2. Кулешов А.А. Математическое моделирование в задачах промышленной безопасности и экологии. // Информационные технологии и вычислительные системы. 2003. № 4. -С. 56 - 70.

3. Морозов А.А., Таранчук В.Б. Программирование задач численного анализа в системе Mathematica: Учеб. пособие.– Мн.: БГПУ, 2005. -145 с.

4. Баровик Д.В., Таранчук В.Б. Библиотека модулей визуализации научных данных в системе Mathematica // Информатизация образования. 2007. № 2. -С. 24 - 31.

АНАЛИЗ УГРОЗЫ УТЕЧКИ ИНФОРМАЦИИ В ЭЛЕКТРИЧЕСКИХ КАНАЛАХ ПЕРЕДАЧИ ЦИФРОВЫХ ДАННЫХ ЗА СЧЕТ «ВЧ-НАВЯЗЫВАНИЯ»

О.К. Барановский, А.Ф. Мельник
Беларусь, г. Минск

Задача защиты коммерческой тайны при обмене информацией в открытых сетях передачи данных типа Интернет, как правило, решается путем использования стойких алгоритмов шифрования, что в большинстве случаев не оставляет шансов третьей стороне дешифровать перехваченные сообщения. В связи с этим единственным техническим способом получения хотя бы части информации является перехват по техническим каналам утечки информации побочных электромагнитных излучений (ПЭМИ), возникающих при обработке информации в открытом (незашифрованном) виде до (или в процессе) шифрования. Например, анализируя ПЭМИ криптографических устройств, можно судить о длине ключа, алгоритме шифрования, выполняемых инструкциях в микропроцессорных устройствах и др. В США существует закрытый стандарт HIJACK, регламентирующий контрмеры по побочным излучениям при обработке и передаче цифровых сигналов. Помимо этого, существует технология Soft TEMPEST скрытой передачи данных по каналу ПЭМИ с применением программных закладок [1].

Одним из методов организации технических каналов утечки информации является высокочастотное навязывание («ВЧ-навязывание»). При реализации метода в линию утечки подается высокочастотный зондирующий сигнал. Частота ВЧ сигнала зависит как от параметров элементов согласования линии связи (например, параметров согласующих трансформаторов), так и характеристик нелинейных элементов, на которых может происходить модуляция зондирующего сигнала с несущими информацию низкочастотными сигналами, возникающими, например, за счет микрофонного эффекта или при наличии побочных электромагнитных излучений. При этом, низкочастотный и высокочастотный сигналы, взаимодействуя, образуют сложную полиномную зависимость. Результирующий сигнал перехватывается организатором канала утечки.

Отыскание частоты утечки информации является весьма сложной задачей ввиду излучений компьютера в широкой полосе частот. Компьютер как объект технической защиты информации является сложной системой, состоящей из

генераторов, модуляторов, нелинейных элементов и антенн. Воздействие посторонних ВЧ колебаний, подаваемых, например, по цепям электропитания или по эфиру, на нелинейные элементы также приводит к появлению заранее трудно предсказуемых комбинационных частот, излучаемых в эфир. Поэтому для защиты информации от утечки за счет «ВЧ-навязывания», как правило, применяют пассивный метод защиты, заключающийся в экранировании компьютера либо его размещении в экранированном шкафу или помещении, а также в установке в цепях электропитания широкополосных помехоподавляющих фильтров. Это позволяет повысить защищенность компьютера от воздействия сигналов «ВЧ-навязывания», передаваемых по эфиру и цепям электропитания.

Однако компьютер – не изолированная система, во многих случаях он находится в составе сетей передачи данных. При этом активное сетевое оборудование также может являться источником электромагнитных колебаний. Эти колебания по проводам кабельной системы сети передачи данных проникают в компьютер и могут вызывать дополнительные информативные излучения на комбинационных частотах. В связи с этим спектр излучений одного и того же компьютера при автономной работе и при работе в сети может значительно отличаться, а кабельные системы сетей передачи данных, в особенности выполненные неэкранированными медными проводами или неэкранированной витой парой, могут являться дополнительной антенной для всех ПЭМИ компьютера, в том числе возникающих при Soft TEMPEST атаке [2]. Применение экранированных проводов или экранированной витой пары значительно улучшает ситуацию, но не гарантирует подавление синфазных наводок. Причин для этого в сети много, но основная – заземление устройств, входящих в состав сети [2].

Невозможно спроектировать и установить в провода кабельной системы сети передачи данных фильтр, подавляющий побочные излучения и внешние сигналы «ВЧ-навязывания», аналогично помехоподавляющему фильтру, устанавливаемому в цепи электропитания. Ведь побочные излучения компьютера (жесткий диск, клавиатура и т.п.) сосредоточены в той же полосе частот, что и спектр импульсов, передаваемых по кабельной системе в процессе сетевого обмена.

Вышеизложенное позволяет сделать вывод, что даже при наличии экранирования устройства обработки и кабельной системы задача защиты информации от утечки за счет «ВЧ-навязывания» сводится к устранению зондирующего ВЧ сигнала на входе в локальную сеть передачи данных и (или) защищаемого компьютера.

Авторами проведен анализ представленных на российском рынке устройств анализа проводных линий на предмет организации каналов утечки информации путем «ВЧ-навязывания», основные из которых представлены ниже:

– система исследования эффекта акусто-электрических преобразований в технических средствах «ТАЛИС»;

– комплекс оценки защищенности по каналу «ВЧ-навязывания» «ВЕПРЬ»;

– обнаружитель неоднородностей телефонных линий «ОТКЛИК»;

– универсальное проверочное устройство проводных линий «УЛАН-2»;

– индикаторный прибор для проверки радиоэлектронной аппаратуры «АРФА».

Как следует из описания, предлагаемые устройства предназначены в основном для исследования каналов утечки за счет «ВЧ-навязывания», возникающих вследствие акусто-электрических преобразований речевых сигналов, хотя и могут быть применены для обнаружения других электромагнитных сигналов в диапазоне 20 - 20 000 Гц. Для обнаружения каналов утечки информации, обрабатываемой, например, системным блоком компьютера, вышеуказанные устройства обнаружения непригодны вследствие их узкого частотного диапазона.

Отсутствие устройств обнаружения каналов утечки информации методом «ВЧ-навязывания» с верхней границей диапазона частот сигналов до сотен МГц требует теоретического исследования данной задачи.

При реализации метода «ВЧ-навязывания» канал утечки и канал передачи данных должны быть разнесены в частотной области для исключения помех и, соответственно, скорейшего обнаружения факта утечки. В связи с этим, если диапазон частот линии связи [f1, f2], то необходимо осуществлять «ВЧ-навязывание» либо выше f2, либо ниже f1.

Предельная максимальная частота навязывания зависит от типа и длины сетевых кабелей, что определяет затухание ВЧ сигнала. Если физический канал связи не позволяет осуществлять «ВЧ-навязывание» выше диапазона рабочих частот линии связи, то злоумышленнику придется частоту ВЧ сигнала выбрать ниже f1. В этом случае пропускная способность канала утечки данных будет значительно меньше объемов передаваемых в линии цифровых данных.

Теоретически существует третий способ организации канала утечки – в полосе частот [f1, f2]. Для устранения искажений в канале утечки, вызываемых передачей данных в сети, злоумышленнику потребуется периодически повторять сообщения, что является практически неразрешимой задачей при отсутствии встроенных в компьютер программных и (или) аппаратных закладок. Однако, в случае повторения типовых операций, например, при кодировании и шифровании данных, содержащаяся в ПЭМИ информация о реализации алгоритмов и их параметрах может многократно модулировать навязываемый ВЧ сигнал, что позволит злоумышленнику его накапливать, усреднять и восстанавливать.

Основная трудность поиска и анализа канала утечки заключается в установлении потенциальных частот и амплитуд сигналов «ВЧ-навязывания». В связи с этим требуется предварительное проведение основательных практических исследований активного сетевого оборудования с последующей разработкой методов и технических средств защиты от утечки информации в электрических каналах передачи цифровых данных за счет «ВЧ-навязывания».

При этом уже сейчас можно с уверенностью предположить, что защита сетей передачи данных с пропускными способностями в 100 Мбит/с и выше от сигналов «ВЧ-навязывания» потребует разработки принципиально новых подходов, основанных на алгоритмах поиска частот организации каналов утечки, а

также активном мониторинге сетей на присутствие «подозрительных» гармоник в их спектрах.

Литература

1. Kuhn M.G., Anderson R.J. Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations, in David Aucsmith (Ed.): Information Hiding, Second International Workshop, IH'98, Portland, Oregon, USA, April 15-17, 1998, Proceedings, LNCS 1525, Springer-Verlag, pp 124-142.

2. «Информационная безопасность офиса». Научно-практический сборник Выпуск первый «Технические средства защиты информации».– К.: ООО «ТИД «ДС», 2003.– 216 с.

ДИСКРЕТНОЕ ЛОГАРИФМИРОВАНИЕ НА МУЛЬТИПЛИКАТИВНОЙ ГРУППЕ ДЛЯ ДВУХСОСТАВНОГО МОДУЛЯ RSA

В.Н.Сюрин, И.Л.Гаврилова, Д.В.Шилко
Беларусь, г. Гродно

Хорошо известно, что дискретное логарифмирование на мультипликативной группе относится к числу NP-полных проблем, которые решаются путем перебора. По-нашему мнению, можно получить некоторые аналитические результаты в этой области, если учитывать специфику решаемой задачи.

Рассмотрим данные особенности на мультипликативной группе G_2 для двухсоставного модуля криптосистемы RSA $N = pq$, где p и q - большие простые числа.

Очевидно, что на группе G_2 в данном случае [1]

$$2^N = 2^{(p-1)(q-1)} \times 2^{p+q-1}, \bmod N = 2^{p+q-1}, \bmod N. \qquad (1)$$

Вычисление (1) снижает порядок исследуемого пространства элементов группы, а также при вычислении логарифма правой его части дает возможность определения p и q путем решения системы уравнений

$$\begin{aligned} p \times q &= N; \\ p + q &= a, \end{aligned} \qquad (2)$$

где $a = \log_2 2^{p+q-1} + 1$, то есть произвести вскрытие криптосистемы RSA.

Логарифм правой части (1) может быть вычислен путем последовательного умножения на элемент, обратный элементу 2^1 и сравнения на каждом шаге с системой заранее вычисленных остатков $2^i, \bmod N$. Для удобства ограничим эту систему значениями $2^0, 2^1, \ldots, 2^i < N$, тогда сравнение с каждым остатком на