УДК 621.396

НЕОБХОДИМЫЕ УСЛОВИЯ СУЩЕСТВОВАНИЯ УПРАВЛЯЮЩИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ РЕАЛИЗАЦИИ ДИНАМИЧЕСКОГО РЕЖИМА ФУНКЦИОНИРОВАНИЯ КОМАНДНО-ТЕЛЕМЕТРИЧЕСКИХ РАДИОЛИНИЙ УПРАВЛЕНИЯ КОСМИЧЕСКИМИ АППАРАТАМИ

Д.Н. Воронов, Ю.С. Литвинов, А.Л. Гостев, В.Н. Шлокин
(Объединенный научно-исследовательский институт ВС Украины, Харьков)

В статье обоснованы необходимые условия существования управляющих последовательностей, а также разработаны требования к их структурным и корреляционным свойствам при реализации динамического режима функционирования командно-телеметрических радиолиний управления космическими аппаратами.

управляющие последовательности, структурные и корреляционные свойства, динамический режим функционирования, космические аппараты

Введение. Успехи одного направления всегда находятся под пристальным вниманием разработчиков другого, что создает дополнительный стимул к совершенствованию образцов, поиску новых технических решений, а часто и к взаимному использованию результатов проектирования и творческих находок (научных, схемотехнических, конструктивных). Такое многолетнее тесное содружество-соперничество обеспечивает, как правило, поочередное превосходство техники то в одной, то в другой области, но в любом случае направлено на достижение максимальных результатов в каждой из них.

Действительность характеризуется ростом вычислительной способности и эффективности систем РЭБ. Быстро развивается и совершенствуется техника, с помощью которой противник вскрывает смысловое содержание передаваемых сообщений, пытается их имитировать или подавить каналы связи и управления. Все вышесказанное вызывает сложность обеспечения стабильной, надежной и эффективной связи.

В свете этого особую актуальность приобретает задача обеспечения достоверности и скрытности информации, передаваемой в системах космической связи и управления [2]. Опыт эксплуатации таких систем показывает, что требуемое качество их функционирования в существенной мере зависит от решения задачи имитостойкости и помехозащищен-

ности командно-телеметрической радиолинии. В настоящее время данные задачи решаются раздельно. Задача обеспечения помехозащищенности решается либо за счет увеличения энергетических ресурсов космической радиолинии, либо за счет применения на физическом уровне сложных сигналов с частотной избыточностью [9]. Требуемая имитостойкость обеспечивается посредством преобразования дискретной информации с использованием специальной аппаратуры [8].

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.

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 применение режима динамической передачи сигналов сдерживается отсутствием строгих доказательств адекватности данного метода передачи сигналов и методов криптографического преобразования информации.

Постановка проблемы и анализ предыдущих исследований. Обеспечить требуемую достоверность информации и команд в радиоканалах управления космическими аппаратами возможно при реализации в них динамического режима «бегущий код» [7]. В [12, 13] был обоснован алгоритм, реализующий динамический режим функционирования, определены и доказаны условия недешифруемости множества (управляющей последовательности), задающего динамический режим функционирования. В [1, 10] был проведен анализ структурных и корреляционных свойств некоторых сложных сигналов, которые можно применять при реализации динамического режима функционирования. Однако, актуальным остается вопрос формирования управляющих последовательностей, необходимых для реализации динамического режима функционирования, обладающих определенными заданными свойствами. Важнейшими из них являются корреляционные и структурные свойства управляющих последовательностей.

Целью данной статьи является обоснование необходимых условий существования и разработка требований к структурным и корреляционным свойствам управляющих последовательностей, необходимым для

реализации динамического режима функционирования командно-телеметрических радиолиний управления космическими аппаратами.

Основная часть. Анализ требований, предъявляемых к практической реализации динамического режима функционирования, проведенный в [11, 14], а также анализ особенностей функционирования командно-телеметрической радиолинии управления космическим аппаратом показали, что основным ограничением будет необходимость работы в реальном масштабе времени при стартстопном методе последовательной передачи и обработки команд и существенных ограничениях на длину передаваемой команды.

Результаты сравнения рассмотренных в [3, 5, 6, 8] методов реализации динамического режима функционирования позволили сделать вывод о том, что единственным методом, который может использоваться в командно-телеметрической радиолинии управления космическим аппаратом, является метод формирования имитовставки на основе поточного преобразования. Это связано с тем, что формирование имитовставки методом поточного преобразования обеспечивает требуемую имитостойкость при ограниченной длине блока (длине команды) и работу в стартстопном режиме передачи команд в реальном масштабе времени [4]. Кроме того, при его использовании появляется возможность формирования различных последовательностей управления по одному и тому же алгоритму.

Проведенные исследования показали, что защищенная команда управления космическим аппаратом может быть сформирована в виде [8].

Достоверное восстановление открытого сообщения U_i возможно лишь в том случае, если сообщение (команда) не искажена, а управляющая последовательность w_i формируется на приемной стороне синхронно с передающей.

При поточном методе формирования управляющей последовательности w_i элементы этой последовательности удовлетворяют рекуррентному соотношению вида [15]

$$w_{n+j} = a_0 w_j + a_1 w_{j+1} + a_2 w_{j+2} + \ldots + a_{n-1} w_{j+n-1}, \qquad (1)$$

где $j = 0, 1, 2, \ldots; n > 0$.

В (1) a_i и w_j принадлежат полю GF(p).

Одним из основных требований, предъявляемых к управляющим последовательностям, является требование к их корреляционным и структурным свойствам.

Сформулируем требования к структурным и корреляционным свой-

ствам управляющих последовательностей.

Пусть уровень боковых лепестков периодической функции автокорреляции управляющей последовательности {W} с числом элементов L ограничен значениями $R_{min}(l) \div R_{max}(l)$, где l – номер циклического сдвига функции корреляции. Тогда система неравенств, определяющая границы вектора автокорреляции во временной области {W} сигнала имеет вид

$$\begin{cases} R(0) = w_1 w_1 + w_2 w_2 + \ldots + w_L w_L; \\ R_{min}(1) \le w_1 w_2 + w_2 w_3 + \ldots + w_L w_1 \le R_{max}(1); \\ R_{min}(2) \le w_1 w_3 + w_2 w_4 + \ldots + w_L w_2 \le R_{max}(2); \\ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \\ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \\ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \\ R_{min}(L-1) \le w_1 w_L + w_2 w_1 + \ldots + w_L w_{L-1} \le R_{max}(L-1), \end{cases} \quad (2)$$

где w_i – элемент управляющей последовательности {W}, $w_i = \{\pm 1\}$.

Требуется определить w_i, удовлетворяющие условию (2) с учетом взаимокорреляционных и ансамблевых характеристик управляющей последовательности, т.е. определить множество управляющих последовательностей $\{W^j\}$ где $j = \overline{1,M}$; M – размерность ансамбля управляющих последовательностей с заданными авто- и взаимокорреляционными свойствами.

Запишем условие того, что управляющие последовательности W^k и W^j имеют периодическую функцию взаимной корреляции, ограниченную значениями $R^{kj}_{min}(l) \div R^{kj}_{max}(l)$ в виде системы нелинейных неравенств:

$$\begin{cases} R^{kj}_{min}(0) \le w^k_1 w^j_1 + w^k_2 w^j_2 + \ldots + w^k_L w^j_L \le R_{max}(0); \\ R^{kj}_{min}(1) \le w^k_1 w^j_2 + w^k_2 w^j_3 + \ldots + w^k_L w^j_1 \le R_{max}(1); \\ R^{kj}_{min}(2) \le w^k_1 w^j_3 + w^k_2 w^j_4 + \ldots + w^k_L w^j_2 \le R_{max}(2); \\ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \\ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \\ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \ \ldots \\ R^{kj}_{min}(L-1) \le w^k_1 w^j_L + w^k_2 w^j_1 + \ldots + w^k_L w^j_{L-1} \le R_{max}(L-1). \end{cases} \quad (3)$$

Проведенные исследования [5] показали, что система (2) при условии (3) в зависимости от L и $R(l)$ может иметь либо M решений, либо вообще не имеет решений.

Рассмотрим ограничения, накладываемые на L и R(l), т.е. определим необходимые условия существования двоичных дискретных управляющих последовательностей с заданными свойствами. С этой целью выразим R(l) через λ_l как число произведений вида $(+l)\cdot(+l)$ в выражении (3) для заданного l. Тогда число произведений вида $(+l)\cdot(-l)$ в (3) равно $(b - \lambda_l)$, где b – число единиц в управляющей последовательности. Число произведений $(-l)\cdot(+l)$ равно $[L - 2(b - \lambda_1) - \lambda_l]$. Учитывая, что произведения вида $(+l)\cdot(+l) = (-l)\cdot(-l)$, по аналогии с [5] получим:

$$\begin{cases} R_1 = L - 4(b - \lambda_1); \\ R_2 = L - 4(b - \lambda_2); \\ \ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots \\ R_n = L - 4(b - \lambda_n); \\ \lambda_1 n_1 + \lambda_2 n_2 + \cdots + \lambda_n n_n = b(b-1); \\ n_1 + n_2 + \cdots + n_n = L - 1, \end{cases} \tag{4}$$

где R_i – i-й уровень бокового лепестка периодической функции автокорреляции $R_{min}(l) \le R_i \le R_{max}(l)$, причем R_i значение имеет место n_i раз.

Анализ выражения (4) показывает, что λ_i также будет принимать n_i различных значений.

Определим величину b, положив

$$\begin{cases} \lambda_n = \lambda_{n-1} + Z_{n-1}; \\ \lambda_{n-1} = \lambda_{n-2} + Z_{n-2}; \\ \ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots \\ \lambda_2 = \lambda_1 + Z_1, \end{cases} \tag{5}$$

где Z_i – любое целое число.

Выразим из (4) λ_l и n_i как

$$\lambda_1 = \frac{R_1 - L + 4b}{4}; \tag{6}$$

$$n_1 = L - n_2 - n_3 - \cdots - n_n - 1; \tag{7}$$

$$\begin{cases} n_2 = n_1 + y_1; \\ n_3 = n_2 + y_2; \\ \ldots \quad \ldots \quad \ldots \\ n_n = n_{n-1} + y_{n-1}, \end{cases} \tag{8}$$

где y_i – любое целое число.

Решая систему (4) относительно b получим

$$\begin{aligned}&\frac{R_i - L + 4b}{4}\left[L - (n-2)n_2 - (y_2 + \cdots + y_{n-1}) - 1\right] + \\ &+\left(\frac{R1 - L + 4b}{4} + Z_1\right)n_2 + \left(\frac{Ri\ \ - L + 4b}{4} + Z_1 + Z_2\right)\cdot(n_2 - y_2) + \\ &+\cdots + \left(\frac{R_i - L + 4b}{4} + Z_1 + Z_2 + \cdots + Z_{n-1}\right)\times \\ &\times\left[(n-1)n_n + (y_2 + y_3 + \cdots + y_{n-1})\right] - b^2 + b = 0.\end{aligned} \tag{9}$$

После преобразований получим

$$L + \left\{\begin{matrix}L - (R_i + 1) - R_i + 4Z_1n_1 + 4(n_2 + y_2)(Z_1 + Z_2) + \\ +\cdots + 4\left[(n-1)n_2 + (y_2 + y_3 + \cdots + y_{n-1})\right](Z_1 + Z_2 + \cdots + Z_{n-1})\end{matrix}\right\}^{\frac{1}{2}} = 2b. \tag{10}$$

По условию b – натуральное число, следовательно, выражение в фигурных скобках также натуральное число Q, удовлетворяющее условию $Q \equiv a(\mathrm{mod}2)$. Тогда полагая, что $L = 4x + a$, а n_i принимает целые положительные значения, определим область допустимых значений Q.

Имеем

$$\begin{aligned}&4(4x + a)\left[(n-1)Z_1 + \cdots + Z_{n-1}\right] - 4\left[(n-1)Z_1 + \cdots + Z_{n-1}\right] + \\ &+ 4R_ix - R_ia - 4x - a \lhd Q.\end{aligned} \tag{11}$$

Если теперь определить значения Z_i, то выражение (11) определяет необходимые условия существования управляющих последовательностей с заданными свойствами.

Выводы. Таким образом, необходимые условия достаточно эффектно сужают множество сигналов, которые могут иметь функцию корреляции с n уровнями и заданным значением R_i, а также определяют условия к практической реализации динамического режима функционирования на физическом уровне. Реализация этих условий в командно-телеметрических радиолиниях управления космическими аппаратами обеспечивает активную имито- и помехозащиту.

ЛИТЕРАТУРА

1. *Воронов Д.Н. Анализ свойств сложных сигналов, используемых в радиолиниях управления космическими аппаратами // Системи обробки інформації. – Х.: НАНУ, ХВУ. – 1998. – С. 38-40.*
2. *Аутентификация и помехоустойчивость спутниковых систем связи // Материалы 1 МНТК. – Х.: ХГТУРЕ. – 1997. – С. 133.*

3. *Разработка аппаратно-программных средств имитозащиты командной информации в радиоканалах управления космическими аппаратами // Отчет об ОКР. – Х.: ХГТУРЭ, 1996. – Т. № 1. – 112 с.*
4. *Лебедев О.Г., Воронов Д.Н., Стасев Ю.В., Пастухов Н.В. Разработка аппаратно-программных средств имитозащиты командной информации в радиолиниях управления космическими аппаратами // Отчет об ОКР, шифр „Управление". – Х.: ХГТУРЭ, 1996. – 103 с.*
5. *Методика испытаний и экспериментальных исследований управляющих последовательностей // Отчет об ОКР, шифр „Управление-М". – Х.: ХГТУРЭ, 1996. – 87 с.*
6. *Спилкер Дж. Цифровая спутниковая связь: Пер. с англ. – М.: Связь, 1999. – 592 с.*
7. *Адресные системы управления и связи / Г.И. Тузов, Ю.Ф. Урядников, В.И. Прытков и др. Под ред. Г.И. Тузова. – М.: Радио и связь, 1993. – 384 с.*
8. *Совмещенная командно-измерительная система „Куб – Контур". – М., 1981. – 336 с.*
9. *Тузов Г.И., Сивов В.А., Прытков В.И. Помехозащищенность радиосистем со сложными сигналами / Под ред. Г.И. Тузова. – М.: Радио и связь, 1985. – 264 с.*
10. *Применение сложных сигналов в командно-телеметрических радиолиниях / Ю.В. Стасев, И.Д. Горбенко, Б.И. Макаренко, А.В. Ивашкин, Д.Н. Воронов // Космічна наука і технологія. – 1997. – Т. 3, № 5/6. – С. 104-108.*
11. *Воронов Д.Н., Касьянов О.В., Ткачев А.Н. Алгоритм повышения достоверности информации в космических системах связи и управления // Научные труды ХВУ. – Х.: ХВУ, 1998. – Вып. 17. – С. 116-119.*
12. *Воронов Д.Н., Ткачев А.Н., Трощило А.С. Алгоритмы формирования управляющих последовательностей // Управление и связь. – Х.: ХВУ. – 1998. – С. 122-125.*
13. *Ткачев А.Н., Воронов Д.Н., Носик А.М. Алгоритм формирования нелинейных ПСП // Зб. наукових праць. – Х.: ХВУ, 1998. – Вип. 17. – С. 119-122.*
14. *Воронов Д.Н., Линник Н.Ф. Алгоритм повышения достоверности информации в радиоканалах систем передачи информации // Системи обробки інформації. – Х.: ХВУ, 2004. – Вип. 4. – С. 46-49.*
15. *Завадская Л.А. Потоковые системы шифрования, основанные на регистрах сдвига // Безопасность информации. – 1995. – № 3. – С. 12-17.*

Поступила 5.01.2006

Рецензент: доктор технических наук, профессор В.И. Антюфеев,
Объединенный научно-исследовательский институт ВС Украины, Харьков.