УДК 681.084

С.Ю. Стасев

Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков

МЕТОД ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В КОСМИЧЕСКИХ СИСТЕМАХ СВЯЗИ И УПРАВЛЕНИЯ

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

Ключевые слова: *безопасность связи, динамическая передача сигналов.*

Введение

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.

Анализ литературы. Проведенные к настоящему времени исследования показали [1 – 8], 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.

Цель статьи разработать метод обеспечения безопасности информации в космических системах связи и управления, базирующийся на динамической передаче сигналов.

Результаты исследований

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

Теорема 1.

Пусть информационному множеству $\{U\} = \{U_1, U_2, ..., U_Z\}$ по правилу преобразующего множества $\{M\}$ ставится в соответствие сигнал из множества $\{S\} = \{S_1, S_2, ..., S_Q\}$. 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 рассматриваемых множеств **U** и **S** можно представить в следующем виде:

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

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

Известно, что

$$H(U,S) = H(U) + H(U/S). \quad (2)$$

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 $H(U/S)$.

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

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

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

Следовательно,

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

В выражении (5) равенство выполняется при условии

$$P(U_j/S_i) \le P(U_j).$$

Выполнение этого условия возможно при статистической независимости U_j и S_i.

Тогда,

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

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

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

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 $\{S\} = \{S_1, S_2, ..., S_Q\}$. 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 $S_{i-1}, S_{i-2}, ..., S_{i-n}$ и равна $P(S_i / S_{i-1}, S_{i-2}...)$.

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

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

Перейдя к натуральному логарифму и усредняя левую часть по k, m, r с весом

$$P(S_k)P(S_m)...P(S_r)$$

с учетом (4) получим с учетом (4) получим

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

Равенство $P(S_i) = P(S_i, S_k, S_m, S_r)$ 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].

Выводы

Таким образом, динамический режим функционирования может обеспечить требуемую защиту информации на физическом уровне. Но, по теории Шеннона, стойкость динамического режима функционирования, как и стойкость динамического режима функционирования, как и стойкость алгоритмов криптографического преобразования 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 помехозащищенность.

Перспективы дальнейших исследований в данном направлении – разработка алгоритма защиты информации в космических системах связи и управления на основе предложенного метода.

Список литературы

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

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

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

4. Есин В.И. Безопасность информационных систем и технологий: учебное пособие / В.И. Есин, А.А. Кузнецов, Л.С. Сорока – Х.: ООО «Эдема», 2010 – 656 с.

5. Основы информационной безопасности: учеб. пособ. для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия-Телеком, 2006. – 544 с.

6. Горбенко І.Д. Захист інформації в інформаційно-телекомунікаційних системах: навч. посібн. Ч. 1 Криптографічний захист інформації / І.Д. Горбенко, Т.О. Гриненко. – Х.: ХНУРЕ, 2004. – 368 с.

7. Хорошков В.А. Методы и средства защиты информации / В.А. Хорошков, А.А. Чекатков; под ред. Ю.С. Ковтанюка. – К.: Издательство Юниор, 2003. – 504 с.

8. IDEA NXT Technical Descrition, MediaCrypt. – [Електрон. ресурс]. – Режим доступу до ресурсу: www.mediacrypt.com.

Надійшла до редколегії 4.06.2012

Рецензент: д-р техн. наук, проф. А.А. Кузнецов, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

МЕТОД ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В КОСМІЧНИХ СИСТЕМАХ ЗВ'ЯЗКУ І УПРАВЛІННЯ

С.Ю. Стасєв

Пропонується метод забезпечення безпеки інформації в космічних системах зв'язку і управління, що базується на динамічній передачі сигналів.

Ключові слова: *безпека зв'язку, динамічна передача сигналів.*

A METHOD OF PROVIDING OF DEFENCE OF INFORMATION IS IN SPACE COMMUNICATION AND MANAGEMENT NETWORKS

S.Yu. Stasev

The method of providing of safety of information is offered in space communication and management networks, being based on the dynamic transmission of signals.

Keywords: *safety of connection, dynamic transmission of signals.*