ОЦЕНКА ЭФФЕКТИВНОСТИ ИМИТОЗАЩИТЫ АВТОМАТИЗИРОВАННЫХ СИСТЕМ РАДИОСВЯЗИ НА ОСНОВЕ ГИПЕРГЕОМЕТРИЧЕСКОЙ СТРАТЕГИИ ИМИТОНАПАДЕНИЯ

Орощук И.М.

РОССИЯ, 690034, г. Владивосток, ул. Громова, д.10, кв.7,
тлф.- (4232)237-573, E-mail: oimscient@mail.primorye.ru

В работе представлен метод оценки потенциальной имитостойкости автоматизированных систем радиосвязи (АСР). Разработанный метод основан на использовании гипергеометрической стратегии имитонападения на АСР. Предложенный метод оценки позволяет строить оптимальные системы имитозащиты цифровых радиоканалов от имитационных помех, действующих на АСР в режиме дежурного приема.

Тенденции широкого внедрения автоматизированных систем радиосвязи (АСР) практически во все отрасли экономики, бизнеса, управления государством, силовыми и другими структурами ставит в определенную зависимость многие важные инфраструктуры от устойчивости работы этих систем и степени безопасности их применения. В этих условиях достаточно быстро развиваются новые направления воздействия на такие системы, основанные на несанкционированном проникновении в них или на более «тонких» способах нарушения функционирования установленных протоколов с диверсионной или корыстной целью. Такого рода воздействие основано на применении имитационных сигналов (имитопомех), которое принято называть имитоатакой или имитонападением. Использование тех или иных способов имитонападения имеет определенный приоритет за счет повышенной скрытности воздействия и достаточно больших возможностей.

Учитывая данную особенность, во многих современных АСР используются те или иные средства защиты, основанные на идентификации и аутентификации корреспондентов. Наиболее серьезной мерой безопасности является метод криптографической защиты, однако в силу специфических аппаратных и организационных сложностей такой вариант используется в основном только в системах специального назначения.

В АСР широкого применения (пейджинговые, сотовые и другие сети) в основном использованы способы идентификации и аутентификации, причем для систем односторонней связи в принципе возможен только первый способ, так как нет обратного канала. Такая особенность способствовала наиболее широкому использованию в сетях способа, основанного на идентификации, степень защиты которой определяется длиной используемого кода. Следует заметить, что данный путь повышения защиты сетей ограничен, так как он существенно снижает пропускную способность систем многостанционного доступа за счет увеличения сервисной части сигнала (рис. 1), цена которой практически определяет рентабельность сети. В этой связи часто возникает проблема выбора оптимальной защиты: каким образом можно определить требуемую степень защиты.

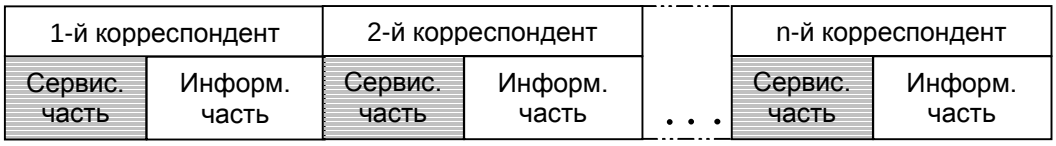

Рис. 1. Обобщенная структура сигнала автоматизированной радиосети

В общем случае существует несколько способов имитонападения на радиосети [1 - 4], наиболее распространенным из которых является вариант воздействия на радиоканалы дежурного приема. Режим такого использования радиоканалов наиболее распространен во многих сетях связи.

Для оценки защищенности радиоканала или АСР предлагается использовать гипергеометрическую стратегию имитонападения, на основе которой можно определить предельные возможности нападающей стороны или получить оценку потенциальной защищенности от имитопомех (потенциальную имитостойкость).

Мерой защиты от рассматриваемого способа имитонападения может служить вводимая в АСР неопределенность некоторых элементов либо всей сервисной части сигнала и других параметров радиоканала. В общем случае АСР энергетически доступны каждому пользователю, в связи с чем для защиты необходимо предусмотреть специальные меры. В модели рассматривается защита основанная на неопределенности состояний АСР. Способом создания неопределенности для неабонированного корреспондента может быть варьируемая структура сервисной части сигнала (в ограниченном сигнатурном пространстве - $\Omega_{FS.\ сист}$), а также использование псевдослучайно перестраиваемых рабочих частот АСР (так называемая ППРЧ). В свою очередь, сигнатурное

@2002, электронная версия подготовлена ЗАО АВТЭКС Санкт-Петербург, http://www.autex.spb.ru

пространство в общем случае может изменяться по нескольким параметрам: побитно в хемминговом подпространстве и в подпространствах определенного вида манипуляции (амплитудной, частотной, фазовой, широтно-импульсной и др.). То есть сигнатурное пространство может быть в общем случае многомерным.

Таким образом, в целом возможность имитонападения на АСР определяется знанием рабочих частот и регламентируемым на данный момент состоянием сигнала в сигнатурном пространстве.

Анализ влияния имитопомех такого типа основан на разработанной вероятностной модели имитонападения на АСР, защита которой определена псевдослучайным изменением ее состояний в масштабе времени в частотно-сигнатурном пространстве. Для формализации процесса осуществлена факторизация частотно–сигнатурного пространства признаков имитонападения ($\Omega_{F,S}$), которое представлено в ортонормированном базисе независимых подпространств (частотно – временное и сигнатурно–временное). На рис. 2, в качестве примера, процесс имитозащиты АСР формально представлен в виде вектора в ортонормированном базисе частотно-сигнатурного пространства, дискретно изменяющего рабочее состояние в масштабе времени, в котором сигнатурное пространство ограничено одномерным подпространством битового изменения структуры сервисной части сигнала. Процесс имитонападения представлен в виде сканирования области неопределенности по гипергеометрической логике, в предположении, что данная область всегда ограничена и известна нападающей стороне. Процесс имитонападения может быть детерминированным и случайным, что определяется особенностями АСР и организационно–техническими требованиями к системе имитонападения. Естественно, это налагает ряд ограничений, а в некоторых случаях дает дополнительный выигрыш для систем имитонападения.

Для оценки эффективности имитонападения на АСР, или противоположного события ее имитостойкости, используются вероятностно-временные оценки:

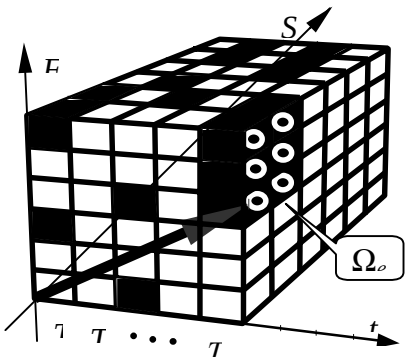

Рис. 2. Формализованное представление состояний пространства сканирования (см. рис. 2).

$$\left.\begin{aligned} P_{\text{ИМН}\,\Sigma} &= W\left(P_{\text{ГГ}}, T_x, \widehat{L}^{Ia}\left(I_i/\Omega_{e\partial}\right)\right); \\ T_x &= W^{-1}\left(P_{\text{ГГ}}, P_{\text{ИМН}\,\Sigma}, \widehat{L}^{Ia}\left(I_i/\Omega_{e\partial}\right)\right), \end{aligned}\right\} \qquad (1)$$

где W - функция, определяющая стратегию выбора (поиска сканированием) разрешенного состояния сигнала по гипергеометрической логике ($P_{\text{ГГ}}$); $\widehat{L}^{Ia}\left(I_i/\Omega_{e\partial}\right)$ - условный оператор правдоподобия, определяющий успех имитонападения при выборе разрешенного состояния АСР для определенного вида имитопомех I_i, зависящего от помехоустойчивости АСР и особенностей построения системы защиты; $\Omega_{e\partial}$ – область разрешенных состояний

В случае возможности применения имитопомех различного вида следует производить оценку имитостойкости для каждого вида [1, 2]. В этом случае для оценки имитостойкости следует пользоваться следующим выражением

$$P_{\text{ИМС}} = \prod_k \left(1 - \chi_k P_{\text{ИМН}.k}\right) \quad , \quad k = \overline{1, K}\,, \qquad (2)$$

где χ_k - индикаторный коэффициент целесообразности k-го вида воздействия;

$$\chi_k = \left\{\begin{matrix} 1, \text{ если применение данного вида имитопомех возможно и целесообразно;} \\ 0, \text{ если применение данных имитопомех невозможно и нецелесообразно.} \end{matrix}\right\};$$

$P_{\text{ИМН}.k}$ - вероятность успешного воздействия имитопомех k-го вида на АСР; K – возможное число видов воздействия на радиоканал имитопомехами.

В качестве примера использования оценки имитостойкости, исследована система связи с протоколом, имеющим линейнозависимую реакцию на имитационный сигнал, вызывающий ее блокировку [1], потенциальную имитостойкость которой в зависимости от параметров защиты и ее технических характеристик можно определить из следующих выражений:

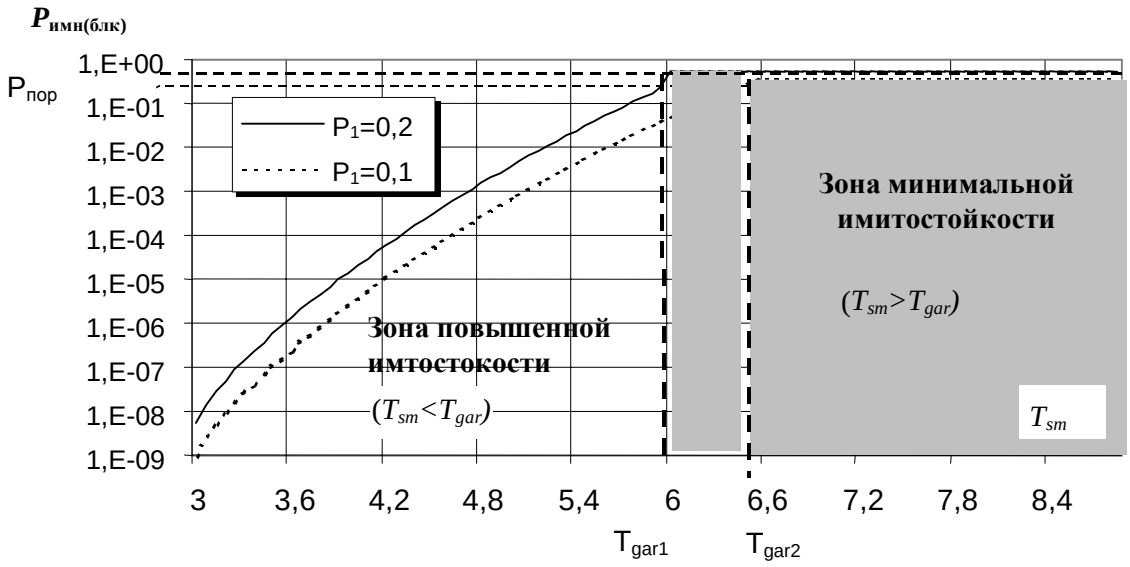

Рис. 3. Эффективность имитонападения с целью блокировки

$$P_{имс/блк/} = \begin{cases} 1 - \dfrac{p_1 B(T_{бл1} + t_c)}{n}, & \text{если } T_{gar} < T_{sm}; \\ 1 - \dfrac{(t_c + T_{бл1})}{T_{sm}} \overline{K}_{ЛЗ}, & \text{если } T_{gar} > T_{sm}, \end{cases} \qquad (3)$$

где T_{sm} – время смены состояний системы; T_{gar} – время гарантированного выбора разрешенного состояния системы; $T_{gar} = \dfrac{n}{B}(F_{сист} S_{сист} - F_{ед} S_{ед} + 1)$;

$$\overline{K}_{ЛЗ} \approx \sqrt{\frac{Kp_1q_1}{2\pi}}\left[\exp\left(-\frac{Kp_1}{2q_1}\right) - \exp\left(-\frac{(Z-Kp_1)^2}{2Kp_1q_1}\right)\right] + Kp_1\left[\Phi_0\left(\frac{(Z-Kp_1)}{\sqrt{Kp_1q_1}}\right) - \Phi_0\left(\sqrt{\frac{Kq_1}{p_1}}\right)\right],$$

в которых $K = Int[T_{sm} B/n]$; $Z = \begin{cases} F_{ед} S_{ед}, & \text{если } K > F_{ед} S_{ед} \\ K, & \text{если } K < F_{ед} S_{ед} \end{cases}$;

p_1 – вероятность успешного выбора разрешенного состояния за одну имитоатаку;

$p_1 = 1 - q_1 = \dfrac{F_{ед} S_{ед}}{F_{сист} S_{сист}}$; $\Phi_0(x)$ – табулированная функция нормированного и центрированного нормального распределения; $\Phi_0(x) = \dfrac{1}{\sqrt{2\pi}} \int_0^x e^{-\frac{t^2}{2}} dt$; B – установленная скорость манипуляции в канале; n –объем информации сервисной части сигнала в битах; t_c – длительность пакета одного корреспондента (см. рис. 1); $T_{бл1}$ – время блокировки системы при ложном запуске.

На рис. 3 показан график эффективности имитонападения (блокировки).

Полученное выражение (3) позволяет оценивать имитостойкость исследуемой АСР от имитопомех, вызывающих в ней несанкционированную блокировку. Из рис. 3 видно, что наибольшая имитостойкость будет достигается при условии, когда $T_{sm} < T_{gar}$. В случае когда $T_{sm} > T_{gar}$ имитостойкость достигает некоторого предельного значения $P_{пред}$, после чего она остается постоянной. Пользуясь полученной оценкой можно устанавливать конкретные параметры заданной системы защиты АСР. Для оценки полной имитостойкости АСР следует рассчитать имитостойкость для всех видов помех, после чего по формуле (2) вычислить окончательную имитостойкость системы.

Литература

1. Орощук И.М. Новые технологии радиоэлектронного подавления автоматизированных систем радиосвязи. – Владивосток, Тихоокеанский военно-морской институт, 2000. – 112 с.

2. Oroshchuk I.M. New technologies of unauthorized influence on automatic radio communication systems // The 3-rd international symposium "Sibconvers'99", TUSUR, V-2, 1999/- 3 с. (на английском).

3. Орощук И.М. Оценка влияния десинхронизирующих имитопомех на цифровые автоматизированные системы радиосвязи // Третья международная конференция: «Цифровая обработка сигналов и их применение» Российское НТОРЭС им. А.С. Попова, Москва, 2000. Доклады – 1. – 4 с.

4. Орощук И.М., Аксенов В.П. Технологические особенности применения десинхронизирующих имитопомех в автоматизированных системах связи // Международная конференция по телекоммуникациям (IEEE/ICC2001/ St. Petersburg), Санкт-Петербург, 2001. – 4 с.

ASSESSMENT OF THE AUTOMATED RADIO COMMUNICATION SYSTEMS IMITOPROTECTION ON THE BASE OF AN IMITOATTACK HYPERGEOMETRIC STRATEGY

Oroshchuk I.

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

The assessment method of the automated radio communication systems (ARCS) potential security from imitaattack (imitoprotection) is represented in the report. The designed method is based on usage of the hypergeometric strategy imitoattack on the ARCS. The offered method of an assessment allows to design optimum protection systems of the digital radio channels from imitohindrences, influencing on the ARCS in a mode of a listening watch.

The tendencies of the automated radio communication systems (ARCS) implantation practically in all branches of economy, business and management puts in defined dependence many important infrastructures from positive stability of the systems operation and security of their usage. In these conditions new directions of effect on such systems are develop quickly. They are based on unauthorized penetration into the systems or on more "thin" methods of their protocols breakup with the subversive purpose. Such influence is accepted to name as imitoattack. Generally there are some methods of an imitoattack on a radio network [1 - 4], most widespread from which is the variant of influence on the radio channels of a listening watch. For an assessment of the ARCS security it is offered to use the hypergeometric strategy of imitoattack, on the basis of which it is possible to define a rating of potential security from imitohindrences (imitoprotection).

In general case the ARCS are power availability to each user, in this connection for protection is necessary to provide the special methods. By measure of protection from a considered method of imitative attack in ARCS can serve the uncertainty of some elements or whole service part of signal and other parameters of radiolink. A varied structure of service part of signal (in limited signature space - $\Omega_{.FS\ сист}$), as well as the use of pseudorandom retuning of the ARCS working frequencies can be a way of creation of uncertainty for unauthorized correspondent. In turn out, signature space in general case can change on several parameters: by byte in Hamming subspace and in subspaces of the certain kind of manipulation. That is signature space can be multivariate in general case.

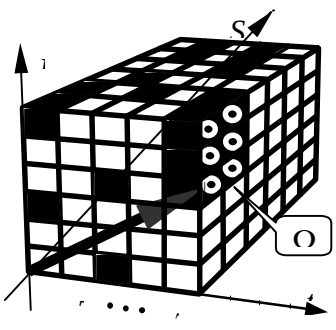

Fig. 1. Formalization of ARCS

The analysis of influence of the such type imitohindrances is based on developed probabilistic model of imitoattack on the automatic radio link, which protection is determined by pseudorandom change of it condition in the time scale in the frequency-signature space. For process formalizations the factorisation of frequency-signature space of the imitoattack attributes ($\Omega_{.F,\ S}$), is carried out, which is represent in the ortonormalize basis of independent subspaces (frequency-temporary and signature-temporary). For example, on fig. 1 the ARCS imitoprotection process is formally present in a kind nf vector in the ortonormalize basis of the frequency-signature space, is discrete varying of the working condition in time scale, in which the signature space is limited by the univariate subspace of bit change of the signal service

part structure. The imitoattack process is submitted in a kind of scanning of the uncertainty area on hypergeometric logic, in the assumption, that the given area is always limited and known for the attack side.

For evaluation of efficiency of imitoattack on ARCS, or opposite event of it imitoprotection, the probabilistic-temporary valuations are used:

$$\left.\begin{aligned} P_{\text{ИМН}\,\Sigma} &= W\left(P_{\text{ГГ}}, T_x, \widehat{L}^{Ia}\left(I_i/\Omega_{ed}\right)\right); \\ T_x &= W^{-1}\left(P_{\text{ГГ}}, P_{\text{ИМН}\,\Sigma}, \widehat{L}^{Ia}\left(I_i/\Omega_{ed}\right)\right), \end{aligned}\right\} \qquad (1)$$

where W - function, determining of choice strategy (search by scanning) of permitted signal condition on the hypergeometric logic ($P_{\text{ГГ}}$); $\widehat{L}^{Ia}\left(I_i/\Omega_{ed}\right)$ - conditional operator of plausibility, determining of imitoattack success by choice of the ARCS permitted condition for a certain kind I_i of imitohindrances, and depends on features of ARCS protection construction; $\Omega_{\text{ед}}$ - area of permitted conditions of the scanning space (see fig. 1).

At possibility of usage of the different aspect imitohindrances it is necessary to manufacture the imitoprotection assessment for each of them [1, 2]. In this case for the imitoprotection assessment it is necessary to use the expression

$$P_{\text{ИМС}} = \prod_k \left(1 - \chi_k P_{\text{ИМН}.k}\right), \quad k = \overline{1, K}, \qquad (2)$$

where χ_k - the display practicability factor of k-th kind of influence;

$$\chi_k = \left.\begin{cases} 1, & \text{if the use of this kind of imitohindrances is possible and expedience;} \\ 0, & \text{if the use of this kind of imitohindrances is not possible and expedience.} \end{cases}\right\};$$

$P_{\text{ИМН}.k}$ - probability of successful influence of k-th type hindrances to ARCS; K - the possible number of influences by imitohindrances on the radio link (imitoattack).

As an example, is probed imitoprotection ARCS at influence the imitohindrances, calling its blocking [1], which assessment is defined by expression

$$P_{имс\,/\,блк\,/} = \begin{cases} 1 - \dfrac{p_1 B\left(T_{бл1} + t_c\right)}{n}, & \text{если } T_{gar} < T_{sm}; \\ 1 - \dfrac{\left(t_c + T_{бл1}\right)}{T_{sm}} \overline{K}_{ЛЗ}, & \text{если } T_{gar} > T_{sm}, \end{cases} \qquad (3)$$

where T_{sm} - time of change of system conditions; T_{gar} - time of guaranteed choice of the allowed system condition; $T_{gar} = \dfrac{n}{B}\left(F_{сист} S_{сист} - F_{ed} S_{ed} + 1\right)$;

$$\overline{K}_{ЛЗ} \approx \sqrt{\frac{Kp_1q_1}{2\pi}}\left[\exp\left(-\frac{Kp_1}{2q_1}\right) - \exp\left(-\frac{(Z - Kp_1)^2}{2Kp_1q_1}\right)\right] + Kp_1\left[\Phi_0\left(\frac{(Z - Kp_1)}{\sqrt{Kp_1q_1}}\right) - \Phi_0\left(\sqrt{\frac{Kq_1}{p_1}}\right)\right],$$

in which $K = Int\left[T_{sm} B/n\right]$; $Z = \begin{cases} F_{ed} S_{ed}, & \text{if } K > F_{ed} S_{ed} \\ K, & \text{if } K < F_{ed} S_{ed} \end{cases}$; $\Phi_0(x)$ - function of normalized and centered normal allocation; p_1 - probability of successful choice of the allowed condition for one imitoattack; $p_1 = 1 - q_1 = \dfrac{F_{ed} S_{ed}}{F_{сист} S_{сист}}$; B - rate of on-off modulation in the channel; n - size of a service part of a signal; t_c - duration of a packet of one correspondent; $T_{бл1}$ - handover time of a system at a fail triggering.

Using an obtained assessment it is possible to install concrete parameters of a preset protection system ARCS. For a complete assessment it is necessary to calculate imitoprotection ARCS for all aspects of imitohindrances, then to calculate the system final imitoprotection under the formula (2).

References:

1. Oroshchuk I.M. New technologies of radioelectronic suppression of the automated radio communication systems. - Vladivostok, Pasific Navel Institute, 2000. - 112 pp.(in Russian).

2. 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.

3. Oroshchuk I.M. Assessment of of influencing of the destabilizing imitohindrances on the digital automated radio communication systems // The Third International Conference: «Digital signal processing and its application», Moscow, 2000. Reports-1.- pp. 219-224.

4. Oroshchuk I.M. Aksenov V.P. Technological features of usage of interferences influencing on the automated radio communication system// International Conference on Communications (IEEE/ICC2001/ St. Petersburg), St.-Petersburg, 2001. - 4 pp. (in Russian).