**В. Н. Думачев, С. Б. Колесников** (Воронеж, ВИ МВД России). **Квантовые схемы измерения для автоморфной коррекции ошибок.**

При передаче информации по каналам связи она может искажаться. Стандартным методом коррекции ошибок является построение таблицы синдромов, по которой определяется ее место. Другим методом является алгоритм функционального определения места ошибки при помощи вычисления комбинаций проверочных битов принятого сообщения. В любом случае (вследствие нелинейности алгоритмов) протоколы коррекции требуют введения дополнительных бит для хранения синдрома или места ошибки. В работе, представленной данным сообщением, рассматривается автоморфный вариант квантового кода Хэмминга QH[7,4], не требующий привлечения дополнительных ресурсов памяти и позволяющий (при использовании имеющихся разрядов) перевести произвольную последовательность (имеющую не более одной ошибки) в неискаженное состояние.

Классическая теория построения кода Хэмминга предполагает добавление к информационной последовательности $(e_1, e_2, e_3)$ трех проверочных бит: $S = (e_1, e_2, e_3, e_4, 0, 0, 0)$. После этого значения информационных бит заносятся оператором $\mathbf{U}$ в проверочные биты согласно алгоритму:

$$S_1 = \mathbf{U}S = (e_1, e_2, e_3, e_4, e_1 \oplus e_2 \oplus e_4, e_1 \oplus e_3 \oplus e_4, e_2 \oplus e_3 \oplus e_4),$$

и сообщение $S_1$ отправляется в канал информации. Допустим, на выходе из канала информации последовательность имеет вид $O = (z_1, z_2, z_3, z_4, z_5, z_6, z_7)$. Действуя на нее тем же оператором $\mathbf{U}$, получим $O_1 = \mathbf{U}O = (y_1, y_2, y_3, y_4, y_5, y_6, y_7)$. Поскольку оператор $\mathbf{U}$ является линейным в базисе Жегалкина, на квантовом уровне он реализуется при помощи оператора CNOT: $\mathbf{P}_{12}\,|x, y\rangle = |x, x \oplus y\rangle$. В работе доказано следующее утверждение.

**Теорема.** *Для последовательности* $(z_1, z_2, z_3, z_4, z_5, z_6, z_7)$, *имеющей не более* 1-*го инвертированного бита*, *выполняются равенства*

$$(y_5 \& y_6 \& y_7) \oplus (y_5 \& y_6) \oplus y_1 = e_1, \quad (y_5 \& y_6 \& y_7) \oplus (y_5 \& y_7) \oplus y_2 = e_2,$$

$$(y_5 \& y_6 \& y_7) \oplus (y_6 \& y_7) \oplus y_3 = e_3, \quad (y_5 \& y_6 \& y_7) \oplus y_4 = e_4.$$

Данные равенства содержат нелинейные элементы, которые в теории квантовой информации могут быть реализованы вентилем Тоффоли $T_{123}\,|x, y, z\rangle = |x, y, (x \& y) \oplus z\rangle$. Наличие такого оператора позволяет построить автоморфный квантовый протокол исправления единичной ошибки. Так, на рис. показан блок коррекции квантового кода Хэмминга QH[7,4], реализованный как квантовая схема измерения, использующая операторы Паули $X = \sigma_1$, контролируемые измерительным прибором $I$.