СПИСОК ЛИТЕРАТУРЫ:

1. Program to recover/crack SHA1, MD5 & MD4 hashes. URL: http://www.golubev.com/files/ighashgpu/readme.htm.
2. World Fastest MD5 cracker BarsWF. URL: http://3.14.by/ru/md5.
3. *Трахтенгерц Э. А.* Программное обеспечение параллельных процессоров. М.: Наука, 1987.
4. Документация по работе с SIMD-архитектурой AMD. URL: http://developer.amd.com/sdks/AMDAPPSDK/assets/AMD_Accelerated_Parallel_Processing_OpenCL_Programming_Guide.pdf.
5. Документация к GPU Nvidia. URL: http://developer.nvidia.com/nvidia-gpu-computing-documentation.

А. А. Панов

ПЕРЕДАЧА ДАННЫХ ЧЕРЕЗ РЕЧЕВЫЕ КАНАЛЫ СИСТЕМЫ GSM

Изначально система GSM позиционировалась как «исключительно речевая» коммуникационная сеть. Одним из известных ее усовершенствований стало добавление возможности передачи данных. Самым распространенным каналом передачи данных, добавленным в сеть GSM, является General Packet Radio Service (GPRS). При этом GPRS-трафик и речевой GSM-трафик разделяют один и тот же радиоканал. Чтобы избежать ухудшения качества обслуживания речевого трафика GSM, речь обладает приоритетом, а остаточная пропускная способность сети отведена под GPRS. Эта пропускная способность напрямую зависит от загрузки сети речевым трафиком, с увеличением которого, соответственно, растет время стояния в очереди на обслуживание пользователей GPRS. К существенным недостаткам GPRS также относятся прерывистая зона покрытия и проблемы совместимости. Кроме того, многие существующие сети GSM имеют ограничение пропускной способности GPRS. Одним из решений данной проблемы может стать использование непосредственно самих речевых каналов GSM для передачи данных.

Другим важным поводом для разработки системы передачи данных по речевым каналам GSM послужила неполная защищенность речи в процессе передачи ее от одного пользователя к другому. Передаваемая речь защищена от несанкционированного доступа лишь на этапе прохождения от абонентского терминала до базовой станции (т. е. в канале радиодоступа). По магистральным каналам GSM и каналам телефонной коммутируемой сети общего пользования (ТфОП) речь передается в открытом виде (PCM — импульсно-кодовая модуляция или ADPCM — адаптивная дискретная импульсно-кодовая модуляция), доступ к ней могут получить как операторы сети, так и неавторизованные пользователи. Решением этой проблемы, в частности, занимались сотрудники английского центра исследований коммуникационных систем, которые свели эту задачу к передаче данных через речевые каналы системы GSM [1].

Входящий речевой сигнал преобразуется в битовый поток речевым кодером, который, в свою очередь, шифруется и направляется в модулятор. На выходе модулятора получаются речеподобные волновые формы, которые и передаются в системе GSM с одного абонентского терминала на другой. Т. е. речь передается как зашифрованные данные.

Таким образом, идея передачи данных по речевым каналам системы GSM сводится к разработке и реализации модема, который на передающей стороне переводит входящий поток данных в набор волновых форм из диапазона тональной частоты (300—3400 Гц) — процесс модуляции, а на приемной стороне осуществляет преобразование полученных волновых форм в битовый поток — процесс демодуляции. По существу, такой модем представляется парой кодер/декодер, кодирующей передаваемые данные в сигнал, который трактуется системой GSM как речь,

позволяя тем самым абонентскому терминалу GSM совершать его передачу в эфир и декодировать этот сигнал обратно в данные. Для сети GSM это выглядит как обычный голосовой вызов.

Имеется ряд конструктивных ограничений на сигнал с выхода такого модема:
- сигнал должен проходить через речевой канал, не создавая «особых» случаев, при которых задействуются вспомогательные системы (например, детектор активности речи), и умещаться в диапазон тональных частот (ТЧ), чтобы избежать искажений, вызываемых фильтрацией;
- сигнал должен быть устойчив к речевому кодеку GSM, т. е. он должен успешно декодироваться после прохождения речевого кодека.

На сегодняшний день имеется ряд исследований по созданию подобных модемов. По своей сути все такие модемы содержат некий набор волновых форм и соответствующие им битовые комбинации (словарь) и функционируют по принципу постановки в соответствие каждой комбинации бит соответствующей волновой формы при кодировании и каждой волновой форме соответствующей битовой комбинации при декодировании. Основным отличием их являются методы генерации волновых форм, в которые отображаются передаваемые данные [1, 2, 4].

В 2006 г. Кристоф Карл ЛаДуэ (Christoph Karl LaDue) запатентовал в США идею создания модема для ограниченных по частоте нелинейных каналов (речевой канал GSM, в сущности, это нелинейный, ограниченный по частоте канал с памятью) на основе эволюционного синтеза (патентный номер US 2006/0293045 A1 от 28 декабря 2006 г.) [3]. Он исходил из того, что если разрабатываемый модем выдает сигнал, который укладывается в диапазон ТЧ, не вызывая чрезвычайных ситуаций при прохождении речевого канала GSM, а сама сеть GSM функционирует корректно, то основным источником ошибок в процессе передачи сигнала по сети GSM является только речевой кодек GSM [4]. Таким образом, для успешной передачи данных через GSM-кодек необходимо создать набор волновых форм, или «символов», которые попадают в диапазон ТЧ и, соответственно, могут быть успешно декодированы модемом после прохождения вокодера. Данные отображаются в символы на передающей стороне и извлекаются из них на приемной стороне. Этот метод представляет собой технологию «перекодировки данных», результат которой воспринимается стандартной системой GSM. Метод состоит в применении эволюционной оптимизации. Для построения желаемого сигнала как набора волновых форм (словаря символов) используется генетический алгоритм (ГА). Этот процесс выполняется автономно, как и сама процедура проектирования модема. Модем берет уже сгенерированные символы и помечает ими (ставит их в соответствие) входные данные. Символы соединяются и передаются в эфир модулем GSM. На приемной стороне каждый символ выводится модулем GSM и конвертируется обратно в данные. Принятыми данными (или их оценкой) является индекс символа из кодовой книги, который максимизирует скалярное произведение с полученным символом (метод максимума скалярного произведения MDP).

Как уже было отмечено выше, методы построения таких модемов отличаются в основном алгоритмами конструирования волновых форм (символов). Разработка подобных алгоритмов сама по себе является весьма трудоемкой и очень важной задачей, так как именно от того, насколько удачно реализованы символы, будут зависеть скорость и правильность передачи данных.

СПИСОК ЛИТЕРАТУРЫ:

1. *Katugampala N., Villette S. and Kondoz A.* Secure voice over GSM and other low bit rate systems, IEE Secure GSM and Beyond: End to End Security for Mobile Communications. London, Feb., 2003.
2. *Rashidi M., Sayadiyan A., Mowlaee P.* A Harmonic Approach to Data Transmission over GSM Voice Channel. Tehran, 2008.

3. United States Patent Application Publication Dec. 28, 2006 US 2006/0293045 A1. Christoph K. LaDue. Evolutionary Synthesis of a Modem for band-limited non-linear Channels.
4. *LaDue C., Sapozhnykov V. and Fienberg K.* A Data Modem for GSM Voice Channel // IEEE Transactions on Vehicular Technology. Vol. 57. № 4. July 2008.

Д. Ю. Персанов

ПРИМЕНЕНИЕ АУТСОРСИНГА КАК СПОСОБА РЕАЛИЗАЦИИ ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

В настоящей статье рассмотрено применение аутсорсинга как способа оказания услуг безопасности. Проанализированы характерные особенности, влияющие на выбор управленческой стратегии в пользу аутсорсинга. Проведен анализ применения аутсорсинга для процессов обеспечения физической, информационной и экономической безопасности. В качестве выводов сформулированы основные рекомендации по использованию аутсорсинга процессов обеспечения безопасности на предприятиях.

1. Авторское видение понятия аутсорсинга процессов обеспечения безопасности.

2. Разделение процессов обеспечения безопасности по уровням управления.

3. Определены возможные факторы, оказывающие влияние на принятие решения по использованию аутсорсинга процессов обеспечения безопасности.

4. Экономические составляющие в обосновании стратегии использования аутсорсинга процессов обеспечения безопасности.

5. Даны рекомендации по применению аутсорсинга процессов физической, информационной и экономической безопасности.

6. Рассмотрены практические примеры использования аутсорсинга процессов обеспечения безопасности.

СПИСОК ЛИТЕРАТУРЫ:

1. ГОСТ Р ИСО/МЭК 27002:2005 «Информационная технология. Методы и средства обеспечения безопасности. Свод правил по управлению защитой информации».
2. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий».
3. Международный стандарт Control Objectives for Information and Related Technology (COBIT) 4.1.
4. Международный стандарт Information security management maturity model (ISM3) 2.10.
5. Материалы маркетинговых презентаций по спектру предоставляемых услуг информационной безопасности ЗАО НИП «ИНФОРМЗАЩИТА».