А. Т. Алиев, **С. А. Крассов**, **Г. Н. Шагов** (Ростов-на-Дону, ФГНУ НИИ «Спецвузавтоматика»). **Построение стеганографических систем с симметричными и открытыми ключами на основе криптографических алгоритмов.**

Ввиду широкого повсеместного использования открытых каналов связи для организации взаимодействия между географически удаленными дуг от друга абонентами, весьма важным становится вопрос организации защищенного и по возможности скрытного взаимодействия абонентов. Задача может быть решена с использованием стеганографических методов [1]. Вместе с тем вопрос защищенности подобного взаимодействия в рамках открытых каналов связи на настоящий момент остается открытым. Особый интерес так же представляют перспективы построения защищенных систем на основе открытых ключей. Возможное решение видится в совместном использовании криптографических и стеганографических методов и алгоритмов.

Как показали проведенные исследования и опыт практической разработки, на настоящий момент существует возможность построения стеганографических систем передачи информации с использованием уже отработанных алгоритмов криптографии с симметричными и открытыми ключами. Для их эффективного использования в стеганографических системах требуется четкое согласование входных и выходных данных для криптографической и стеганографической частей системы. Алгоритмы согласования позволяют осуществить перевод равномерно распределенных битовых строк полученных на выходе алгоритмов шифрования, в битовые строки аналогичные извлекаемым стеганографическими алгоритмами из пустых контейнеров. Стеганографическая система, построенная на совместном применении криптографических алгоритмов, методов стеганографии, а также алгоритмов согласования называется криптостеганографической [2]. Для подобных систем доказательство общей стойкости системы может быть основано на доказательстве надежности алгоритмов согласования и определенного уровня практической стойкости стеганографической части.

Применение криптостеганографических систем позволяет закрыть пустующую на настоящий момент нишу систем скрытой связи с доказуемой стойкостью, и при этом позволяет эффективно использовать более простые безключевые стеганографические алгоритмы, а также уже прошедшие процедуру стандартизации алгоритмы шифрования.

СПИСОК ЛИТЕРАТУРЫ

1. *Балакин А. В.*, *Репалов С. А.*, *Шагов Г. Н.* Современная стеганография: модели и методы преобразования информации. Ростов-на-Дону: Изд-во СКНЦ ВШ, 2004, 240 с.
2. *Алиев А. Т.*, *Сергеев Д. В.* Криптостеганографические системы: теоретические основы, принципы построения и перспективы. — Материалы IX Международной научно-практической конференции «Информационная безопасность». Ч. 2. Таганрог: Изд-во ТТИ ЮФУ, 2007, с. 49–54.