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.