**Д. В. Самойленко**, **О. А. Финько** (Краснодар, КВВУ (ВИ)).
**Оценка помехоустойчивости криптосистемы, основанной на Китайской теореме об остатках, для $N$ каналов с шумом и имитирующим злоумышленником.**

В [1–2] предложена модулярная помехоустойчивая криптографическая система (КС), способная противостоять непреднамеренным (шумы) и преднамеренным (имитирующим действиям аналитика) деструктивным воздействиям. Сущность КС состоит в том, что множеству криптограмм $0 \leqslant C^{(1)} < m^{(1)}, 0 \leqslant C^{(2)} < m^{(2)}, \ldots, 0 \leqslant C^{(n)} < m^{(n)}$ сопоставлены символам модулярного кода по соответствующим модулям $m^{(1)}, m^{(2)}, \ldots, m^{(n)}$. По дополнительно введенным $r$ модулям $m^{(n+1)}, \ldots, m^{(n+r)}$ вычисляются избыточные криптограммы $C^{(n+1)} = |X|_{m^{(n+1)}}, \ldots, C^{(n+r)} = |X|_{m^{(n+r)}}$, соответствующие избыточным элементам модулярного кода, где $X$ — решение системы сравнений: $X \equiv C^{(1)} \pmod{m^{(1)}}, X \equiv C^{(2)}\ 9\mathrm{mod}\, m^{(2)}, \ldots, X \equiv C^{(n)} \pmod{m^{(n)}}$, причем НОД $(m_i, m_j) = 1$ для $i, j = 1, 2, \ldots, n + r$, и $m^{(1)}, \ldots, m^{(n)} < m^{(n+1)} < \cdots < m^{(n+r)}$. В совокупности полученное множество криптограмм $C^{(1)}, c^{(2)}, \ldots, C^{(n+r)}$ образует избыточный модулярный $R$-код.

Пусть ошибки кратности $0 \leqslant q < l$, вызванные *непреднамеренными* воздействиями во множестве криптограмм $C^{(1)}, C^{(2)}, \ldots, C^{(n+r)}$, где $l$ — длина блока криптограммы, являются независимыми и вероятность их возникновения определяется *биномиальным* законом. Имитирующие действия аналитика на криптограмму $C^{(i)}$ носят аналитический характер, поэтому *преднамеренные* искажения в $C^{(i)}$ будем считать *равновероятными*, также пусть $p_{\mathrm{bit}}$ — вероятность искажения одного бита криптограммы, вызванная действиями аналитика. Тогда вероятность $q$-кратной ошибки в произвольной криптограмме $C^{(i)}$ для каналов связи с биномиальным распределением ошибок равна $p_{\mathrm{cr}.1} = p_{\mathrm{bit}} \sum_{i=q+1}^{n} \binom{n}{q} / 2^n$, где $\sum_{q=i+1}^{n} \binom{n}{q}$ — количество необнаруживаемых ошибок в $C^{(i)}$, $q$ $(i + 1 \leqslant q \leqslant n)$ — кратность необнаруживаемых ошибок, $2^n$ — количество всех возможных ошибок. Однако в предлагаемой КС вероятность $q$-кратной ошибки в произвольной криптограмме $C^{(i)}$ равна $p_{\mathrm{cr}.2} = p_{\mathrm{bit}}$, так как КС контролирует ошибки любой кратности в масштабе одной криптограммы $C^{(i)}$.

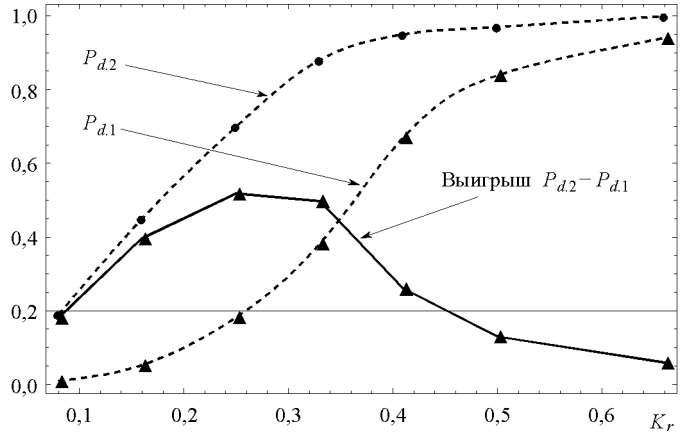
Тогда для КС-прототипа, в которой используются линейные коды, вероятность гарантированно обнаруживаемых ошибок равна

$$P_{d.1} = \sum_{q=1}^{n} \binom{n}{q} p_{\mathrm{cr}.1}^{q} (1 - p_{\mathrm{cr}.1})^{n-q},$$

а для предложенной КС вероятность гарантированно обнаруживаемых ошибок —

$$P_{d.2} = \sum_{q=0}^{d_{\min}-1} \binom{n}{q} p_{\mathrm{cr}.2}^{q} (1 - p_{\mathrm{cr}.2})^{n-q},$$

где $d_{\min}$ — минимальное кодовое расстояние. Зависимости $P_{d.1}$, $P_{d.2}$ и выигрыша $P_{d.1} - P_{d.2}$ от коэффициента избыточности применяемого (линейного в первом случае, модулярного во втором) кода представлены на рис. при ограничениях $p_{\mathrm{bit}} = 0,15$, $k = 12$. Здесь $K_r = 1 - n/k$ есть коэффициент избыточности, где $k = n + r$.




СПИСОК ЛИТЕРАТУРЫ

1. *Финько О. А.* Многоканальные модулярные системы, устойчивые к искажениям криптограмм. — В сб.: Международная научная конференция «Модулярная арифметика». http://www.computer-museum.ru/books/archiv/sokcon18.pdf.
2. *Финько О. А.* Групповой контроль асимметричных криптосистем методами модулярной арифметики. — В сб.: Научные труды XIV Международной школы-семинара «Синтез и сложность управляющих систем». Нижний Новгород: Изд-во Нижегородского пед. ун-та, 2003, с. 85–86.