двери и окна в комнате, где расположен проверяемый объект.

Для исключения влияния многократно переотраженного светового и инфракрасного излучения, попадающих в комнату через окна, окна в комнате, где проводятся проверки, должны быть зашторены.

Однако, изменения температуры в помещении из-за изменений погодных условий (температуры и освещения) могут приводить к изменениям температуры проверяемых объектов. Эксперименты показали, что температура проверяемых объектов в течении часа может изменяться на 0,3 °С. Кратковременные изменения температуры (в течении 10 минут) проверяемого объекта не превышают 0,1 °С. Чувствительность тепловизора составляет 0,04 ^{0}С, что является достаточным для проверки вычислительной техники на наличие аппаратных средств НДВ. Тепловые шумы из-за влияния рассмотренных выше факторов не превышают 0,1 °С.

В состав комплекса проверки входили следующие функциональные устройства. Генератор провоцирующих электромагнитных сигналов Agilent N5172B предназначен для создания электромагнитных провоцирующих полей в области расположения проверяемой вычислительной техники на наличие аппаратных средств НДВ. Параметры генератора провоцирующих электромагнитных сигналов следующие:

– диапазон сканирования по частоте от 10 до 3000 МГц с точность установки частоты не более 0,01%;

– мощность сигнала на выходе генератора не менее минус 10 dBm с точность не менее ± 1 dBm в диапазоне частот от 10 до 3000 МГц.

Рамочная антенна 6512 ETS LINDGREN предназначена для создания провоцирующего электромагнитного поля в диапазоне частот от 10 до 30 МГц, а биконическая антенна BicoLOG 20300 AARONIA для создания провоцирующего электромагнитного поля в диапазоне частот от 30 до 3000 МГц. Антенны подключены к генератору Agilent N5172B через согласующее устройство. Согласующее устройство разделяет диапазон частот от генератора на два диапазона с полосами частот от 10 до 30 МГц для антенны 6512 ETS LINDGREN и от 30 до 3000 МГц для антенны BicoLOG 20300 AARONIA

Генератор провоцирующих акустических сигналов предназначен для создания акустических полей в области расположения проверяемой вычислительной техники на наличие аппаратных средств НДВ. Генератор провоцирующих акустических сигналов выполнен программно на управляющем компьютере и позволяет формировать речеподобные или гармонические сигналы. Воспроизведение акустических сигналов выполняется с помощью акустических преобразователей на базе акустической системы SVEN SPS-611S. Интегральный уровень звукового давления провоцирующих акустических воздействий должен быть не менее 70 дБ в диапазоне частот от 100 до 8000 Гц.

Тепловизор Flir T640, входящий в состав комплекса, предназначен для съема распределения теплового поля по проверяемой вычислительной технике или ее отдельным функциональным узлам и передачи данных на управляющий компьютер. Разрешающая способность тепловизора должна быть не хуже 0,04 °С в диапазоне от 8 до 14 мкм. Более высокая разрешающая способность тепловизора не нужна, так как конвекционные потоки и колебания температуры проверяемой вычислительной техники из-за различного вида тепловых и световых помех составляют ± 0,1 °С. Меньшего значения колебаний температуры проверяемого объекта вычислительной техники достичь не удалось при использовании доступных методов защиты от тепловых и световых помех.

Управление комплексом осуществлялось переносным компьютером. Генератор провоцирующих акустических сигналов (речеподобных и гармонических сигналов) выполнен программно и установлен на персональный компьютер для управления комплексом. Для формирования речеподобных сигналов использовалась база аллофонов диктора. База аллофонов диктора создавалась по записям речи диктора. Аллофон был представлен в виде отдельного wav файла с присвоением файлу имени аллофона. Синтез речеподобных сигналов выполнялся с учетом вероятностей длины предложений и длины слов в русской речи, а также вероятностей появления определенных аллофонов в русской речи. Распределение вероятностей длины предложений (числа слов в предложении) для русской речи является не определяющим параметром при синтезе речеподобных сигналов. Лучше использовать при синтезе речеподобных сигналов длину синтагмы, на которые делится предложение (фраза)

и количество фраз в фоноабзаце. Среднее число слов в предложении для русской речи составляло 10,38. Эти характеристики для каждого диктора могут быть свои.

Генератором провоцирующих электромагнитных сигналов N5172B формировались сигналы с различными видами модуляции и протоколами связи.

Развертка гармонических сигналов в диапазоне частот от 10 до 3000 МГц выполнялась по логарифмическому закону. Это обусловлено тем, что относительная скорость перестройки должна оставаться постоянной. Время перестройки частоты генератора должно быть выбрано таким образом, чтобы прохождение частотной полосы приемника, настроенного на какую-то частоту, составляло не менее 0,5 с. Если на несущей частоте в 10 МГц ширина полосы принимаемых сигналов составляет 5 кГц, то развертка частоты от 10 до 10,005 МГц должна быть выполнена за время не менее 0,5 с. Исходя из этого время развертки гармонических сигналов в частотном диапазоне от 10 до 3000 МГц составит 96 мин.

Все виды провоцирующих электромагнитных сигналов были записаны в память генератора и управляющего компьютера и их воспроизведение выполнялось последовательно в автоматическом режиме.

Обнаружение радиоприемных устройств основано на приеме входным каскадом радиоприемного устройства провоцирующего гармонического сигнала на частоте работы радиоприемного устройства и усилении его до уровня необходимого для дальнейшей обработки. При усилении радиоприемным устройством провоцирующего гармонического сигнала температура его повышается, что будет зафиксировано с помощью тепловизора и передано на управляющий компьютер.

Обнаружение радиопередающих устройств основано на повышении температуры выходного каскада радиопередатчика при работе на передачу и фиксирование повышения температуры радиопередающего устройства с помощью тепловизора и управляющего компьютера. Встроенные передатчики НДВ могут работать на передачу лишь короткое время в течение суток или другого отрезка времени, накапливая информацию для передачи. Поэтому целесообразно проверку не прерывать при смене провоцирующих воздействий. При этом проверка при всех видах провоцирующих воздействий займет время не более 14 ч.

Обнаружение устройства съема акустической информации выполнялось путем контроля теплового режима аудиокодека при провоцирующих акустических воздействиях. Одним из вариантов построения НДВ для съема акустической информации может быть замена керамических конденсаторов, включенных на микрофонных или линейных входах аудиокодека на такие же керамические конденсаторы с такой же емкостью, но с высокими пьезоэлектрическими свойствами (пьезоэлектрический микрофон). При отсутствии микрофонного штекера в разъеме один конденсатор оказывается закороченным на "землю", а с другого может сниматься аудио информации и далее обрабатываться кодеком. В случае наличия в микрофонном разъеме штекера сигналы от микрофонов будут поступать в фазе на дифференциальный вход и разностный сигнал от керамических микрофонов будет равен нулю и не вызовет никаких подозрений и внешний микрофон буден выполнять свои функции. Если подключен не стереофонический микрофон, то сигнал от внешнего микрофона и от микрофона НДВ будут складываться и будет впечатление что это один сигнал акустической обстановки в помещении. Следует отметить, что некоторая разность фаз сигналов от двух микрофонов будет иметь место, но на слух это определить чрезвычайно сложно, так как сигнал от микрофона НДВ может быть по амплитуде значительно меньше, чем сигнал от внешнего микрофона.

Такие методы обнаружения возможных радиоканалов утечки информации являются весьма трудоемкими.

Более предпочтительным методом может быть мониторинг наличия электромагнитных сигналов (радиосигналов) в ближней зоне во время радиообмена с устройством приема информации. Так как время радиообмена его продолжительность, а также частота и протокол радиообмен неизвестны, то мониторинг электромагнитных сигналов в ближней зоне необходимо вести параллельно по каналам с шириной каждого канала в одну октаву. При наличии 10 каналов перекрывается диапазон частот от 7 до 7000 МГц. Такое разделение по каналом позволит обнаруживать как широкополосные сигналы, так и кратковременные с длительностями не менее 35 мс. Весь частотный диапазон разбит на каналы с октавными полосами частот. Среднегеометрические частоты полос равны: 10, 20, 40, 80, 160, 320, 1250, 2500, 5000 МГц. Для приема электромагнитных сигналов в ближней зоне используются разнесенные штыревые антенны. Непосредственно штыревые антенны устанавливаются на экранированные малошумящие усилители.

На входе малошумящих усилителей включены октавные полосовые фильтры 7-го порядка. Малошумящие усилители являются одновременно и октавными полосовыми фильтрами с затуханием в полосе задерживания (на двойной частоте от граничной) 54 дБ. Неравномерность частотной характеристики в полосе пропускания составила не более 7 дБ. В устройстве использовались логарифмические усилители с детекторами на выходе. Далее сигналы поступали на схемы сравнения и обработки и потом на индикаторную панель и в блок памяти.

На индикаторной панели устройства мониторинга отображается в цифровом виде величина градиента электромагнитного поля для каждого канала. При превышении градиента электромагнитного поля порогового значения в одном из каналов информация о таком событии записывается в протокол с указанием диапазона частот, величин градиента электромагнитного поля по всем каналам, времени произошедшего события.

Проведенные исследования показали, что для обеспечения защиты информации в вычислительной технике кроме ряда мероприятий по проверке ее на наличие недекларированных возможностей перед вводом в эксплуатацию, необходимо вести мониторинг наличия электромагнитных сигналов в ближней зоне от вычислительной техники во время ее эксплуатации, с целью выявления каналов утечки информации, которые не были обнаружены.

Список использованных источников

1. Хореев А.А., Чумаков А.А. (2025) Метод защиты средств вычислительной техники от НСД по шине I2S/SMBus с использованием радиомодулей RFID, интегрированных в центральный процессор. *Информационно-методический журнал INSIDE Защита информации.* (1), 6-19.

References

1. Khoryev A.A., Chumakov A.A. (2025) Method of protecting computing equipment from unauthorized access via the I2S/SMBus bus using RFID radio modules integrated into the central processor. *Information and methodological journal INSIDE Information Security.* (1), 6-19 (in Russian).

Сведения об авторах

Давыдов Г.В., к.т.н., в.н.с., НИЛ 5.3, учреждение образования « «Белорусский государственный университет информатики и радиоэлектроники», nil53@bsuir.edu.by.
Попов В.А., с.н.с., НИЛ 5.3, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», nil53@bsuir.edu.by.
Потапович А.В., с.н.с., зав. НИЛ 5.3, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», nil53@bsuir.edu.by.

Information about the authors

Davydau H.V.. PhD. researcher of SRL 5.3 of R&D department. Educational Institution "Belarusian State University of Informatics and Radioelectronics", nil53@bsuir.edu.by.
Papou V.A., researcher of SRL 5.3 of R&D department. Educational Institution "Belarusian State University of Informatics and Radioelectronics", nil53@bsuir.edu.by.
Patapovich A.V., researcher of SRL 5.3 of R&D department. Educational Institution "Belarusian State University of Informatics and Radioelectronics", nil53@bsuir.edu.by.