Nagornaya Marina Your'evna, PhD in Technology Science, Associated Professor of Department of Radio Communication, Broadcasting and Television, Povolzhskiy State University of Telecommunications and Informatics, Samara, Russian Federation. Tel. +7 846 339 11 06. E-mail: nm@psati.ru
Galochkin Vladimir Andreevich, PhD in Technology Science, Associated Professor of Department of Radio Communication, Broadcasting and Television, Povolzhskiy State University of Telecommunications and Informatics, Samara, Russian Federation. Tel. +7 846 926 32 83. E-mail: galochkin.vladimir@yandex.ru

References

1. Dzhakoniya V.E. *Televidenie* (Television). Moscow, Radio i Svyaz' Publ., 2004, 615 p.
2. Krivocheev M.I., Fedunin V.G. *Interaktivnoe TV* (Interactive TV). Moscow, Radio i Svyaz' Publ., 2000, 342 p.
3. Lokshin B.A. *Cifrovoe veshchanie: ot studii k telezritelyu* (Digital broadcasting: from studios to the viewer). Moscow, Kompaniya Sajrus-sistems Publ., 2001, 446 p.
4. Zubarev YU.B., Krivosheev M.I., Krasnosel'skij I.N., *Cifrovoe televizionnoe veshchanie* (Digital television broadcasting). Moscow, NIIR Publ., 2001, 550 p.
5. Sanjay Paul. *Digital Video Distribution in Broadband, Television, Mobile and Converged Networks*: *Trends, Challenges and Solutions*. Wiley, 2010, 384 p. (Russ ed.: Sehndzhoj P. Raspredelenie cifrovogo video po shirokopolosnym TV mobil'nym i konvergentnym setyam. Tendencii, problemy, resheniya. Moscow, Tekhno-sfera Publ., 2012, 440 p.)
6. Tyuhtin M.F. *Sistemy Internet-televideniya* [Internet television system]. Moscow, Goryachaya liniya – Telekom Publ. 2008, 320 p.

Received 17.12.2014

ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ И БЕЗОПАСНОСТЬ ОБОРУДОВАНИЯ

УДК 003.26

УСТОЙЧИВЫЕ К АТАКАМ НА КОНТЕЙНЕР СТЕГАНОГРАФИЧЕСКИЕ АЛГОРИТМЫ

Смагин А.А.[1], Валишин М.Ф.[2]
[1] Ульяновский государственный университет, Ульяновск, РФ
[2] ОАО «ГНЦ НИИАР», Димитровград, РФ
E-mail: smaginaa1@mail.ru

В статье рассматривается задача построения стеганографических алгоритмов, способных организовывать скрытый канал передачи данных в условиях проведения целенаправленной атаки на контейнер. Разработаны теоретические методы на основе редукции множества контейнеров и оценки вносимого в результате атаки искажения. Приведена практическая реализация стеганографического алгоритма, устойчивого к операции преобразования цветного изображения в оттенки серого и JPEG компрессии.

Ключевые слова: стеганография, стегоанализ, активная атака, робастность, стеганографический алгоритм, цифровая обработка изображений, JPEG компрессия.

Введение

Стеганография – наука о скрытой передаче данных путем сохранения в тайне самого факта передачи данных. Современная стеганография имеет дело с цифровыми объектами, в основном изображениями, аудио- и видеоданными. Основным критерием стеганографических систем является устойчивость к обнаружению. Изначально рассматривалась устойчивость к визуальному обнаружению, однако по мере развития методов стеганографии появился особый раздел стеганографии: стегоанализ, наука о выявлении факта передачи скрытой информации. В настоящее время рассматривается устойчивость стеганографических алгоритмов к статистическим тестам, методам классификации и т.д.

Стеганография позволяет решать ряд прикладных задач, не связанных с «задачей заключенных» [1]. Чаще всего сокрытие дополнительной информации позволяет расширить функционал

формата данных. Для решения прикладных задач критерий устойчивости к обнаружению не является приоритетным, так как наличие внедренных в цифровой объект данных не скрывается. Таким образом, одним из главных требований к прикладной стеганосистеме — это обеспечение устойчивости к случайным или умышленным атакам [2].

Постановка задачи

Этапы трансформации цифрового объекта могут быть представлены в виде диаграммы (см. рис. 1). Состояния нумеруются, причем нулевым состоянием будет объект до внедрения, первым – после него. Переход между двумя состояниями характеризует искажение, вносимое в исходный объект. Если искажение порождает множество различных объектов, соответствующее состояние на диаграмме помечается знаком бесконечности, символизирующим отношение «один ко многим».

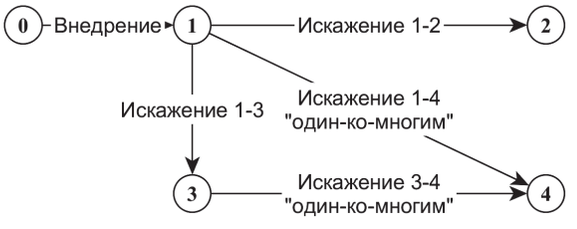

Рис. 1. Диаграмма этапов трансформации цифрового объекта

Для решения прикладных задач необходима стеганографическая система, способная извлекать скрытую информацию из всех ненулевых состояний цифрового объекта. В процессе редактирования цифровых фотографий, например, могут быть применены различные приемы: цветокоррекция, ретушь, аффинные преобразования, фильтры, сжатие с потерями и т.д. Функцией извлечения будем называть любое отображение множества контейнеров K во множество кодовых символов S:

$$F_{inp}(k) = s\,. \tag{1}$$

Для цифровых изображений контейнером может быть цвет отдельного пикселя в формате RGB, то есть тройка неотрицательных целых чисел в диапазоне [0 … 255]. Функция извлечения может иметь следующий вид:

$$F_{lsb}(r,g,b) = LSB(b)\,, \tag{2}$$

где $LSB(b)$ – функция извлечения младшего бита.

Отдельный символ стеганограммы может быть передан с помощью различных контейнеров. Для выбора вводится дополнительный критерий – условие минимизации вносимого в исходный контейнер искажения. Мерой искажения можно считать расстояние между парой контейнеров $p(k_1, k_2)$.

Таким образом, стеганографический алгоритм имеет вид:

$$\begin{aligned} &G_{out}(k_{inp}, s, p) = k_{out};\\ &F_{inp}(k_{out}) = s;\\ &p(k_{inp}, k_{out}) \to \min, \end{aligned} \tag{3}$$

где k_{inp}; k_{out} – входной и выходной контейнеры; s – внедряемый символ кодового алфавита. Для растровых изображений в качестве расстояния между контейнерами (цветами) целесообразно использовать следующую формулу:

$$p(k_1, k_2) = \sum_{i=0}^{7} 2^i (k_1^i \; xor \; k_2^i)\,, \tag{4}$$

где k^i – это *i*-ый бит. Функции извлечения и внедрения вместе с правилом построения последовательности контейнеров из цифрового объекта образуют стеганографический алгоритм.

Атакой на цифровой объект будем называть преобразование вида

$$A(k) = k^*. \tag{5}$$

Стеганографический алгоритм устойчив к атаке на контейнер, если выполняется условие:

$$F_{inp}(k) = F_{inp}(A(k))\,. \tag{6}$$

Метод редукции множества контейнеров

Пусть дан стеганографический алгоритм, такой, что для некоторого $K^* \subset K$ выполняется (6). Тогда, выбирая для внедрения контейнер из подмножества K^*, получается устойчивый к атаке стеганографический алгоритм:

$$\begin{aligned} &G_{out}(k_{inp}, s, p) = k_{out};\\ &F_{inp}(k_{out}) = s;\\ &p(k_{inp}, k_{out}) \to \min, \end{aligned} \tag{7}$$

где $k_{inp} \in K, k_{out} \in K^*$.

Метод оценки искажения

Пусть дан стеганографический алгоритм над двоичным алфавитом, такой, что для некоторого l выполняется условие:

$$p(k, A(k)) < l\,, \tag{8}$$

где $p(k_1,k_2)$ – расстояние между парой контейнеров, такое, что (K,p) образует метрическое пространство. Введем функции извлечения и внедрения в следующем виде:

$$F^*_{inp}(k)=\left\lfloor\frac{p(k_{inp},k_0)}{2l}\right\rfloor \bmod 2, \tag{9}$$

$$G^*_{out}(k_{inp},s,p)=k_{out} \Leftrightarrow$$
$$\Leftrightarrow p(k_{out},k_0)=2l\times\left(\left\lfloor\frac{p(k_{inp},k_0)}{2l}\right\rfloor+\right.$$
$$\left.+s \text{ xor}\left(\left\lfloor\frac{p(k_{inp},k_0)}{2l}\right\rfloor \bmod 2\right)\right)+l, \tag{10}$$

где k_0 – произвольный фиксированный контейнер.

Покажем, что функции $F^*_{inp}(k)$, $G^*_{out}(k_{inp},s,p)$ вместе с правилом построения последовательности контейнеров из цифрового объекта образуют устойчивый к атаке A стеганографический алгоритм.

Доказательство. Так как (K,p) – метрическое пространство, то выполняется обратное неравенство треугольника:

$$\left|p(k_{out},k_0)-p(A(k_{out}),k_0\right|<p(k_{out},k_0)<l \Rightarrow$$
$$p(k_{out},k_0)-l<p(A(k_{out}),k_0)<p(k_{out},k_0)+l. \tag{11}$$

Введем обозначение:

$$t=\left\lfloor\frac{p(k_{inp},k_0)}{2l}\right\rfloor+s \text{ xor }\left(\left\lfloor\frac{p(k_{inp},k_0)}{2l}\right\rfloor \bmod 2\right). \tag{12}$$

Подставляя (10) и (12) в (11), имеем:

$$2l\times t<p(A(k_{out}),k_0)<2l\times(t+1) \Rightarrow$$
$$t\le\left\lfloor\frac{p(A(k_{out}),k_0)}{2l}\right\rfloor<t+1. \tag{13}$$

Последнее означает, что

$$\left\lfloor\frac{p(A(k_{out}),k_0)}{2l}\right\rfloor=t, \tag{14}$$

то есть выполняется условие (6):

$$F^*_{inp}(k_{out})=\left\lfloor\frac{2l\times t+l}{2l}\right\rfloor \bmod 2=t \bmod 2=$$
$$=\left\lfloor\frac{p(k_{out},k_0)}{2l}\right\rfloor \bmod 2=F^*_{inp}(A(k_{out})). \tag{15}$$

Осталось показать, что, применяя функцию извлечения (9) к выходному контейнеру, мы получаем требуемый символ стеганограммы $F^*_{inp}(k_{out})=s$:

$$F^*_{inp}(k_{out})=t \bmod 2=\left(\left\lfloor\frac{p(k_{out},k_0)}{2l}\right\rfloor+\right.$$
$$+s \text{ xor }\left(\left\lfloor\frac{p(k_{out},k_0)}{2l}\right\rfloor \bmod 2\right) \bmod 2=$$
$$=\left(\left\lfloor\frac{p(k_{out},k_0)}{2l}\right\rfloor \bmod 2\right) \text{ xor } s \text{ xor }=$$
$$=\left(\left\lfloor\frac{p(k_{out},k_0)}{2l}\right\rfloor \bmod 2\right)=s. \tag{16}$$

Для предложенной схемы построения стеганографического алгоритма оценка вносимого искажения имеет вид:

$$p(k_{inp},k_{out})\le 3l. \tag{17}$$

Алгоритм может быть улучшен за счет небольшого изменения в функцию внедрения. Пусть такие, что:

$$p(k_{1,2},k_0)=2l\times\left(\left\lfloor\frac{p(k_{inp},k_0)}{2l}\right\rfloor\pm\right.$$
$$\left.\pm s \text{ xor}\left(\left\lfloor\frac{p(k_{inp},k_0)}{2l}\right\rfloor \bmod 2\right)\right)+l. \tag{18}$$

Тогда выходной контейнер выбирается следующим образом:

$$k_{out}=k_i\left|p(k_i,k_{inp})\to\min,i=1,2.\right. \tag{19}$$

Оценка искажения для данной схемы имеет вид:

$$p(k_{inp},k_{out})\le\frac{3}{2}l. \tag{20}$$

Практическое применение

Рассмотрим представленные методы на практических примерах.

Построим устойчивый к преобразованию цветного изображения в градации серого стеганографический алгоритм. Градации серого – цветовой режим изображений, которые отображаются в оттенках серого цвета, размещенные в виде таблицы в качестве эталонов яркости цвета. Широко применяется в цветоведении и колористике, для оценки и измерений качества тонопередачи при фотографической съемке, сканирова-

нии, при копировальных и печатных процессах. В компьютерном представлении распространена серая шкала, которая использует на каждый пиксель изображения один байт информации. Таким образом, шкала передает 256 градаций серого цвета, или яркости. Для преобразования цветного изображения в режим градаций серого вычисляется яркость каждого пикселя. Яркость рассчитывается в виде взвешенной суммы красной, зеленой и голубой компонент исходного цвета. Согласно спецификации Rec. 709 (стандарт телевидения высокой четкости) формула имеет вид:

$$Y(r,g,b) = 0{,}2126 \times r + \\ + 0{,}7152 \times g + 0{,}0722 \times b. \quad (21)$$

Диаграмма состояний изображения для данной задачи представлена на рис. 2.

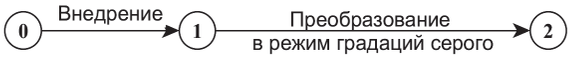

Рис. 2. Трансформации цифрового изображения для задачи построения устойчивого к преобразованию в оттенки серого стеганографического алгоритма

Таким образом, задача сводится к построению стеганографического алгоритма, способного извлекать сообщение из цветного изображения и после его преобразования в градации серого.

Пусть в качестве функции извлечения используется метод наименьших бит (2). Оценим воздействие преобразования на младший бит изображения. Сравним последовательности кодовых символов, полученные из оригинального изображения и преобразованного, и вычислим количество инвертированных битов. На серии из цифровых фотографий высокого разрешения (4912×3264 пикселей) было получено, что в результате приведения по формуле (21) исходного изображения в режим градаций серого изменяется ~48,9% битов. Последнее означает, что использование известных стеганографических алгоритмов, основанных на LSB методе, невозможно.

В то же время значительное число контейнеров сохраняет младший бит после преобразования. Это означает, что устойчивую стеганографическую систему можно построить с помощью метода редукции множества контейнеров (7).

Стеганографический алгоритм реализован на языке программирования Python 2.7 с использованием библиотеки PIL (версия 1.1.7):

```
def extract(img):
    code = []
    if img.mode == "L":
        B = img
    else:
        R, G, B = img.split()
    rnd.seed(seed)
    data = B.getdata()
    keys = range(len(data))
    rnd.shuffle(keys)
    for k in keys:
        code.append(data[k] & 0b0000001)
    message = []
    for i in range(len(code) / 7):
        m = ""
        for b in range(7):
            m += str(code[b+7*i])
        message.append(m)
    message = map((lambda s: int(s, 2)), \
            message)
    message = message[:message.index(0)]
    message = "".join(map(chr, message))
    return message

def embed(img, text):
    message = map(ord, list(text))
    message.append(0)
    code = []
    for m in message:
        for c in map(int, \
            list("{0:07b}".format(m))):
            code.append(c)
    data = list(img.getdata())
    rnd.seed(seed)
    keys = range(len(data))
    rnd.shuffle(keys)
    for key, c in enumerate(code):
        r, g, b = data[keys[key]]
        b = (b & 0b11111110) + c
        r0, g0, b0 = r, g, b
        count = 0
        while (int(round(0.2126*r+\
                0.7152*g+0.0722*b+ \
                1e-5)) & 1) != c:
            k = (-1) ** (count % 2) * \
                (count / 2)
            r = max(0, min( r0+ \
                int(0.2126*k+1e-5), 255))
            g = max(0, min(g0+ \
                int(0.7152*k+1e-5), 255))
            b = max(0, min(b0+ \
                2*int(0.0361*k+1e-5), 255))
            count += 1
        data[keys[key]] = (r, g, b)
    out = Image.new(img.mode, img.size)
    out.putdata(data)
    return out
```

Последовательность контейнеров в реализации стеганографического алгоритма перемешивается псевдослучайным образом на основании ключа, что позволяет распределить кодовую последовательность по всему изображению. Алгоритм внедряет текстовое сообщение в кодировке ASCII, урезанной до 7 бит.

Самым распространенным графическим на сегодняшний день форматом является JPEG. Сохранение в формат JPEG вносит искажение в исходное изображение ввиду дискретного преобразования Фурье и последующего сжатия. При этом сложность и нетривиальность алгоритма не позволяет математически построить модель вносимого искажения. Более того, одинаковые контейнеры могут быть искажены по-разному в зависимости от смежных с ними пикселей.

Рассмотрим этапы трансформаций цифрового изображения, которое, помимо преобразования в режим градаций серого, может быть сохранено в формат JPEG (см. рис. 3).

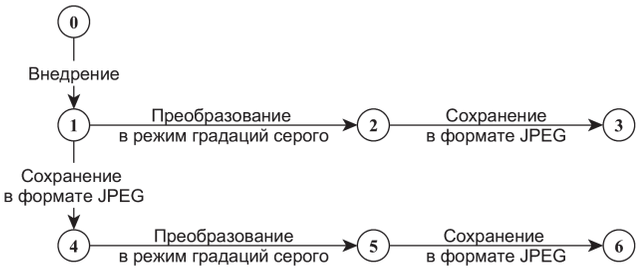

Рис.3. Трансформации цифрового изображения для задачи построения устойчивого к преобразованию в оттенки серого стеганографического алгоритма и JPEG-компрессии

Для данной диаграммы существует шесть возможных модификаций изображения со скрытой информацией. Кроме того, формат JPEG позволяет устанавливать качество сжатия. Будем полагать, что данный параметр не ниже 95%.

При сохранении в JPEG исходное растровое изображение из формата RGB преобразуется в формат YcbCr. Яркость пикселя (Y) сохраняется с наименьшими потерями. Последнее означает, что если ввести соответствующую метрику над множеством контейнером, то вносимое искажение будет удовлетворять неравенству (2) для некоторого значения l. В качестве метрики предложена следующая формула:

$$p(k_1,k_2)=\left|Y(r_1,g_1,b_1)-Y(r_2,g_2,b_2)\right|.$$

Так как по изложенным выше причинам оценить вносимое искажение теоретически затруднительно, была проведена серия расчетов, при которых попиксельно сравнивалось расхождение яркости растрового изображения в формате BMP и сжатого в формат JPEG с качеством 95%.

Средняя величина разброса, равно как и максимальное значение, варьируется для разных исходных изображений, но в основном не превосходит четырех единиц, то есть $p(k_1,k_2)<4$. Это означает, что устойчивую стеганографическую систему можно построить с помощью метода оценки искажения (9)-(10).

Стеганографический алгоритм реализован на языке программирования Python 2.7, библиотека PIL (версии 1.1.7). Код представлен в листинге 2. Последовательность контейнеров, как и в первом алгоритме, перемешивается псевдослучайным образом.

```
ALPHA = 2 * l
def extract(img):
        code = []
        if img.mode == "L":
                B = img
        else:
                B = img.convert("L", (0.2126, \
            0.7152,0.0722,0))
        rnd.seed(seed)
        data = B.getdata()
        keys = range(len(data))
        rnd.shuffle(keys)
        for k in keys:
                code.append((data[k] / \
                  ALPHA) % 2)
        message = []
        for i in range(len(code) / 7):
                m = ""
                for b in range(7):
                        m += str(code[b+7*i])
                message.append(m)
        message = map((lambda s: int(s, 2)),\
                message)
        message = message[:message.index(0)]
        message = "".join(map(chr, message))

        return message

def gray(r,g,b):
        return int(round(0.2126 * r + \
         0.7152 * g + 0.0722 * b + 1e-5))

def embed(img, text):
        message = map(ord, list(text))
        message.append(0)
        code = []
for m in message:
                for c in map(int, \
          list("{0:07b}".format(m))):
                        code.append(c)
        data = list(img.getdata())
        rnd.seed(seed)
        keys = range(len(data))
        rnd.shuffle(keys)
        for key, c in enumerate(code):
                r, g, b = data[keys[key]]
                gr = gray(r,g,b)
                div = gr / ALPHA
                if (div % 2 != c):
                        div += 1
                if div >= (255/ALPHA):
                        div -= 2
                new_g = div * ALPHA + ALPHA / 2
                r0, g0, b0 = r, g, b
                count = 0
```

```
            while gray(r,g,b) != new_g:
                    k = (-1) ** (count % 2) *\
                (count / 2)
                    r = max(0, min(r0+\
            int(0.2126*k+1e-5), 255))
                    g = max(0, min(g0+\
            int(0.7152*k+1e-5), 255))
                    b = max(0, min(b0+\
        2*int(0.0361*k+1e-5), 255))
                    count += 1
                data[keys[key]] = (r, g, b)
    out = Image.new(img.mode, img.size)
    out.putdata(data)
    return out
```

Заключение

В данной статье представлен способ отображения этапов трансформации цифрового объекта с помощью диаграмм. Сформулированы определения для стеганографической системы, меры искажения, функций извлечения и внедрения. Рассмотрены два метода построения устойчивых стеганографических алгоритмов – метод редукции множества контейнеров и метод оценки искажения. Предложенные в статье методы построения стеганографических систем опробованы на практике. Разработаны две стеганографические системы, устойчивые к преобразованию цветного изображения в режим градаций серого. Для второй системы добавлена устойчивость к JPEG-компрессии.

Литература

1. Gustavus J. Simmons. The Prisoner's Problem and the Subliminal Channel, Advances in Cryptology: Proceedings of Workshop on Communications Security (Crypto'83, David Chaum, ed.). Plenum Press. 1984. – P. 51-67.
2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006. – 288 с.

Получено 20.11.2014

Смагин Алексей Аркадьевич, д.т.н., профессор, заведующий Кафедрой телекоммуникационных технологий и сетей Ульяновского государственного университета. E-mail: smaginaa1@mail.ru

Валишин Марат Фаритович, м.н.с. физико-технической лаборатории ОАО «ГНЦ НИИАР» (г. Димитровград). E-mail: valmar.ktn@gmail.com

STEGANOGRAPHY ALGORITHMS ROBUST TO ACTIVE ATTACS

Smagin A.A., Valishin M.F.

The aim of this work is to develop a steganographic algorithm, which is able to organize covert channel data in terms of a targeted attack on a container. Robust against an active attack on a steganographic algorithms is used to solve a number of applied problems. For example, the task of adding a new functionality to a fixed format. It is proposed to use the state diagram to describe the possible transformations of a digital object as a result of the attacks. The transition between the two states is characterized by the distortion introduced in the original object, and if the distortion produces a number of different objects, the corresponding state in the diagram is marked with infinity symbolizes sign which the attitude of «one-to-many». Thus, the problem of constructing robust against an active attack steganography is reduced to obtaining an algorithm that is able to extract hidden information from all the states in the diagram. There are two theoretical methods of construction robust against an active attack steganography: method of reducing a plurality of containers and method of assessing distortion. The first method is based on the assumption that among a plurality of containers. There can be such containers that the attack does not destroy embedded information. The second method allows you to build a robust embedding algorithm if the distortion introduced by the attack is limited by modulo in a metric space of containers. This paper gives a practical application of the proposed methods for the construction of steganography system that is robust against conversion of color images to grayscale. The program implementation in the programming language Python is given.

Keywords: *steganography, steganalysis, active attacks, robust, steganographic algorithm, digital image processing, jpeg compression.*

Smagin Aleksei Arkadievich, Doctor of Technical Science, Professor, Head of Department of Telecommunication Technologies and Networks, Ulyanovsk State University, Ulyanovsk, Russian Federation. E-mail: smaginaa1@mail.ru

Valishin Marat Faritovich, Junior Research Fellow of Physico-Technical Laboratory, State Scientific Center-Research Institute of Atomic Reactors, Dimitrovgrad, Russian Federation. E-mail: valmar.ktn@gmail.com

References

1. Gustavus J. Simmons. *The prisoner's problem and the subliminal channel, advances in cryptology*: *proceedings of workshop on communications security* (Crypto'83, David Chaum, ed.), Plenum Press, 1984, pp. 51-67.

2. Konakhovich G.F., Puzyrenko A.Yu*Kompyuternaya steganografi ya. Teoriya i praktika* [Computer stenography. Theory and practice]. MK-Press, 2006, 288 p.

Received 20.11.2014

УДК 621.397

ОБЕСПЕЧЕНИЕ ПОМЕХОЗАЩИЩЕННОСТИ БЕСПРОВОДНЫХ УСТРОЙСТВ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Аббасова Т.С.
Финансово-технологическая академия, Королев, Московская обл., РФ
E-mail: abbasova_univer@mail.ru

Проанализированы проблемы процессов измерений, анализа и диагностики при создании эффективной системы эксплуатации, контроля и обеспечения качества телекоммуникационных систем, включающих локальные радиосети передачи данных и беспроводные устройства; осуществлена оценка электромагнитной совместимости для беспроводных устройств малого радиуса действия при тестировании оборудования для поддержки инфокоммуникационных технологий.

Ключевые слова: локальные радиосети, беспроводные устройства, электромагнитная совместимость.

Введение

На современном этапе развития инфокоммуникационных систем на базе телекоммуникационных каналов связи широко применяется их интеграция с локальными радиосетями передачи данных с использованием беспроводных устройств для тестирования и радиочастотной идентификации портов оборудования как проводных, так и беспроводных сетей. Постоянное увеличение плотности размещения портов и радиоэлектронных средств (РЭС) беспроводных сетей и средств для тестирования оборудования при ограниченном частотном ресурсе приводит к увеличению уровня взаимных помех, нарушая нормальную работу этих средств [1-3]. Поскольку использование беспроводных устройств для тестирования оборудования интегрированных инфокоммуникационных систем принимает массовый характер, необходимо оценить их электромагнитную совместимость (ЭМС) с другими РЭС инфокоммуникационных систем.

Оценка внутриканальных помех и блокировка методом совокупных потерь

Беспроводные устройства для тестирования могут выступать в качестве источников помех (интерференции) для других систем и сами могут подвергаться воздействию внешних помех. Интерференция возникает, если устройства работают с перекрытием частоты; в непосредственной близости друг от друга; одновременно; с перекрытием диаграмм направленности антенн; а также зависит от плотности размещения передатчиков в пространстве [4-7]. Плотное размещение антенн приводит к тому, что электромагнитные поля, излучаемые антеннами радиопередатчиков (РПД), могут создавать в антеннах радиоприемников (РПМ) высокочастотную ЭДС, что может привести к перегрузке входных каскадов и нарушению нормального функционирования РПМ или даже к выходу из строя.

Не менее опасным является одновременное воздействие нескольких сигналов, порождающих в выходных каскадах и выходных каскадах РПМ интермодуляционные помехи, которые могут попасть в полосу рабочих частот приемников и ухудшать условия приема полезных сигналов. Принципы измерений, анализа и диагностики должны совершенствоваться для создания эффективной системы эксплуатации, контроля и обеспечения качества телекоммуникационной инфраструктуры инфокоммуникационных систем.

Рассмотрим принцип действия разработанной схемы радиочастотной идентификации портов оборудования [8] и используемые в ней беспро-