КОМПЬЮТЕРНАЯ СТЕГАНОГРАФИЯ — ИННОВАЦИОННЫЙ ИНСТРУМЕНТ ЗАЩИТЫ ИНФОРМАЦИИ

Л. С. Раткин, действительный член Международной академии информатизации, к. т. н.

В статье кратко рассматриваются различные аспекты применения технологии двойного назначения (ТДН) — компьютерной стеганографии (КС) в современных информационных системах и анонсируется авторская концепция КС-форума.

Согласно Указу Президента Российской Федерации от 05.05.2004 № 580 «Об утверждении списка товаров и технологий двойного назначения, которы е могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль» [1] к числу ТДН относятся:

- программное обеспечение (ПО) стеганографических систем, в том числе ПО и математические модели систем, разработанных для обеспечения аутентификации мультимедийной информации, наблюдаемой в условиях шумов, а также для организации канала скрытой передачи данных в речевых и видеосообщениях;
- технологии, связанные со стеганографической защитой информации, позволяющие решать задачи встраивания данных в потоковый контейнер в масштабе реального времени, внедрения в мультимедийную информацию (МИ) невидимых электронных «водяных» знаков (НЭВЗ), не разрушающихся при различных операциях обработки сигналов (сжатие, зашумление, аффинные преобразования, «обрезания краев» и т. п.), и внедрения в МИ НЭВЗ, позволяющих выявить факт вмешательства и его характер.

Что же представляет собой компьютерная стеганография? Чем обусловлено ее применение в двойных технологиях и технологиях двойного назначения? Почему интерес к разработкам в данной области проявляют не только силовые министерства и ведомства разных стран (включая Россию), но и другие организации, в частности финансовые институты?

Слово «стеганография» происходит от греческого «steganos» и «graphy». Первое слово означает «тайна, секрет», второе — «запись». Таким образом, «тайнопись», или «секретная запись» является средством защиты информации, используемой в различных областях.

КС как наука изучает множество стеганографических приемов, реализуемых на вычислительных средствах. (Отметим, что уже давно существуют некомпьютерные стеганографические методы, но в настоящем цикле публикаций они не рассматриваются.)

Принципиальным отличием «секретной записи» от криптографии является форма обработки сообщения (то есть данных, которые необходимо защитить). Если в криптографии в качестве средства защиты информации используется шифрование сообщения, то в «тайнописи» скрывается сам факт его передачи. Достигается это помещением сообщения в стеганографический контейнер (стегоконтейнер). При этом предполагается, что возможные стеганографические методы известны противнику (то есть лицу, заинтересованному во взломе контейнера и получении доступа к тексту сообщения), располагающему базой знаний для проведения стегоанализа контейнеров с целью выявления в них «информационных закладок». Поэтому для повышения устойчивости к взлому рекомендуется проводить специальную процедуру обработки информации (так называемое повышение стегоустойчивости).

Различия методов обработки информации в криптографии и стеганографии становятся еще более очевидными, когда необходимо алгоритмизировать процесс решения задачи по защите данных, написать и отладить соответствующий программный комплекс. Так, в компьютерной криптографии основным инструментом является блок генерации ключа шифрования (например, на основании эвристического анализа значений отдельных его компонентов). В стеганографии же необходимо установить факт сокрытия сообщения, что предполагает настройку и неоднократную перенастройку предметной области на возможные методы сокрытия данных в стегоконтейнерах разных типов по набору определенных признаков. В этом случае задача усложняется, поскольку реконфигурирование предметной области предполагает, в частности, классификацию существующих и прогнозирование возможных (разрабатываемых) стеганографических методов, распознавание ситуаций по степени сложности, а также оптимизацию поиска решения в заданном временном интервале.

Решение стегозадачи по «информационной закладке» с заданным уровнем стегоустойчивости (задача 1) и обратной задачи по проведению стеганоанализа и извлечению стеганографического сообщения с обеспечением его целостности в режиме реального времени (задача 2) неизбежно приводит к привлечению дополнительных вычислительных ресурсов.

Из приведенного описания следует, что стеганография как информационная технология может быть с успехом использована для решения широкого круга задач (например, в военно-промышленном комплексе — для защиты данных о продукции оборонного и двойного назначения на различных стадиях его жизненного цикла и о применяемых при изготовлении изделий двойных технологиях). КС сама является двойной технологией, так как может применяться не только в оборонной, но и в гражданской промышленно-

сти, а также в военной и правительственной связи, для решения задач обеспечения информационной безопасности Минобороны, МВД, ФСО, ФСБ, СВР и других силовых министерств и ведомств России (например, по защите государственной тайны).

Не меньший интерес к КС проявляют финансовые институты, банковские структуры, коммерческие организации. Возможности, представляемые КС, ее преимущества по сравнению с компьютерной криптографией позволяют рассматривать данную информационную технологию как средство защиты коммерческой тайны (например, сведений о результатах проведенных переговоров с потенциальными потребителями продукции или заказчиками работ, содержание протоколов о намерениях, договоров и контрактов на поставку изделий или услуг). Финансовые институты и коммерческие структуры более избирательны в проводимой ими политике информационной безопасности предприятий, поэтому их капиталовложения в разработку новых средств защиты имеют целевой характер, при этом объем инвестиций гораздо больше, чем на государственных предприятиях.

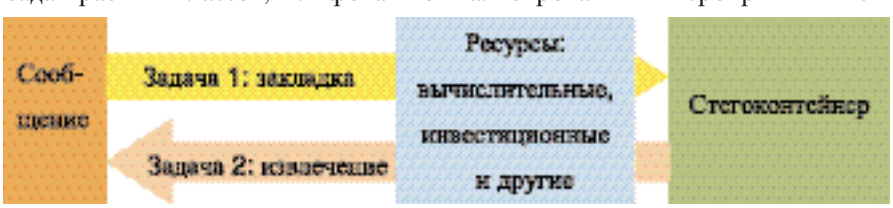
Рассматривая ситуацию со средствами защиты информации (СЗИ), в том числе криптографическими и стеганографическими, можно провести аналогию с разработкой компьютерных вирусов (КВ) и антивирусного программного обеспечения (АПО). Подобно «золотому правилу механики», можно сформулировать «золотое правило защиты информации»: не существует стопроцентной защиты данных, на каждый текущий момент времени разработаны СЗИ (например, АПО), пока не имеющие средств их взлома; взлом СЗИ (в частности, новыми КВ) будет стимулировать создание средств защиты информации нового поколения. Поэтому поединок, противоборство в решении задач 1 и 2 нередко сопровождается финансовыми потоками, инвестированием каждой из сторон, что способствует самостоятельному развитию методов решения задач разных классов, шлифованию отдельных алгоритмов, а также апробированию новых и совершенствованию существующих научных подходов (см. рисунок).

Подробно основные типы задач, решаемые КС, описаны в специализированной литературе [2—5]. Развиваясь параллельно с компьютерными технологиями, в настоящее время на базе математического аппарата КС существуют различные семейства программно-информационных комплексов систем, предназначенные для решения задач по обеспечению защиты данных. Наибольший интерес вызывают:

1. антитеррористические аспекты применения КС;
2. использование КС при проектировании репозиториев в промышленных информационных системах (так называемых стегорепозиториев);
3. криминалистические КС-приложения (например, «стеганографическая дактилоскопия»);
4. охрана служебной и коммерческой информации (в частности, банковских данных) посредством КС;
5. защита документов и авторских прав с помощью специализированных КС-систем.

Отдельного рассмотрения заслуживает **авторская концепция КС-форума**. На наш взгляд, целесообразно проведение конференции или «круглого стола» по вопросам применения стеганографических методов в информационных системах с участием авторов ряда публикаций по тематике КС под эгидой и при поддержке Минобороны, МВД, ФСБ, ФСО, СВР и ряда других силовых министерств и ведомств. В России до сих пор специализированных стеганографических мероприятий не проводилось, но в силу растущей популярности КС такая необходимость давно назрела.

Суть концепции: «Информационный мост», соединяющий теоретические наработки и практическое применение КС-систем, поможет определить основные проблемы и перспективы развития компьютерной стеганографии в России. (Специализированных мероприятий международного уровня по КС также не проводилось, хотя аналогичные зарубежные публикации существуют, что предполагает со временем организацию международного КС-форума.)



Российский КС-форум предпочтительно проводить в Москве. В числе участников и гостей мероприятия целесообразно присутствие представителей силовых министерств и ведомств РФ, высших учебных заведений, печатных изданий (например, «COMPUTERWORLD Россия», «PC WEEK / RE», «Банковские технологии», «Вопросы оборонной техники», «Защита информации. INSIDE», «КомпьюЛог», «Мир ПК», «Открытые системы», «Промышленная политика в Российской Федерации», «Системы безопасности», «Специальная техника»), коммерческих и банковских структур (в том числе при их финансовой поддержке), а также авторов ряда статей.

Предлагаемое автором концепции название **Первого российского КС-форума: «Теория и практика построения КС-систем: проблемы и перспективы развития»**.

Автором статьи предлагается обсудить предлагаемую концепцию и проблематику КС-форума на страницах журнала «Информост». В частности, планируется серия публикаций по вопросам (1–5).

ЛИТЕРАТУРА

Нормативно-правовая система «Консультант плюс», 2005.

Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. — М.: СОЛОН-Пресс, 2002.

Бондаренко С., Двораковская М. Невидимые секреты// Компьютерная газета. — 2002. — 20 сент. — С. 7.

Медведев Н.В., Устименко А.С. Исследование методов сокрытия информации в аудиофайлах RIFF// Научно-техническая конференция «Информационная безопасность — 2002»: Сборник докладов. — М.: МГТУ им. Н.Э. Баумана, «КомпьюЛог», 2002.

Медведев Н.В., Камагин Д.В. Стеганоанализ: возможности применения и их границы (на примере BPCS-стеганографии)// Научно-техническая конференция «Информационная безопасность — 2002»: Сборник докладов. — М.: МГТУ им. Н.Э. Баумана, «КомпьюЛог», 2002.