

ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ НА ОСНОВЕ НЕЛИНЕЙНО ФОРМИРУЕМЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Дубровский В.В., Половения С.И., Стефанович А.К.

Белорусский государственный университет информатики и радиоэлектроники, Беларусь

E-mail: rtu.bsuir@gmail.com

Аннотация — Численным моделированием оценена степень защищённости от несанкционированного доступа систем на основе нелинейно формируемых последовательностей. Указаны пути практической реализации алгоритмов.

1. Введение

Последовательности, формируемые нелинейными динамическими системами (НДС), обладают высокой структурной сложностью, что плодотворно влияет на защищённость информации от несанкционированного доступа. Уже простейшие нелинейные функции одного аргумента, включаемые в цепь обратной связи НДС, при выполнении определённых условий способны существенно перемешивать фазовые траектории колебательного процесса, называемого хаотическим.

В предлагаемом материале для случая манипуляции хаотических режимов и корреляционного приёма показана возможность сокрытия передаваемой информации и оценена степень её защищённости.

2. Синтез алгоритма

Пусть необходимо передать бинарный информационный сигнал. В качестве ИХП, для определённости, будем использовать генератор с нелинейностью вида $\pm F(p, h_{k-1})$, где p — криптографический параметр; h_{k-1} — состояние процесса, предшествующее текущему.

Алгоритм различения сигналов основан на формировании и максимизации функций правдоподобия.

Для гауссовских аддитивных помех алгоритм сводится к следующему

$$\sum_{k=1}^N [r_k - F_1(r_{k-1})]^2 \underset{\theta^*=-1}{\overset{\theta^*=1}{>}} \sum_{k=1}^N [r_k - F_2(r_{k-1})]^2$$

или

$$\sum_{k=1}^N [r_k^2 - 2r_k F_1(r_{k-1}) + F_1^2(r_{k-1})] \underset{\theta^*=-1}{\overset{\theta^*=1}{>}} \sum_{k=1}^N [r_k^2 - 2r_k F_2(r_{k-1}) + F_2^2(r_{k-1})], \quad (1)$$

где r_k , r_{k-1} — текущее и предыдущее состояние обрабатываемого процесса; F_1 , F_2 — нелинейные формирующие функции.

При равенстве энергий хаотических процессов на интервале длительности информационного символа выражение (1) можно записать в виде

$$\sum_{k=1}^N r_k F_1(r_{k-1}) \underset{\theta^*=-1}{\overset{\theta^*=1}{>}} \sum_{k=1}^N r_k F_2(r_{k-1}).$$

Согласно приведенному алгоритму на рис. 1 показана структурная схема различителя бинарных сообщений.

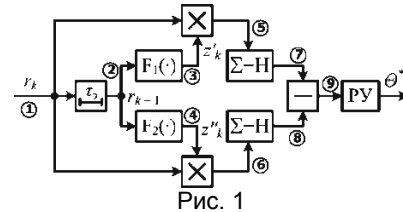


Рис. 1

На рис. 2 показана зависимость логарифма минимальной относительной точности воспроизведения параметра p от величины самого параметра для периодической кусочно-линейной функции вида $\frac{2}{\pi} \arcsin[\sin(p\pi h)]$.

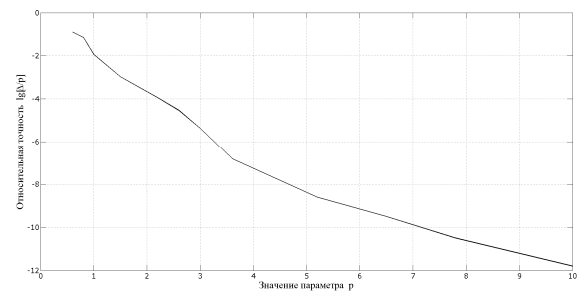


Рис. 2

Из рис. 1 следует, что для простейшей функции одной переменной с увеличением параметра p существенно возрастает необходимая точность воспроизведения параметра. Если вычислительное средство методом прямого перебора проверяет 1 млн. вариантов параметра в секунду, то при $p=10$ в первом приближении потребуется порядка 278 часов для определения его значения.

3. Заключение

При реализации алгоритма ставится задача подбора оптимальных пар функций $F_1(\cdot)$ и $F_2(\cdot)$, обеспечивающих большую помехоустойчивость. Желательно, чтобы значения процесса на выходе описывались равномерным законом распределения. Если это условие выполняется, то процесс будет наиболее энтропийным, а его значения — наименее предсказуемыми.

4. Список литературы

- [1] Капранов М.В. Система скрытной связи с использованием корреляционного приема и синхронного хаотического отклика / М.В. Капранов, А.И. Томашевский // Электромагнитные волны и электронные системы. — 2003. — Т.8, № 3. — С. 35 — 48.

INFORMATION PROTECTION IN SYSTEMS BASED ON NONLINEAR SEQUENCIES

Dubrovsky V.V., Polovenia S.I., Stefanovich A.K.

Belarusian State University of Informatics and Radioelectronics, Belarus

Abstract — The level of an information protection in nonlinear chaotic systems was estimated. Ways of practical implementation of the algorithm are discussed.