В. М. Деундяк, **В. В. Мкртичян** (Ростов-на-Дону, ФГНУ НИИ «Спецвузавтоматика»)**. О границах применения специальной схемы защиты информации, основанной на ОРС-кодах.**

При решении ряда актуальных проблем защиты информации от несанкционированного доступа в последние годы интенсивно применяются современные методы теории помехоустойчивого кодирования [1]. В работе [2] рассмотрен перспективный способ защиты легально тиражируемой цифровой продукции от несанкционированного копирования, называемый *схемой специального широковещательного шифрования* (ССШШ). Известно, что злоумышленники, являющиеся легальными пользователями ССШШ, могут объединяться в коалиции мощности c и пытаться атаковать ССШШ. В [2] доказано, что для эффективного поиска всей коалиции мощности $c \geqslant 2$, или, по крайней мере, ее непустого подмножества, можно применять обобщенные коды Рида–Соломона (ОРС-коды) и списочный декодер Гурусвами–Судана с параметрами, зависящими от c. В [3], [4] построена математическая модель эффективной схемы специального широковещательного шифрования, проведено экспериментальное исследование надежности и применение ССШШ.

В работе, представленной данным сообщением, исследованы условия применения ССШШ, основанной на ОРС-кодах и списочном декодере Гурусвами–Судана, в случае превышения мощности коалиции c. С этой целью построена иерархия множеств компрометации легальных пользователей ССШШ, возникающей в ходе проверки контролером. Пусть C — ОРС-код, r_{00} — радиус работы декодера Гурусвами–Судана. Пусть $\Omega_1(C)$ — множество мощностей таких коалиций, при которых для некоторого кодового слова существует коалиция, у которой хотя бы один из потомков расположен на расстоянии не далее r_{00} от данного кодового слова. Пусть $\Omega_2(C)$ — множество мощностей всех коалиций, при которых для некоторого кодового слова существует такая коалиция, у которой хотя бы один из потомков расположен не далее от данного кодового слова, чем от любого элемента коалиции. Пусть $\Omega_3(C)$ — множество мощностей всех коалиций, при которых для некоторого кодового слова существует такая коалиция, у которой хотя бы один из потомков является данным кодовым словом. Доказывается, что $\Omega_3(C) \subseteq \Omega_2(C) \subseteq \Omega_1(C)$. Основным результатом работы являются оценки для мощности коалиции c, позволяющие определить степень компрометации невиновных пользователей в ходе проверки контролером.

СПИСОК ЛИТЕРАТУРЫ

1. Криптографические методы защиты информации. Кн. 4. М.: Радиотехника, 2007, 312 с.
2. *Silverberg A.*, *Staddon J.*, *Walker J.* Application of list decoding to tracing traitors. — In: Advances in Cryptology - ASIACRYPT 2001 (LNCS 2248), 2001, p. 175–192.
3. *Мкртичян В. В.* Об экспериментальном исследовании надежности и применении схемы специального широковещательного шифрования. — Известия ЮФУ. Технические науки, 2008, № 8, с. 203–210.
4. *Деундяк В. М.*, *Мкртичян В. В.* Математическая модель эффективной схемы специального широковещательного шифрования и исследование границ ее применения. — Известия вузов. Северо-Кавказский регион. Естественные науки, 2009, № 1, с. 5–8.