ОЦЕНКА ВЛИЯНИЯ ДЕСИНХРОНИЗИРУЮЩИХ ИМИТОПОМЕХ НА ЦИФРОВЫЕ АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ РАДИОСВЯЗИ

Орощук И.М.

РОССИЯ, 690034, Владивосток, ул. Громова, д.10, кв.7,
т. 237-573, E-mail: kassandr@mail.primorye.ru

В работе представлены результаты исследования имитостойкости автоматизированных цифровых радиоканалов, используемых для односторонней связи в системах многостанционного доступаВ ней показан один из методов имитационного воздействия на автоматизированные системы радиосвязи [2], основанный на использовании десинхронизирующих имитопомех. Рассмотрена одна из стратегий имитонападения данным способом и метод оценки ее эффективности, а также результаты анализа имитостойкости радиоканала при различных условиях воздействия имитопомех по прохождению радиоволн. Область применения данных исследований актуальна для современных автоматизированных сетей радиосвязи специального назначения, а также сетей радиосвязи используемых в коммерческих, банковских и других отраслях, требующих специальной защиты от противоборствующих и конкурирующих сторон.

Преодоление технологической проблемы аналого-цифрового преобразования сигналов послужило широкому цифровых радиоканалов в современных телекоммуникационных сетях, характеристики которых по большинству параметров превосходят ранее используемые аналоговые каналы связи. Сегодня эти каналы бесспорно занимают ведущее и перспективное место развитии практически всех телекоммуникационных сетей.

Основным направлением развития современных телекоммуникационных сетей является автоматизация процессов обмена информацией, возможности которых раскрылись именно благодаря внедрению цифровых каналов, в которых происходит синтез двух прогрессивных технологий: цифровой обработки сигналов и использование для этого элементов вычислительной техники. Использование новых технологий значительно улучшает характеристики каналов и расширяет их возможности, а также области их применения.

В тоже время использование цифровых каналов связи раскрыло новое направление радиоэлектронной борьбы как в специальных областях их применения, так и для каналов общего пользования. Использование, так называемых, имитационных помех в системах радиоподавления (РП) позволяет скрытно несанкционированно воздействовать на устройства сервисной обработки сигналов в приемном тракте канала связи. Одним из возможных вариантов является воздействие на системы тактовой и цикловой синхронизации канала [2], причем такая возможность существует в любой момент сеанса связи (передачи сигнала) (рис. 1). Чаще всего каналы защищены от несанкционированного запуска специальным паролем или другими способами, в связи с чем более целесообразным способом является вариант воздействия после запуска приемной аппаратуры в момент передачи информационной части сигнала (см. рис. 1). Недостатком такого воздействия имитационных помех (имитонападения) является необходимость ведения радионаблюдения (РН), а также обеспечение энергетического превосходства помехи над сигналом в точке приема [2]. Но тут же следует заметить, что длительность воздействия помехи, как правило, намного меньше длительности всего сигнала, в связи с чем такой способ имитонападения является эффективным и вполне вероятным.

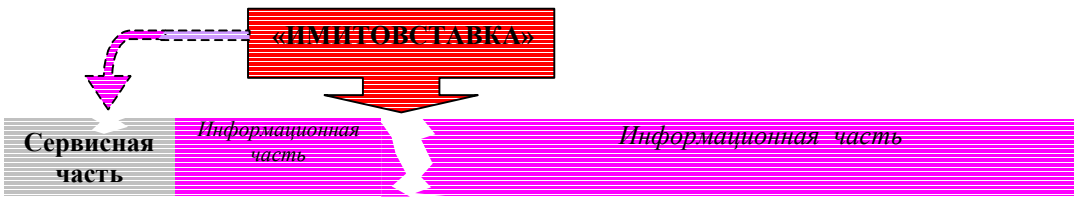

Рис. 1. Варианты применения десинхронизирующих имитопомех

Анализ рассмотренных показателей влияющих факторов показывает, что в общем случае эффективность имитонападения несет вероятностный характер. При решении внутренней задачи вероятность обеспечения энергетического превосходства можно принять равной $P(h \geq h_N) \approx 1$. Но даже в этом случае из-за больших дестабилизирующих факторов задержки сигнала разовой имитоатаки будет недостаточно. В этом случае необходимо произвести повторение атак. Однако в силу ограниченности длительности самого сигнала и по другим причинам (например, скрытности или энергетических ограничений) время, отведенное на имитонападение, будет всегда ограничено. При таких условиях, учитывая, что успеху имитонападения соответствует хотя бы одна удачная попытка выражение, определяющее эффективность имитонападения, можно представить в виде

$$P_{имн}(\Delta t_c) = \chi_{\text{рр+рп}} \hat{L}^{(дес)}_{имн/\chi}(\sigma_\tau, t_c), \quad (1)$$

где $\chi_{\text{рр+рп}} = \begin{cases} 1, \text{если } \Delta t_c > 0 \\ 0, \text{если } \Delta t_c \le 0 \end{cases}$; $\Delta t_c = t_c^* - (t_{PP} - t_{опов} - t_{РП}) = t_c^* - t_{обр}$ – отрезок времени сигнала после обработки в системах РН и РП, на котором воздействие будет целесообразным; $\hat{L}^{(дес)}_{имн/\chi}(\sigma_\tau, t_c)$ - оператор, определяющий успех имитонападения для определенной стратегии.

Так, например, особенности распространения декаметровых волн таковы, что за счет непрерывных изменений в ионосфере происходит стохастическое изменение времени задержки принимаемого сигнала. Влияние этого фактора описывается нормальным законом распределения времени задержки сигнала [2] (рис. 3):

$$\omega(\varepsilon) = e^{-\frac{1}{2}\left(\frac{\varepsilon}{\sigma}\right)^2} \Big/ \sigma\sqrt{2\pi}\,, \tag{2}$$

где $\varepsilon = \Delta t / \tau_0$ – относительное отклонение значащих моментов регистрации фронтов элементарной посылки; $\sigma = \sigma_\tau / \tau_0$ – относительная величина среднеквадратичного отклонения (СКО) времени задержки сигнала.

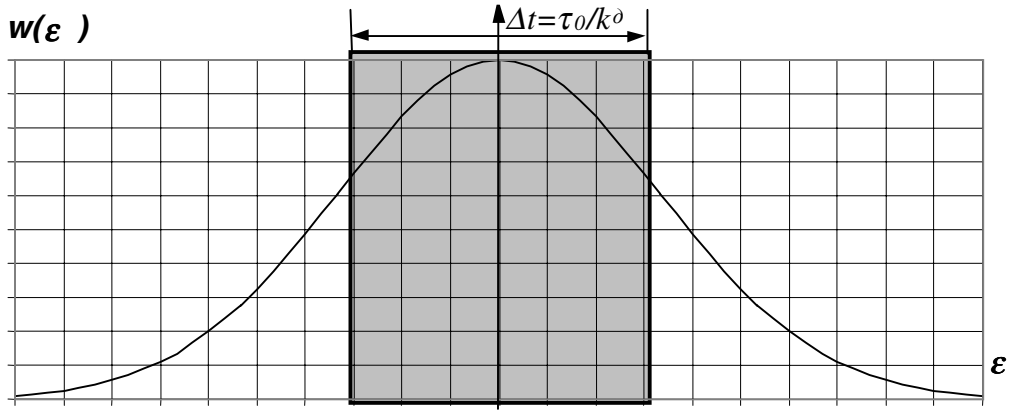

Рис. 2. Функция распределения вероятностей времени задержки сигнала

Пользуясь данным распределением, вероятность правильного приема одного фронта элементарной посылки можно определить из следующего выражения

$$p_{\tau 1} = 2\Phi_0(\Delta t / 2\tau_0\sigma) = 2\Phi_0(\Delta t / 2\sigma_\tau), \tag{3}$$

где $\Phi_0(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-\frac{t^2}{2}} dt$ – функция центрированного нормального распределения; Δt – шаг коррекции системы синхронизации автоматизированной системы радиосвязи.

В рассматриваемом варианте имитонападения необходимо учитывать, по меньшей мере, задержку сигнала на двух радиотрассах: радиосвязи и радиоподавления. В этом случае максимальное расхождение фаз в точке приема будет соответствовать двойной задержке, т. е. в формуле (3) необходимо использовать удвоенное значение дисперсии времени задержки сигнала $\left(\sigma_\Sigma^2 = 2\sigma_\tau^2\right)$.

При анализе системы тактовой синхронизации необходимо учесть некоторые особенности ее работы. Процесс коррекции фазы в системах тактовой синхронизации осуществляется после накопления в реверсивном счетчике установленного числа обнаруженных *S* сдвигов в ту или иную сторону; при отсутствии требуемого числа сдвигов через определенное число элементов счетчик устанавливается в исходное состояние. Учитывая эту особенность в общем случае процесс подстройки можно разделить на циклы, состоящие из установленного для сброса счетчика (очищения счетчика) числа элементов.

Проанализируем работу счетчика в течение одного цикла. В общем случае счетчик по окончании цикла может принять три состояния (рис. 4): при накоплении не менее чем требуемого числа сдвигов в определенную сторону выдается импульс на опережение или отставание фазы тактовой частоты; если суммарное значение счетчика не превысит емкости счетчика *S*, он сбрасывается на "0". Причем следует отметить, что при выдаче импульсов сдвига (+1 или –1) счетчик также сбрасывается в исходное состояние.

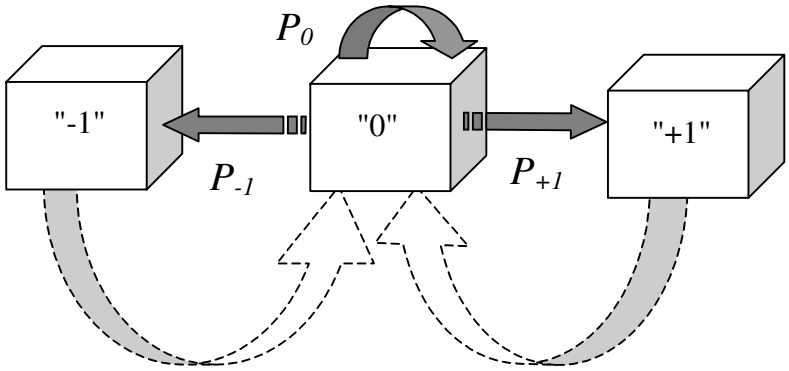

Рис. 3. Пояснение состояний реверсивного счетчика тактовой синхронизации

Пользуясь известным значением элементарной вероятности правильного приема значащего момента фронта импульса вероятности всех возможных состояний счетчика можно определить из следующих выражений:

$$\left.\begin{aligned} P_{-1} &= \sum_{i=S+1}^{V} \binom{V}{i} p_{\tau 1}^{i} (1-p_{\tau 1})^{V-i}; \\ P_{+1} &= \sum_{i=S+1}^{V} \binom{V}{i} p_{\tau 1}^{V-i} (1-p_{\tau 1})^{V}; \\ P_0 &= 1-P_{+1}-P_{-1}, \end{aligned}\right\} \qquad (4)$$

где P_{+1}, P_{-1}, P_0 – соответствующие вероятности перехода счетчика в состояние "+1", "-1", "0"; S – емкость реверсивного счетчика; V – длительность цикла синхронизации, выраженная в долях элементарных посылок сигнала. Пользуясь данными выражениями, определена вероятность сложного события, состоящего в том, что за установленный период имитонападения в системе синхронизации произойдет сдвиг более чем на пол-элемента в положение $-\tau/2$, чему соответствует к концу имитоатаки суммарный сдвиг на отставание, превышающий значение $-k_\partial/2$:

$$P_{имн/дес/}(\delta_t) \approx \chi\left\{\Phi_0\left[\sqrt{\frac{\delta_t Q_{-1}}{P_{-1}}}\right] - \Phi_0\left[\frac{1}{4}\left(\frac{1+k_\partial}{\sqrt{\delta_t P_{-1} Q_{-1}}} + (2-4P_{-1})\sqrt{\frac{\delta_t}{P_{-1}Q_{-1}}}\right)\right]\right\}, \qquad (5)$$

где $\delta_t = Int\left[\frac{\Delta t_c}{V}\right]$; $\qquad Q_{-1} = 1-P_{-1}$.

На рис. 4 показана зависимость вероятности успешного имитонападения от длины подавляемого сигнала при различных значениях СКО времени задержки сигнала.

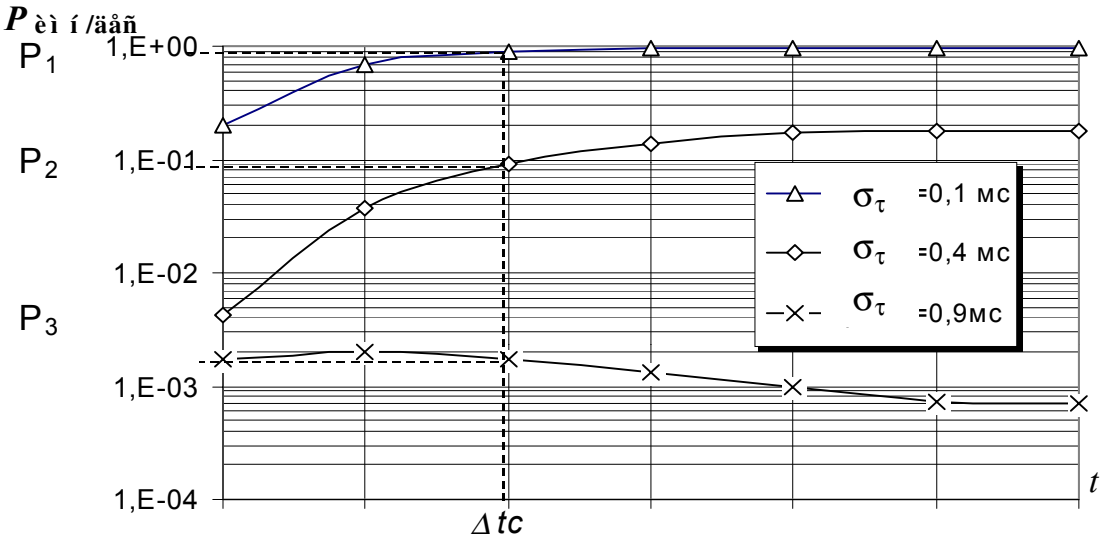

Рис. 4. Эффективность имитонападения в процессе сеанса связи

Из данного рисунка видно, что эффективность имитонападения будет всегда ограничена и зависеть только от длительности поражаемого сигнала. Однако можно заметить, что для трасс с большим значением СКО времени задержки сигнала увеличение времени имитонападения не повышает ее эффективность. В данном случае функция [см. формулу (5)] изменяет знак. Это происходит в том случае, когда во втором слагаемом значение $P_{-1} < 0{,}5$, т. е. существует некоторое пороговое значение СКО времени задержки сигнала $\sigma_{\tau.пор}$, при превышении которого эффективность имитонападения с ростом времени имитоатаки не возрастает. Ее значение можно найти из p_τ, соответствующего $P_{-1} = 0{,}5$.

Следовательно, повысить эффективность имитонападения можно только при изменении трассы подавления с меньшим СКО времени задержки сигнала. Повышению же имитостойкости способствует снижение в некоторых пределах длительности сигнала, а также повышение скорости манипуляции (в ущерб помехоустойчивости). Наиболее существенным способом защиты может служить система с независимой синхронизацией, однако ее применение имеет некоторые ограничения.

Результаты работы можно использовать для разработки систем РП автоматизированных радиоканалов, а также для разработки систем защиты автоматизированных систем радиосвязи. В дополнение следует заметить, что сегодняшний день пока не разработаны совершенные методы защиты систем синхронизации, т.е. вопрос их защиты остается открытым

Литература

1. Oroshchuk I.M. New technologies of unauthorized influence on automatic radio communication systems //The 3-rd international symposium «Sibconvers'99», TUSUR, V- 2, 1999/- p. 336-338.

2. Орощук И.М. Новые технологии радиоэлектронного подавления каналов автоматизированных систем радиосвязи. – Владивосток, ТОВМИ им. С.О. Макарова, 2000. – 112 с.

ASSESSMENT OF INFLUENCING OF THE DESTABILIZING IMITOHINDRANCES ON THE DIGITAL AUTOMATED RADIO COMMUNICATION SYSTEMS

Oroshchuk I.M.

10-7 Gromova street, Vladivostok, 690034, RUSSIA,
phone (4232) 237-573, E-mail: oimscient@mail.primorye.ru

Abstract. Results of research imitoprotection of the automated digital radio channels used for one-way communication in the systems of the multiple-access are submitted in the work. One of the methods of imitative effect to the automated radio communication systems [2], based on usage unclocking imitohindrances is submitted; one of the strategies of imitoattack implemented by the given means and the method of the assessment of its efficiency are reviewed, and also the results of the imitoprotection analysis of the radio channel under different conditions of the radio waves propagation. The field of the researches data application is actual for the modern automated networks of special-purpose radio communication, and also for the networks of radio communication used in commercial, banking and other spheres, requiring special protection against the opposing and competitive parties.

The principal direction of the modern telecommunication networks development is the automation of the information exchange processes, the capabilities which ones have been opened due to an application of the digital channels, in which ones synthesizing of two progressive technologies occurs: digital signals processing and usage for this purpose computer technology elements. Usage of the new technologies considerably improves the characteristics of the channels and expands their capabilities, and also the area of their application.

At the same time usage of digital channels communication has opened a new direction in the electronic warfare activity both in special areas of their application, and for the channels of general use. Usage of so-called imitative hindrances in the radio countermeasure systems (RCS) allows secretly and unauthorized to affect devices of the service signal processing in the receiver section of the communication channel. One of the optional versions is the effect to the systems of pulsing and frame synchronization of the channel [2], and such capability exists at any moment of the communication session (transmission of the signal). More often the channels are protected from unauthorized starting by the special password or some other ways, in this connection the more expedient way is the version of the effect taking place after starting of the receiving equipment, at the moment of the information part of the signal transmission. Lack of such effect of imitative hindrances (imitoattack) is the necessity of radio observation (RO), and also maintenance of the power superiority of the hindrances over the signal in the point of reception [2]. But here it is necessary to note, that the duration of the hindrance effect as a rule, is much less than duration of the whole signal, in this connection such way of the imitoattack is effective and quite probable.

The analysis of the reviewed parameters of the influential factors demonstrates that generally efficiency imitoattack performs probabilistic nature. At the solution of the internal problem the probability of the power superiority maintenance of can be accepted to be equal to a unity. But even in this case because of the large destabilizing factors of the signal delay application of the single imitoattack will be unsufficient. In this case it is necessary to make repetition of attacks. However due to limitation of the signal duration and to other reasons the time given to imitoattack, will be always limited.

So, for example, the features of radio propagation of the decameter waves are those , that at the expense of continuous changes in the ionosphere there is a stochastic delta time of the received signal delay. The influence of this factor is described by the normal distribution law of the signal delay [2]:

$$\omega(\varepsilon) = e^{-\frac{1}{2}\left(\frac{\varepsilon}{\sigma}\right)^2} \Big/ \sigma\sqrt{2\pi} \ , \qquad (1)$$

where $\varepsilon = \Delta t / \tau_0$ - relative deviation of meaningful instants of registration of the elementary sending fronts; Δt - step of correction of the the automated radio communication synchronization system; $\sigma = \sigma_\tau / \tau_0$ - relative value of standard deviation (SD) of the signal delay. Using the distribution, the probability of the exact reception of one front of the elementary sending can be determined from the following expression

$$p_{\tau 1} = 2\Phi_0\left(\Delta t / 2\tau_0\sigma\right) = 2\Phi_0\left(\Delta t / 2\sigma_\tau\right), \qquad (2)$$

where $\Phi_0(x)-$ is the function of the centered normal distribution.

In the considered version of the imitoattack it is necessary to take into account the signal delay as minimum as two radiolines: radio communication and radio countermeasures. In this connection in the formula (2) it is necessary to use the doubled value of the signal delay dispersion.

The process of the phase equalization in the systems of tact synchronization is implemented after accumulation of the established number detected S - shifts to this or that direction in the reversible meter; at absence of required number of shifts after definite number of elements the meter is set to the reset condition. Considering this feature the general process of tuning can be sectioned into cycles, consisting of the established number of elements for the meter reset, determined by statuses of the meter, which ones can be determined by the following expressions:

$$P_{-1} = \sum_{i=S+1}^{V} p_{\tau 1}^{i} (1-p_{\tau 1})^{V-i}; \ P_{+1} = \sum_{1=S+1}^{V} p_{\tau 1}^{V-i} (1-p_{\tau 1})^{i}; \ P_0 = 1 - P_{+1} - P_{-1}, \qquad (3)$$

where P_{+1}, P_{-1}, P_0 - corresponding probabilities of the meter transition to the status "+1" , "-1","0"; S - capacity of the reversible meter; V - duration of the synchronization cycle , expressed in portion of elementary sendings of the signal.

Using the expressions, the probability of composite event is determined , which consists in that, that during established period of the imitoattack in the system of synchronization there will be a shift to more than the half-element in the position -τ/2:

$$P_{имн/дес/}(\delta_t) \approx \chi\left\{\Phi_0\left[\sqrt{\frac{\delta_t Q_{-1}}{P_{-1}}}\right] - \Phi_0\left[\frac{1}{4}\left(\frac{1+k_\partial}{\sqrt{\delta_t P_{-1} Q_{-1}}} + (2-4P_{-1})\sqrt{\frac{\delta_t}{P_{-1}Q_{-1}}}\right)\right]\right\}, \quad (4)$$

where $\delta_t = Int[\Delta t_c / V]$; $Q_{-1} = 1 - P_{-1}$.

The analysis demonstrates , that the efficiency of the imitoattack will be always limited and it will depend only on duration of the struck signal. However it is possible to note , that for routes with large value SD of the signal delay the increase of the imitoattack time does not increase its efficiency. In this case the function [see formula (4)] changes the sign, that is there is some threshold value SD of the signal delay $\sigma_{\tau.пор}$, at the excess of which the efficiency of the imitoattack does not increase with the increase of the imitoattack time. Its value can be found from $p_{\tau 1}$, applicable $P_{-1} = 0{,}5$.

Therefore, to increase the imitoattack efficiency it is possible only by means of changing of the suppression route with smaller SD time of the signal delay. The imitoprotection increase is promoted by the decrease in some limits of the signal duration, and also the increase of the manipulation speed (at the expense of the hindrance immunity). The most essential way of protection can be served by the system with independent synchronization, however its application has many limitations. The conducted analysis demonstrates, that the problem of the synchronization systems protection remains opened up today.

References

1. Oroshchuk I.M. New technologies of unauthorized influence on automatic radio communication systems // The 3-rd international symposium "Sibconvers'99", TUSUR, V-2, 1999/- pp. 336-338. (in English).
2. Oroshchuk I.M. New technologies of the radio electronic suppression of channels of the automated radio communication systems. - Vladivostok, Pacific Navel Institute, 2000. - 112 pp. (in Russian).