7. Головин О.В., Простов С.П. Системы и устройства коротковолновой радиосвязи. М.: Горячая линия – Телеком, 2006. – 598 с.
8. Назаров С.Н. Применение элементов декаметровой радиосвязи в современных беспроводных сетях // Труды РНТО им. А.С. Попова. Сер. «Цифровая обработка сигналов и ее применение». Вып. XI-1, 2009. – С. 228-230.
9. Назаров С.Н. Общий подход к построению современных гибридных сетей беспроводной связи // Труды РНТО им. А.С. Попова. Сер. «Научная сессия, посвященная Дню радио». Вып. LXIV, 2009 – С. 22-24.
10. Вишневский О.В., Семенова О.В. Системы полинга: теория и применение в широкополосных беспроводных сетях. М.: Техносфера, 2007. – 312 с.
11. Вишневский О.В., Ляхов А.И., Портной С.Л., Шахнович И.В. Широкополосные беспроводные сети передачи информации. М.: Техносфера, 2005. – 592 с.
12. Вишневский В.М. Теоретические основы проектирования компьютерных сетей. М.: Техносфера, 2003. – 512 с.
13. Bianchi G. Performance Analysis of the IEEE 802.11 Distributed Coordination Function // IEEE Journal on Selected Areas in Communications. V.18, 2000. – P. 535-548.
14. Melamed B. Times in Queueing Networks // Math. Oper. Res. V.7, N2, 1982. – P. 337-352.
15. Шаров А.Н., Степанец В.И., Комашинский В.И. Сети радиосвязи с пакетной передачей информации. СПб.: Изд. ВАС, 1994. – 216 с.

RESEARCH OF THE BASIC CHARACTERISTICS OF A HYBRID NETWORK OF WIRELESS TRANSFER OF THE INFORMATION

Nazarov S.N.

In modern networks of wireless communication multipurpose devices with the several built - in transceivers are used. They enable the subscriber to move on various distances and directions. Therefore there is a necessity of support by mobile platforms (MT) of process of information interchange in different frequency ranges and standards. There is a necessity of a hybrid network of wireless transfer of the information which represents complex set of the connected technologies, networks and the standards, realizing in itself algorithms of the centralized and distributed management.

Submission of such network of the uniform purpose – satisfaction of needs of users in granting of telecommunication services by him with required quality and cost, is complex many criterions a problem demanding realization of the analysis of principles of functioning of local, regional and global wireless networks of transfer of the information, constructed on the basis of standards 802.11,16, radio communications; the analysis of methods of research, development of criteria and realization of a rating of efficiency of their functioning. Present article is devoted to the decision of the given problem.

Keywords: *mobile platforms, telecommunication technologies, adaptive algorithm of management, function of collective access.*

Назаров Сергей Николаевич, к.т.н., доцент Кафедры «Информатика» Ульяновского высшего авиационного училища гражданской авиации. E-mail: art3456@rambler.ru

ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ И БЕЗОПАСНОСТЬ ОБОРУДОВАНИЯ

УДК 004.056

СКРЫТАЯ ПЕРЕДАЧА ДАННЫХ В ЗВУКОВЫХ ФАЙЛАХ ФОРМАТА WAV

Алексеев А.П., Аленин А.А.

Существует острая проблема защиты конфиденциальной информации и авторских прав. Разработка новых методов защиты информации ведется с помощью приемов, разработанных в криптографии и стеганографии [1]. Криптографические методы защиты информации основаны на модификации (преобразовании) защищаемого сообщения. Стеганография позволяет скрыть сам факт передачи сообщения. В статье рассматриваются методы совершенствования защиты информации путем ее сокрытия в звуковых файлах.

Ключевые слова: информация, стеганография, скрытность, сигнал, разряд, осциллограмма, контейнер, тишина, искажения, оценка.

Методы внедрения информации в звуковые файлы различных форматов

Файл формата WAV содержит в себе цифровые отсчеты амплитуды, сделанные в дискретные моменты времени. Для файла формата WAV наиболее известным методом внедрения информации является метод замены наименьшего значащего бита (НЗБ). Способ имеет приемлемую стойкость к взлому и позволяет скрывать достаточный объем информации в одном звуковом файле. Например, при длине файла 16 Мбайт и размере выборки 16 бит в нем можно скрытно разместить 1 Мбайт информации.

Другими методами сокрытия информации, применимыми к файлам формата WAV, являются методы, основанные на преобразовании спектров звукового сигнала и подмешивании эхо-сигнала [2].

Суть метода модификации спектра фаз заключается в изменении фазы каждой частотной составляющей дискретного сигнала. Для этого исходный сигнал разбивают на серию коротких сегментов, содержащих одинаковое количество отсчетов. Затем к каждому сегменту применяют дискретное преобразование Фурье. В результате для каждого сегмента создаются массивы фаз и амплитуд. Для обеспечения скрытности сообщения необходимо сохранить разность фаз между соседними сегментами. Модификацию фаз производят в массиве фаз первого сегмента. Встраивание информации осуществляют путем замены исходного значения фазы на значение, равное $-\pi/2$, если бит скрываемого сообщения равен 0, и на значение $\pi/2$, если бит сообщения равен 1. Чтобы сохранить существующую разницу фаз, полученный массив фаз первого сегмента суммируют с вычисленной ранее разностью между первым и вторым массивом фаз. Аналогично поступают с остальными сегментами. Для восстановления звукового сигнала выполняют обратное дискретное преобразование Фурье.

В методе расширения спектра информацию встраивают в звуковой сигнал с помощью незначительного изменения амплитуды сигнала. Помехоустойчивость обеспечивается тем, что энергия сигнала распределяется по всему возможному диапазону частот.

Для сокрытия информации в звуковом сигнале данные умножают на псевдослучайную последовательность и на основной несущий сигнал. Чтобы сделать шум, вносимый полученной последовательностью незаметным, его ослабляют до уровня в одну сотую долю от исходного уровня сигнала. Ослабленный сигнал суммируют с основным несущим сигналом.

Метод внедрения информации с помощью эхо-сигнала основан на том, что человек не может обнаружить разницу между основным сигналом и эхо-сигналом, если задержка между этими двумя сигналами меньше определенного значения. Для встраивания информации в сигнал используют два времени задержки: одно для кодирования нуля, другое для кодирования единицы.

Для сжатого файла формата MP3 применять метод замены наименее значащего бита нельзя. Но можно применить метод, похожий на НЗБ. Файл формата MP3 состоит из нескольких фреймов. Фрейм MP3 состоит из заголовка и блока данных. Суть метода заключается в том, что если изменить какое-нибудь значение в заголовке фрейма на недопустимое, то проигрыватель просто не воспроизведет этот фрейм и перейдет к следующему. Следовательно, для внедрения данных можно использовать этот фрейм.

Экспертная оценка слышимости искажений контейнера

При внедрении информации в звуковые файлы приходится решать задачу выбора номера разряда отсчета, в который допустимо помещать скрываемую информацию, с учетом двух конфликтующих требований. С одной стороны, необходимо увеличивать объем передаваемой информации в одном файле (увеличивать пропускную способность), а с другой стороны – нужно удерживать высокую степень скрытности передачи информации.

Для решения этой задачи была проведена экспертная оценка слышимости искажений в зависимости от номера разряда отсчета, в который происходило внедрение скрываемой информации.

При проведении экспериментальных исследований учитывались требования, перечисленные в [3]. Для исследования были подготовлены 15 файлов с записью информации в различные разряды отсчетов (от младшего разряда до предпоследнего старшего разряда). Исходный файл содержал запись «полной тишины», он искажался поочередной записью информации в различные разряды. Запись внедряемой информации в каждый файл производилась следующим образом: в четные отсчеты записывался 0, а в нечетные отсчеты записывалась 1.

Восемнадцать экспертов (в возрасте 18…19 лет) оценивали громкость звучания предъявлен-

ных файлов по пятибалльной системе (от 0 до 4). Наибольшей громкости звучания соответствовал балл 4, а файлу без вложения («полная тишина») соответствовал балл 0. При прослушивании (тестировании) каждого файла для сравнения воспроизводились файл с записью «полной тишины» и файл с записью битов, скрытых в старшем разряде.

При обработке экспериментальных данных вычислялись среднее арифметическое значение громкости звучания для каждого файла и дисперсия. Значение дисперсии находилось в пределах 3…12% от среднего арифметического значения громкости звучания и позволяло контролировать наличие промахов при проведении исследований. При этом одну запись (с использованием правил статистической обработки данных) пришлось удалить, определив ее как промах (ошибку) эксперта.

Результаты экспертной оценки приведены на рис. 1. По горизонтали отложены номера разрядов отсчетов, по вертикали громкость звучания, выраженная в баллах. На рис. 1 младшему разряду отсчета соответствует номер $n = 16$. Экспериментально полученные данные были аппроксимированы логистической функцией

$$g = a + \frac{b}{1 + \left(\frac{n}{c}\right)^d},$$

где g – громкость звучания, выраженная в баллах; n – номер разряда, в который происходило внедрение скрываемой информации; коэффициенты $a = -0{,}165$; $b = 5{,}504$; $c = 3{,}25$; $d = 2{,}325$. Исследования показали, что для скрытой передачи информации можно использовать два младших разряда звукового контейнера.

Визуальная оценка искажения синусоидального сигнала

Проверка полученной выше оценки слышимости искажений была повторно проведена визуально с помощью звукового редактора Sound Forge 7.0. Для этого исследовались искажения осциллограмм синусоиды в зависимости от номера разряда, выбранного для внедрения.

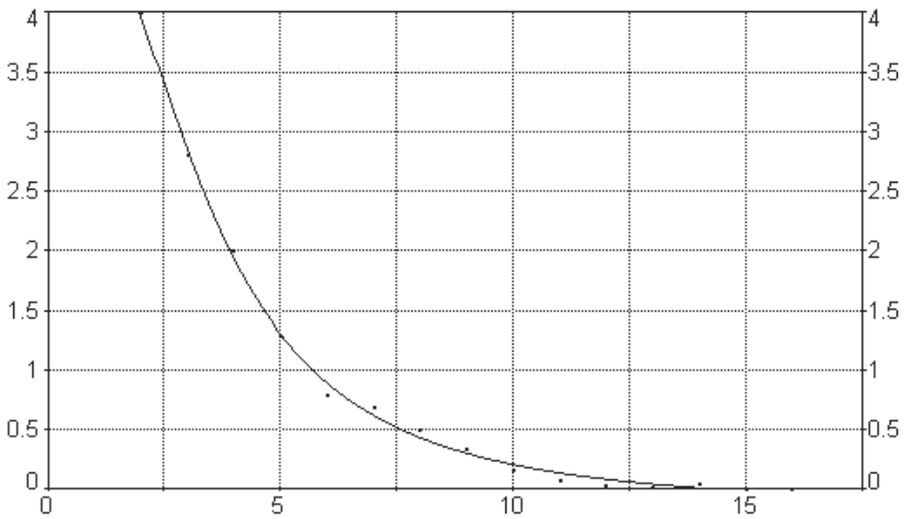
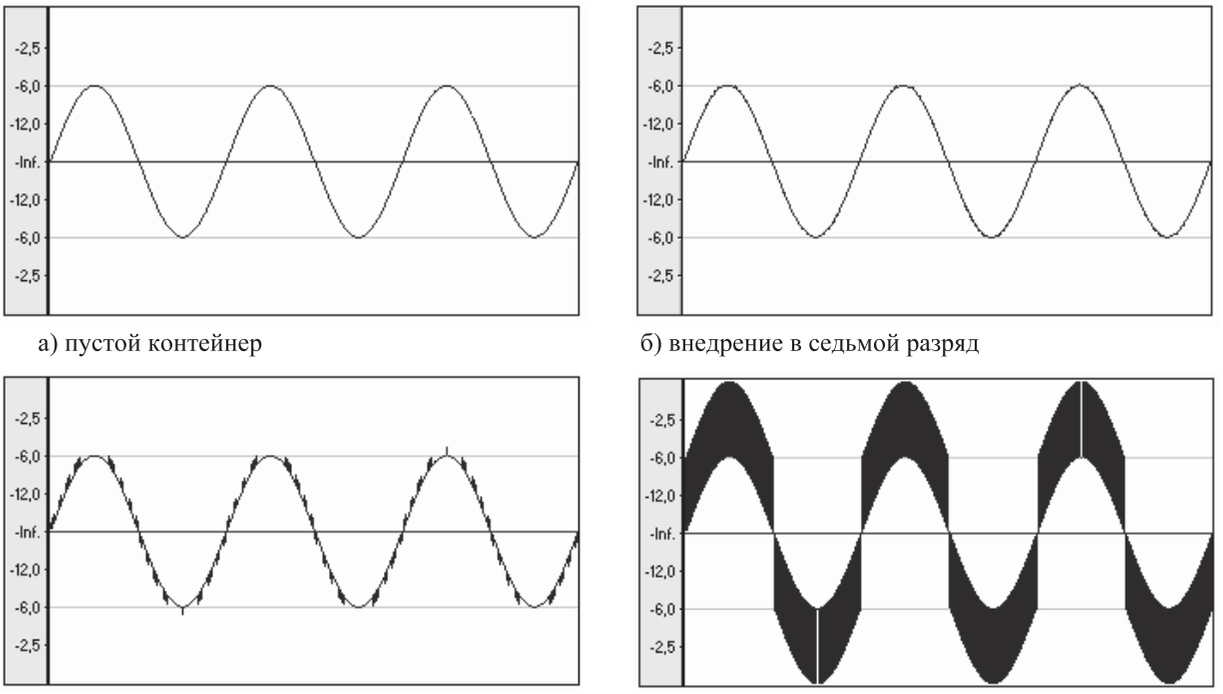


Рис. 1. Результаты экспертной оценки слышимости вложений

Временной интервал задавался в виде $t = 0{:}1/44100{:}10$. Функция для генерации сигнала $x = 0.5*sin(1350*t)$.

Генерация звукового файла формата WAV с частотой дискретизации 44100 Гц и уровнем квантования 16 бит осуществлялась функцией wavwrite(x,44100,16,'c:\sin.wav'). Информация в сигнал внедрялась путем замены очередного бита, с учетом знака отсчета. Сначала информация внедрялась в шестнадцатый (младший) разряд. В нечетные отсчеты внедрялась логическая единица, а в четные отсчеты – логический нуль. В следующем файле внедрение осуществлялось в пятнадцатый разряд и т.д. до второго разряда.

Экспериментально установлено, что визуально можно определить наличие вложения в сигнале при изменении седьмого разряда в отсчете. Внедрение информации в разряды 9…16 визуально обнаружить практически невозможно. Данные оценки иллюстрирует рис. 2.



а) пустой контейнер

б) внедрение в седьмой разряд

в) внедрение в пятый разряд

г) внедрение во второй разряд

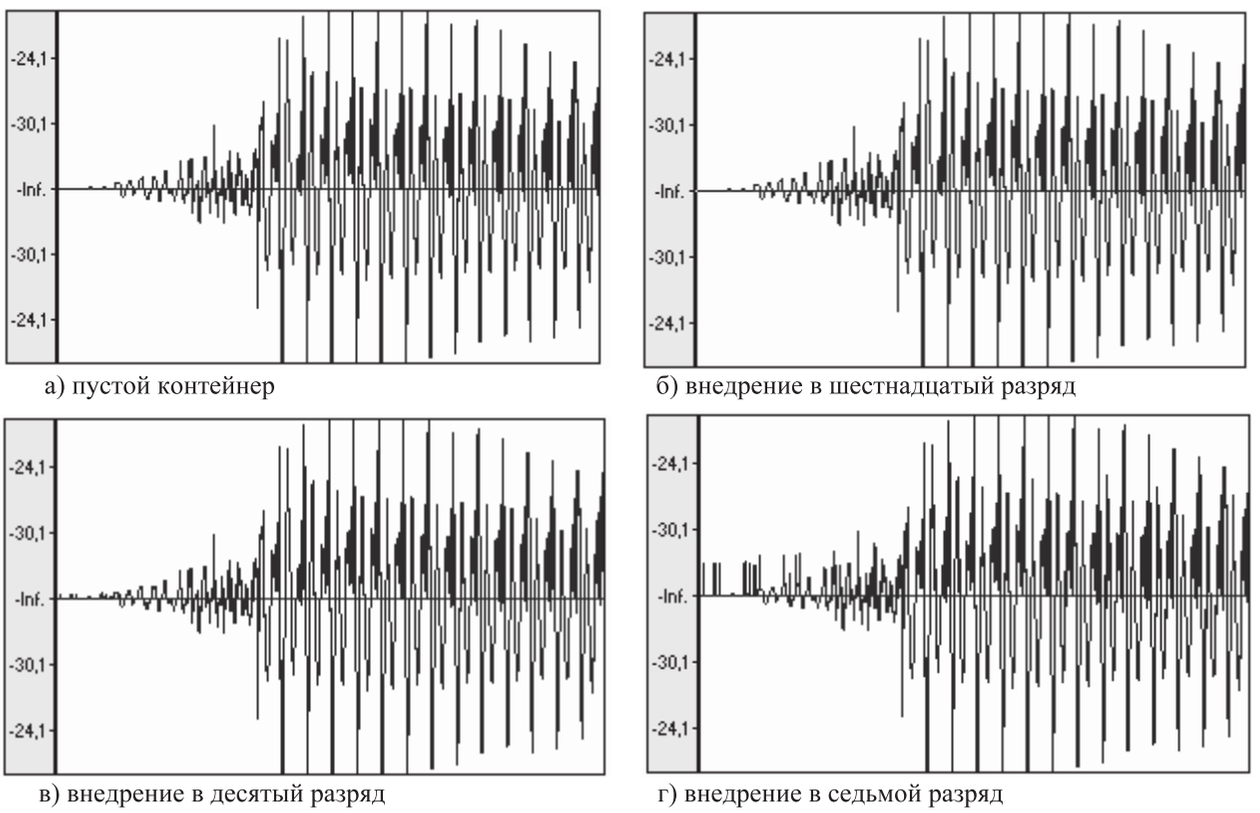
Рис. 2. Осциллограммы синусоидального сигнала с модифицированными битами

Визуальная оценка искажений звукового сигнала

Искажения, вносимые методом замены наименьшего значащего бита в реальном звуковом сигнале, можно также визуально оценить с помощью осциллограмм.

В качестве контейнера использовался звуковой файл с уровнем квантования 16 бит, содержавший запись инструментального, симфонического произведения. На рис. 3а изображена осциллограмма пустого контейнера.

Внедрение в шестнадцатый разряд (самый младший) каждого отсчета не вносило заметных



а) пустой контейнер

б) внедрение в шестнадцатый разряд

в) внедрение в десятый разряд

г) внедрение в седьмой разряд

Рис. 3. Внедрение информации в звуковой файл

искажений (рис. 3б). Изменения в десятом разряде надежно выявлялись на осциллограммах (рис. 3в), но не различались на слух. При внедрении информации в седьмой разряд искажения были различимыми на слух (рис. 3г). Наиболее заметные искажения регистрировались на участках с низким уровнем сигнала (тишина). Если исключить внедрение информации на участках с низким уровнем громкости, то для внедрения можно использовать разряды с 9 по 16.

Программы Crypto и WaveCrypto

Результаты экспериментальных исследований были учтены при разработке программ Crypto и WaveCrypto (программа разработана совместно с Сомковым С.А.).

Программа Crypto предназначена для скрытой передачи сообщений в файл-контейнерах с использованием принципов стеганографии [4]. В частности, в данной программе применяется метод замены наименьшего значащего бита.

Для повышения скрытности внедренной информации в данной программе использован модифицированный метод замены наименьшего значащего бита. Информация разделяется на фрагменты и распределяется по нескольким звуковым файлам. Программа позволяет распределять информацию по десяти звуковым файлам. В программе в качестве контейнера используется файл формата WAV. Ключом для извлечения сообщения служит последовательность файлов, в которых были скрыты фрагменты сообщения. Для повышения степени защиты информации скрываемое сообщение можно предварительно зашифровать с использованием различных симметричных алгоритмов, которые реализованы в данной программе: шифр Цезаря, шифр Атбаш, квадрат Полибия, прямоугольник Плейфейра, метод перестановок, метод гаммирования, аффинные преобразования, шифр Виженера.

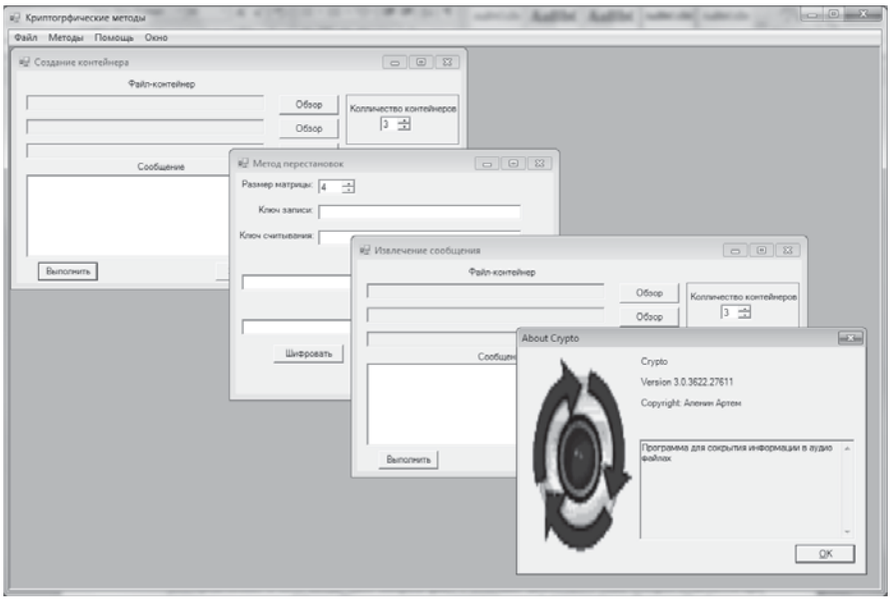


Рис. 4. Главное окно программы Crypto

Программа WaveCrypto позволяет внедрять информацию в один звуковой файл с использованием ключа, распределяющего внедряемую информацию по всему контейнеру. Ключ распределения генерируется в зависимости от требующегося соотношения между наполняемостью и скрытностью, а также размера файла таким образом, чтобы информация распределилась по всему контейнеру. Если в контейнере содержится «тишина», то есть нулевые отсчеты, то программа пропускает их, внедряя информацию только в звук. Для пропуска тишины файл-контейнер разбивается на серии от «тишины» до «тишины», а в серии информация внедряется по ключу распределения.

Выводы

1. При выборе номера разряда, в который допустимо осуществлять внедрение информации, следует ориентироваться на наиболее уязвимые случаи. Полученные экспертным путем оценки показывают, что внедрение допустимо делать в два младших разряда отсчета при 16-битном кодировании звуковых файлов.

2. Разработанные программы Crypto и WaveCrypto создают несколько уровней защиты

информации: шифруют открытый текст одним из криптографических методов, внедряют зашифрованный текст в звуковые файлы, распыляя биты внутри одного или нескольких контейнеров.

3. Рассмотренный метод сокрытия информации может быть использован для формирования «водяных знаков» (защиты авторских прав).

Литература

1. Алексеев А.П., Орлов В.В. Стеганографические и криптографические методы защиты информации. Самара: Изд. ПГУТИ, 2010. – 330 с.
2. Bender W., Gruhl D. u.a. Techniques for data hiding // IBM Systems Journal. №35(3&4), 1996. – P.313-336.
3. Алдошин И.А., Вологдин Э.И. и др. Электроакустика и звуковое вещание. М.: Горячая линия – Телеком, Радио и связь, 2007. – 872 с.
4. Аленин А.А., Алексеев А.П. Пространственное распределение информации в звуковых файлах // Тезисы XVI РНТК ПГУТИ, 2009. – С. 171-172.

HIDDEN DATA TRANSMISSION A SOUND FILE TO WAV FORMAT

Alekseev A.P., Alenin A.A.

There is an acute problem of protecting confidential information and copyrights. Development of new methods of information protection is performed using techniques de-veloped in cryptography and steganography. Cryptographic methods of information security based on a modification (transformation) of the protected message. Steganography allows you to hide the fact of the transfer message. In article results of experimental researches and the program for introduction of the information in sound files are described.

Keywords: *information, steganography, secrecy, signal, level, waveform, container, silence, distortion, evaluation.*

Алексеев Александр Петрович, к.т.н., доцент Кафедры «Информатика и вычислительная техника» Поволжского государственного университета телекоммуникаций и информатики. Тел. (8-846) 228-00-59. E-mail: apa2008@rambler.ru

Аленин Артем Алефтинович, старший преподаватель Димитровградского института технологий, управления и дизайна (филиал Ульяновского государственного технического университета). Тел. (8-842) 355-74-43; 357-25-94. E-mail: styleal@mail.ru

УДК 004.056

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ НА ОСНОВЕ АНАЛИЗА СЕТЕВОГО ТРАФИКА

Ажмухамедов И.М., Марьенков А.Н.

Предложена схема повышения безопасности компьютерных систем и сетей на основе анализа сетевого трафика. К преимуществам данной схемы относятся скорость реагирования на угрозы, минимальное использование вычислительных ресурсов системы, отсутствие необходимости разборки пакетов и, как следствие, независимость от сигнатур вредоносных программ.

Ключевые слова: безопасность, трафик, сеть, самоподобие, сетевые аномалии, сетевые атаки, IP-пакеты, циклический анализ, метод Хольта, компьютерные системы, моделирование, прогнозирование.

Введение

В последнее время сложилась устойчивая тенденция увеличения количества атак на компьютерные сети из Internet. Механизмы атак и способы взлома постоянно совершенствуются. Все это делает разработку и внедрение новых методов и средств защиты информации в компьютерных сетях весьма актуальным.

Одним из методов борьбы с атаками через Интернет может служить отслеживание аномального поведения сетевого трафика, поскольку резкое увеличение количества передаваемой или принимаемой извне информации обычно является признаком начала атаки на сетевой ресурс.

Анализ трафика в силу ряда особенностей эксплуатации компьютерных сетей является новой и еще не до конца проработанной в методическом плане задачей.

В этом направлении в настоящее время существует несколько разработок.