Б. Ф. Кирьянов, **Д. В. Кирьянов** (Великий Новгород, НовГУ).
Модель системы обмена конфиденциальной информацией по каналам связи.

Предлагается модель обмена информацией по компьютерным каналам связи с высокой степенью защиты информации от возможности ее «взлома».

Согласно модели, на объектах системы связи используются генераторы псевдослучайных кодов (ГПСК) на основе M-последовательностей. Каждый ГПСК может входить в режим синхронизма с генератором любого другого объекта. Для ввода в синхронизм генератора вызываемого объекта вызывающий объект с шагом t передает по каналу связи несколько кодов $X(t)$ генерируемой его ГПСК последовательности кодов. На вызываемом объекте при выполнении условия $X(t+1) = AX(t)$, где A — матрица над полем GF (2), определяющая работу генераторов, в ГПСК заносится код $X(t+1)$, и он начинает работать в режиме синхронизма с ГПСК вызвавшего его объекта. Ошибочное выполнение приведенного условия, обусловленное помехами в канале связи, приводит к ложному синхронизму ГПСК.

После установки синхронизма ГПСК выполняется следующее: с объекта-передатчика вместо последовательности ГПСК в канал связи посылается цифровой шум, обеспечивающий, в частности, синхронизацию ГПСК объекта-приемника; указанные ГПСК одновременно переходят на генерирование другой последовательности, которая в канал связи не передается и используется для определения моментов приема-передачи полезной информации; при появлении в выбранных разрядах ГПСК кода, принятого в качестве пароля на текущий интервал времени (например, на сутки), на объекте-передатчике в цифровой шум вставляется очередной фрагмент открытой или зашифрованной полезной информации; на объекте-приемнике этот фрагмент извлекается из цифрового шума и заносится в накопитель полезной информации.

Проведено моделирование процесса установления связи. При этом структуры ГПСК (матрицы A) определялись кодами из локальной базы данных. Ниже приведены значения оценок вероятностей P входа ГПСК двух объектов в правильный или в ложный синхронизм на указанных шагах t при вероятности q неверного приема двоичного символа, равной 0,2, 8-разрядных кодах и 100000 сеансах установления связи.

Интервал t	$t \leqslant 50$	$50 < t \leqslant 100$	$100 < t \leqslant 150$	$150 < t \leqslant 200$	$200 < t \leqslant 250$	$t > 250$
$P_{\text{синхр. пр.}}$	0,738	0,164	0,037	0,002	0,001	0
$P_{\text{синхр. ложн.}}$	0,039	0,008	0,002	0	0	0

Поскольку реально значение $q < 0,01$, полученные результаты свидетельствуют о высокой надежности установления ГПСК системы в синхронизм.