

**В. В. Видякин** (Москва, ИТМиВТ РАН). **Необходимое и достаточное условие существования скрытого информационного канала.**

В работе [1] было дано следующее определение информационного канала.

**О п р е д е л е н и е 1.** Кorteж  $(\Omega, D_u, M_u, d_u)$ , где  $\Omega, D_u$  — любые множества,  $M_u$  — множество преобразований  $m_a^u(\omega), a \in D_u$  из  $\Omega$  в  $\Omega$ ,  $d_u(\omega)$  — отображение из  $\Omega$  на  $D_u$  такие, что для всех  $a \in D_u$  и  $\omega \in \Omega$

$$d_u(m_a^u(\omega)) = a, \quad (1)$$

называется *информационным каналом*.

Дадим уточненное определение непосредственного скрытого информационного канала.

**О п р е д е л е н и е 2.** Будем называть информационный канал  $(\Omega, D_f, M_f, d_f)$  *непосредственным скрытым информационным каналом канала*  $(\Omega, D_u, M_u, d_u)$ ,  $|D_f| \geq 2$ , если для любых  $a \in D_u$  и  $b \in D_f$

$$d_u(m_b^f(\omega)) = a \quad \text{для} \quad \forall \omega \in d_u^{-1}(a). \quad (2)$$

Введем следующие определения.

**О п р е д е л е н и е 3.** Информационный канал  $(\Omega', D_s, M_s, d_s)$  называется *подканалом канала*  $(\Omega, D_u, M_u, d_u)$ , если существует  $k > 1$  такое, что

$$D_s = D_u \setminus \{a : |d^{-1}(a)| < k\},$$

$$\Omega' = \Omega \setminus \bigcup_{a: |d^{-1}(a)| < k} d^{-1}(a),$$

$d_s$  есть ограничение  $d_u$  на множествах  $\Omega'$  и  $D_s$ ,  $M_s$  — множество преобразований  $m_a^s(\omega), a \in D_s$  из  $\Omega'$  в  $\Omega'$ , являющихся ограничениями  $m_a^u(\omega)$  на множество  $\Omega'$ . Значение  $k$  для которого выполняются условия определения будем называть рангом подканала  $(\Omega', D_s, M_s, d_s)$ .

**О п р е д е л е н и е 4.** Будем называть информационный канал  $(\Lambda, D_l, M_l, d_l)$  *скрытым информационным каналом канала*  $(\Omega, D_u, M_u, d_u)$ , если он является непосредственным скрытым информационным каналом одного из подканалов канала  $(\Omega, D_u, M_u, d_u)$ .

Исходя из введенных определений можно доказать следующее утверждение.

**Утверждение.** Пусть  $(\Omega, D_u, M_u, d_u)$  — информационный канал. Тогда существует скрытый информационный канал канала  $(\Omega, D_u, M_u, d_u)$  тогда и только тогда, когда отображение  $d_u$  небиективно.

Смысл утверждения состоит в том, что если существует некоторая неоднозначность при передаче информации по каналу, то имеется возможность манипуляции состоянием системы, незаметной для штатной системы контроля информационного канала.

## СПИСОК ЛИТЕРАТУРЫ

1. Видякин В. В. О связи скрытых информационных каналов и субпротоколов. — Обозрение прикл. и промышл. матем., 2006, т. 13, в. 1, с. 87–88.
2. Мартин Н., Ингленд Дж. Математическая теория энтропии. М.: Мир, 1988.
3. Инструментальный анализ мутных протоколов. / Под ред. А. В. Князева и А. Ф. Ронжина — Обозрение прикл. и промышл. матем., 2007, т. 14, в. 4, с. 577–646.