Космічна наука і технологія. 1996. Т. 2. № 5-6. С. 64—68.

УДК 621.391

Безопасность информации в космических системах связи и управления

И. Д. Горбенко[1], **Ю. В. Стасев**[2]

[1]Інститут інформаційних технологій НАН України, Харків

[2]Харківський військовий університет

Надійшла до редакції 10.04.96

Пропонується новий метод забезпечення безпеки інформації в космічних системах зв'язку та керування, що базується на динамічній передачі сигналів. Доводиться адекватність даного методу з методами криптографічного перетворення інформації. Формулюються і доводяться необхідні і достатні умови реалізації динамічного режиму функціонування.

1. ВВЕДЕНИЕ

Создание и применение систем космической связи и управления является одним из наиболее развитых направлений практического использования космического пространства. В настоящее время созданы и десятки лет эксплуатируются более 40 систем космической связи и управления как коммерческого, так и военного назначения. Опыт эксплуатации этих систем показывает, что требуемое качество их функционирования в существенной мере зависит от решения проблемы безопасности передаваемой информации. Решение проблемы безопасности информации, передаваемой в космических системах связи и управления, связывают с решением проблем помехозащищенности и имитостойкости. Многочисленные исследования показывают, что в настоящее время эти проблемы решаются раздельно. Проблема помехозащищенности решается либо за счет увеличения энергетических ресурсов космической радиолинии, либо за счет применения на физическом уровне сложных сигналов с частотной избыточностью. Требуемая имитостойкость обеспечивается посредством преобразования дискретной информации с использованием специальной аппаратуры.

Однако в такой концепции защиты информации, как показали исследования, не реализуются потенциальные возможности космических систем связи и управления, достигаемые за счет динамической передачи сигналов, при которой соответствие «информационный символ — сигнал-переносчик» изменяется во времени по псевдослучайному закону. Идея динамической передачи сигналов была высказана в 1980-х годах и нашла воплощение в системе MILSTAR (США) (Тузов и др., 1993). Ряд фирм, например Transcrypt Europe (Великобритания), Metricom (США) и другие, связывают решение проблемы безопасности информации с реализацией режима динамической передачи сигналов.

Реализация режима динамической передачи сигналов позволяет на физическом уровне решить проблему защиты от несанкционированного доступа к каналу, а также обеспечивает скрытие смыслового содержания передаваемых сообщений. Кроме того, реализация режима динамической передачи сигналов обеспечивает активную имитозащиту системы — защиту, при которой имитационные сигналы воспринимаются получателем информации как помеховые. Однако широкое внедрение режима динамической передачи сигналов в системы безопасности информации сдерживается, по нашему

мнению, отсутствием строгих доказательств адекватности данного метода передачи сигналов и методов криптографического преобразования информации.

В статье на основе теории Шеннона доказываются возможности обеспечения безопасности информации на физическом уровне и формулируются требования к реализации режима динамической передачи сигналов.

2. МОДЕЛЬ ДИНАМИЧЕКОГО РАДИОКАНАЛА

Структурная схема системы космической связи и управления, реализующая режим динамической передачи сигналов, представлена на рисунке.

Источник сообщений порождает открытое сообщение $\{U\} = \{U_1, U_2, ..., U_Z\}$, содержащие символы некоторого конечного алфавита, в качестве которого часто используется двоичный алфавит {0, 1}. Устройство кодирования отображает информационные символы во множество сигналов $\{S\} = \{S_1, S_2, ..., S_Q\}$. В системах, в которых не реализуется режим динамической передачи сигналов, это преобразование имеет вид

$$S_j = F(U_j). \quad (1)$$

Отметим, что сигнал S_i является функцией алфавита открытого сообщения и не изменяется во времени. Как следует из рисунка, на приемной стороне выполняется обратное преобразование вида

$$U_j^* = F(S_i). \quad (2)$$

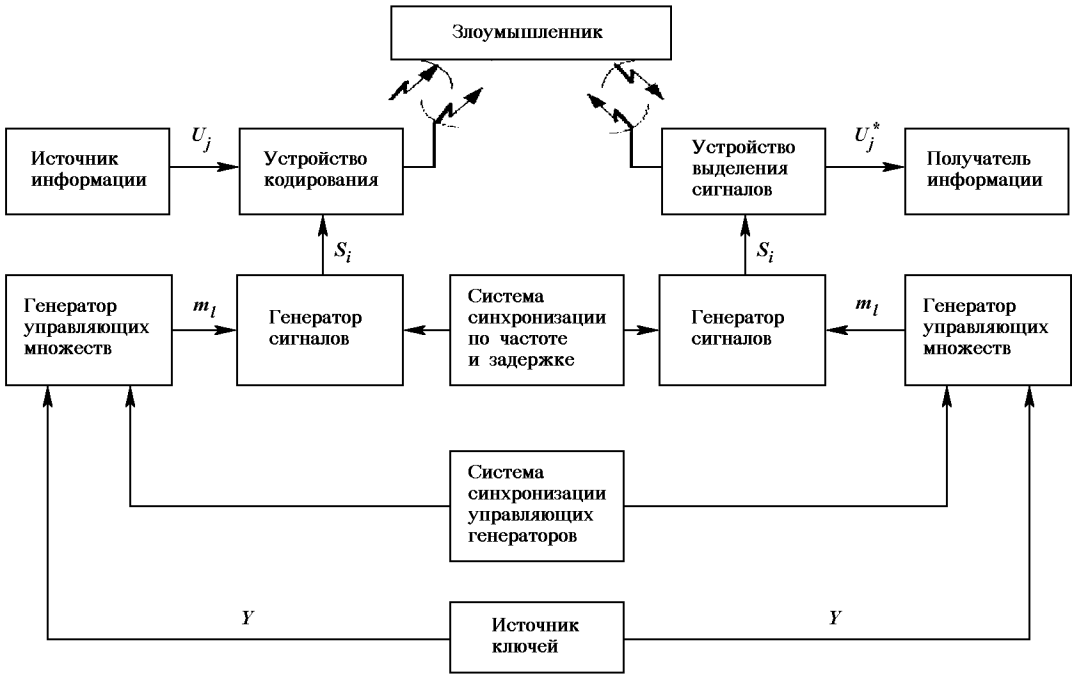
Злоумышленник, принимая сигналы S_i и выполняя преобразование вида (2), восстанавливает открытое сообщение.

Реализация режима динамической передачи сигналов предполагает, что соответствие «информационный символ — сигнал-переносчик» изменяется во времени по закону управляющего множества $\{M\} = \{m_1, m_2, ..., m_n\}$:

$$S_j = F(U_j, m_l). \quad (3)$$

В этом случае соответствие сигнала S_i информационному символу U_i определяется не только информационными символами, но и элементами управляющего множества $\{M\}$.

Синхронность работы наземной и бортовой аппаратуры обеспечивают системы синхронизации по частоте и задержке, а также генераторов управляющих множеств.



Структурная схема системы космической связи и управления, реализующая режим динамической передачи сигналов

Важной частью такой системы является конфиденциальный ключ, порожденный в источнике ключа и защищенный от перехвата. Используемые в космической системе связи и управления ключи, в зависимости от реализованного алгоритма формирования управляющего множества, могут быть как симметричными (совпадающими в наземной и бортовой аппаратуре), так и несимметричными (не совпадающими).

В дальнейшем будем полагать, что злоумышленнику известны все детали процесса формирования множеств $\{S\}$ и $\{M\}$, кроме используемых ключей Y.

3. НЕОБХОДИМЫЕ И ДОСТАТОЧНЫЕ УСЛОВИЯ НЕДЕШИФРУЕМОСТИ ДИНАМИЧЕСКОГО РЕЖИМА ФУНКЦИОНИРОВАНИЯ

Если с точки зрения злоумышленника любой сигнал S_i является отображением j-го значения сообщения U_j, то при независимом появлении сигналов энтропия раскрытия n элементов сообщения будет определяться

$$H = \sum_{j=1}^{n} H_j, \tag{4}$$

где H_j — частная энтропия раскрытия j-го сообщения.

Физически энтропия раскрытия j-го сообщения представляет собой математическое ожидание количества информации в одном сообщении о множестве, реализующем динамический режим функционирования.

Определим условия недешифруемости множества, реализующего динамический режим функционирования. Для этого 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 U и S можно представить в виде

$$H(U, S) = -\sum_{j=1}^{Z} \sum_{i=1}^{Q} P(U_j, S_i)\log_2 P(U_j, S_j), \tag{5}$$

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

Известно, что

$$H(U, S) = H(U) + H(U/S). \tag{6}$$

В выражении (6) $H(U, S)$ принимает максимальное значение, если $H(U)$ и $H(U/S)$ максимальны.

В работе Кузьмина и др. (1986) показано, что $H(U)$ принимает максимальное значение при статистически независимых сообщениях.

Найдем максимум $H(U/S)$

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

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

$$H(U/S) \le H(U). \tag{8}$$

Следовательно,

$$-\sum_{j=1}^{Z} \sum_{i=1}^{Q} P(U_j, S_i)\log_2 P(U_j/S_i) \le -\sum_{j=1}^{Z} P(U_j)\log_2 P(U_j). \tag{9}$$

В выражении (9) равенство имеет место при условии

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

Выполнение этого условия возможно при статистической независимости U_j и S_i. Следовательно,

$$P(U_j, S_i) = P(U_j)P(S_i). \tag{10}$$

Подставив (10) в (7), получим

$$H(U/S) = -\sum_{j=1}^{Z} \sum_{i=1}^{Q} P(U_j)P(S_i)\log_2 P(U_j). \tag{11}$$

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

$$H(U/S) = -\sum_{j=1}^{Z} P(U)\log_2 P(U_j) = H(U). \tag{12}$$

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 раскрытия 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 PS_i. Вероятность появления сигнала S_i зависит от появления сигнала S_{i-1}, S_{i-2}, ..., S_{i-n} и равна $P(S_i/S_{i-1}, S_{i-2},...)$. Тогда согласно работе Кузьмина и Кедруса (1986) справедливо неравенство

$$H_j(S_i/S_{i-1}, S_{i-2}, S_{i-3}, \ldots) \le H_j(S_i). \qquad (13)$$

Средняя условная энтропия H_j равна

$$H_j(S_i/S_{i-1}, S_{i-2}, S_{i-3}, \ldots) =$$

$$= \sum_{k=1}^{i-1} \sum_{m=1}^{i-2} \ldots \sum_{r=1}^{i-m} P(S_k)P(S_m) \ldots P(S_r) \times$$

$$\times P(S_i/S_k, S_m, \ldots, S_r)\log_2 \frac{1}{P(S_i/S_k, S_m, \ldots, S_r)}. \qquad (14)$$

Преобразуем выражение (13) и (14) к виду

$$\log e \sum_{k=1}^{i-1} \sum_{m=1}^{i-2} \ldots \sum_{r=1}^{i-n} P(S_k)P(S_m)P(S_r)P(S_i/S_k, S_m, \ldots, S_r)\times$$

$$\times \log \frac{1}{P(S_i/S_k, S_m, \ldots, S_r)} \le \log e \sum_{i=1}^{Q} P(S_i)\ln \frac{1}{P(S_i)}. \qquad (15)$$

Усредняя левую часть (15) по k, m, r с весом $P(S_k)P(S_m)P(S_r)$, получим

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

$$\le \sum_{i=1}^{Q} P(S_i)\ln \frac{1}{P(S)}. \qquad (16)$$

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

Теорема 3. Пусть информационному множеству $\{U\} = \{U_1, U_2, \ldots, U_z\}$ по закону преобразующего множества $\{M\} = \{m_1, m_2, \ldots, m_n\}$ ставится в соответствие сигнал из множества $\{S\} = \{S_1, S_2, \ldots, S_Q\}$. Тогда условная энтропия источника, задающего динамический режим функционирования, после перехвата сообщения $H(M/U)$ будет принимать максимальные значения при независимом появлении элементов из множества $\{M\}$ от информационного множества $\{U\}$.

Доказательство. Определим $H(M/U)$ как

$$H(M/U) = \sum_{k=1}^{z} \sum_{i=1}^{m} P(m_i)P(U_k/m_i) = \log \frac{1}{P(U_k/m_i)}.$$

Действительно, если злоумышленник при перехвате k сигналов $k = 1, 2, \ldots, Z$, не может уточнить имеющиеся у него априорные вероятности на основе вычисления апостериорных вероятностей

$$P(U_j/m_i) = P(U_j)P(m_i/U_j);$$

$$P(S_i/U_j) = \frac{P(m_i)P(U_j/m_i)P(m_i)}{P(U_j)}; \qquad (17)$$

т. е.

$$P(U_j/m_i) = P(U_j);$$

$$P(m_i/U_j) = P(m_i), \qquad (18)$$

то задача раскрытия закона изменения преобразующего множества сводится к методам статистического опробования всевозможных вариантов, а условная энтропия $H(M/U)$, определяемая выражением

$$H(M/U) = H(M) = \sum_{k=1}^{m} P(m_k)\log \frac{1}{P(m_k)} \qquad (19)$$

принимает максимальное значение при независимом появлении элементов из множества $\{M\}$ от информационного множества $\{U\}$.

4. ТРЕБОВАНИЯ К ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ ДИНАМИЧЕСКОГО РЕЖИМА ФУНКЦИОНИРОВАНИЯ

Сформулированные и доказанные выше теоремы определяют необходимые и достаточные условия теоретической недешифруемости динамического режима функционирования и не противоречат основным положениям теории Шеннона (1963).

Практическая реализация динамического режима функционирования в космических системах связи базируется на следствиях из теорем 1—3.

Следствие 1. Количество информации о преобразующем множестве, задающем динамический режим функционирования, определяемое выражением

$$I(U, M) = H(M) - H(M/U), \qquad (20)$$

равно нулю, если условная энтропия источника, задающего динамический режим функционирования, максимальна.

Следствие 2. Избыточность, содержащаяся в информации о преобразующем множестве, определяемая выражением

$$D = \frac{H(M) - H(M/U)}{H(M)}, \qquad (21)$$

равна нулю, если условная энтропия источника, задающего динамический режим, максимальна.

Результаты исследований показывают, что при практической реализации динамического режима функционирования должны выполняться следующие условия:

— вероятность передачи сигнала не должна зависеть от передаваемых информационных символов и переданных ранее сигналов;
— размер ансамбля используемых сигналов должен удовлетворять требованиям по имито- и помехозащищенности;
— стойкость управляющего множества, задающего динамический режим функционирования не должна снижаться в случаях, когда злоумышленникам становится известен метод реализации динамического режима;
— избыточность, содержащаяся в информации о множестве, задающем динамический режим функционирования, должна быть минимальна.

5. ЗАКЛЮЧЕНИЕ

Выше мы отметили, что динамический режим функционирования может обеспечить требуемую защиту информации на физическом уровне. Однако согласно работе Шеннона (1963), 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, обеспечит активную имито- и помехозащищенность.

Кузьмин И. В., Кедрус В. А. Основы теории информации и кодирования. — Киев: Вища школа, 1986.—238 с.

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

Шеннон К. Э. Теории связи в секретных системах // Работы по теории информации и кибернетике. — М: Изд-во инлстр. лит-ры, 1963.—С. 333—402.

INFORMATION SECURITY IN SPACE COMMUNICATION AND CONTROL SYSTEMS

I. D. Gorbenko and Yu. V. Stasev

We propose a new method for providing information security in space communication and control system. The method is based on dynamic signaling, and it is similar to the methods of cryptographic transformations of information. Necessary and sufficient conditions for the realization of dynamic operation mode are formulated.