Е.Г. Белоглазов

E.G. Beloglazov

Моделирование технических каналов утечки информации с целью улучшения их защищенности

Modelling of the technical channels of information leakage for their protection improvement

Аннотация, abstract: В статье описываются математические модели технических каналов утечки информации в среде MATLAB с целью проверки их защищенности. Для проверки таких средств защиты как фильтры (электрический, электромагнитный, акустический, оптический) и генераторы шума предлагается использовать моделирование защищенного на их основе канала с целью выявления утечки информации (в статье это названо модельным аудитом). Теоретически, проведение модельного аудита основывается на решении задачи деконволюции сигналов на выходе режекторных фильтров, а в практическом плане – на применении для этой цели инверсных фильтров. Для повышения защищенности, в случае выявления уязвимости типовой защиты на основе режекторных фильтров и генераторов шума, рекомендуется применение адаптивных фильтров.

The article presents the mathematical models of information leakage via technical channels created in MATLAB environment for their protection examination. The model of channel protected by means of such security equipment as filters (electric, electromagnetic, sonic, optical) and noise-generators shall apply for their examination and detection of the information leakage (in the article this method refer to as model audit). In theory the execution of model audit substantiates by problem-solution of signals' deconvolution in output of the reject filters, in practice for this purpose should be used the inverted filters. The adaptive filters

should be set-in for the protection improvement in case of vulnerability detection in the standard protection system based on the reject filters and noise-generators.

Ключевые слова, keywords: модельный аудит, режекторные фильтры, инверсные фильтры, адаптивные фильтры, генераторы шума, деконволюция, model audit, reject filters, inverted filters, adaptive filters, noise signal generators, deconvolution.

Автор, author: Белоглазов Евгений Григорьевич – Московский Университет МВД России им. В.Я. Кикотя, кандидат технических наук, профессор кафедры специальных информационных технологий учебно-научного комплекса информационных технологий.

Beloglazov, Yevgeniy G. – Moscow University of the Ministry of the Interior of the Russian Federation named after V.Y. Kikot, Russia, Moscow; PhD, professor of department.

УДК: 004.942

Статья поступила: 15.05.2015

Статья принята к печати: 13.06.2015

Введение

Защита технических каналов от утечки информации является одним из важнейших направлений противодействия технической разведке, как со стороны организованных преступных формирований, так и иностранных государств. Среди всего многообразия методов, программно-технических средств и методик обеспечения защиты технических каналов от утечки информации в данной статье будут рассматриваться только такие методы и их реализация на практике, которые основаны на технологиях фильтрации сигнала и (или) генерации шума. Поскольку данные методы относительно просты в реализации, доступны в экономическом отношении на практике и широко распространены для защиты информации представленной в различных формах, будем относить их к типовым методам защиты технических каналов от утечки информации.

При этом исследование типовых каналов утечки информации сводится к изучению математических моделей фильтров без привязки к их различным физическим реализациям (электрический, электромагнитный, акустический, оптический) и математическим моделям случайных процессов, которые используются в генераторах шума различного назначения.

В методическом плане математическая модель типового канала утечки информации необходима для того, чтобы оценить возможность полной или частичной блокировки сигнала утечки в данном канале с использованием противником самых современных методов и технологий восстановления и выделения сигнала из шума. Такая технология проверки утечки информации по техническим каналам, оснащенным типовыми средствами защиты, будет представлять собой модельный аудит защищенности канала, что менее затратно, чем проведение его на реальном объекте.

В том случае, если в результате модельного аудита конкретных технических средств зашиты, становится ясно, что сигнал утечки информации может быть доступен (в том числе, и противнику), то следует признать недостаточность типовой защиты. В этом случае необходимо усиливать эту защиту, причем одним из современных методов усиления защиты может служить применение адаптивных фильтров, требования к которым необходимо сформулировать.

Технические каналы утечки информации и их типовая защита

В теории и практике инженерно-технической защиты информации выделяются следующие технические каналы утечки информации:

– акустический;
– оптический;
– электрический;
– электромагнитный.

В качестве типовой защиты в данных каналах применяется заградительные (режекторные) фильтры и генераторы шума.

В акустических каналах утечки информации активно применяются генераторы акустического шума, а также акустические фильтры в виде звукоизолирующих материалов.

В оптических каналах утечки информации оптическая фильтрация заключается в установке жалюзей на окна и других частично и полностью оптически непроницаемых экранов.

В электрических каналах наибольшее распространение получили широкополосные заградительные фильтры для устранения побочных электромагнитных помех.

В электромагнитных каналах утечки информации нашли широкое применение генераторы электромагнитного шума.

В соответствии Решением ГКРЧ при Мининформсвязи РФ от 28.11.2005 N 05-10-03-001(редакция 2011г.) введены следующие требования к генераторам радиошума [1]:

1. Выделить полосу радиочастот 0,1 – 1000 МГц для разработки, производства и модернизации гражданами Российской Федерации и российскими юридическими лицами генераторов.

2. Соблюдать не превышение указанных в таблице 1 допустимых значений уровней напряженности поля для генераторов радиошума, используемых в качестве средств защиты информации.

Таблица 1. Допустимые значения напряженности поля для генераторов радиошума, используемых в качестве средств защиты информации

Полоса частот, МГц	Напряженность поля, дБ мкВ/м
от 0,1 до 0,5 включительно	60
от 0,5 до 2,5 включительно	54
от 2,5 до 140 включительно	46
от 140 до 1000 включительно	32

Примечания.

1. Допустимые квазипиковые значения напряженности поля не должны превышать значений, приведенных в таблице:

– для объектов на расстоянии 10 м от границы со всех сторон защищаемого объекта;

– для вновь разрабатываемых средств на расстоянии 10 м от антенн генераторов радиошума.

2. Испытания генераторов радиошума на соответствие указанным требованиям должны проводиться:

– для разрабатываемых и модернизируемых генераторов радиошума – при приемочных испытаниях;

– для производимых (серийно выпускаемых) и ввозимых из-за границы генераторов радиошума – при периодических, типовых и сертификационных испытаниях;

– для защищаемых объектов – при оформлении регистрации и в процессе применения генераторов радиошума.

3. Измерения на соответствие указанным требованиям должны проводиться в соответствии с Нормами 8-95.

В соответствии с руководящим документом [2] “Средства защиты информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам” устанавливаются требования по безопасности информации, которым должны соответствовать сетевые помехоподавляющие фильтры, применяемые для защиты информации от утечки по каналам ПЭМИН, а также общие технические требования к этим фильтрам.

Фильтры устанавливаются в цепь питания технических средств или непосредственно в помещениях, в которых производится обработка конфиденциальной информации, или же за пределами этих помещений, например, во вводных распределительных устройствах, в технических помещениях и в коридорах зданий у распределительных устройств.

В первом случае фильтры классифицируются как «фильтры для локальных цепей». Они, как правило, рассчитаны на электропитание одного или нескольких технических средств и обеспечивают подавление информативных сигналов в фазном, нулевом и в заземляющем проводах розеточной сети.

Вторая группа фильтров, классифицируемая как “объектовые фильтры”, устанавливается в цепи электропитания группы технических средств или объекта информатизации в целом, благодаря чему достигается подавление информативных сигналов в кабелях питания трехфазной сети. Требования, предъявляемые к фильтрам как к средствам защиты информации от утечки за счет ПЭМИН (специальные требования), приведены в таблице 2.

Таблица 2. Специальные требования к фильтрам

№ п/п	Наименование параметра	Требуемое значение параметра
1	Полоса подавления по синфазным токам и напряжениям, МГц	0,15 – 1000
2	Полоса подавления по противофазным токам и напряжениям, МГц	0, 15- 1000
3	Величина вносимого затухания в полосе подавления фильтра по синфазным и противофазным токам и напряжениям на нагрузке 50 Ом, не менее, дБ	одно из значений ряда 40, 60, 80. 100, 120
4	Напряжение на шинах фильтра при воздействии акустического давления в речевом диапазоне частот 1 Па (94 дБА), не более, мкВ	Значения определяются «Нормами эффективности защиты информации от утечки за счет ПЭМИН»
5	Напряжение на шинах фильтра при воздействии внешних электромагнитных полей речевого диапазона частот напряженностью Е=5 В/м и Н=0,1 А/м при номинальной нагрузке, не более, мкВ	То же

, где Е – напряженность электрического поля, Н – напряженность магнитного поля.

1. Требования п.п. 4 и 5 таблицы 1 распространяются только на фильтры, которые должны устанавливаться в выделенных помещениях

2. Значения нижней и верхней частот полосы подавления фильтра могут задаваться в более широких пределах по требованиям технических условий. Рекомендуется для объектовых фильтров полосу подавления задавать в пределах 0.02-1000 МГц. Для фильтров, устанавливаемых в экранированных сооружениях, полосу подавления рекомендуется устанавливать в пределах 0,02-10 000 МГц.

3. Для объектовых фильтров величину вносимого затухания рекомендуется задавать на уровне не менее 60-80 дБ.

Методы преодоления типовой защиты

Для преодоления типовой защиты технического канала от утечки с целью модельного аудита программно-технических средств режекторной фильтрации и генерации шума могут быть применены методы деконволюции сигналов в условиях шума.

Основное назначение деконволюции (deconvolution) – восстановление истинной формы сигнала, несущего информацию об исследуемом физическом или технологическом процессе, явлении природы и т.п., после его искажения при регистрации какой-либо линейной системой – измерительным трактом прибора (аппаратной или приборной функцией) или каналом связи. Естественно, что для восстановления необходимы сведения о

характеристиках искажающей системы, и в первую очередь, об импульсном отклике системы или его частотной передаточной функции [3].

Практическая реализация метода деконволюции основывается на решение задачи обратной фильтрации, которая для преодоления типовой защиты технического канала от утечки на практике реализуется посредством фильтров передаточная функция которых, является обратной. В математическом плане такая задача относится к некорректно поставленным задачам: а именно, ее постановка заключается в нахождении по известным наблюдаемым значениям на выходе системы и ее передаточной функции неизвестных входных сигналов. Указанная выше задача, в общем, является некорректно-поставленной, то есть могут не выполняться три условия устойчивости по Адамару.

1. Решение задачи может не существовать.

2. Решений может иметь бесконечное множество.

3. Решение может быть неустойчивым.

Для решения некорректно-поставленных задач разработаны специальные методы на основе регуляризации (выбора из возможных решений наиболее близкого к истинному). Поэтому для преодоления типовой защиты технического канала от утечки возможно применение метода деконволюции с регуляризацией для построения инверсных фильтров.

Адаптивные фильтры и традиционные области их применения

Для повышения защищенности каналов от утечки информации в случае обнаружения утечки информации, оснащенных типовой защитой, целесообразно применение адаптивных фильтров.

Адаптивный фильтр – это фильтр с изменяемыми в процессе работы параметрами, набор которых во многом зависит от критерия работы адаптивного фильтра. Этим критерием часто является достижение минимума некоторой целевой функции, как правило, квадратичной функции ошибки между так называемым требуемым и выходным сигналом адаптивного фильтра [4].

Область применения адаптивных фильтров весьма обширна:

– идентификация неизвестной линейной системы;

– компенсация эхо-сигнала в телефонных и других линиях связи;

– выравнивание характеристик электрических каналов связи (адаптивные эквалайзеры);

– адаптивные антенные решетки;

– шумоочистка сигналов;

– линейное предсказание сигналов.

В качестве одного из новых направлений адаптивной фильтрации предлагается использовать ее для обеспечения оптимальной защищенности, например, электрического канала от утечки информации, посредством адаптивного режекторного фильтра.

Разработка требований к адаптивному фильтру

Адаптивные фильтры находят применение в заградительной фильтрации сигналов, что наиболее применимо в электрических каналах (для защиты от ПЭМИН) и электромагнитных каналах (для блокирования несущей частоты), так и для генерации шума в электромагнитных каналах.

Применение режекторных фильтров может позволить решить несколько очень важных проблем защиты информации от утечки посредством современных радиозакладных устройств:

– снижение их мощности меньше 0.1 -2,5мВт у антенны прибора;

– присутствие сигнала не больше 20 – 100мксек;

При применении генераторов шума (промышленного назначения) основной проблемой является завышенная мощность шума, что приводит к засорению эфира электромагнитным излучением в излишне широком диапазоне частот. Применения адаптивных фильтров для выделения узкополосного шума, постоянно подстраевомого по частоте к электромагнитному сигналу утечки информации, позволяет сформировать адаптивную помеху с мощностью не превышающую стандартизованный уровень или даже ниже его без ущерба для блокирования нежелательного сигнала.

Заключение

В настоящей статье предложена основа методологии повышения защищенности технических каналов от утечки. Эту технологию составляют такие методы как цифровая фильтрация, инверсная фильтрация и адаптивная фильтрация сигналов. Их совокупность совместно с программно-техническим и методическим обеспечением аудита технических каналов утечки информации должны наполнить эту методологию теоретическим содержанием и практической направленностью. При этом методической основой при разработке всех компонентов данной методологии должно служить математическое моделирование исследуемых технических средств, информационных процессов и явлений.

Литература

1. Решение ГКРЧ при Мининформсвязи РФ от 28.11.2005 N 05-10-03-001 «О выделении полосы радиочастот 0,1 – 1000 МГц для генераторов радиошума, используемых в качестве средств защиты информации».

2. «Средства защиты информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам» (руководящий документ) // Сборник руководящих документов по защите информации от несанкционированного доступа. М.: Гостехкомиссия России, 1998.

3. Джиган В.И. Адаптивная фильтрация: теория и практика. М., 2013.