УДК 681.084

УСЛОВИЯ РЕАЛИЗАЦИИ АЛГОРИТМА ЗАЩИТЫ ИНФОРМАЦИИ В КОСМИЧЕСКИХ СИСТЕМАХ СВЯЗИ И УПРАВЛЕНИЯ

д.т.н. Ю.В. Стасев, О.Г. Лебедев, Д.Н. Воронов

В докладе предлагается метод обеспечения безопасности информации в космических системах связи и управления, базирующийся на динамической передаче сигналов.

Создание и применение систем космической связи и управления является наиболее развитым направлением практического использования космического пространства. В настоящее время созданы и эксплуатируются более 40 систем космической связи и управления. Опыт эксплуатации этих систем показывает, что требуемое качество их функционирования в существенной мере зависит от решения проблемы помехозащищенности и имитостойкости радиоканалов управления.

Проведенные к настоящему времени исследования показали [2], что обеспечить активную помехо– и имитозащиту радиосистем возможно при реализации динамического режима "бегущий код". Сущность динамического режима "бегущий код" заключается в том, что каждому информационному биту ставится в соответствие по псевдослучайному закону один из сложных сигналов из ансамбля разрешенных сигналов.

Определим условия недешифруемости множества, реализующего динамический режим функционирования. Для чего докажем следующие теоремы.

Теорема 1.

Пусть информационному множеству $\{U\} = \{U_1, U_2, \ldots, U_z\}$ по правилу преобразующего множества $\{M\}$ ставится в соответствие сигнал из множества $\{S\} = \{S_1, S_2, \ldots, S_Q\}$. Тогда энтропия $H_j(U_j, S_i)$ раскрытия j – го сообщения будет принимать максимальные значения при независимом появлении сигналов и сообщений.

Доказательство.

Совместную энтропию совокупности U и S можно представить в виде:

$$H(U,S) = -\sum_{j=1}^{Z}\sum_{i=1}^{Q} P(U_J, S_1)\log_2 P(U_j, S_j), \qquad (1)$$

где $P(U_j, S_i)$ – вероятность совместного появления U_j сообщения и сообщения S_i сигнала.

Известно, что

$$H(U, S) = H(U) + H(U/S).$$

В выражении (2) $H(U, S)$ принимает максимальное значение, если $H(U)$ и $H(U/S)$ максимальны.

В [2] показано, что $H(U)$ принимает максимальное значение при статистически независимых сообщениях.

Найдем максимум $H(U/S)$

$$H(U/S) = -\sum_{j=1}^{Z}\sum_{i=1}^{Q} P(U_j, S_i)\log_2 P(U_j / S_i). \qquad (3)$$

Для условий энтропии $H(U/S)$ справедливо неравенство

$$H(U/S) \le H(U). \qquad (4)$$

Следовательно,

$$-\sum_{j=1}^{Z}\sum_{i=1}^{Q} P(U_j, S_i)\log_2 P(U_j / S_i) \le -\sum_{j=1}^{Z} P(U_j)\log_2 P(U_j). \qquad (5)$$

В выражении (5) равенство выполняется при условии

$$P(U_j/S_i) = P(U_j).$$

Выполнение этого условия возможно при статистической независимости U_j и S_i.

Тогда,

$$P(U_j/S_i) = P(U_j)\ P\ (S_i). \qquad (6)$$

Подставив (6) в (3) получим

$$H(U/S) = -\sum_{j=1}^{Z}\sum_{i=1}^{Q} P(U_j)P(S_i)\log_2 P(U_j). \quad (7)$$

Учитывая, что $\sum_{i=1}^{Q} P(S_i) = 1$ имеем

$$H(U/S) = -\sum_{j=1}^{Z} P(U)\log_2 P(U_j) = H(U). \quad (8)$$

Следовательно, при статистически независимых множествах $\{U\}$ и $\{S\}$ энтропия раскрытия максимальна.

Теорема 2.

Пусть информационному множеству $\{U\} = \{U_1, U_2, U_Z\}$ по правилу преобразующего множества ставится в соответствие сигнал из множества $\{S\} = \{S_1, S_2, \ldots S_Q\}$. Тогда энтропия H_j раскрытая j - го сообщения будет принимать максимальные значения при независимом появлении сигналов из множества $\{S\}$.

Доказательство.

Пусть информационному множеству $\{U\}$ по закону преобразующего множества $\{M\}$ ставится в соответствие сигнал из множества $\{S\}$ с вероятностью $P(S_i)$. Вероятность появления сигнала S_i зависит от появления сигнала $S_{i-1}, S_{i-2} \ldots S_{i-n}$ и равна $P(Si / Si_{-1}, S_{i-2} \ldots)$.

Средняя условная энтропия $H_j(S_i / S_{i-1}, S_{i-2}, S_{i-3}, \ldots)$ этого события равна

$$H_j(S_i / S_{i-1}, S_{i-2}, S_{i-3} \ldots) = \sum_{k=1}^{i-1}\sum_{m=1}^{i-2}\ldots\sum_{r=1}^{i-n} P(S_k)P(S_m)\ldots P(S_r)\times$$
$$\times P(S_i / S_k, S_m \ldots S_r)\log_2 \frac{1}{P(S_i / S_k, S_m \ldots S_r)}. \quad (9)$$

Перейдя к натуральному логарифму и усредняя левую часть по k, m, r с весом $P(S_k)P(S_m)\ldots P(S_r)$ с учетом (4) получим с учетом (4) получим

$$\sum_{i=1}^{Q} P(S_i, S_k \ldots S_r)\ln \frac{1}{P(S_i / S_k, S_m \ldots S_r)} \le \sum_{i=1}^{Q} P(S_i)\ln \frac{1}{P(S_i)}. \quad (10)$$

Равенство $\mathbf{P(S_i) = P(S_i, S_k, S_m, S_r)}$ имеет место только при независимом появлении сигналов, что и требовалось доказать.

Сформулированные и доказанные выше теоремы определяют необходимые и достаточные условия теоретической недешифруемости динамического режима функционирования и не противоречат основным положениям теории Шеннона [3].

Таким образом, динамический режим функционирования может обеспечить требуемую защиту информации на физическим уровне. Но, по теории Шеннона, стойкость динамического режима функционирования, как и стойкость динамического режима функционирования, как и стойкость алгоритмов криптографического преобразовывания информации должна опираться не на теоретическую невозможность их раскрытия, а на практическую сложность такого раскрытия.

Следует отметить, что реализация динамического режима функционирования позволит решить проблему защиты космических систем связи и управления от несанкционированного доступа к каналу, обеспечить активную имито – и помехозащещенность.

ЛИТЕРАТУРА

1. Тузов Г.И., Урядников Ю.Ф., Прытков В.И. и др. Адресные системы управления и связи. Вопросы оптимизации. – М.: Радио и связь, 1993. – 384 с.

2. Кузьмин И.В., Кедрус В.А. Основы теории информации и кодирования. – К.: Вища школа, 1986. – 238 с.

3. Шеннон К.Э. Теории связи в секретных системах. – М.: ИЛ, 1963. – С. 333 – 402.