

## АЛГОРИТМ ПОВЫШЕНИЯ ДОСТОВЕРНОСТИ ИНФОРМАЦИИ В РАДИОКАНАЛАХ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ

к.т.н. Д.Н. Воронов, Н.Ф. Линник  
(представил д.т.н., проф. В.И. Долгов)

*Предлагается алгоритм повышения достоверности информации в радиоканалах систем передачи информации, базирующийся на динамической передаче сигналов.*

**Введение.** В настоящее время все более важное значение приобретает задача обеспечения достоверности и скрытности информации, циркулирующей в системах передачи информации (СПИ) самого различного назначения. Создание и применение СПИ является широко развитым направлением в технике связи. Однако, как показывает практика, существующие СПИ недостаточно хорошо защищены от несанкционированного проникновения и незаконного пользования информацией, циркулирующей в них. Особенно незащищенными являются радиоканалы СПИ. Опыт эксплуатации этих систем показывает, что требуемое качество их функционирования в существенной мере зависит от решения проблемы помехозащищенности и имитостойкости радиоканалов СПИ [1, 2, 5].

**Постановка проблемы и анализ предыдущих исследований.** Проведенные к настоящему времени исследования показали [1, 3], что обеспечить требуемую достоверность 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.

**Целью данной статьи** является обоснование алгоритма, реализующего динамический режим функционирования СПИ.

**Основная часть.** Определим условия недешифруемости множества, реализующего динамический режим функционирования. Динамический режим функционирования базируется на следующих теоремах.

**Теорема 1.** Пусть информационному множеству

$$\{U\} = \{U_1, U_2, \dots, U_Z\}$$

по правилу преобразующего множества  $\{M\}$  ставится в соответствие

сигнал из множества  $\{S\} = \{S_1, S_2, \dots, S_Q\}$ . 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

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

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

Известно, что

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

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

В [3] 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 условной энтропии  $H(U/S)$  справедливо неравенство

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

Следовательно,

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

В выражении (5) равенство выполняется при условии

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

Выполнение этого условия возможно при статистической независимости  $U_j$  и  $S_i$ .

Следовательно,

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

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

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

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

**Теорема 2.** Пусть информационному множеству

$$\{U\} = \{U_1, U_2, \dots, U_Z\}$$

по правилу преобразующего множества ставится в соответствие сигнал из множества  $\{S\} = \{S_1, S_2, \dots, S_Q\}$ . 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 правилу преобразующего множества  $\{M\}$  ставится в соответствие сигнал из множества  $\{S\}$  с вероятностью  $P(S_i)$ . Вероятность появления сигнала  $S_i$  зависит от появления сигнала  $S_{i-1}, S_{i-2}, \dots, S_{i-n}$  и равна  $P(S_i / S_{i-1}, S_{i-2}, \dots, S_{i-n})$ .

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

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

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

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

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

Сформулированные и доказанные выше теоремы определяют необходимые и достаточные условия теоретической недешифруемости дина-

мического режима функционирования и не противоречат основным положениям теории Шеннона [4].

**Выводы.** Таким образом, динамический режим функционирования может обеспечить требуемую защиту информации в СПИ на физическом уровне. Однако, по теории Шеннона, стойкость динамического режима функционирования, как и стойкость алгоритмов криптографического преобразования, 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 СПИ от несанкционированного доступа к каналу, а также обеспечить активную имито- и помехозащищенность.

## ЛИТЕРАТУРА

1. 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.
2. Линник Н.Ф. *Повышение помехоустойчивости систем передачи данных при применении усеченных ансамблей параллельных фазо-частотно-модулированных сигналов // Вестник Национального технического университета «ХПИ». Сборник научных трудов. Тематический вып.: Информатика и моделирование.* – Х.: НТУ «ХПИ». – 2003. – № 26. – С. 173 – 178.
3. Кузьмин И.В., Кедрус В.А. *Основы теории информации и кодирования.* – К.: Вища школа, 1986. – 238 с.
4. Шеннон К.Э. *Теория связи в секретных системах.* В кн. Шеннон К.Э. *Работы по теории информации и кибернетике.* – М.: Иностранная литература, 1963. – С. 333 – 402.
5. Рассомахин С.Г., Злыдень И.В., Линник Н.Ф. *Методы сокращения внеполосных излучений сигналов с комбинированной модуляцией // Системы обработки информации.* – Вып. 2(12). – Х.: НАНУ, ПАНМ, ХВУ. – 2001. – С. 163 – 165.

Поступила 20.02.2004

**ВОРОНОВ Дмитрий Николаевич**, канд. техн. наук, научный сотрудник научного центра при ХВУ. В 1995 году окончил ХВУ. Область научных интересов – защита информации в системах передачи данных.

**ЛИННИК Николай Федорович**, старший инженер научного центра при ХВУ. В 1986 году окончил ХВВКИУ. Область научных интересов – исследование частотных характеристик сложных сигналов.