А. В. Б а б а ш (Москва, МЭСИ). **Период выходной последовательности обобщенного узла выборки при заданной входной периодической последовательности.**

Торетико-автоматный подход к синтезу управляющих блоков шифрсистем предполагает построение автоматов с гарантированными периодами выходных последовательностей. Классы таких автоматов представлены в работах [1–8]. Потребности криптографии многогранны. В данном докладе речь идет о построении обобщенных узлов выборки с гарантированныи периодами выходных последовательностей.

Обозначим X некий алфавит, $x \in X$, а X^∞ — множество всех бесконечных последовательностей алфавита X. Нас будут интересовать периодические последовательности из X^∞. Множество всех чисто периодических последовательностей из X^∞ обозначим $X^\infty_{\text{п}}$.

О п р е д е л е н и е. *Обобщенным узлом выборки шага* H (ОУВ *шага* H), $H \in \{1, 2, \ldots\}$, с параметрами $(k_1, k_2, \ldots, k_m; H)$, $m \leqslant H$, $k_j \in \{1, 2, \ldots, H\}$, $k_1 < k_2 < \cdots < k_m$, назовем устройство, реализующее отображение φ: $X^\infty \to X^\infty$ вида $\varphi(x_1, x_2, \ldots) = x(k_1), x(k_2), \ldots, x(k_m), x(H + k_1), x(H + k_2), \ldots, x(H + k_m), \ldots, x(jH + k_1), x(jH + k_2), \ldots, x(jH + k_m), \ldots$

Далее мы сохраняем обозначение φ для его ограничения на начальных словах $x(1), x(2), \ldots, x(L)$ бесконечной последовательности $x(1), x(2), \ldots$

Для введенного устройства ОУВ рассмотрим вектор $(\varepsilon(1), \varepsilon(2), \ldots, \varepsilon(H))$ из F_2^H, $F_2 = \{0, 1\}$, где $\varepsilon_j = 1$, $j \in \{1, 2, \ldots, H\}$, тогда и только тогда, когда $j \in \{k_1, k_2, \ldots, k_m\}$. Очевидно, такой вектор однозначно определяет ОУВ с параметрами $(k_1, k_2, \ldots, k_m; H)$. Рассмотрим вспомогательную двоичную последовательность

$$\varepsilon(1), \varepsilon(2), \ldots, \varepsilon(H), \varepsilon(1), \varepsilon(2), \ldots, \varepsilon(H), \varepsilon(1), \varepsilon(2), \ldots, \varepsilon(H), \ldots, \tag{1}$$

элементы данной последовательности повторяются через H шагов. Поэтому период этой последовательности является делителем величины H. Далее мы рассматриваем только так называемые «приведенные» ОУВ шага H, т. е. ОУВ, для которых период последовательности (1) совпадает с H.

Теорема. *Пусть* $x(1), x(2), \ldots$ — *периодическая входная последовательность периода* ω *устройства ОУВ с параметрами. Тогда период* W *выходной последовательности ОУВ* $\varphi((x(1), x(2), \ldots) = x'(1), x'(2), \ldots$ *является делителем величины* $(\text{НОК}(\omega, H)/H)m$. *Если дополнительно* $(H, \omega) = 1$, *то период* W *кратен* ω, $W = c\omega$, *где* c *делит* m. *Если выполнено еще одно дополнительное условие* $\omega > 3H - 2$, *то* $W = m\omega$.

СПИСОК ЛИТЕРАТУРЫ

1. *Бабаш А. В.* О периодичности последовательности состояний автомата, отвечающей его начальному состоянию и входной периодической последовательности. — Дискретн. матем., 2002, т. 14, в. 2, с. 54–64.
2. *Babash A. V.* Isoperiods of output sequences of automata. — Probabilistic Methods in Discrete Mathematics. Utrecht: VCP, 2002, p. 147–158.
3. *Бабаш А. В.* Внешне периодические автоматы. — Дискретн. матем., 2005, т. 17, в. 1.
4. *Бабаш А. В.* G-изопериод выходной последовательности автономного последовательного соединения автоматов. — Обозрение прикл. и промышл. матем., 2000, т. 7, в. 1, с. 87–88.
5. *Бабаш А. В.* Локальные периоды выходных последовательностей некоторых классов автоматов. — Обозрение прикл. и промышл. матем., 2000, т. 7, в. 1, с. 88–89.
6. *Бабаш А. В.* Приближенные периоды выходных последовательностей одного класса автономных автоматов. СПб.: 2000, с. 91–93.

7. *Бабаш А. В.* О периодах выходных последовательностей автоматов без потери информации при заданных периодических входных последовательностях. — Дискретн. матем., 2009, т. 21, в. 4.
8. *Бабаш А. В.* О периодичности выходных последовательностей автомата с потерей информации. — Ученые записки, 2010, № 3, с. 26–34.