сервер так и клиент передают данные одним блоком только в том случае, если его длина не превышает 8192 байта, иначе данные разбиваются на несколько блоков. Кроме того строка, передаваемая методом SendText не должна содержать символы, коды которых меньше 32. При достаточно быстрой отправке нескольких блоков данных друг за другом, эти блоки соединяются и отправляются как один блок.

Автором была разработана программа LSX Controller, которая предназначена для управления удаленным компьютером по локальной сети. Она работает под операционными системами Windows 98 или Windows Me и предназначена для того, чтобы администраторы сетей под этими ОС смогли следить за действиями пользователей и при необходимости вмешиваться в их работу.

LSX Controller состоит из двух частей: агентской и управляющей. Агентская часть должна быть запущена на компьютере, которым необходимо управлять. Она прописывает себя в файл Win.ini или реестр и автоматически запускается при загрузке Windows. С помощью функций RegisterServiceProcess из kernel32.dll и ShowWindow агентская часть делается невидимой без специальных программ.

Управляющая часть программы сканирует введенный пользователем диапазон IP-адресов в поисках запущенных агентских частей и налаживает с ними связь. Далее пользователь управляющей части может:

- видеть экран удаленного компьютера;
- отслеживать и управлять передвижениями мыши и нажатиями на нем клавиш;
- выполнять команды;
- выключать или перегружать его;
- блокировать клавиатуру и мышь;
- в программу встроен чат администратора с пользователем, функция захвата экрана и рисования по нему.

При разработке программы использована информация с сайта www.doit.com.

ИСПОЛЬЗОВАНИЕ ИЗБЫТОЧНОСТИ БИТОВЫХ МАТРИЦ МУЛЬТИМЕДИЙНЫХ ФАЙЛОВ ДЛЯ СОКРЫТИЯ ДАННЫХ

А. Н. Волкович
Научный руководитель – Л.В. Рудикова
Гродненский государственный университет имени Янки Купалы

Проблема сокрытия информации имеет глубокие исторические корни. Еще в Античной Греции были разработаны различные методы защиты важной информации: скитала, квадрат Полибия, первые «сдвиговые» шифры. Позже, возникли шифры «простой замены» и «перестановочные». В XVIII веке появился шифр «по книге», который можно рассматривать как развитие шифра Цезаря. Все представленные методы защиты информации обладали достаточной стойкостью, но, при определенных усилиях, все-таки могли быть расшифрованы за конечный промежуток времени. Поэтому возникла необходимость не шифрования, а сокрытия наличия информации.

Данный подход получил название «стеганография» (от греч.: «steganos» – секрет, тайна, «graphy» – запись) и означает «тайнопись». Первые упоминания стеганографических методов встречаются уже в Древней Греции, где тексты писались на дощечках, покрытых воском. Хорошо известны также различные способы сокрытия информации между строк обычного письма, от применения молока до использования сложных химических реакций с последующей обработкой при чтении. Другие методы стеганографии включают использование микрофотоснимков, незначительные различия в написании рукописных символов, маленькие проколы определенных напечатанных символов и т.д., скрывающие истинный смысл тайного сообщения в открытой переписке.

Компьютерные технологии способствовали развитию и совершенствованию стеганографии. В области защиты информации появилась цифровая или компьютерная стеганография. Одновременно развиваются и новые методы, предназначенные для обеспечения безопасности и сохранности передачи данных по каналам телекоммуникаций, использования их в различных целях. Данные методы позволяют скрывать сообщения в файлах (контейнерах), учитывая естест-

венные неточности устройств оцифровки и избыточность аналогового видео или аудио сигнала и скрывая сам факт наличия и передачи информации. Это является главным отличием стеганографических методов от методов, используемых в криптографии.

Использование избыточности аудио и визуальной информации является в настоящее время наиболее продуктивным направлением стеганографии. Цифровые фотографии, цифровая музыка и цифровое видео представляются матрицами чисел, которые шифруют интенсивность в дискретные моменты в пространстве и/или во времени.

Цифровая фотография представляет собой матрицу чисел, определяющих интенсивность света в некоторый момент времени. Цифровой звук — это также матрица чисел, которая фиксирует интенсивность звукового сигнала в последовательно идущие моменты времени. Все эти числа не являются достаточно точными в силу того, что не точны устройства оцифровки аналоговых сигналов и присутствуют шумы квантования. Младшие разряды цифровых отсчетов содержат минимум полезной информации о текущих параметрах звука и визуального образа. Их заполнение ощутимо не влияет на качество восприятия, что и дает возможность для скрытия дополнительной информации. Например, графические цветные файлы со схемой смешения RGB шифруют каждую точку рисунка тремя байтами. Любая такая точка состоит из аддитивных составляющих: красного, зеленого, синего. Изменение каждого из трех наименее значимых бит приводит к изменению менее 1% интенсивности данной точки. Это теоретически позволяет скрывать в стандартной графической картинке объемом 800 Кбайт около 100 Кбайт информации, что реально не заметно при просмотре изображения.

Стоит упомянуть также и о возможностях сокрытия информации в медиа-файлах. Так, только одна секунда оцифрованного звука с частотой дискретизации 44100 Гц и уровнем отсчета 8 бит в стерео режиме теоретически позволяет сокрыть за счет замены наименее значимых младших разрядов на скрываемое сообщение около 10 Кбайт информации. При этом изменение значений отсчетов составляет менее 1%. Такая девиация, практически, не обнаруживается при прослушивании файла большинством людей. Таким образом, избыточность медиа-файлов открывает широкие возможности для сокрытия информации.

Для внедрения данных в некомпрессированные файлы, использующие битовые матрицы для хранения информации, автором была разработана стеганографическая система. В данном плане характерным примером является использование графического файла bmp-формата и звукового wave-файла PCM-подформата.

Система представляет собой библиотеку, включающую в себя ряд функций:

- шифрование / дешифрование информации;
- анализ возможности внедрения информации в файл;
- внедрение информации в файл;
- извлечение информации из файла.

Данная библиотека разработана в среде Borland Delphi 6 с использованием CLX-совместимости. Таким образом, система является работоспособной как с использованием Windows-архитектуры, так и под управлением Linux (с использованием Borland Kylix).

Одновременно библиотека может использоваться и совместно с другими средствами разработки. Предлагаемая система размещает внутри медиа-файлов битовый массив, поэтому библиотека позволяет скрывать в звуковых файлах не только текст, но и документы, изображения, приложения.

Анализ тенденций развития компьютерной стеганографии указывает на то, что в ближайшие годы интерес к развитию методов компьютерной стеганографии будет усиливаться. А главным стимулирующим фактором выступает развитие глобальной компьютерной сети Internet, порождающей актуальность проблемы информационной безопасности (защита авторского права, защита прав на личную тайну, организация электронной торговли, противоправная деятельность хакеров, террористов и т.п.)