**УДК 621.391.7-027.45**

# ОБЕСПЕЧЕНИЕ НАДЕЖНОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ В КАНАЛАХ С КОГНИТИВНОЙ СВЯЗЬЮ

ПАНЬКОВА В. В., САЛОМАТИН С. Б.

*Белорусский государственный университет информатики и радиоэлектроники*
*(г. Минск, Республика Беларусь)*

**Аннотация.** В работе рассмотрена модель передачи информации с когнитивной связью для возможности обеспечения в топологии сети области с надежным каналом передачи данных.

**Abstract.** The paper considers a model of information transfer with cognitive connection for the possibility of providing an area with a reliable data transmission channel in the network topology.

## Введение

Вопрос защиты информации требует комплексного подхода. Обязательным условием является использование наиболее приемлемых методов помехоустойчивого кодирования и криптографии. Не менее важное направление обеспечения безопасности в сетях передачи данных состоит в том, что обмен транзакциями должен выполняться только посредством надежного канала, который гарантирует аутентичность передаваемой информации, доказательства отправления и получения, а также невозможность отказа от самого факта обмена данными.

## Марковские каналы с когнитивной связью

Каналы с когнитивной связью используют кодеры, одному из которых заранее известно сообщение другого [1,2]. Используются два независимых сообщения $W_1 \in [1,2^{nR1}]$, $W_2 \in [1,2^{nR2}]$, которые передаются блоками размером $n$, со скоростями $R_1$ и $R_2$ соответственно. Легитимный приемник принимает сообщение $Y^n$, а подслушивающий – $Z^n$.

В режиме когнитивного кодирования один из пользователей формирует код $X_1^n$, кодируя сообщения $W_1$ и $W_2$ с помощью кодера $f_1$. Другой пользователь формирует код $X_2^n$, кодируя сообщение $W_2$ с помощью кодера $f_2$. В кодовых словах $X_1^n = f_1(W_1, W_2, S_1, S_{1,2})$ и $X_2^n = f_2(W_2, S_2, S_{1,2})$ используются независимые случайные переменные с произвольной энтропией $S_1$, $S_2$ и $S_{1,2}$, что делает процесс кодирования стохастическим.

Кодовые слова передаются по дискретному каналу без памяти с вероятностным распределением $p(y,z \mid x_1,x_2)$.

Декодеры принимают $Y = X_1 + X_2 + N_y$ и $Z = \alpha_1 X_1 + \alpha_2 X_2 + N_z$, где $N_y$ и $N_z$ – гауссовские случайные переменные, $\alpha_j$ – затухание сигнала в канале для несанкционированного узла. В процессе декодирования происходит вычисление оценок сообщений $g_n(Y^n) = (W_1^*, W_2^*)$.

Уровень секретности можно оценить, используя понятие условной энтропии канала подслушивания $H(W_1, W_2 \mid Z^n)$. При этом считаем, что скорости $(R_1, R_2)$ достижимы с малой вероятностью ошибки $P_e^{(n)} = Pr\{g_n(Y^n) \neq (W_1,W_2)\} \to 0$ и ограничением на секретность (нормализованная неопределенность) $H(W_1, W_2 \mid Z^n) \mid H(W_1, W_2) \to 1$.

Понятие емкости защищенного канала определим через замкнутое множество всех достижимых скоростей, при этом размеры такой емкости зависят от условных распределений $p(y \mid x_1, x_2)$ и $p(z \mid x_1, x_2)$.

Принимается, что каналы авторизованных пользователей менее зашумлены, чем подслушивающий канал, а распределение $p(z \mid x_1, x_2)$ удовлетворяет условию марковости $p(z \mid x_1, x_2) = \Sigma\, p(y \mid x_1, x_2)\, p'(z \mid y)$ для некоторого условного распределения $p'(z \mid y)$.

Определим кодовые книги пользователей как $V_1$ и $V_2$. Это означает, что для множества переменных, удовлетворяющих марковской цепи $V - (X_1, X_2) - (Y, Z)$, выполняется неравенство для количества информации $I(V; Y) - (V; Z) \geq 0$.

Скорости передачи, достижимые в защищенной области, удовлетворяют следующим неравенствам:

$$\mathrm{U}\{(R_1, R_2): R_1, R_2 \geq 0;\ R_1 \leq I(V_1; Y \mid V_2, Q) - I(V_1; Z \mid Q);\ R_2 \geq I(V_2; Y \mid V_1, Q) - I(V_2; X \mid Q);$$
$$R_1 + R_2 \leq I(V_1, V_2 \mid Q) - I(V_1, V_2; Z \mid Q)\},$$

где объединение берется по всем совместным распределениям вида

$$p(q)\, p(x_1, v_1 \mid q)\, p(x_2, v_2 \mid q)\, p(y, z \mid x_1, x_2),$$

а переменная $Q$ учитывает режим разделения времени.

Емкость дискретного канала с подслушиванием для возможного множества скоростей удовлетворяет неравенствам

$$R_1 \leq I(X_1; Y \mid X_2),\ R_1 + R_2 \leq (I(V_1, V_2; Y \mid Q) - I(V_1, V_2; Z \mid Q))$$

для распределений вида

$$p(q)\, p(v_1, v_2 \mid q)\, p(x_1, x_2 \mid v_1, v_2)\, p(y, z \mid x_1, x_2).$$

**Заключение**

Таким образом, в каналах с когнитивной связью происходит снижение эффективности прослушивания за счет работы подслушивающего узла сети в режиме приема на фоне помехи и, как следствие, обеспечивается возможность создания областей с более высоким уровнем защиты данных.

**Список использованных источников**

18. Giorgio Taricco A Lower Bound to the Receiver Operating Characteristic of a Cognitive Radio Network. arXiv: 1007.5408v1 [cs.IT] 30 Jul 2010.
19. C.R. Stevenson, G. Chouinard, Z. Lei, W. Hu, S.J. Shellhammer, and W. Caldwell, «IEEE 802.22: The first cognitive radio wireless regional area network standard», IEEE Communications Magazine, vol. 47, no.1, pp. 130-138, Jan. 2009.