УДК 621.391

КРИТЕРИИ ЭФФЕКТИВНОСТИ СКРЫТЫХ МЕТОДОВ ПЕРЕДАЧИ

ГОРОХОВ С.М., ЗАХАРЧЕНКО Н.В., КОРЧИНСКИЙ В.В.

Одесская национальная академия связи им. А. С. Попова

CRITERIA OF EFFICIENCY OF HIDDEN COMMUNICATION TECHNIQUES

GOROKHOV S.M., ZAKHARCHENKO N.V., KORCHINSKY V.V.

Odessa national academy of telecommunications n.a. O.S. Popov

Аннотация. *Рассмотрены критерии эффективности скрытых методов передачи с учетом условий функционирования конфиденциальной системы связи (КСС). Показаны пути повышения априорной неопределенности параметров используемых сигналов в КСС с целью увеличения трудоемкости поисковых процедур средств радиоэлектронного противодействия (РЭП) противника. Проведен анализ повышения энергетической скрытности передачи в условиях РЭП. Даны определения критериев эффективности основных показателей скрытностей: энергетической, структурной и информационной.*

Abstract. *The criteria of efficiency of hidden communication techniques with the conditions of functioning of a confidential communication system (CCS) is considered. Ways of increasing a priori uncertainty of the parameters used in the CCS signals in order to increase the complexity of the search procedures electronic countermeasures equipment (ECE) of the enemy is shown. Analysis of improving the energy stealthiest in secrecy transmission ECE is shown. Given the definitions of the main indicators of performance criteria stealth: energy, structural and informational.*

ВВЕДЕНИЕ

Вхождение Украины в мировое информационное сообщество определяется успехом в решении задачи Национальной программы информатизации и создании Национальной сети связи Украины. Однако этот процесс сопровождается такими негативными явлениями, как компьютерные преступления и несанкционированный доступ (НСД) к секретной и конфиденциальной информации, промышленный шпионаж и прочее [1]. Решение данной проблемы относится к задачам информационной безопасности и является важнейшей прерогативой любого государства. В стандартах ISO 7498-2, 10181-1-10181-7 предусматривается комплекс услуг безопасности с помощью различных механизмов защиты информации и, в том числе, реализуемых на основе криптографических систем на верхних уровнях эталонной модели OSI [1]. Анализ тенденции противостояния криптографии и криптоанализа показывает, что какой бы надежной не была бы созданная криптографическая система, ее компрометация по истечении определенного срока эксплуатации очевидна. Учитывая данное обстоятельство, особый интерес приобретают методы защиты информации, которые реализуются на первом и втором уровнях эталонной модели OSI [2-5]. Особенно это важно при обеспечении безопасности беспроводных сетей (например, для стандарта Radio Ethernet, SM, GPRS, DPRS, CDMA и других радиосетей), так как на уровне физического канала она наиболее уязвима для перехвата передаваемых сообщений средствами НСД [3]. Одним из путей решения этой проблемы является использование в КСС радиоэлектронной маскировки (РЭМ), которая представляет собой комплекс технических и организованных мероприятий, направленных на снижение эффективности средств радиотехнической (РР) и радиолокационной разведки. РЭМ может быть решена за счет методов передачи, обеспечивающих энергетическую, структурную, информационную и другие виды скрытности сигнальных конструкций [3,4].

Методам повышения скрытности передачи посвящено достаточно много работ [2-4], однако в литературе недостаточно уделено внимание вопросам выбора критериев эффективности скрытых методов передачи, учитывающих условия функционирования КСС и работу систем РЭП. Поэтому, целью работы является разработка рекомендаций по выбору критериев эффективности скрытых методов передачи с учетом условий функционирования КСС.

КРИТЕРИИ ЭФФЕКТИВНОСТИ И МЕТОДЫ ОБЕСПЕЧЕНИЯ СКРЫТНОСТИ СИГНАЛЬНЫХ КОНСТРУКЦИЙ

Конфликтное информационное взаимодействие характеризуется противоположными интересами противоборствующих сторон, что приводит к увеличению уровня априорной неопределенности относительно параметров и характеристик используемых сигналов. Как правило, это связано с тем, что одним из участников взаимодействия предпринимаются специальные меры по сокрытию или искажению информации, направленные на усложнение работы противоборствующей стороны.

С учетом выполняемых своих задач радиотехнические системы можно классифицировать на три основных класса [3]:

1) радиотехнические системы передачи и управления – относятся к классу КСС, предназначенных для передачи и данных, и сигналов управления;

2) системы разрушения информации – относятся к системам РЭП, целью которых является постановка преднамеренных помех, имитации ложных информационных сигналов и перехвата управления;

3) системы извлечения информации – относятся к классу систем НСД и решают задачи по несанкционированному перехвату передаваемых сообщений, определению структуры и параметров сигналов, дешифрированию криптотекстов и т.д.

Для оценки степени защищённости КСС от систем РЭП противника и НСД целесообразно использовать понятие помехозащищённость.

Помехозащищённость – это свойство системы не только наиболее точно воспроизводить передаваемую информацию на приемной стороне, но и способность обеспечивать её безопасность и целостность от средств РЭП и НСД с помощью реализации эффективных методов скрытности передачи.

Показатели скрытности характеризуют различные возможности системы по маскировке передаваемого сигнала по различным его параметрам. В связи с этим различают энергетическую, структурную, информационную и другие показатели скрытности. Не менее важным показателем помехозащищённости является помехоустойчивость, которая определяет способность системы противостоять вредному воздействию помех естественного и искусственного происхождений.

Мерой маскировки работы КСС обосновано использовать некоторую вероятностную характеристику, которая должна учитывать основные показатели качества скрытности передачи (энергетической, структурной, информационной и др.). Такой характеристикой может быть вероятность доступности средств радиоразведки к передаваемой информации КСС [3]:

$$P_{\text{р}} = P_{\text{эн}} P_{\text{стр}} P_{\text{инф}}, \qquad (1)$$

где $P_{\text{р}}$ – условная вероятность успешного решения разведкой своих задач при условии, что сигнал может быть принят, $P_{\text{эн}}$ – условная вероятность обнаружения сеанса передачи КСС, т.е. передаваемый сигнал демаскирован за счёт решения РР проблемы энергетической скрытности; $P_{\text{стр}}$ – условная вероятность распознавания структуры сигнала, т.е. решена проблема защиты сигнальной конструкции за счет структурной скрытности при условии, что сигнал был перехвачен; $P_{\text{инф}}$ – условная вероятность распознавания (дешифрирования) смыслового содержания перехваченного сигнала при условии, что структура сигнала была раскрыта.

Таким образом, распознавание смыслового содержания перехваченного сообщения при НСД возможно при успешных событиях обнаружения, приема и распознавании структуры сигнальной конструкции. Для оценки качества обнаружения сигнала используется вероятность его обнаружения при его приеме средством радиоразведки $P_{\text{обн}}$, которая определяет условную вероятность правильного решения о наличии сигнала на входе приемника при условии, что этот сигнал действительно есть. Такой показатель отождествляется с характеристикой энергетической скрытности, т.е. $P_{\text{эн}} = P_{\text{обн}}$. Очевидно, что для повышения энергетической скрытности передачи сигнала целесообразно снижать мощность основного излучения КСС, что возможно при использовании широкополосных сигналов с базой $B = \Delta f \cdot T >> 1.$ Расширение базы сигнала позволяет создавать сигнальные

конструкции с очень малой спектральной плотностью мощности, что затрудняет их обнаружение при некогерентной обработке в приемнике средствами РР. Кроме этого, используя несущие сигналы с неизвестной структурой можно увеличить априорную неопределённость приёма при несанкционированном доступе РР.

Общая основная проблема, которая связана с построением систем связи находится в противоречии между необходимостью, с одной стороны, передавать с предельной скоростью как можно больше информации, а, с другой стороны, обеспечить при этом высокую достоверность её приема. Для КСС не менее важным также является обеспечение энергетической скрытности передачи.

Теорема. Можно обеспечить сколь угодно высокую энергетическую скрытность передачи информации при условии, что база сигнала $B \to \infty$.

Доказательство. Рассмотрим формулу К. Шеннона о пропускной способности канала:

$$C = \Delta F \log_2\left(1 + \frac{P_{\text{с}}}{P_{\text{ш}}}\right), \tag{2}$$

где ΔF – полоса частот, отводимая для передачи информации; $P_{\text{с}}$ и $P_{\text{ш}}$ – мощности сигнала и шума, соответственно. Из формулы Шеннона следует, что теоретически информацию по каналу можно передавать с любой скоростью, не превышающей C и с любой заданной достоверностью. Доказательство теоремы проведем с точки зрения теории кодирования и теоремы кодирования. Пусть для повышения помехоустойчивости в качестве расширяющей последовательности используется помехоустойчивый код (n, k), где n – общая длина кода, k – количество информационных элементов. Тогда $n - k = r$ определит количество избыточных бит кода, которые можно использовать для обнаружения или исправления ошибок. При этом предполагается, что введение дополнительных проверочных символов r осуществляется за счет уменьшения длительности элементарной посылки t_0, т.е.

$$t_0 < t_0^*,$$

где t_0 – длительность элементарной посылки до кодирования; t_0^* – длительность элементарной посылки после помехоустойчивого кодирования. Такое уменьшение длительности импульса равносильно уменьшению его энергии. Тогда длительность элементарной посылки

$$t_0^* = \frac{k}{n} t_0 = \gamma_{\text{к}} t_0,$$

где $\gamma_{\text{к}} = k/n$ – кодовая скорость помехоустойчивого кода. Скорость передачи информации при этом падает в n/k раз, а достоверность приема увеличивается при условии, что полоса пропускания канала ΔF не ограничена. Таким образом, уменьшая скорость передачи за счет увеличения избыточности кодирования теоретически можно получить сколь угодно высокую достоверность передачи информации. Запишем соотношение формулы Шеннона (2) в следующем виде:

$$\frac{1}{\log_2\left(1 + \frac{P_{\text{с}}}{P_{\text{ш}}}\right)} = \Delta F T. \tag{3}$$

Левую часть равенства (3) возьмём под знак предела при условии, что $S/N \to 0$, тогда

$$\lim_{\frac{P_{\text{с}}}{P_{\text{ш}}} \to 0} \frac{1}{\log_2\left(1 + \frac{P_{\text{с}}}{P_{\text{ш}}}\right)} \to \infty. \tag{4}$$

При $P_{\text{с}}/P_{\text{ш}} \to 0$ знаменатель (3) стремится к нулю, поэтому левая часть равенства стремится к бесконечности (4), а это равносильно увеличению базы сигнала $B = \Delta F T >> 1$, что и следовало

доказать. Из этого доказательства следует, что применение сигналов с большой базой позволяет обеспечить теоретически не только любую достоверность передачи информации, но и высокую энергетическую скрытность сигнальных конструкций. Таким образом, система связи со сложными широкополосными сигналами способна работать при соотношении $P_с/P_ш<1$, то есть $P_с<<P_ш$. Это свойство обеспечивает, с одной стороны, скрытность работы передатчика конфиденциальной системы, а с другой – возможность кодового разделения каналов.

Определим критерии эффективности обеспечения скрытности передачи в канале.

Определение 1. Критерием эффективности методов скрытности передачи является достижение максимума для средств радиотехнической разведки уровня априорной неопределенности используемых параметров сигналов с криптозащищенной структурой при маскировке данных конфиденциальных сообщений в канале связи.

Определение 2. Критерием эффективности энергетической скрытности передачи является достижение минимально возможного значения соотношения сигнал/шум, при котором достигается максимальный эффект при маскировке энергии сигнальной конструкции на фоне шумов в канале при условии, что при этом обеспечивается требуемая достоверность приема конфиденциальной информации.

Определение 3. Критерием эффективности структурной скрытности передачи является достижение максимального значения показателя двоичного логарифма от числа сигнальных конструкций, которые используются для переноса данных конфиденциального сообщения в канале.

Определение 4. Критерием эффективности информационной скрытности является минимум вероятности раскрытия смыслового содержания перехваченного сообщения, заложенного в сигнальных конструкциях с известной структурой.

ВЫВОДЫ

В процессе радиоэлектронного конфликта, с одной стороны, выступает КСС, а с другой – система РЭП противника. В задачу РЭП входит обнаружение сигнала, создание преднамеренных помех или несанкционированный доступ к информации. В таких условиях работы КСС должна принимать меры, которые способствуют выполнению ею своих задач за счет алгоритмического и сигнального ресурса. При реализации методов скрытности в условиях радиоэлектронного противодействия необходимо учитывать требования к помехоустойчивости канала связи.

ЛИТЕРАТУРА

1 Шаньгин А.И. Информационная безопасность компьютерных систем и сетей / Шаньгин А.И.. – М.: ИД «Форум»: ИФРА-М, 2008. – 416 с.

2 Куприянов А.И. Теоретические основы радиоэлектронной борьбы / А. И. Куприянов, А. В. Сахаров. – М.: Вузовская книга, 2007. – 356 с.

3 Помехозащищенность систем радиосвязи с расширением спектра сигналов модуляцией несущей псевдослучайной последовательностью [Борисов В. И., Зинчук В. М., Лимарев А. Е. и др.]; под ред. В. И. Борисова. – М.: Радио и связь, 2003. – 640 с.

4 Захарченко Н. В. Многопользовательский доступ в системах передачи с хаотическими сигналами / Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Восточно-Европейский журнал передовых технологий. – 2011. – № 5/9(53). – С. 26–29.

5 Захарченко Н. В. Скрытность передачи в системах связи с хаотическими сигналами / Н. В Захарченко, С. М. Горохов, В. В. Корчинский, Б. К. Радзимовский // Міжнародний науково-технічний журнал “Вимірювальна та обчислювальна техніка в технологічних процесах”. – 2013. – № 3. – С. 161–164.