УДК 621.396

СПОСОБ ПОВЫШЕНИЯ ИМИТОСТОЙКОСТИ ЦИФРОВОЙ СИСТЕМЫ УПЛОТНЕНИЯ СИГНАЛОВ С ИСКУССТВЕННО СОЗДАВАЕМЫМИ ГРЕБЕНЧАТЫМИ СПЕКТРАМИ

к.т.н. Д.Н. Воронов, к.т.н. Ю.С. Литвинов, к.т.н. А.Г. Снисаренко
(представил д.т.н., проф. А.А. Рось)

В статье првдложен способ повышения имитостойкости цифровой системы уплотнения сигналов с искусственно создаваемыми гребенчатыми спектрами. Проведена оценка имитостойкости информации, циркулирующей в данной системе уплотнения сигналов с использованием предложенного способа.

Постановка проблемы. Анализ работы цифровой системы уплотнения сигналов с искусственно создаваемыми гребенчатыми спектрами (ЦСУС СГС), обеспечивающей уплотнение сигналов [1 – 3], показал, что принцип уплотнения сигналов позволяет обеспечить временную стойкость, не изменяя архитектуры системы. В [4] проведена оценка криптостойкости ЦСУС СГС. Более детальный анализ показал, что данная система не обладает достаточной имитостойкостью. Данный факт объясняется тем, что система разрабатывалась для других целей, а именно уплотнение сигналов с применением нового класса сигналов. Однако, как оказалось, принцип формирования спектра исходного выходного сигнала позволяет обеспечить криптостойкость на достаточно высоком уровне, имитостойкость при этом оказывается низкой, что является существенным недостатком при современных требованиях. Статья посвящена разработке способа повышения имитостойкости ЦСУС СГС, что позволит значительно расширить сферу применения данной системы.

Цель статьи. Разработать способ повышения имитостойкости ЦСУС СГС, оценить эффективность применения предложенного способа.

Разработка способа повышения имитостойкости ЦСУС СГС. Проблема имитостойкости систем передачи информации в настоящее время решается на основе криптографического преобразования дискретной информации.

Используемые алгоритмы базируются на вводе в информационные пакеты дополнительной избыточной информации, способной обнару-

жить попытки навязывания ложных сообщений и обеспечивают пассивную имитозащиту, основанную на отказе от принимаемой информации, если в принятом сообщении имеются ошибки. В ЦСУС СГС предлагается использовать один из каналов системы уплотнения для передачи сигналов синхронизации и дополнительной избыточной информации – имитовставки, содержащей в себе изменяющиеся во времени и содержания информации параметры. К этим параметрам отнесем:

– время передачи информационного пакета;
– дату передачи информационного пакета;
– количество работающих в данный момент времени каналов;
– признак обнуления счетчика информационных посылок;
– номер передаваемой информационной посылки;
– признак контроля четности;
– контрольный блок.

Контрольный блок формируется на основе специального преобразования с использованием значений всех параметров, рис. 1.

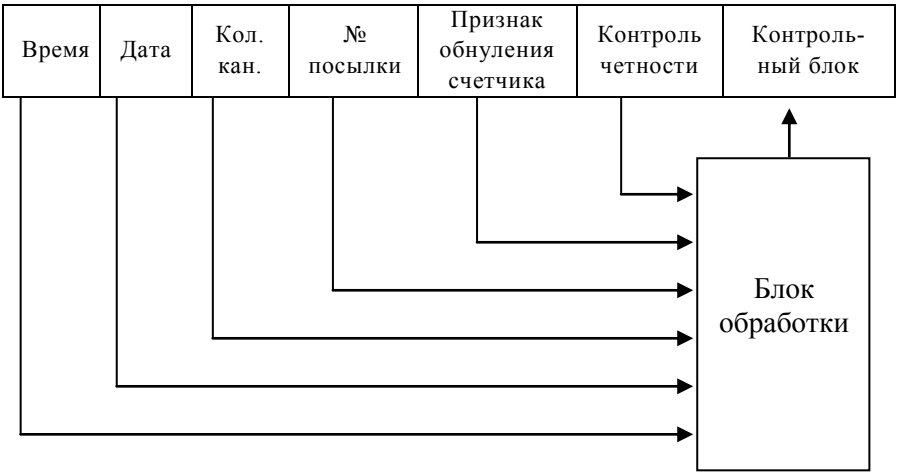

Рис. 1. Принцип формирования имитовставки

На приемной стороне производится аналогичное формирование с получением контрольного блока. Значения полученного и сформированного контрольного блока сравниваются. Если они не совпадают, принимается решение о ложности информационной посылки и отказе от принятой информационной посылки.

Оценить эффективность имитозащиты можно используя показатель вероятность имитации. Вероятность имитации в данном случае будет зави-

сеть от сложности вскрытия системы, поскольку не зная содержания имитовставки невозможно точно имитировать информационные пакеты. В любом случае такие пакеты будут отвергнуты. Процедура определения сложности вскрытия системы подробно описана в [4]. Согласно ей вероятность вскрытия одного канала системы определяется как [4]

$$P = 1 \Big/ \nu^{n}, \tag{1}$$

где ν – число степеней свободы, определяемое как [4]

$$\nu = 180 \Big/ \arcsin \frac{p}{n} \cdot \frac{90}{\pi}, \tag{2}$$

где p – проекция вектора шумов неортогональности; n – размерность образующей матрицы (количество каналов в системе).

Оценить вероятность имитации информации, передаваемой в ЦСУС СГС можно используя выражение (3)

$$P_{им} = P_{вскр} \frac{1}{n}, \tag{3}$$

где n – количество каналов в системе уплотнения.

Зависимость вероятности имитации информации, передаваемой в ЦСУС СГС от количества каналов в системе уплотнения n приведена на рис. 2.

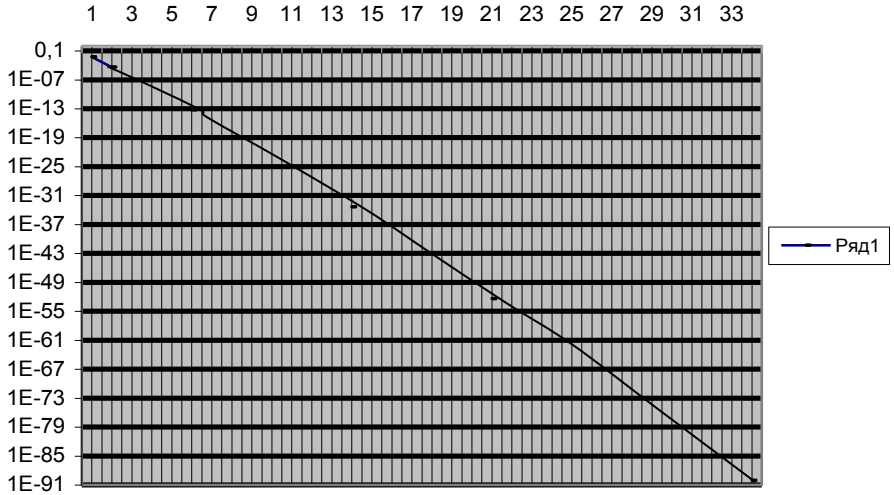

Рис. 2. Зависимость вероятности имитации информации, передаваемой в ЦСУС СГС от количества каналов в системе уплотнения n

Из графика зависимости видно, что вероятность имитации умень-

шается с увеличением числа каналов в системе и увеличением сложности вскрытия каналов цифровой системы уплотнения сигналов с искусственно создаваемыми гребенчатыми спектрами.

Выводы. Разработан способ повышения имитостойкости ЦСУС СГС. Получен выигрыш по имитостойкости при незначительном снижении пропускной способности. ЦСУС СГС способна обеспечить безопасность информации с временной стойкостью и с достаточной имитостойкостью, что в комплексе позволяет достичь очень высоких показателей безопасности передаваемой информации, а также использовать данную систему в самых различных областях применения.

ЛИТЕРАТУРА

1. *Рассомахин С.Г., Лученко С.В. Способ объединения сигналов с гребенчатыми спектрами // Изв. ВУЗов. Радиоэлектроника. – 1994. – 37, № 11. – С. 19 – 27.*
2. *Рассомахин С.Г. Горбачов В.В., Авдєєв В.Г. Енергетична ефективність сигналів з гребінчастим спектром // Вестник науки и техники. – Х. – 2003. – № 2 – 3(13 – 14). – 66 с.*
3. *Рассомахин С.Г. Горбачев В.В., Ильченко М.Е. Метод формирования системы сигналов с гребенчатым спектром // Вестник науки и техники. – Х. – 2003. – Вып. 1. – С. 87.*
4. *Сорока Л.С., Воронов Д.Н., Снисаренко А.Г., Рассомахин С.Г. Оценка безопасности передачи информации цифровой системой уплотнения сигналов с искусственно создаваемыми гребенчатыми спектрами // Системы обработки информации. – Х.: ХВУ. – 2004. – Вып. 5. – С. 211 – 219*

Поступила 24.11.2004

***ВОРОНОВ Дмитрий Николаевич**, кандидат технических наук, научный сотрудник научно-исследовательского отдела Объединенного научно-исследовательского института Вооруженных Сил. Окончил Харьковский военный университет в 1995 году. Область научных интересов – защита информации в системах передачи информации.*

***ЛИТВИНОВ Юрий Семёнович**, кандидат технических наук, начальник научно-исследовательского отдела Объединенного научно-исследовательского института Вооруженных Сил. Окончил Ленинградскую ВА связи им. С.М. Будённого в 1987 году. Область научных интересов – эффективность сложных систем.*

***СНИСАРЕНКО Андрей Георгиевич**, кандидат технических наук, с.н.с., начальник научно-исследовательского управления Объединенного научно-исследовательского института Вооруженных Сил. В 1985 году окончил ХВВКИУ РВ. Область научных интересов – системы передачи информации в АСУ.*