УДК 006.91

УСЛОВИЯ ТЕОРЕТИЧЕСКОЙ НЕДЕШИФРУЕМОСТИ ДИНАМИЧЕСКОГО РЕЖИМА ФУНКЦИОНИРОВАНИЯ РАДИОСЕТИ УПРАВЛЕНИЯ

Ан.М. Носик[1], Ал.М. Носик[1], В.В. Калачева[2]
([1]Научный метрологический центр военных эталонов, Харьков,
[2]Харьковский университет Воздушных Сил им. И. Кожедуба)

Сформулированы необходимые и достаточные условия теоретической недешифруемости динамического режима функционирования радиосети управления, не противоречащие основным положениям теории Шеннона.

теоретическая недешифруемость, динамический режим, радиосеть управления

Постановка проблеми. Разработанные и нашедшие к настоящему времени широкое применение способы передачи информации в радиосети управления либо не обеспечивают требуемые значения помехозащищенности и имитостойкости, либо обеспечивают пассивную имитозащиту, заключающуюся в том, что при воздействии имитационных помех приемная аппаратура отключается. Обеспечить активную имито- и помехозащиту радиосети управления возможно при реализации динамического режима "бегущий код".

Анализ публикаций. Исследования проведенные до настоящего времени в работах [1, 2] показывают, что обеспечить необходимую защиту информации в радиосети управления возможно при реализации динамического режима "бегущий код". Однако стойкость динамического режима информации, как стойкость алгоритмов криптографичекого преобразования информации, как показано в [4] должна опираться не только на теоретическую невозможность ее разрытия, но и практическую сложность такого раскрытия.

Цель статьи: разработать необходимые и достаточные условия теоретической недешифруемости динамического режима функционирования радиосети управления.

Основная часть. 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.

Такой способ передачи информации позволяет не только обеспечить активную имитозащиту радиосети управления, но и повышает смысловую скрытность передаваемых сообщений. Структурная схема радиосети управления, реализующая динамический режим "бегущий код" представлена на рис. 1.

Источник сообщений порождает открытое сообщение $\{U\} = \{U_1, U_2, ..., U_z\}$, содержащие символы некоторого конечного алфавита, в качестве которого часто используется двоичный алфавит $\{0,1\}$.

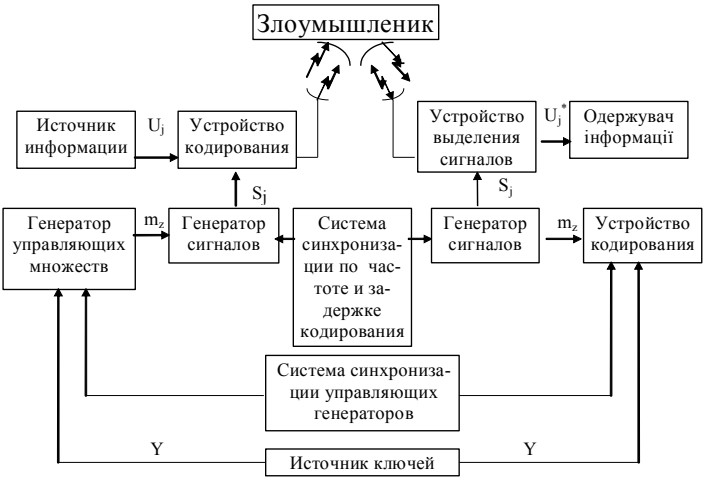

Рис. 1. Структурная схема радиосети управления

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. На приемной стороне выполняется обратное преобразование вида

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

Злоумышленник принимая сигналы S_i и выполнив преобразование вида восстанавливает открытое сообщение.

Реализация режима динамической передачи сигналов предполагает, что соответствие "информационный символ – сигнал переносчик" изменяется во времени по закону управляющего множества $\{M\} = \{m_1, m_2, ..., m_z\}$

$$S_j = \overline{F}(U_i, m_z). \quad (3)$$

В этом случае соответствие S_i сигнала U_i информационному символу 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.

Важной частью такой системы является конфиденциальный ключ, порожденный в источнике ключа и защищенный от перехвата. Используемые в радиосети управления ключи, в зависимости от реализованного алгоритма формирования управляющего множества, могут быть как симметричные (совпадающие в наземной и бортовой аппаратуре), так и несимметричные (не совпадающие).

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

Если с точки зрения противника любой сигнал S_i является отображением j-го значения сообщения U_j; то, при независимости появления сигналов энтропия раскрытия n-элементов сообщение будет определятся

$$H = \sum_{j=1}^{n} H_j, \quad (4)$$

где H_j – частная энтропия раскрытия j-го сообщения.

Физическая 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 чего докажем следующие теоремы.

Теорема 1. Пусть информационному множеству $\{U\} = \{U_1, U_2, ..., U_z\}$ по правилу преобразующего множества {M} ставиться 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 максимальное значение при независимом появлении сигналов и сообщений.

Доказательство.

Совместная энтропия совокупности U и S можно представить в виде:

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

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

Известно, что

$$H(U,S) = H(U) + H(U/S). \quad (6)$$

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

В [1] показано, что $H(U)$ принимает максимальное значение при статистически независимых сообщениях.

Найдем максимум $H(U/S)$:

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

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

$$H(U/S) \le H(U). \quad (8)$$

Следовательно

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

В выражении (9) равенство выполняется при условии

$$P(U_j/S_i) \le P(U_j). \quad (10)$$

Выполнение этого условия возможно при статистической независимости U_j и S_i.

Следовательно

$$P(U_j,S_i) = P(U_j)P(S_i). \quad (11)$$

Подставив (10) в (11) получим

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

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

$$H(U/S) = -\sum_{j=1}^{Z} P(U)\log_2 P(U_j) = H(U). \quad (13)$$

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 ставиться 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} ставиться 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-z} и равна $P(S_i / S_{i-1}, S_{i-2}, ...)$. Тогда, как следует из [2, 4] справедливо неравенство

$$H_j(S_i / S_{i-1}, S_{i-2}, S_{i-3}, ...) \le H_j(S_i). \qquad (14)$$

Средняя условная энтропия $H_j(S_i / S_{i-1}, S_{i-2}, S_{i-3}, ...)$ равна

$$H_j(S_i / S_{i-1}, S_{i-2}, S_{i-3}, ...) = \sum_{k=1}^{i-1}\sum_{m=1}^{i-2}\dots\sum_{r=1}^{i-m} P(S_k)\,P(S_m)\dots P(S_r)\times$$
$$\times P(S_i / S_k, S_m, \dots, S_r)\log_2 \frac{1}{P(S_i / S_k, S_m, \dots, S_r)}. \qquad (15)$$

Преобразуем выражение (14) и (15) к виду:

$$\log e \sum_{k=1}^{i-1}\sum_{m=1}^{i-2}\dots\sum_{r=1}^{i-m} P(S_k)\,P(S_m)\,P(S_r)\,P(S_i / S_k, S_m, \dots, S_r)\times$$
$$\times \log \frac{1}{P(S_i / S_k, S_m, \dots, S_r)} \le \log e \sum_{i=1}^{q} P(S_i)\ln \frac{1}{P(S_i)}.$$

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

$$\sum_{i=1}^{q} P(S_iS_k \dots S_r)\ln \frac{1}{P(S_i / S_k, S_m, \dots, S_r)} \le \sum_{i=1}^{q} P(S_i)\ln \frac{1}{P(S_i)}. \qquad (17)$$

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 $\{U\} = \{U_1, U_2, ..., U_z\}$ преобразующего множества $\{M\} = \{m_1, m_2, ..., m_a\}$ ставиться в соответствие сигнал из множества $\{S\} = \{S_1, S_2, ..., S_q\}$. 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

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

Действительно, если противник при перехвате k символов, $k = \overline{1, Z}$, не может уточнить имеющиеся у него априорные вероятности на основе вычисления апостериорных вероятностей:

$$H(U_j / m_i) = P(U_j)P(m_i / U_j); \quad H(S_i / U_j) = \frac{P(m_i)\, P(U_j / m_i)\, P(m_i)}{P(U_j)}, \quad (18)$$

т.е.

$$H(U_j / m_i) = P(U_j); \quad H(m_i / U_j) = P(m_i), \quad (19)$$

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

$$H(M / U) = H(M) = \sum_{k=1}^{n} P(m_k) \log \frac{1}{P(m_k)}, \quad (20)$$

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

Выводы. Реализация динамического режима функционирования позволит решить проблему защиты радиосети управления от несанкционированного доступа к каналам информации и обеспечить активную имито- и помехозащиту. Сформулированные и доказанные выше теоремы определяют необходимые и достаточные условия теоретической недешифруемости динамического режима функционирования и не противоречат основным положениям теории Шеннона (Шеннон К.Э., 1963 [3]).

Дальнейшие исследования будут направлены на практическую реализацию динамического режима функционирования на физическом уровне.

ЛІТЕРАТУРА

1. *Кузьмин И.В., Кедрус В.А. Основы теории информации и кодирования – К.: Вища школа, 1986. – 238 с.*
2. *Адресные системы управления и связи. Вопросы оптимизации / Г.И. Тузов, Ю.Ф. Урядников, В.И. Прытков и др.; Под ред. Г.И. Тузова. – М.: Радио и связь, 1993. – 384 с.*
3. *Шеннон К. Математическая теория связи / В. кн.: К. Шеннон Работы по теории информации и кибернетике. – М.: ИЛ, 1963. – С. 243-332.*
4. *Назаров Н.Г., Персиков В.А., Тарасенко В.Ф. О стойкости криптограмм использующих псевдослучайную последовательность чисел // Кибернетика. – 1983. – № 3. – С. 103-106.*

Поступила 26.01.2006

Рецензент: доктор технических наук, профессор Ю.В. Стасев,
Харьковский университет Воздушных Сил им. И. Кожедуба.