УДК 621.391

Алгоритмы защиты информации в системах телекоммуникаций методами нелинейной динамики

Посвящается нашему Учителю Валерию Аркадьевичу Чердынцеву

В.В. ДУБРОВСКИЙ, доцент кафедры РТУ УО БГУИР, канд. физ.-мат. наук, доцент

С.И. ПОЛОВЕНЯ, заведующий кафедрой ТКС УО БГАС, канд. техн. наук

Предложены алгоритмы и подходы к реализации некриптографических методов защиты информации в дискретных системах, охваченных существенно нелинейной обратной связью. Указаны достоинства и недостатки подходов. Предложены пути практической реализации методов и алгоритмов.

Введение. Большинство существующих методов защиты информации, передаваемой по открытым каналам связи, базируются на теории чисел, где показана экспоненциально возрастающая сложность операций факторизации или дискретного логарифмирования больших чисел. Такие алгоритмы доказали свою эффективность и нашли широкое применение в банковской сфере при осуществлении финансовых транзакций, в IP-сетях при передаче двоичных потоков информации, при шифровании данных, хранимых на жестких дисках или съемных носителях и т. п. Существенным ограничением применимости классических криптографических подходов является принципиальная сложность их применения при шифровании данных, передаваемых по радиоканалу или иным каналам с помехами, где требуется гарантированная точность воспроизведения шифропотока для последующего его однозначного декодирования.

Методы нелинейной динамики в своей основе реализуют близкие по своей сущности преобразования нешифрованных данных, однако отличаются заметной устойчивостью к воздействию шумов и помех в канале [1, 2], а также аппаратурной нестабильности устройства приема и обработки сигнала в целом. При своей сравнительной простоте шифраторы и дешифраторы, построенные на основе систем с существенно нелинейной обратной связью, дают возможность разработчикам криптографических систем гибко регулировать помехоустойчивость и криптостойкость алгоритмов. Укладывающиеся в заданные пределы отклонения в принятой реализации сигнала, несущего шифропоток, позволяют однозначно извлечь информацию. Однако не все алгоритмы на основе нелинейной динамики пригодны для практической реализации. Здесь требуется выявить разумный баланс между двумя противоречивыми показателями: степенью защищенности от несанкционированного доступа и помехозащищенностью системы.

В работе предложен новый большой класс алгоритмов шифрования информационного потока на основе системы связанных колец, охваченных перекрестными обратными связями нелинейного характера. Для достижения приемлемой помехоустойчивости предлагается использовать одномерные нелинейные формирующие функции (НФФ) с ограниченным углом касательных на всей области значений каждой из функций.

Постановка задачи и алгоритм кодирования. Базовая нелинейная формирующая функция f_1 определяется одномерным отображением множества аргументов:

$$\begin{cases} h'_k = f_1(p_{\max}; h_{1,k-1}, h_{2,k-1}, ..., h_{N,k-1}); \\ h_k = F\{h'_k\}, \end{cases} \quad (1)$$

где $p_{\max}$ – фиксированное максимальное значение тангенса угла наклона касательной к НФФ;
$h_{1,k-1}, h_{2,k-1}, ..., h_{N,k-1}$ – состояния каждого из N смежных колец в момент времени, предстоящий текущему;
h'_k – ненормированное значение последовательности;
$F\{\cdot\}$ – функция приведения, ограничивающая область возможных значений формируемой последовательности отрезком [–1; 1];
h_k – отсчеты нелинейной последовательности, или хаотический процесс.

Множество $\{f_i\}$ дополнительных НФФ, определяющих характер поведения смежных колец, зададим в полиномиальной форме как наиболее просто реализуемой на практике:

$$f(h) = p_0 + p_1 h_1 + p_2 h_2 + ... + p_N h_N, \quad (2)$$

где $p_0, p_1, \ldots$ – известные на передающей и приемной стороне постоянные коэффициенты полинома, причем p_0 может изменяться произвольно на отрезке [–1; 1].

$$\begin{cases} p_0 \in [-1; 1], \\ |p_i| \le p_{\max}, \ i = \overline{1, N}. \end{cases} \quad (3)$$

Как следует из приведенных выражений, формирующий полином имеет фиксированную структуру, однако аргументы функции изменяются на каждом такте работы кодера, что приводит к нерегулярности фазовых траекторий формируемого процесса.

Общее выражение, определяющее структуру генератора хаотического процесса, записывается следующим образом:

$$\begin{cases} h'_{1,k} = p_{1,0} + p_{1,1} h_{1,k-1} + p_{1,2} h_{2,k-1} + ... + p_{1,N} h_{N,k-1}; \\ h_k = F\{h'_{1,k}\}; \\ h'_{2,k} = p_{2,0} + p_{2,1} h_{1,k-1} + p_{2,2} h_{2,k-1} + ... + p_{2,N} h_{N,k-1}; \\ h_{2,k} = F\{h'_{2,k}\}; \\ \ldots \\ h'_{N,k} = p_{N,0} + p_{N,1} h_{1,k-1} + p_{N,2} h_{2,k-1} + ... + p_{N,N} h_{N,k-1}; \\ h_{N,k} = F\{h'_{N,k}\}; \end{cases} \quad (4)$$

Здесь принято, что коэффициенты полинома $p_{i,1}, p_{i,2}, \ldots, p_{i,N}$, для различных вспомогательных колец различны. Необходимость нормировочной функции $F\{\cdot\}$ для каждого кольца обусловлена тем, что конечный полином на бесконечном интервале всегда является бесконечно убывающей или бесконечно возрастающей функцией, что для вычислительных устройств с конечной разрядностью неприемлемо, так как неизбежно ведет к переполнению регистров. Штрих в записи $h'_{i,k}$ означает неприведенное к отрезку [–1; 1] значение процесса.

Свободные коэффициенты $p_{j,0}$ изменяются на всей области допустимых значений и требуют для своего формирования отдельных генераторов хаотических процессов, что вносит дополнительную стохастизацию в результирующий процесс h_k.

Вспомогательная нормировочная функция $F\{\cdot\}$ является важным элементом генератора сигнальной конструкции, так как вносит дополнительную существенную нелинейность в характер отображения $\{h_{k-1}, h_k\}$. В [3] предложены два подхода к реализации функции $F\{\cdot\}$. Первый связан с простым ограничением фазового состояния сигнала по уровню ±1. Второй, более предпочтительный в случае применения в качестве НФФ простейших полиномов, предполагает «зеркальный излом» функции при ее выходе за пределы разрешенной области:

$$F(h) = \begin{cases} 2 - h, \text{ если } h > 1; \\ -2 - h, \text{ если } h < -1. \end{cases} \quad (5)$$

В качестве информационной модуляции предложим метод нелинейного подмешивания как обеспечивающий эффективное перемешивание входного потока с хаотическим процессом:

$$h_k = (1 - \gamma) F\{h'_{1,k-1}\} + \gamma \lambda_k, \quad (6)$$

где $\gamma \in (0; 1)$ – уровень подмешивания информационного процесса к хаотическому;
$\lambda_k = \{\pm 1\}$ – отсчет информационного процесса на такте $k = 1, 2, \ldots$.

Перемешивание информации с хаотической последовательностью согласно (6) имеет ярко выраженный нелинейный характер, что является физической основой эффективного сокрытия передаваемой информации при ее передаче по открытым каналам связи. Функциональная схема алгоритма шифрования информационного потока методами нелинейной динамики представлена на рисунке 1.

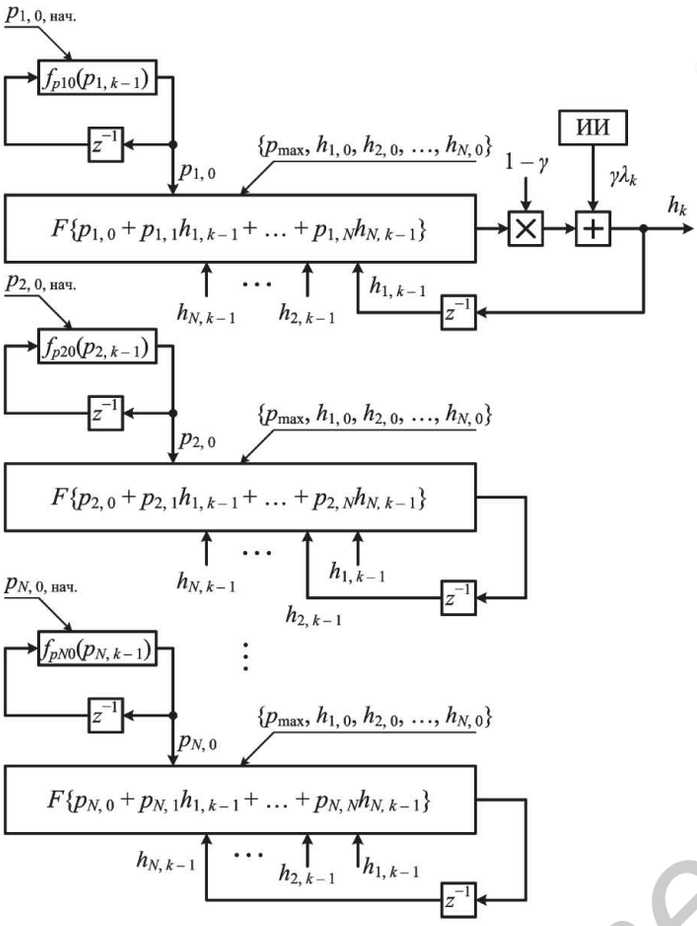

Рисунок 1 – Функциональная схема информационного кодера
«ИИ» на рисунке – источник информации.

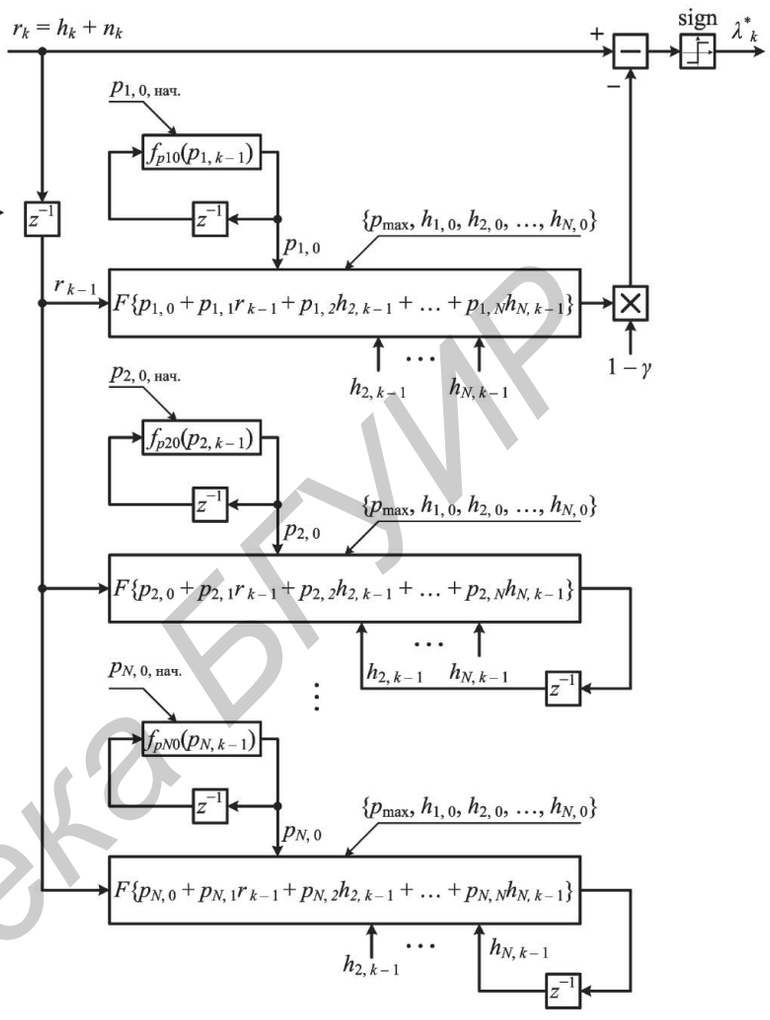

Рисунок 2 – Функциональная схема устройства извлечения информационного потока

Декодер шифрованного потока. Из (6) следует простой алгоритм извлечения информационного потока из шифрованного сигнала:

$$\lambda_k = \frac{1}{\gamma}\left[h_k - (1-\gamma)F\{h'_{1,k-1}\}\right]. \quad (7)$$

Обратим внимание, что в данной нотации полезный сигнал не обязательно должен являться двоичным – это может быть совершенно произвольный сигнал, например многоуровневая последовательность. Если же передаваемая информация представляет собой двоичный поток, то алгоритм декодер несколько упрощается:

$$\lambda_k = \mathrm{sign}\left[h_k - (1-\gamma)F\{h'_{1,k-1}\}\right], \quad (8)$$

где функция sign – знаковая функция, физически реализующая решающее устройство.

Согласно выражениям (4), (5) и (8) можно представить функциональную схему информационного декодера.

На рисунке 2 $r_k = h_k + n_k$ представляет собой смесь полезного сигнала и помехи n_k. Соответственно, отсчеты $h_{1,k}$ заменены на r_k.

Результаты численного моделирования. Численное моделирование представленных алгоритмов кодирования и декодирования информационного потока подтвердили их работоспособность и эффективность. Моделирование проводилось для системы из трех колец: первое – главное (ведущее), оставшиеся два – вспомогательные.

Коэффициенты $p_{i,1}$, $p_{i,2}$, ..., $p_{i,N}$ были приняты различными, но не превышающими значение $p_{\max} = 0{,}1$, что способствовало достижению сравнительно высокой помехоустойчивости декодера при сохранении стохастизации фазовой траектории результирующего колебания h_1. Свободные коэффициенты $p_{1,0}$, $p_{2,0}$, …, $p_{N,0}$ генерировались тремя дополнительными хаос-генераторами с

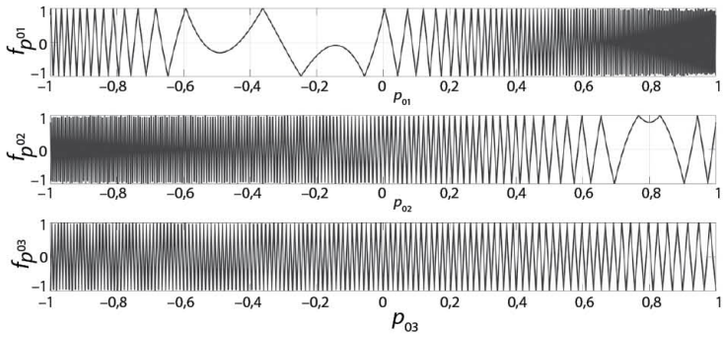

Рисунок 3 – Нелинейные формирующие функции свободных коэффициентов полинома (2)

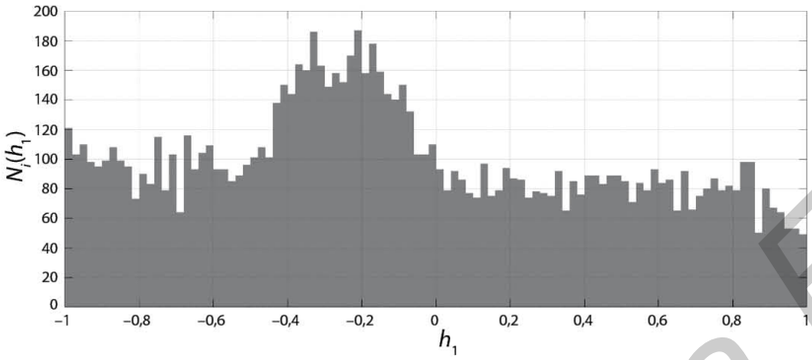

Рисунок 4 – Гистограмма процесса

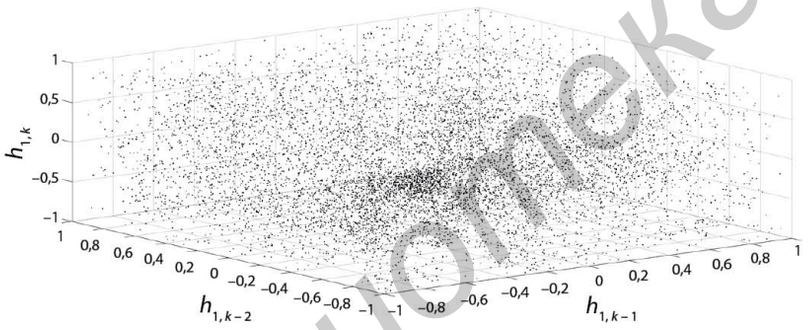

Рисунок 5 – Двумерное отображение процесса

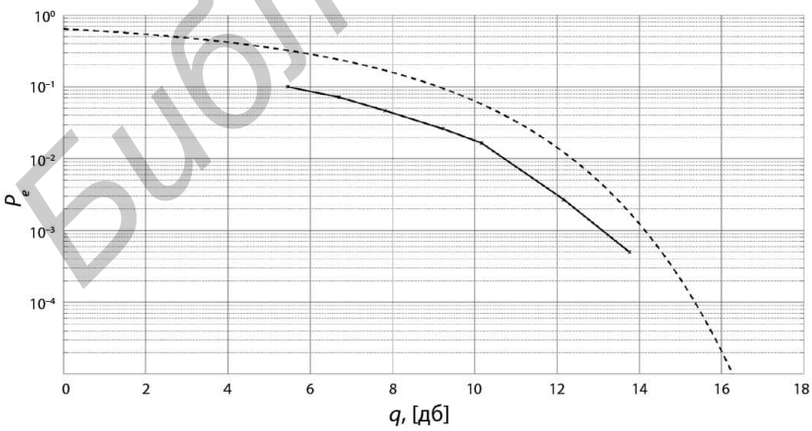

Рисунок 6 – Кривая помехоустойчивости для трехкольцевой системы

Таблица 1 – Результаты исследования помехоустойчивости трехкольцевой системы

q, дБ	5,46	6,70	7,82	9,22	10,18	12,16	13,76
P_e	0,0996	0,0716	0,0465	0,0260	0,0166	0,0027	0,0005

нелинейными функциями, представленными на рисунке 3.

Исследованию подверглись спектры, авто- и взаимокорреляционные функции, законы распределения вероятностей (рисунок 4) и отображения (рисунок 5) формируемых процессов.

В подавляющем большинстве случаев при изменении параметров НФФ генерируемый процесс сохранял свою схожесть со случайными процессами: равномерность спектра, автокорреляционную функцию в форме близкой к δ-функции, равномерное распределение значений и т. п.

Исследования помехоустойчивости показали в основном хорошие и отличные результаты, близкие аналогичным показателям для классических сигналов с простыми видами информационной модуляции (PSK, QAM). В таблице 1 приведена функция относительного количества ошибок P_e от отношения сигнал-шум q на входе декодера.

Штриховой линией на рисунке 6 показаны результаты более обстоятельных исследований на предмет выявления верхней границы помехоустойчивости (наихудший случай) нелинейной системы, состоящей из трех колец.

Заключение. Предложенные алгоритмы отличаются исключительной простотой формирования полезного сигнала в сравнении с известными решениями, что позволяет реализовать генератор случайно-подобной последовательности, кодер и декодер сигнала на простейших ПЛИС или сигнальных процессорах. Простота формирования сигнальной конструкции, например, с использованием полиномов в качестве НФФ,

не приводит к регулярностям в траектории сигнала, так как последний формируется в системе взаимно связанных колец с перекрестными обратными связями, где каждое из N – 1 колец случайно-подобным образом управляет выходным состоянием системы в целом.

В качестве сведений, санкционирующих доступ к передаваемой информации, или кода аутентификации, используются:

1) начальные условия хаос-генератора (каждого из колец) – $h_0, h_{2,0}, \ldots, h_{N,0}$;

2) вектор начальных условий генератора-формирователя свободного коэффициента полиномов $P_{j,0}$, $j = \overline{1, N}$;

3) матрица постоянных или изменяющихся коэффициентов $[p_{1,i}; p_{2,i}; \ldots, p_{N,i}]$, $i = \overline{1, N}$.

В случае если коэффициенты $p_{1,i}; p_{2,i}; \ldots, p_{N,i}$ изменяются по псевдослучайному или хаотическому закону, необходимыми дополнительными сведениями для корректного декодирования шифропотока будут являться начальные условия каждого из генераторов, формирующих указанные коэффициенты. Кроме того, обязательным условием возможности санкционированного доступа к информации является знание точной структуры хаос-генератора, количества используемых колец и характер перекрестных связей.

Без точного знания каждого из вышеуказанных параметров извлечение информации из шифропотока не представляется возможным даже по результатам длительного наблюдения реализации кодированного сигнала, что характерно для простейших систем на основе однокольцевых систем с одномерными, и даже двумерными отображениями. Исследования показали, что относительная ошибка на уровне 10^{-5} в одном из параметров генератора процесса h_k приводит к невозможности извлечения информации уже на 6-м такте работы декодера. Ошибки в двух и более параметрах заставляют декодер выдавать ложный информационный поток сразу по мере его работы. Для точной оценки криптостойкости предлагаемого семейства алгоритмов шифрования информации требуются дополнительные изыскания.

Характерной и уникальной особенностью описанных подходов к формированию шифропотока является то, что при жесткой необходимости точного воспроизведения параметров генератора искажения, вносимые в сигнал, допускаются. Сказанное означает, что алгоритмы сохраняют работоспособность в условиях действия помех и шумов, неизбежно наличествующих в радиоканале. Данное свойство шифрующих систем на основе нелинейной динамики может вывести на новый уровень средства связи и телекоммуникаций, в которых высокая степень защищенности передаваемой информации от несанкционированного доступа сочеталась бы с приемлемой помехоустойчивостью.

ЛИТЕРАТУРА

1. **Половеня, С.И., Дубровский, В.В.** Модуляция хаотических процессов на основе отображений в трехмерном пространстве фазовых состояний // VIII международная молодежная научно-техническая конференция «Современные проблемы радиотехники и телекоммуникация» (Севастополь, апрель, 2012 г.).
2. **Половеня, С.И., Дубровский, В.В.** Обработка хаотических процессов на основе отображений в трехмерном пространстве фазовых состояний // VIII международная молодежная научно – техническая конференция «Современные проблемы радиотехники и телекоммуникация» (Севастополь, апрель, 2012 г.).
3. **Дубровский, В.В.,** Обеспечение скрытности информации хаотическими сигналами на основе отображений, распределенных во времени / Половеня С.И., Чердынцев В.А., Дубровский В.В. // Вестник БГУ. Сер. 1.– Минск, 2012. – № 3. – С. 50–55.

The algorithms and approaches to the implementation of noncryptographic methods of information protection in discrete systems, covered essentially nonlinear feedback. Shown advantages and disadvantages of approaches. Suggested ways practical realization of methods and algorithms.

Получено 08.02.2016