В докладе предлагаются методы действия персонала при обнаружении признаков активации *ПЗ*.

Исследуется необходимость разработки, и внедрения технических средств познакового документирования всей вводимой с пультов информации с жестким непрерывным административным контролем регламента пультового времени.

Также в докладе рассматриваются аспекты защиты информации исключением передачи по *ОКС* № 7 от международного центра коммутации к станциям *АМТС* сообщений с нетелефонными функциями (для предотвращения активации *ПЗ*, форматов *TCAP* и *OMAP*). В докладе предлагается разработка и установка на международном участке специальных тестирующих устройств, обеспечивающих обнаружение и фиксацию всех случаев передачи нетелефонных сообщений четвертого уровня.

Рассматривается обеспечение защиты от несанкционированного доступа к передаваемой информации, которое может быть достигнуто обнаружением искажений в передаваемой информации, реализуемое, например, методом контрольных сумм.

Литература

1. Технические аспекты защиты информации в АТСЦ-90 // http://kiev-security.org.ua
2. Бобов М.Н., Конопелько В.К. Обеспечение безопасности информации в телекоммуникационных системах. Мн.: БГУИР, 2002, 164 с.

ВЫБОР СТРУКТУРЫ АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ВИДЕОКОНФЕРЕНЦИЙ

В.Е. САМСОНОВ, В.С. ШАРАК

В связи с широким распространением систем видеоконференций актуальной задачей является обеспечение защиты сетевого трафика в этих системах. Повышенные требования к пропускной способности сетевой инфраструктуры видеоконференций требуют аппаратной реализации криптографической защиты сетевого трафика.

В докладе изложены результаты экспериментальных работ по аппаратной реализации криптографической защиты информации на сетевом уровне стека протоколов TCP/IP для использования в системах видеоконференций.

Экспериментальный образец устройства выполняет все функции интерфейса PCI шины и управляется драйвером ядра ОС Windows NT, 2000.

Были исследованы такие параметры как скорость аппаратного шифрования одного, скорость преобразования одного IP-пакета, время выполнения передачи пакета в память ЭВМ в режиме DMA, время реакции на прерывания устройства в т.ч. по завершению DMA, а также различные варианты построения драйвера устройства в операционных системах Windows NT, 2000. На основании проведенных оценок выбрана оптимальная структура устройства и метод построения драйвера, позволяющих эффективно производить криптографическое закрытие информации в системах видеоконференций.

ВНЕДРЕНИЕ ВОДЯНОГО ЗНАКА В ПО НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ СТАТИСТИЧЕСКИХ СВОЙСТВ ИСПОЛНЯЕМОГО КОДА

С.С. ПОРТЯНКО

Уже на протяжении многих лет компании, разрабатывающие ПО с целью его продажи, теряют значительную часть доходов из-за компьютерного пиратства. Для того, чтобы препятствовать незаконному тиражированию ПО и для идентификации своих продуктов с целью обеспечения возможности доказательства принадлежности ПО разработчику, чьей интеллектуальной собственностью оно является, используется ряд методик. К их числу относится использование программно-аппаратных ключей (Software Dongles), стеганографические методы, такие как внедрение водяных знаков (watermarks) и "отпечатков пальцев" (fingerprints).

Предлагаемый метод идентификации исполняемого кода приложения является адаптацией основной идеи метода Patchwork, предложенного в [1] применительно к графическим изображениям, к использованию её для внедрения в код программы некоторого признака, характеризующего её принадлежность тому или иному разработчику. Метод основан на использовании статистических свойств исполняемого кода программы, определяющихся частотами встречаемости той или иной команды при осуществлении их случайной выборки.

Проведённые экспериментальные исследования показали, что для конкретной программно-аппаратной платформы распределение инструкций в исполняемых файлах имеет определённый вид, незначительно меняющийся от приложения к приложению.

Непосредственно внедрение водяного знака в программу заключается в модификации вида распределения индексов команд для некоторого подмножества команд программы, полученного в результате случайной выборки, таким образом, что бы оно существенно отличалось от типичного распределения команд для исполняемых файлов для данной программно-аппаратной платформы.

Для того, что бы при статистическом анализе исполняемого кода перейти от символик либо кодов инструкций к числам, производится назначение каждому типу команды индекса.

При внесении изменений в исполняемый код программы, одни группы команд заменяются на другие, являющиеся эквивалентными, чем и достигается модификация частот встречаемости определённых команд, а значит и вида их распределения.

Оптимальное построение списка взаимозаменяемых групп команд обеспечивает наибольшую эффективность процедур замены команд.

В [2] предложен ряд способов трансформаций исполняемого кода программы, служащих для минимизации времени её выполнения, которые могут быть применены и для воздействия на частоты встречаемости определённых команд.

Литература

1. W. Bender, D. Gruhl, N. Morimoto, A. Lu Techniques for data hiding.
2. David F. Bacon, Susan L. Graham and Oliver J. Sharp Compiler transformations for high performance computing.

УСТРОЙСТВО ПОИСКА ДЛЯ СИСТЕМ ТРАЕКТОРНЫХ ИЗМЕРЕНИЙ И СКРЫТНОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ

И.И. АСТРОВСКИЙ, В.К. КОНОПЕЛЬКО

Применение в современных системах радиолокации, радионавигации и связи сигналов с большой базой требует решения сложных проблем, связанных с ускорением генерирования и обработки сигналов, обеспечением помехоустойчивости и скрытной передачи информации.

Наибольшие временные или аппаратурные затраты, как правило, приходятся на поиск по временному положению (задержке). Задержка обычно определяется либо величиной перестройки опорного генератора до получения синхронного положения опорного сигнала приемника со входным, либо временем рассогласования начала входного сигнала с условными моментами отсчетов эталонного времени. Требованиям практики не удовлетворяет как одноканальный обнаружитель из-за больших временных затрат, так и многоканальный из-за больших аппаратурных затрат.

В работах [1, 2] было предложено использовать для целей поиска бинарные псевдослучайные последовательности Велти [3], которые генерируются на основе функций Радемахера и имеют регулярную структуру. Начальные отрезки, длительность которых кратна степени двойки, регулярно повторяются в прямом или инверсном по знаку виде, что позволяет организовать дихотомический поиск, который требует вместо $N/2$ (в среднем) только около $\log_2 N$ вычислительных процедур, сходных с вычислением корреляционной функции.

В докладе предлагается дихотомическая процедура поиска на основе функции суммы модулей, которая вычисляется путем последовательного суммирования абсолютных значений коротких корреляционных функций отрезков входной и опорной последовательностей.

Обосновывается криптостойкость совмещенных систем траекторных измерений и скрытной передачи информации. Показано, что алгоритм построения последовательностей Велти аналогичен алгоритму построения древовидных свёрточных кодов. Причем длина и мощность кода пропорциональны степени двойки, а начальные комбинации регулярно повторяются в прямом или инверсном виде. При отсутствии информации о длине последовательности код приобретает свойство криптостойкости. Случайный перебор длин не решает проблемы.

Предлагается процедура дополнительной манипуляции по знаку исходной последовательности в соответствии с передаваемой низкочастотной информацией. Эта манипуляция не нарушает принципов используемых алгоритмов поиска, не ухудшает качественные характеристики предложенных ранее систем поиска.

Литература

1. Клюев Л.Л., Астровский И.И. Синхронизация приемных устройств по задержке при приеме Д-последовательности. — "Радиотехника и электроника", 1975, т. 20, № 1, с. 178–181
2. Астровский И.И., Клюев Л.Л. Устройство синхронизации псевдошумовых сигналов по задержке. А.С. СССР. № 520716. — "БИ",1976, № 25.
3. Велти. Четверичные коды для импульсного радиолокатора. — "Зарубежная радиоэлектроника", 1961, № 4.

ИСКАЖЕНИЯ ЭЛЕКТРОДИНАМИЧЕСКИХ ПАРАМЕТРОВ СИГНАЛОВ В РАДИОКАНАЛЕ НАД АНИЗОТРОПНЫМ ВКЛЮЧЕНИЕМ

П.М. КАТЛЕРОВ, Д.В. ГОЛОЛОБОВ

Одной из основных причин частичного или полного искажения информационных параметров сигнала в реальном радиоканале без искусственных помех являются процессы электродинамического взаимодействия электромагнитной волны (ЭМВ) с естественными или искусственными неоднородностями. В общем случае неоднородности, возникающие в радиоканале, следует считать анизотропными, описываемыми тензорами диэлектрической и магнитной проницаемости.

Данная проблема может возникнуть в транкинговых системах связи, компьютерных радиосетях, радиорелейных линиях связи, которые работают в различных диапазонах частот на дальних расстояниях.

Проведена оценка электродинамических параметров ЭМВ при распространении по радиотрассе с естественным анизотропным включением, образованным за счет подмагниченного электронно-ионного потока в среде с потерями.