УДК 519.683.8.004.424

Рекиш А.О., Шаталова В.В., Шахно Н.В., Алексеев В.Ф.

ПОСТРОЕНИЕ СТЕГАНОГРАФИЧЕСКОЙ СИСТЕМЫ НА БАЗЕ ПРОТОКОЛА ICMP

УО «Белорусский Государственный Университет Информатики и Радиоэлектроники», Минск

В связи с развитием аппаратных средств вычислительной техники и огромным количеством каналов передачи информации появились новые стеганографические методы, в основе которых лежат особенности представления информации в файлах, вычислительных сетях и т. п. В данной статье рассматриваются возможности стеганографии в Internet Control Message Protocol (ICMP).

Стеганографическая система или стегосистема – совокупность средств и методов, которые используются для формирования скрытого канала передачи информации [1].

Обобщенная модель стеганографической системы представлена на рисунке 1.

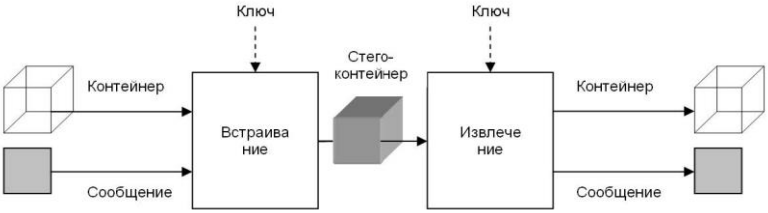

Рисунок 1 – Обобщенная модель стеганографической системы

Контейнер – любая информация, пригодная для сокрытия в ней сообщений.

Стего-контейнер – контейнер, содержащий скрытое сообщение.

Ключ (стего-ключ) – секретный ключ, необходимый для шифрования (расшифровки) сообщения с целью усиления защиты.

При построении стегосистемы следует учитывать следующие положения:

1. Потенциальный противник имеет полное представление о стеганографической системе и деталях ее реализации. Единственной информацией, которая остается неизвестной противнику, является ключ, с помощью которого его владелец может установить факт присутствия скрытого сообщения и его содержание.

2. Свойства контейнера должны быть модифицированы таким образом, чтобы стего-контейнер беспрепятственно проходил по каналу связи, никоим образом не привлекая внимание потенциального противника.

3. Стегосистема должна быть надежной. А именно: предполагать защиту от потери, дублирования и нарушения очередности получения стего-контейнеров, и осуществлять контроль целостности сообщения [2].

Результаты тестирования стегосистемы приведены в таблице 1.

Таблица 1. Тестирование стегосистемы на базе ICMP

Число маршрутизаторов	Длина сообщения (байт)	Интервал2 (сек)	Число дубликатов	Подтверждение получения	Длина поля Data (байт)	Стего-контейнеров		Время отправки (сек)	Отправлено (байт)
						всего	Уникальных		
0	1024		3	да	32	516		4503	30960
6	512			нет			129	4013	
			0..7	да	56	499		4793	41916
				нет		346		2147	29064
			3	да	32	260		2427	15600
		0..60		нет			65	2253	
13	256		0..7	да	56	259		2283	21756
				нет		276		2411	23184
			3	да	32	132	33	1276	7920
				нет				1023	
			0..7	да	56	161		1399	13524
				нет		147		1140	12348

В процессе написания данной статьи была разработана программа, реализующая стегосистему на базе ICMP. Число маршрутизаторов – количество маршрутизаторов, которые прошел стего-контейнер от отправителя к получателю. Интервал2 – задержка между отправкой стего-контейнеров, не являющихся дубликатами. Число маршрутизаторов определялось с помощью программы traceroute.

1. О. В. Генне, “Основные положения стеганографии”. Журнал “Защита информации. Конфидент”, №3, 2000.

2 Брюс Шнайер, Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. – Триумф, 2002 – 816с.

Rekish A.O., Shatalova V.V., Shahno N.V., Alekseev V.F.

CONSTRUCTION OF THE STEGANOGRAPHIC SYSTEM ON THE BASIS OF ICMP PROTOCOL

Belarusian State University Informatics and Radioelectronics, Minsk

Summary

This article carried out the construction of the stegosystem based on the ICMP protocol.