«Оптика атмосферы и океана», **14,** № 11 (2001)

УДК 519.71:(535.3; 535.182)

И.В. Измайлов, Б.Н. Пойзнер

Варианты реализации нелинейно-оптического устройства скрытой передачи информации

Томский государственный университет

Поступила в редакцию 7.10.2001 г.

В качестве обобщенной структурной модели шифраторов в нелинейно-динамической криптологии выбран нелинейный кольцевой интерферометр (НКИ). Введенное понятие цепочек транспозиционных точек (ЦТТ) позволяет представить НКИ как систему, оптико-физические взаимодействия в которой имеют структуру графа. Для анализа и синтеза подобных систем построен «маршрутно-операторный формализм». С его помощью описаны процессы в НКИ и синтезирована модель дешифратора, использующего хаотический отклик. Указываются возможные основания классификации устройств нелинейно-динамической криптографии и вытекающие отсюда варианты их реализации. Приведены примеры компьютерной имитации (де)шифрации в режиме динамического хаоса и в статическом режиме, а также иллюстрируется влияние параметров модели на степень конфиденциальности связи. Обсуждается понятие детерминированного пространственного хаоса, возникающего в статическом режиме динамической системы. Выявлена связь ЦТТ с дискретными отображениями.

Нелинейный кольцевой интерферометр и модель процессов в нем

В связи с прогрессом лазерной физики и техники, а также оптических систем связи возникает необходимость разработки методов и приборов скрытой передачи оптической информации.

Одним из оптических устройств, в котором имеют место явления, относящиеся к компетенции как нелинейной динамики (синергетики), так и криптологии, служит нелинейный кольцевой интерферометр (НКИ). В его разработку, теоретическое и экспериментальное изучение определяющий вклад внесли С.А. Ахманов, М.А. Воронцов, А.В. Ларичев, В.И. Шмальгаузен и др. [1]. В ряде работ этой научной школы в конце 1980-х – начале 1990-х гг. доказана перспективность применения НКИ для обработки информации.

Прогресс методов синергетики позволил в 1990-е гг. по-новому взглянуть на задачу скрытой передачи информации, поскольку устройства, работающие в режиме детерминированного (динамического) хаоса, способны искажать информационный сигнал до такого вида, по которому трудно определить содержание передаваемого сообщения. Это открывает новые возможности конфиденциальной связи с помощью хаотических режимов в нелинейных системах. Поскольку природа этих систем может быть самой разнообразной, то правомерно говорить о новом научно-техническом направлении – нелинейно-динамической криптологии. Ее исторически первой и важнейшей сегодня частью является традиционная криптология. Известно, что криптологию составляют: криптография, занимающаяся математическими методами преобразования информации с целью ее защиты от угроз противника, и криптоанализ, предмет которого составляют способы осуществления угроз противника, например, приемы «взлома» шифров. Заметим, что, по мнению Д. Дойча, непредсказуемость, вызванная детерминированным хаосом, в общем случае перекрывается квантовой неопределенностью [2, с. 223]. Тем самым формулируется проблема поиска предметных областей, где оптимальна кооперация подходов нелинейно-динамической и квантовой криптографии.

Нелинейно-динамическая криптология демонстрирует расширяющееся множество вариантов реализации устройств и режимов функционирования, а также методов повышения конфиденциальности связи [3]. Классификация систем передачи информации с использованием хаотических сигналов предложена С.Н. Владимировым и В.В. Негрулем [4]. Судя по литературе, с наибольшим темпом развиваются криптографические системы скрытой связи радиодиапазона.

Как представляется авторам, в данном проблемном контексте актуальны следующие задачи.

1) Обоснование возможностей создания устройств нелинейно-динамической криптографии оптического диапазона на основе знания закономерностей синергетических явлений в оптических системах. Примеры такого обоснования средствами численного моделирования содержатся в работах [5–9].

2) Использование эвристического потенциала методов описания структурогенеза в нелинейно-оптических системах [10–12] для развития криптологии.

3) Взаимный лизинг (аренда [13]) методов описания и организации систем криптографии/криптоанализа радио- и оптического диапазонов.

4) Синтез оптических логических элементов на основе бистабильных устройств [14], многопучкового лазера [15] и др.

5) Практическое осуществление и оптимизация нелинейно-оптических устройств криптологии, использующих лазерное излучение.

Оставаясь в рамках первых трех задач (исключая криптоанализ), рассмотрим нелинейный кольцевой интерферометр. По мнению авторов, он может стать приборной основой нелинейно-динамической криптологии в оптике [5–7, 9]. Для изучения такой возможности нами использовалась модель структурообразования в поперечном сечении лазерного пучка в НКИ [10]. Модель учитывает наличие многих проходов оптического поля и модуляции амплитуды, фазы входного лазерного пучка, а также времени распространения поля в НКИ. Его схема приведена на рис. 1,

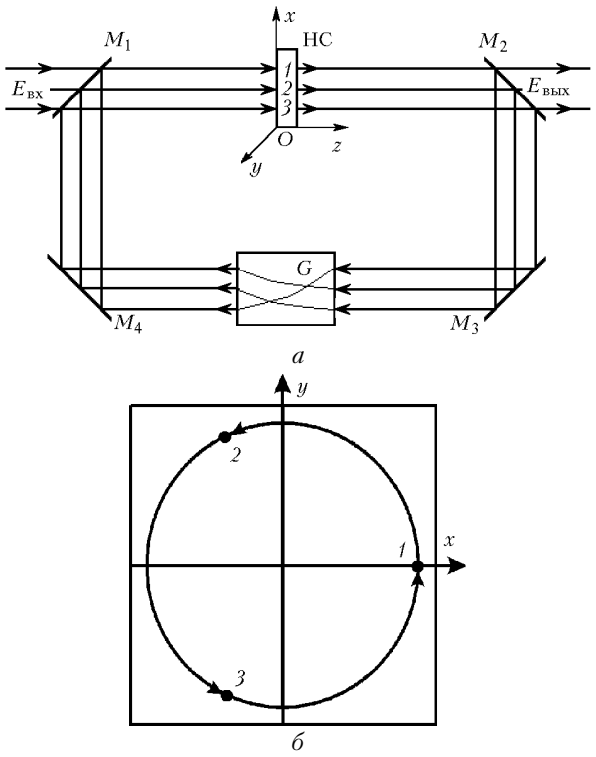


Рис. 1. Схема НКИ. При повороте элементом G светового поля на $\Delta = 120°$ (в поперечной плоскости xOy пучка) траектории трех лучей *1*, *2*, *3* замыкаются после трех обходов НКИ (*а*); проекция замыкающихся траекторий лучей *1*, *2*, *3* на плоскость xOy поперечного сечения пучка (*б*)

где НС – нелинейный элемент (керровская среда), зеркала M_1, M_2 обладают коэффициентом отражения по интенсивности R, для M_3, M_4 он есть 1, G – линейный элемент, осуществляющий крупномасштабное преобразование поля, например поворот, сдвиг, растяжение (сжатие) лазерного пучка. Более того, G может обеспечивать деление лазерного пучка, далее – перечисленные преобразования его частей, а затем сведение их в один пучок.

В случае отсутствия деления лазерного пучка модель имеет вид

$$\tau_n \partial U(\mathbf{r}, t)/\partial t = K A^2_{\text{НС}}(\mathbf{r}, t)/(1 - R) + D_e \Delta_{xy} U(\mathbf{r}, t) - U(\mathbf{r}, t),$$

$$A^2_{\text{НС}}(\mathbf{r}, t) = (1 - R) A^2_{\text{вх}}(\mathbf{r}, t) + \gamma (1 - R)^{1/2} A_{\text{вх}}(\mathbf{r}, t) A_{\text{НС}}(\mathbf{r}', t - \tau) \times \cos(\omega\tau + \varphi(\mathbf{r}, t) - \varphi_{\text{НС}}(\mathbf{r}', t - \tau))/\sigma + [\gamma A_{\text{НС}}(\mathbf{r}', t - \tau)/(2\sigma)]^2, \quad (1)$$

где $\mathbf{r} \equiv (x, y)$ – радиус-вектор поперечного сечения xOy; τ_n – время релаксации нелинейной части показателя преломления керровской среды (например, жидкого кристалла) НС протяженностью L; D_e – нормированный коэффициент диффузии молекул нелинейной среды; σ – коэффициент растяжения пучка, создаваемого элементом G; $\gamma = \gamma(\mathbf{r}', t)$ – удвоенный коэффициент потерь; $K = (1 - R)\, n_2 L |\mathbf{k}| A^2_{\max\{x,y,t\}}$ – параметр, определяющий силу нелинейных эффектов; n_2 – параметр нелинейной рефракции; $|\mathbf{k}| = \omega/c$ – волновое число; $A_{\max\{x,y,t\}}$ – максимальное значение амплитуды входного поля; $A_{\text{вх}}$ и $A_{\text{НС}}$ – амплитуды поля на входе НКИ и на входе НС соответственно, нормированные к значению $A_{\max\{x,y,t\}}$; φ и $\varphi_{\text{НС}}$ – фазы поля на входе НКИ и на входе в НС соответственно; $\tau \equiv \tau(\mathbf{r}', t) = t_e(\mathbf{r}', t) + U(\mathbf{r}', t - t_e(\mathbf{r}', t))/\omega$, t_e – эквивалентное время запаздывания в НКИ, изменяемое модулятором в контуре обратной связи (на рис. 1 не показан).

Описание маршрута движения лучей через нелинейный кольцевой интерферометр

Если пренебречь диффузией молекул в НС (жидкий кристалл), то из уравнения (1) можно получить «точечную модель» процессов $U(\mathbf{r}, t)$ и $A_{\text{НС}}(\mathbf{r}, t)$ в поперечном сечении лазерного пучка xOy. Название «точечная модель» оправдано тем, что все множество точек поперечного сечения xOy – в зависимости от вида крупномасштабного преобразования поля элементом G в контуре обратной связи интерферометра – разбивается на бесконечное число подмножеств. Они не зависят друг от друга в смысле отсутствия физического взаимодействия: между полями $A_{\text{НС}}(\mathbf{r}, t)$, между нелинейными фазовыми набегами $U(\mathbf{r}, t)$, а также между $U(\mathbf{r}, t)$ и $A_{\text{НС}}(\mathbf{r}, t)$. Но эти подмножества (принадлежащие плоскости xOy) представляют собой *цепочки точек*, в которых последовательно осуществляется взаимодействие между световыми полями и нелинейными фазовыми набегами (см. рис. 1).

Иными словами, световой сигнал (переносимый отдельным лучом лазерного пучка), проходя через нелинейную среду и контур обратной связи НКИ в точке i, приобретает фазовый набег U_i и испытывает временную задержку $t_{e\,i}$. Из-за наличия элемента G сигнал (луч) попадает в точку $i + 1$. Здесь, «складываясь» с одним из входных лучей интерферометра, он, согласно модели (1), воздействует на темп изменения величины нелинейного фазового набега U_{i+1}.

Именно так набег U_i в точке i влияет на набег U_{i+1} в точке $i+1$. Данный тип точек мы называем *транспозиционными* точками (от лат. *trans* – через + *positio* – положение) [11]. Если число точек в упомянутых подмножествах конечно, равно m, а луч из m-й точки попадает в первую, то говорят о вырожденной двумерной обратной связи m-го порядка [1], а число m называют порядком транспозиции. При такой организации обратной связи траектория луча замыкается после m обходов НКИ. Согласно принятому способу нумерации транспозиционных точек под записью $i+1$ следует подразумевать операцию $((i+1) \bmod m)+1$, где символ $(i+1) \bmod m$ означает остаток от деления $i+1$ на m. Физически это как раз и значит, что луч из m-й точки попадает в первую [11].

Например, согласно смыслу рис. 1,*б*, точки *1*, *2*, *3* образуют *замкнутую* цепочку транспозиционных точек (ЦТТ), где $m=3$. Вообще говоря, при других преобразованиях поля элементом G в НКИ (см. рис. 1,*а*) формируются как замкнутые, так и *незамкнутые* ЦТТ с различным ((бес)конечным) количеством точек.

В методическом плане обращение к понятию ЦТТ представляется удобным, поскольку структура ЦТТ отображает *маршрут* движения лучей через НКИ. При этом количество обходов НКИ служит мерой длины пройденной части маршрута. ЦТТ естественно квалифицировать как графы. Как известно, графы можно задавать различными способами: матрицами смежности и инцидентности, списками, например пар вершин, соединенных с ребрами (дугами), заданием для каждой вершины множества смежных с ней вершин [16, с. 162]. Специфика оптико-физических процессов в НКИ состоит в том, что акты прохождения лучей лазерного пучка через НС, элемент G, где возможны разветвление лучей, их линейные преобразования и сведение их в общий пучок, образуют строгую последовательность. Стремясь закрепить эту специфику в формализме, предлагаем использовать следующий язык описания структуры цепочек.

(g_i) или (g) – точка (вершина графа) g_i или g, которая является «родителем» (от лат. *generator*). То есть обозначаемое записью внутри круглых скобок «( )» является родителем по отношению к обозначаемому записью, следующей за закрывающейся скобкой «)».

$(g)\ i$ – i-я точка, следующая за точкой g (i-й «потомок» родителя g). Причем $(g)\ 0 \equiv g$. Но если далее следует символ «]», то значение i трактуется иначе.

$[(g)\ 0]_m$, $[(g)]_m$ – *развилка* (точка развилки) мощности m: в точке g одна линия разветвляется на m линий.

$[(g)\ d]_m\ i$ – i-й элемент (точка) d-й подпоследовательности, начинающейся в развилке $[(g)]_m$. Причем $[(g)\ d]_m\ 0 \equiv [(g)]_m \equiv g$.

$[(g)\ d]_m\ \forall$ – d-я подпоследовательность (путь, линия), начинающаяся в развилке $[(g)]_m$ (все элементы (точки) d-й подпоследовательности). Причем $[(g)\ d]_m\ 0 \in [(g)\ d]_m\ \forall$.

$[(g)\ d]_m$ – отрезок пути (ребро либо дуга графа), соединяющий точку g с точкой $[(g)\ d]_m\ 1$. В дальнейшем ради простоты не будем различать понятия ребра и дуги.

$[(g)\ \forall]_m$ – любой из отрезков пути, выходящих из точки g.

$\{(g)\}_m$ – *схождение* (точка схождения) мощности m: в точке g m линий сходятся в одну.

$\{(g)\}_m\ i$ – i-й элемент (точка) подпоследовательности, начинающейся в схождении $\{(g)\}_m$. Причем $\{(g)\}_m\ 0 \equiv \{(g)\}_m \equiv g$.

fin_i – финальный элемент цепочки, т.е. точка, на которой цепочка обрывается, нижний индекс – идентификационный номер финальной точки.

Очевидно, что любая точка g является развилкой и одновременно схождением, по крайней мере мощности *1*.

Отсутствие символов между символом «)» и следующим за ним символом схождения «}» делает необязательным наличие пары скобок «( )», т.е. имеют место тождества: $\{((g)\ i)\}_m \equiv \{(g)\ i\}_m$; $\{([(g)\ d]_n\ i)\}_m \equiv \{[(g)\ d]_n\ i\}_m$ и т.д.

В ряде случаев открывающиеся скобки можно опускать, но иногда их следует сохранять. Пусть, например, в точке (g_1) *4* имеется развилка мощности *3*. И каждая из «родившихся» последовательностей содержит разное количество элементов n_1, n_2, n_3, причем они сходятся в одной точке, после которой на пятом элементе цепочка точек заканчивается, т.е. пятый элемент является финальным. Тогда эту ситуацию можно выразить символически так: $\{[(g_2)\ 1]_3\ n_1;\ [(g_2)\ 2]_3\ n_2;\ [(g_2)\ 3]_3\ n_3\}_3\ 5 = fin$, где $(g_1)\ 4 \equiv g_2$. Если же каждая из подпоследовательностей содержит равное количество элементов ($n_i = n$), то эту ситуацию можно выразить более компактно: $\{[(g_2)\ \forall]_3\ n\}_3 = fin$ или даже так: $\{[(g_2)]_3\ n\}_3 = fin$.

Любое выражение, имеющее смысл в обозначенном выше контексте и использующее предложенный формализм, задает некий маршрут луча лазерного пучка в НКИ либо множество маршрутов. Причем точка является маршрутом нулевой длины. Этот формализм позволяет судить о числе развилок и схождений (о числе маршрутов), о длине маршрутов. По нашему мнению, определенное множество маршрутов может служить еще одним способом задания графа.

Интерферометр как система, имеющая структуру графа, и «маршрутно-операторный формализм»

Опишем наиболее простые типы цепочек транспозиционных точек, реализующиеся в нелинейном кольцевом интерферометре.

Если элемент G (см. рис. 1) осуществляет зеркальное отображение относительно прямой, лежащей в поперечной плоскости лазерного пучка и проходящей через его центр, то все ЦТТ описываются выражением $(g_k)2 = g_k$, где k – идентификатор ЦТТ и $g_k \neq g_l$ при $k \neq l$ (далее смысл индексов k и l остается прежним). Для точек, расположенных на линии зеркального отображения, верно и выражение $(g_k)1 = g_k$.

При сдвиге лазерного пучка на расстояние Δx верно выражение $(g_k)\ m_k = fin_k$, где $fin_k \neq g_k$ и m_k зависит от Δx и расположения точки g_k. Для квадратной апертуры лазерного пучка и сдвига $\Delta x = a/m$ вдоль стороны квадрата длиной a все $m_k = m - 1$. Очевидно, что ЦТТ незамкнута, а ее конфигурацию можно назвать *линейной*.

При повороте лазерного пучка на угол $\Delta = 2\pi n/m$ в плоскости xOy верно выражение $(g_k)\ m = g_k$, где n, m – взаимно простые. Заметим, что для центра пучка g_c можно положить $m = 1$ при любом Δ. В этом случае ЦТТ замкнута (в кольцо) и конфигурацию ее логично именовать *кольцевой*. Очевидно, что если $m = 2$ ($\Delta = 180°$), то данное выражение сводится к формуле для зеркального отображения.

Если угол поворота $\Delta \neq 2\pi n/m$, то ЦТТ содержит бесконечное количество точек, причем нельзя выделить начала и конца цепочки: $(g_{k,i})\ 1 = g_{k,i+1}$, где i – номер точки в цепочке, $i \in (-\infty; +\infty)$.

При сжатии лазерного пучка ($\sigma < 1$) верны выражения $\{(g_k)\ \infty\}_\infty = g_c$, $\{(g_c)\ 1\}_\infty = g_c$, поэтому в плане (не)замкнутости ЦТТ оказывается комбинированной, и ее конфигурации отвечает образ «сходящейся» *звезды* с бесконечным числом лучей.

При растяжении лазерного пучка ($\sigma > 1$) верны выражения $[(g_c)\ k]_\infty = fin_k$, $(g_c)1 = g_c$ либо $\{(fin_k)\ \infty\}_\infty = g_c$, $(g_c)1 = g_c$. Последние (вопреки реальной хронологии обхода лучами НКИ) описывают «обратный» маршрут: из финальных точек fin_k цепочек, находящихся на периферии пучка, в их общую начальную точку g_c. ЦТТ также является комбинированной, но с ее конфигурацией ассоциируется образ «расходящейся» *звезды* с бесконечным числом лучей.

Примем во внимание то, что в НКИ имеются точки ввода $g_{\text{вх}}$ и вывода $fin_{\text{вых}}$ потока энергии лазерного пучка. Для определенности будем считать, что вывод энергии происходит по первому пути: $[(g_i)1]_m$.

Тогда для случая зеркального отображения, опуская индекс k, выражение $(g_k)\ 2 = g_k$ можно дополнить следующим образом:

$$\{(g_{\text{вх}\ i})\ 1;\ [(g_j)\ 2]_2\ 1\}_2 = g_i \quad \text{и} \quad [(g_j)\ 1]_2\ 1 = fin_{\text{вых}\ j}$$

либо

$$[(\{(g_{\text{вх}\ i})1;\ [(g_j)2]_2\ 1\}_2 = g_i\ )\ 1]_2\ 1 = fin_{\text{вых}\ i},$$

где $i, j = 1, 2$ или $2, 1$.

Для случая сдвига пучка выражение $(g_k)\ m_k = fin_k$ заменяется тремя:

$$[((g_{\text{вх}\ 1})1 = g_1)\ 1]_2\ 1 = fin_{\text{вых}\ 1},$$

$$[(\{\ (g_{\text{вх}\ i})1;\ [(g_{i-1})\ 2]_2\ 1\ \}_2 = g_i\ )\ 1]_2\ 1 = fin_{\text{вых}\ i},$$

$$[(g_m)\ 2]_2\ 1 = fin,$$

где $i \in [2; m]$. Третье выражение описывает тот факт, что ЦТТ не замыкается, поскольку луч из точки g_m, попадая в контур обратной связи НКИ по пути, обозначаемому символом 2: $[(g_m)\ 2]$, – поглощается в точке fin (на диафрагме, например).

Для случая поворота пучка на угол $\Delta = 2\pi n/m$ выражение $(g_k)\ m = g_k$ заменяется следующим:

$$[(\{(g_{\text{вх}\ i+1})1;\ [(g_i)2]_2\ 1\ \}_2 = g_{i+1}\ )\ 1]_2\ 1 = fin_{\text{вых}\ i+1},$$

где $i \in [1; m]$, а если $i + 1 = m + 1$, то такое значение индекса следует заменить на 1.

Если $\Delta \neq 2\pi n/m$, то верно:

$$[(\{(g_{\text{вх}\ i+1})1;\ [(g_i)2]_2\ 1\}_2 = g_{i+1}\ )\ 1]_2\ 1 = fin_{\text{вых}\ i+1},$$

где $i \in (-\infty; +\infty)$. В случае сжатия пучка вместо выражений $\{(g_k)\ \infty\}_\infty = g_c$, $\{(g_c)1\}_\infty = g_c$ имеем

$$[((g_{\text{вх}\ 1})1 = g_1)\ 1]_2\ 1 = fin_{\text{вых}\ 1}$$

– для начальной точки g_1 ЦТТ, лежащей на периферии;

$$[(\{(g_{\text{вх}\ i})1;\ [(g_{i-1})\ 2]_2\ 1\}_2 = g_i)\ 1]_2\ 1 = fin_{\text{вых}\ i}$$

– для внутренних точек g_i ЦТТ, где $i \in [2; m-1]$;

$$[(\{(g_{\text{вх}\ m})1;\ [(g_{m-1})\ 2]_2\ 1\ \}_\infty = g_m\ )\ 1]_2\ 1 =$$

$$= fin_{\text{вых}\ m},\ \{(g_m)1\}_\infty = g_m$$

– для точки g_m, являющейся пределом g_c последовательности ЦТТ: при $m \to \infty$ $g_m \to g_c$.

В случае растяжения пучка вместо пары выражений $[(g_c)\ k]_\infty = fin_k$, $(g_c)1 = g_c$ имеем

$$\{(g_{\text{вх}\ c})1;\ [(g_c)\ 2]_\infty\ 1\}_2 = g_c,\ \ [(g_c)\ 1]_\infty\ 1 = fin_{\text{вых}\ c}$$

– для начальной точки ЦТТ $g_1 = g_c$;

$$[(\{(g_{\text{вх}\ 2})1;\ [(g_1)\ 2]_\infty\ 1\}_2 = g_2)\ 1]_2\ 1 = fin_{\text{вых}\ 2};$$

$$[(\{(g_{\text{вх}\ i})1;\ [(g_{i-1})\ 2]_2\ 1\}_2 = g_i)\ 1]_2\ 1 = fin_{\text{вых}\ i}$$

– для внутренних точек g_i ЦТТ, где $i \in [3; m)$;

$$[(g_m)\ 2]_2\ 1 = fin$$

– для точки g_m, являющейся пределом последовательности ЦТТ, при $m \to \infty$. А вместо выражения для «обратного» маршрута $\{(fin_k)\ \infty\}_\infty = g_c$, $(g_c)1 = g_c$ верны выражения:

$$[(\{(fin_{\text{вых}\ m})1;\ (fin)1\}_2 = g_m)\ 1]_2\ 1 = g_{\text{вх}\ m}$$

– для точки g_m, являющейся пределом последовательности ЦТТ при $m \to \infty$;

$$[(\{(fin_{\text{вых}\ i})1;\ [(g_{i+1})\ 2]_2\ 1\}_2 = g_i)\ 1]_2\ 1 = g_{\text{вх}\ i}$$

– для внутренних точек g_i ЦТТ $i \in [2; m)$;

$$[(\{(fin_{\text{вых}\ c})1;\ [(g_2)\ 2]_2\ 1\}_\infty = g_c\ )\ 1]_2\ 1 = g_{\text{вх}\ c}$$

– для начальной точки ЦТТ $g_1 = g_c$.

В приведенных примерах формулы маршрута полностью задают структуру ЦТТ в НКИ, расположение точек ввода в НКИ и вывода из НКИ лазерного

излучения. Нетрудно видеть, что для «неособых» (внутренних) точек ЦТТ справедлива формула маршрута:

$$[(\{(g_{\text{вх } i+1})1;\ [(g_i)\ 2]_2\ 1\}_2 = g_{i+1})\ 1]_2\ 1 = fin_{\text{вых } i+1}. \quad (2)$$

Очевидно, следует включить в формулы маршрутов описание физических воздействий, претерпеваемых лазерным пучком. Для этого необходимо точкам маршрута и отрезкам пути (вершинам и ребрам графа) поставить в соответствие некие *операторы* (коэффициенты передачи, функционалы и пр.), описывающие физические процессы в элементах маршрута. Тем самым удается описать преобразования над сигналом (лучом лазерного пучка) в элементах графа.

Применительно к НКИ (см. рис. 1) указанное соответствие реализуется следующим образом. Транспозиционные точки g_i (точки схождения) локализуются в нелинейной среде. В этих точках происходит сложение оптических полей, результирующее поле испытывает задержку, и мерой ее служит нелинейный фазовый набег $U(\mathbf{r}, t)$, эволюционирующий под действием интенсивности результирующего поля согласно дифференциальному уравнению в (1).

На языке предлагаемого *маршрутно-операторного формализма* это означает, что в соответствующих вершинах графа сигналы суммируются, приобретают фазовую задержку $U_i(t)$. Из-за нелинейности среды суммарный сигнал изменяет характеристики оператора (коэффициент передачи), реализуемого данной вершиной. Нетрудно видеть, что ребрам $[(g_i)\ 1]_2$ и $[(g_{\text{вх } i})\ 1]_1$ можно поставить в соответствие коэффициент передачи $(1-R)^{1/2}$, а ребру $[(g_i)\ 2]_2$ – коэффициент передачи по амплитуде $\gamma/2$ и задержку $t_{e\,i}(t)$. Находящуюся на диафрагме финальную точку *fin* луча будем описывать как идеальный поглотитель. Все остальные элементы маршрута по умолчанию имеют единичный коэффициент передачи, так как им не приписывается взаимодействия с полем лазерного пучка.

Оператор, соответствующий точке ввода $g_{\text{вх } i}$ лазерного пучка, можно задать как функцию времени и индекса i, репрезентирующего пространственную зависимость. Эта функция должна описывать динамику сигнала (амплитуды $A_i(t)$) на входе НКИ.

Точку вывода $fin_{\text{вых } i}$ пучка естественно трактовать как место расположения интерфейса, т.е. сопряжения НКИ с последующими устройствами. Зная их характеристики, можно конкретизировать оператор, соответствующий точке $fin_{\text{вых } i}$. При их отсутствии точку $fin_{\text{вых } i}$ следует описывать как идеальный поглотитель.

Широту применения «маршрутно-операторного формализма» для синтеза математических моделей обеспечивает общность лежащего в его основе предположения о том, что существенные (в плане моделирования) акты взаимодействия в системе имеют структуру графа. Примеры подобных объектов исследования нетрудно обнаружить среди оптических, радиотехнических, коммуникационных (как технических, так и социокультурных) систем.

Применение «маршрутно-операторного формализма» для построения модели дешифратора

Если интерпретировать НКИ как устройство шифрования, то предложенный формализм должен служить средством синтеза динамической системы, выполняющей роль дешифратора. Логично рассматривать выражение для маршрута, связывающее входной и выходной сигналы НКИ с учетом операторов, реализующихся элементами маршрута, как *уравнение относительно входного сигнала* $A(\mathbf{r}, t)$. Изложим опыт такого синтеза.

Прежде всего отметим, что теперь точке $fin_{\text{вых } i+1}$ соответствует отнюдь не идеальный поглотитель, а вход дешифратора: $fin_{\text{вых } i+1} = g_{\text{вх } d\ i+1}$.

Из содержания формулы маршрута (2) и приведенного сопоставления операторов с элементами (2) нетрудно видеть, что на выход шифратора $fin_{\text{вых } i+1}$ сигнал попадает по ребру $[(g_{i+1})\ 1]_2$ с коэффициентом передачи $(1-R)^{1/2}$. Значит, должен существовать элемент дешифратора, например точка ввода излучения $(g_{\text{вх } d\ i+1})$, реализующий оператор $(1-R)^{-1/2}$, обратный оператору ребра шифратора $[(g_{i+1})\ 1]_2$.

В точках g_i шифратора сигналы, приходящие по ребрам $[(g_{\text{вх } i+1})\ 1]_1$ и $[(g_i)\ 2]_2$, суммируются, испытывают задержку $U_i(t)$ и разделяются. Заметим, что согласно (2) и содержанию операторов результатом деления являются сигналы (на каждом из выходов делителя), идентичные сигналу на его входе. Следовательно, операция деления не меняет сигнала.

Соответственно должны существовать две точки дешифратора: в точке $g_{d\ i+1}$ осуществляется фазовая задержка $U_{d\ i+1}(t) = -\,U_{i+1}(t)$. В точке $(g_{d\ i+1})1$ происходит вычитание сигнала, равного сигналу S_i, поступающему по ребру шифратора $[(g_i)\ 2]_2$, из сигнала, приходящего от вершины $(g_{d\ i+1})$. Пусть точка $g_{d\ i+1}$ расположена на ребре $[(g_{\text{вх } d\ i+1})\ 1]_m$, т.е. $[(g_{\text{вх } d\ i+1})\ 1]_m\ 1 = g_{d\ i+1}$, где мощность развилки m определится далее.

Учтем, что на ребро $[(g_i)\ 2]_2$ сигнал поступает из точки (g_i), причем ему равен сигнал, приходящий из точки $(g_{\text{вх } d\ i})$. Поэтому для формирования сигнала S_i в дешифраторе достаточно создать копию $[(g_{\text{вх } d\ i})\ 2]_m$ ребра $[(g_i)\ 2]_2$. Копию, но с тем отличием, что фазовая задержка, реализуемая ребром $[(g_{\text{вх } d\ i})\ 2]_m$, разнится от $\omega t_{e\ i}(t)$ на π. Тем самым обеспечивается операция вычитания – теперь уже в сумматоре $(g_{d\ i+1})1$.

Ребру $[(g_{\text{вх } i})\ 1]_1$ шифратора соответствует коэффициент передачи $(1-R)^{1/2}$, поэтому в дешифраторе необходим оконечный элемент, компенсирующий потери излучения. Пусть им будет точка $(g_{d\ i+1})1$.

Очевидно, что необходимое количество путей из точки $(g_{\text{вх } d\ i})$ не превышает двух, т.е. следует считать $m = 2$. С учетом сказанного можно сконструировать формулу, описывающую преобразования сигнала в дешифраторе:

$$\{([(g_{\text{вх}\,d\,i+1})\,1]_2\,1 = g_{d\,i+1})1;\ [(g_{\text{вх}\,d\,i})\,2]_2\,1\}_2\,1 = \\ = fin_{\text{вых}\,d\,i+1}, \qquad (3)$$

где точка $(g_{\text{вх}\,d\,i+1})$ имеет коэффициент передачи $(1-R)^{-1/2}$; точка $(g_{d\,i+1})$ осуществляет фазовую задержку $U_{d\,i+1}(t) = -U_{i+1}(t)$, ребро $[(g_{\text{вх}\,d\,i})\,2]_2$ имеет коэффициент передачи $\gamma/2$ и осуществляет фазовую задержку $\omega t_{e\,i}(t) + \pi$. Точка схождения $(g_{d\,i+1})1$ суммирует входящие сигналы и передает их с коэффициентом усиления $(1-R)^{-1/2}$.

Для того чтобы осуществить в дешифраторе задержку $U_{d\,i+1}(t) = -U_{i+1}(t)$, достаточно обеспечить в нем выполнение равенства для коэффициентов нелинейности (де)шифратора $K_d = -K$ выбором НС, для которой $n_{2d} = -n_2$. Но если не брать на себя задачи выбора НС, для которой $K_d = -K$, то достаточно в ребре $[(g_{\text{вх}\,d\,i})\,2]_2$ обеспечить выполнение условий: $\omega t_{e\,d\,i}(t) \approx \omega t_{e\,i}(t) + \pi$ и $\text{frac}\,(\omega t_{e\,d\,i}(t)/(2\pi)) = -\text{frac}(\omega t_{e\,i}(t)/(2\pi) + 0{,}5)$, где символ frac обозначает дробную часть числа. При этом поле на выходе дешифратора имеет ту же самую амплитуду, а его фаза сдвинута на π относительно ситуации, когда $K_d = -K$.

Сопоставляя формулы (3) и (2), можно отметить их существенные различия: на входе дешифратора присутствует разветвитель (делитель) лазерного пучка, а не сумматор, как на входе шифратора; напротив, на выходе дешифратора – сумматор вместо делителя; пройдя через ребра $[(g_{\text{вх}\,d\,i})\,\forall]_2$ дешифратора, все лучи покидают его, не возвращаясь обратно, т.е. дешифратор оказывается нелинейной системой *без обратной связи*, какой обладает шифратор. Поэтому для дешифратора верно лишь дифференциальное уравнение модели (1), а сам дешифратор не в состоянии генерировать динамический хаос. Таким образом, дешифратор работает в режиме *хаотического отклика*, или, по терминологии [4], в режиме пассивной синхронизации. Ограничимся в дальнейшем этим случаем.

Синтез модели дешифратора (3) проведен исходя из условия полного восстановления дешифратором сигнала, поступающего с выхода НКИ, до сигнала $A_{\text{вх}\,i}(t)$, поданного на вход НКИ: $A_{\text{вх}\,i}(t) = A_{\text{вых}\,d\,i}(t)$. Если же смягчить это требование до условия $A_{\text{вых}\,d\,i}(t) = \text{const}\,A_{\text{вх}\,i}(t)$, то содержание операторов, реализуемых элементами маршрута в модели дешифратора (3), можно изменить.

Например, точка $(g_{\text{вх}\,d\,i+1})$ имеет коэффициент передачи 1; точка $(g_{d\,i+1})$ осуществляет задержку $-U_{i+1}(t)$. Точка схождения $(g_{d\,i+1})1$ суммирует сигналы и осуществляет их передачу с коэффициентом 1. Ребра дешифратора $[(g_{\text{вх}\,d\,i})\,1]_2$ и $[(g_{di})\,1]_1$ имеют коэффициент передачи $(1-R)^{1/2}$. В свою очередь, это требует в ребре $[(g_{\text{вх}\,d\,i})\,2]_2$ корректирующего ослабления амплитуды в $(1-R)$ раз. Это ребро имеет коэффициент передачи $\gamma(1-R)/2$ и осуществляет задержку $\omega t_{e\,i}(t) + \pi$. Ребро шифратора $[(g_i)\,1]_2$ и ребро дешифратора $[(g_{\text{вх}\,d\,i})\,1]_2$ имеют коэффициент передачи $(1-R)^{1/2}$, поэтому требуется скорректировать коэффициент нелинейности дешифратора по правилу: $K_d = -K/(1-R)^2$. Для дешифратора с такими параметрами верно соотношение: $A_{\text{вых}\,d\,i}(t) = (1-R)^2\,A_{\text{вх}\,i}(t)$. Его схема показана на рис. 2, где корректирующее изменение амплитуды поля происходит в фазовращателе π.

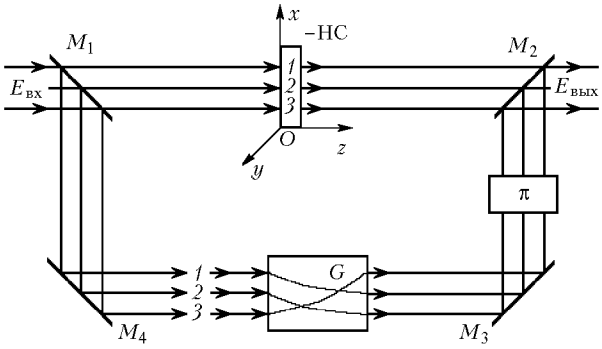


Рис. 2. Схема дешифратора. При повороте элементом G светового поля на $\Delta = 120°$ (в поперечной плоскости пучка) траектории лучей *1* и *3*, *2* и *1*, *3* и *2* после прохода интерферометра суммируются на выходном зеркале

Варианты устройств нелинейно-динамической криптографии: классификационный аспект

Как видно, предложенный формализм помогает синтезировать схему дешифратора по известной маршрутно-операторной схеме шифратора безотносительно к его материально-конструктивному воплощению. Более того, теперь структура ЦТТ, т.е. строение формул маршрутов, в частности, (2) и, следовательно, (3), способны служить классификационным признаком при типологизации известных и предсказании возможных вариантов криптографических методов и устройств нелинейно-динамической криптологии. Известно, что в криптологии такими признаками являются: число ключей (наличие открытого ключа), математические принципы, лежащие в основе шифрования/дешифрации.

Очевидно, такие характеристики ЦТТ шифратора, как структура (замкнутая, незамкнутая, комбинированная), конфигурация (линейная, типа «(ра)сходящаяся» звезда, кольцевая, фракталоподобная и пр.), число точек – каналов связи (одна, две, более двух, бесконечное число), можно распространить на соответствующие классифицируемые пары (де)шифраторов.

Необходимо принять во внимание и режим функционирования шифратора (хаотический, статический и пр.). Например, статический режим неизбежен при незамкнутой ЦТТ и при любом постоянном сигнале на входе шифратора.

Классификационными признаками естественно также считать возможности одновременной передачи различных сообщений: по одному каналу связи данной цепочки (модуляция фазы и амплитуды одновременно), по различным каналам связи данной ЦТТ (путям $g_{\text{вх}\,i} \to fin_{\text{вых}\,d\,i}$), по различным совокупностям каналов связи из разных цепочек, – и назначение одного

канала связи (одного из путей $fin_{\text{вых } i} \to g_{\text{вх } d\ i}$): для передачи сообщений, для синхронизации, для того и другого одновременно. А также долю каналов, предназначенных для указанных процедур.

Сигнал $S_i(t)$, приходящий в точку $g_{\text{вх } d\ i}$ в момент времени t, после различных преобразований в дешифраторе является «информационным замаскированным сигналом» $In_i(t) = F_{In\ i}(S_i(t - \tau_{In\ i}))$. Но он может служить и «опорным сигналом» $B_i(t) = F_{B\ i}(S_i(t - \tau_{B\ i}))$. Кроме того, $S_i(t)$ выступает как внешнее воздействие на различные элементы дешифратора, т.е. выполняет функцию синхронизующего сигнала. В зависимости от той или иной функции сигнал $S_i(t)$ уместно называть «информационным замаскированным», «опорным», синхронизующим.

Выделение собственно информационного сигнала $I_i(t)$, подававшегося на вход $g_{\text{вх } i}$ шифратора в предшествующие моменты времени, происходит в результате бинарной операции – вычитания:

$$I_i(t) = In_i(t) - B_j(t) =$$

$$= F_{In\ i}(S_i(t - \tau_{In\ i}) - F_{B\ j}[S_j(t - \tau_{B\ j})].$$

Заметим, что процедура выделения может быть основана на иной бинарной («+», «⊕» и т.д.) или, скажем, N-арной операции.

В акте выделения сигнала $I_i(t)$ сигнал $S_i(t - \tau_{In\ i})$ является информационным замаскированным, а сигнал $S_j(t - \tau_{B\ j})$ – опорным; синхронизующим же могут являться оба – в зависимости от того, действительно ли они оказывают синхронизующее воздействие на элементы дешифратора.

Если ЦТТ замкнута и состоит из одной точки, то $i = j$. Это соответствует одноканальной (по классификации [4]) системе конфиденциальной связи, хотя в случае НКИ число ЦТТ не ограничено. Надо сказать, что для криптографических систем радиодиапазона, использующих хаотический отклик при дешифрации, характерны выполнение равенства $In_i(t) = S_i(t)$ и расположение нелинейного элемента в контуре обратной связи шифратора (см. [17, рис. 2,*б*]).

Тем самым три функции сигнала S_i при выделении $I_i(t)$ разнесены во времени: сигнал S_i, пришедший в дешифратор на отрезке времени $(-\infty;\ t - \tau_{B\ i})$, сначала обеспечивает его синхронизацию (первая функция). Затем S_i играет роль опорного сигнала $S_i(t - \tau_{B\ i})$ (вторая функция). Далее $S_i(t)$ переносит элемент сообщения $I_i(t)$ (третья функция), которое выделяется благодаря наличию опорного сигнала в предварительно синхронизованном дешифраторе.

Если ЦТТ не замкнута и состоит из двух точек, т.е. $i \neq j$ (такая ситуация в НКИ возможна при сдвиге), $K = 0$ и на первую точку подается хаотический сигнал, а на вторую – информационный, то это соответствует двухканальной (с отдельным каналом (пассивной) синхронизации) [4] системе конфиденциальной связи. В случае НКИ число ЦТТ по-прежнему не ограничено.

В акте выделения сигнала $I_2(t)$ сигнал $S_2(t - \tau_{In\ 2})$ является информационным замаскированным, а сигнал $S_1(t - \tau_{B\ 1})$ – синхронизующим и опорным.

Тем самым три функции сигнала S_i при выделении $I_2(t)$ *разнесены и во времени, и в пространстве* (по каналам 1 и 2): сигнал S_1, пришедший в дешифратор на отрезке времени $(-\infty;\ t - \tau_{B\ 1})$, сначала обеспечивает его синхронизацию (первая функция). Затем S_1 играет роль опорного сигнала $S_1(t - \tau_{B\ 1})$ (вторая функция). Далее $S_2(t)$ переносит сообщение $I_2(t)$ (третья функция), которое дешифруется.

Разнесение функций сигнала S_i во времени и(или) в пространстве сказывается на помехозащищенности системы передачи. Предположим, на канал связи действует аддитивный шум. Тогда при разнесении функций S_i в пространстве пагубное влияние на результат дешифрации оказывает отличие средних (по трассе распространения) величин шума $\langle N_i(t)\rangle$ в каналах (например, 1 и 2), где t – время прихода сигнала S_i на i-й вход дешифратора. А при разнесении во времени значимо изменение уровня $\langle N_i(t)\rangle$ за время $\Delta\tau = |\tau_{In\ i} - \tau_{B\ j}|$. Разумеется, здесь необходимо учитывать и влияние преобразований $F_{In\ i}(S_i(t - \tau_{In\ i}))$ и $F_{B\ j}(S_j(t - \tau_{B\ j}))$, совершаемых над сигналами S_i и S_j. Но мы ограничимся лишь учетом времен $\tau_{In\ i}$ и $\tau_{B\ j}$.

Очевидно, что в одноканальной системе связи на помехозащищенность влияет только изменение $\langle N_1(t + \Delta\tau)\rangle - \langle N_1(t)\rangle$. Величина $\Delta\tau$, вообще говоря, определяется временем запаздывания в контуре обратной связи шифратора.

В двухканальной системе связи с отдельным каналом синхронизации на помехозащищенность влияет величина $\langle N_2(t - \tau_{In\ 2})\rangle - \langle N_1(t - \tau_{B\ 1})\rangle$, т.е. оба фактора. Однако разнесение во времени функций S_i можно ликвидировать посредством линий задержек в обоих каналах на входе и выходе шифратора. При достижении равенства: $\tau_{In\ 2} = \tau_{B\ 1}$ влиять будет только разнесение в пространстве: $\langle N_2(t)\rangle - \langle N_1(t)\rangle$.

Таким образом, если выполняются условия $\langle N_1(t + \Delta\tau)\rangle - \langle N_1(t)\rangle \ll \langle N_2(t)\rangle - \langle N_1(t)\rangle$ либо $\langle N_1(t + \Delta\tau)\rangle - \langle N_1(t)\rangle \gg \langle N_2(t)\rangle - \langle N_1(t)\rangle$, то преимуществом в помехозащищенности будет обладать одно- либо двухканальная система конфиденциальной связи. Заметим, что в [4] указывается на преимущество последней.

Очевидно, что в системе связи на основе НКИ возможны различные соотношения между числом каналов (количеством точек в ЦТТ), отводимых под передачу сообщений и для синхронизации. Это порождает отличия от известных систем. Пусть, например, в НКИ лазерный пучок поворачивается на угол $\Delta = 2\pi n/m$ или испытывает зеркальное отображение, т.е. реализуется замкнутая ЦТТ. Если в шифраторе и дешифраторе НС расположена непосредственно перед элементом G по ходу лучей (рис. 3, где корректирующее изменение амплитуды поля происходит в фазовращателе π), а $K_d = K/(1 - R)$, то возможна следующая ситуация.

Канал связи $fin_{\text{вых } i} \to g_{\text{вх } d\ i}$ используется для передачи сигнала S_i, синхронизующего и опорного по отношению к информационному маскированному сигналу S_{i+1}, передаваемому по каналу $fin_{\text{вых } i+1} \to g_{\text{вх } d\ i+1}$. В свою очередь, сигнал S_{i+1} используется как синхронизующий и опорный по отношению к информационному маскированному сигналу S_{i+2}, передаваемому по

каналу $fin_{\text{вых } i+2} \to g_{\text{вх } d\ i+2}$, etc. Иначе говоря, каждый сигнал S_i (канал $fin_{\text{вых } i} \to g_{\text{вх } d\ i}$) несет информацию, одновременно являясь синхронизующим и опорным для S_{i+1}. Тем самым доля служебных (исключительно синхронизующих) каналов равна нулю.

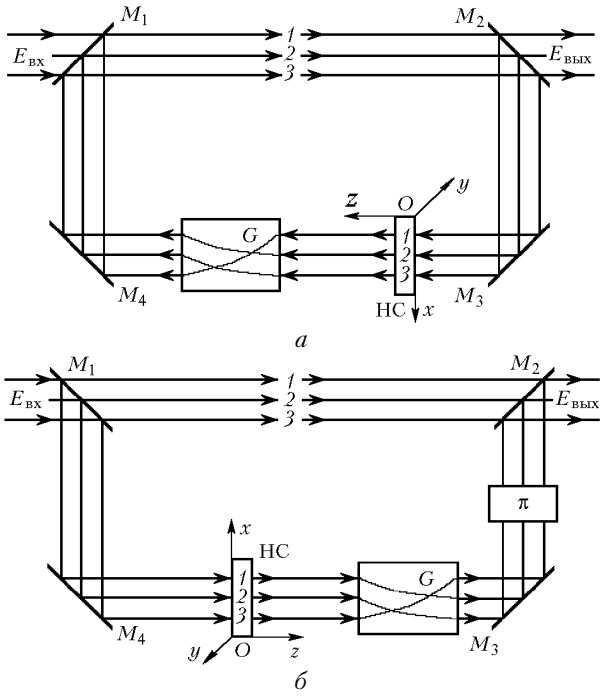


Рис. 3. Схема шифратора (*а*) и дешифратора (*б*), когда НС помещена в контур обратной связи шифратора. Траектории лучей соответствуют повороту светового поля на $\Delta = 120°$

Если же в НКИ лазерный пучок испытывает сдвиг, т.е. реализуется незамкнутая ЦТТ, то целесообразно, чтобы сигнал S_1 (канал $fin_{\text{вых } 1} \to g_{\text{вх } d\ 1}$) служил синхронизующим и опорным, но не переносил информации. Остальные сигналы и каналы, как и в предыдущем примере, могут играть все три роли. В этом сюжете доля служебных каналов определяется как отношение $1/m$, где m – число точек в ЦТТ. В двухканальных системах с отдельным каналом (пассивной) синхронизации [4] эта доля равна $1/2$.

В статье [8] моделируются процессы в оптической системе скрытой передачи информации на основе пары четырехзеркальных интерферометров – генераторов детерминированного пространственно-временного хаоса. В этой системе дешифратор работает в режиме активной синхронизации, в модели учитывается дифракция, нелинейной средой является насыщающийся поглотитель, глубина пространственной модуляции амплитуды информационным сигналом, видимо, составляет 0,005. Имитируется передача статического изображения, которое в результате дешифрации становится вполне различимым при коэффициенте связи 0,7, но все же восстанавливается с некоторыми искажениями.

Предположим, что выходное зеркало дешифратора *OM* на рис. 4 в системе, предложенной авторами [8], сделано полностью отражающим. Тем самым разорвана обратная связь в дешифраторе, в силу чего он лишается способности генерировать хаос и превращается в нелинейный дискриминатор. Предположим

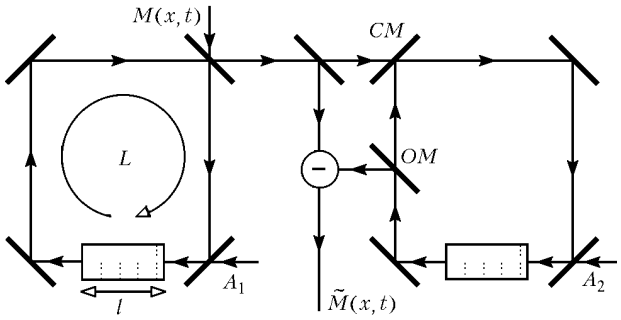


Рис. 4. Схема передачи пространственно-временной информации, использующая оптический хаос [8]. *CM* и *OM* – зеркала связи и вывода излучения; A_1, A_2 – амплитуды плоских волн, постоянно поступающих в резонаторы; $M(x,t)$ и $\tilde{M}(x,t)$ с тильдой – шифруемый и дешифрованный сигналы; l – длина нелинейного элемента (насыщающегося поглотителя); L – оптическая длина интерферометров

также, что вместо раздельной подачи сигналов $M(x,t)$ и A_1 в шифратор подается их суперпозиция (в направлении $M(x,t)$ на рис. 4). Соответственно амплитуда волны $A_2 = 0$. Тогда структура пары интерферометров (шифратор + дешифратор) на рис. 4 будет практически эквивалентна паре интерферометров, изображенной на рис. 3, если изъять из последней элемент G либо положить $\Delta = 2\pi$. Кроме того, если на рис. 4 увеличить степень нелинейности нелинейного элемента дешифратора, то, вероятно, станет возможно полное (безошибочное) восстановление сигнала – подобно тому, как это происходит в системе на рис. 3. Напомним, что в нашей работе моделируется режим хаотического отклика без учета дифракции. Отметим, что явным недостатком схемы на рис. 4 оказывается требование к когерентности трех лазерных пучков: A_1, A_2, $M(x,t)$.

Имитация скрытой передачи изображений: режим детерминированного пространственно-временного хаоса

Приведем примеры имитации (де)шифрации изображений, выполненной методом вычислительного эксперимента на основе моделей (1) и (3) применительно к устройствам конфиденциальной связи, чьи схемы изображены на рис. 1, 2.

Результаты, полученные в случае замкнутой ЦТТ из четырех точек ($\Delta = 90°$, $\tau_n = 10^{-9}$ с, $R = 0{,}5$, $t_e = \tau_n$, $\gamma = 0{,}5$), приведены на рис. 5. Здесь глубина пространственной модуляции амплитуды лазерного пучка равна 0,048, что приблизительно в 10 раз выше, чем в модели [8]. Из его содержания вытекает возможность (де)шифрации двумерного, представленного последовательностью кадров изображения, при работе шифратора в режиме детерминированного пространственно-временного (иначе говоря, динамического)

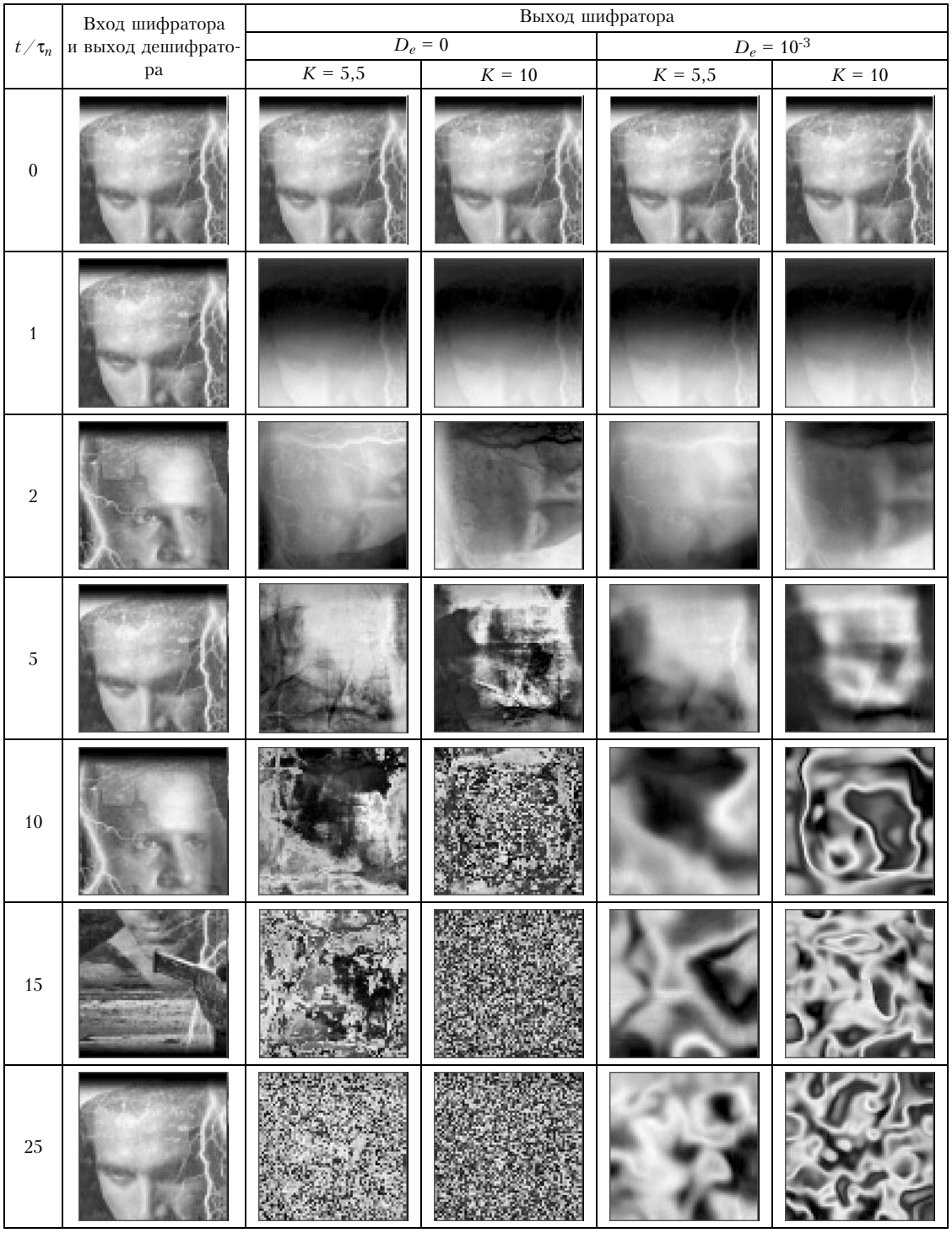


Рис. 5. Кадры процесса имитации (де)шифрации изображения в режиме динамического хаоса при различных значениях коэффициента нелинейности K и нормированного коэффициента диффузии D_e в НКИ

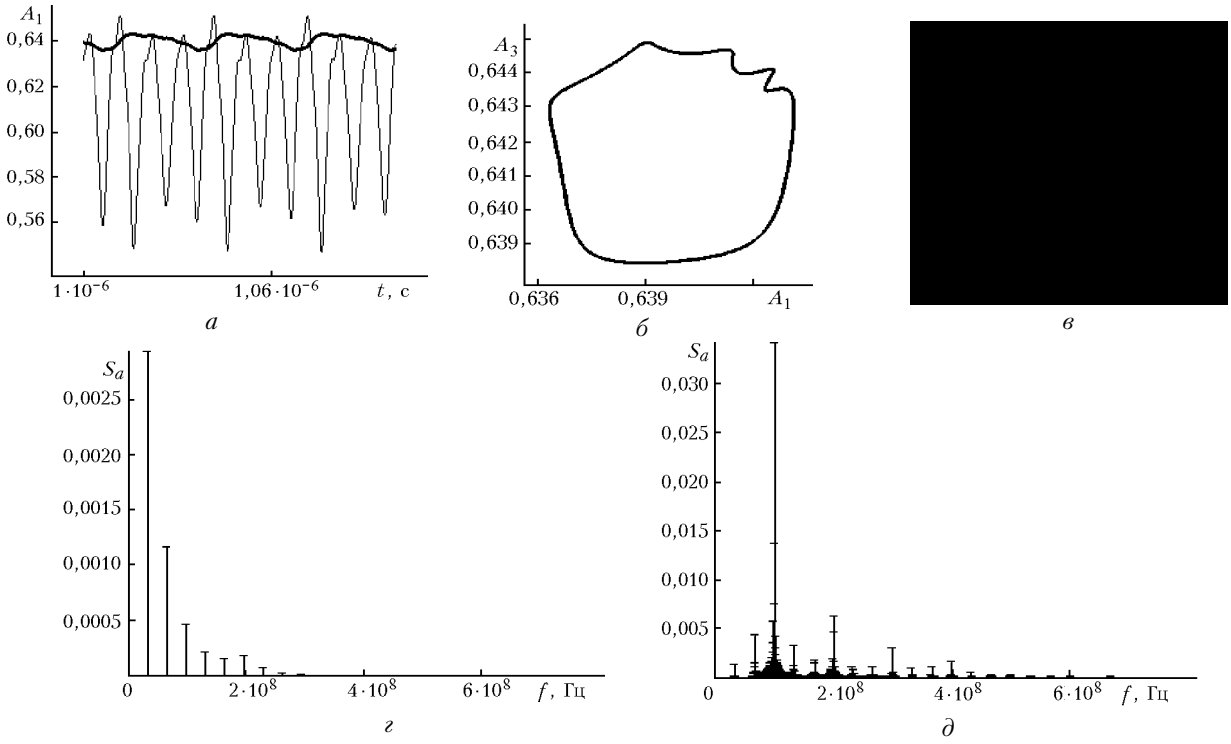
хаоса. Из визуального анализа изображений на рис. 5 можно заключить:

– с ростом времени t/τ_n степень скрытности сообщения возрастает;

– время «разогрева» шифратора составляет не менее $5\tau_n$;

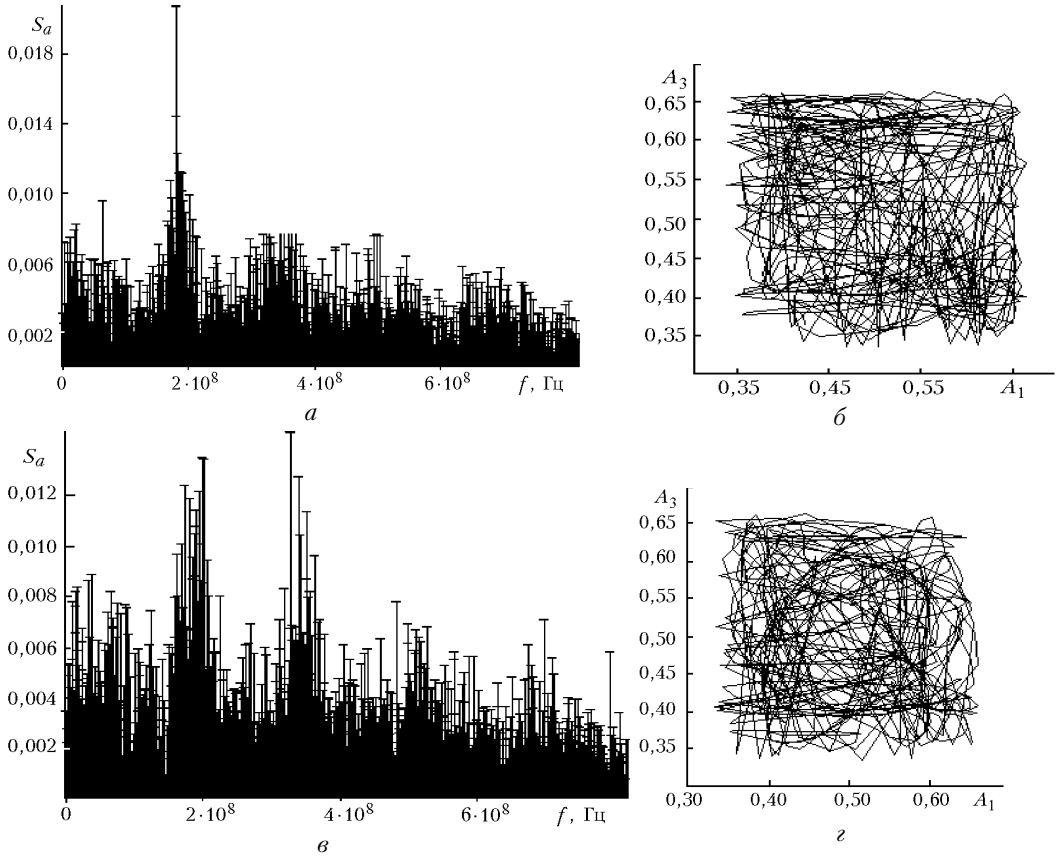
– скрытность и скорость ее нарастания зависят от комбинаций параметров НКИ.

Повышение степени скрытности связи с ростом коэффициента нелинейности K НКИ можно оценить методами спектрального анализа, обратившись к рис. 6, 7. На них представлены временные реализации, фазовые портреты, Фурье-спектры амплитуды A_i волны на выходе, где i – номер транспозиционной точки в ЦТТ, $D_e = 0$.



а *б* *в* *г* *д*

Рис. 6. Временная реализация A_1 (*а*), фазовые портреты (*б*, *в*), Фурье-спектры S_a выходной амплитуды A_1 волны (*г*, *д*) в случае автономного режима (*а* (жирная кривая), *б*, *г*) и режима амплитудной модуляции (*а* (тонкая кривая), *в*, *д*). $A_1 = A(\mathbf{r},t)$, где $\mathbf{r} = (0{,}5;\ 0)$; $A_3 = A(\mathbf{r},t)$, где $\mathbf{r} = (0;\ 0{,}5)$. $K = 4{,}55$. Закон модуляции: $A_{\text{вх}}(\mathbf{r},\ t) = [1 + 0{,}01 \cdot \cos(2\pi f_1\ t)]/1{,}01$, где $f_1 = 1/(30{,}618 \cdot 10^{-9}) \approx 0{,}3266 \cdot 10^8$ соответствует частоте гармоники Фурье-спектра, имеющей максимальную амплитуду (*г*)



а *б* *в* *г*

Рис. 7. Фурье-спектры S_a выходной амплитуды A_1 волны (*а*, *в*) и фазовые портреты (*б*, *г*) в случае автономного режима (*а*, *б*) и режима амплитудной модуляции (*в*, *г*) – тех же, что и на рис. 6. $K = 10$

Имитация скрытой передачи изображений: режим детерминированного пространственного хаоса

Рис. 8 доказывает возможность (де)шифрации двумерного изображения при работе шифратора в *статическом режиме*. При этом скрытность передачи сообщения зависит от комбинаций параметров НКИ. Статический режим, означающий отсутствие изменений во времени, как это ни парадоксально, отнюдь не исключает явления хаотизации статической пространственной структуры (двухмерной, трехмерной, N-мерной). В силу чего такое явление авторы предлагают называть *детерминированным пространственным хаосом*. Термин «детерминированный», как это принято, указывает на то, что неупорядоченность подчиняется некой закономерности, заложенной в математической модели, а не порождено случайным фактором. Тем самым подчеркивается аналогия/контраст с широко известным временным, т.е. динамическим (детерминированным), хаосом в моделях одномерных систем и пространственно-временным хаосом, или турбулентностью, в моделях многомерных систем. Детерминированный пространственный хаос естественно противопоставить пространственному порядку, демонстрируемому объектами, обладающими симметрией, фракталами и т.п. Визуальный анализ рис. 8 свидетельствует о принципиальной возможности существования детерминированного пространственного хаоса.

Цепочка транспозиционных точек как эквивалент дискретного отображения

В нашем случае детерминированный пространственный хаос реализуется в модели, состоящей из алгебраических уравнений (или равенств, если ЦТТ не замкнуты), получающихся из (1), когда $\partial U(\mathbf{r},t)/\partial t = 0$ и $D_e \Delta_{xy} U(\mathbf{r},t) = 0$. Как было показано выше, эквивалентом алгебраических уравнений (или равенств) является маршрутно-операторное уравнение (2). При этом значение динамической переменной ($U(\mathbf{r}, t)$ либо амплитуды лазерного пучка $A_{\text{НС}}(\mathbf{r}, t)$) в точках ЦТТ предлагается рассматривать как ее значения в точках дискретного отображения. Тем самым устанавливается связь между дифференциальными уравнениями для статического режима и дискретными отображениями. По нашему мнению, она составляет *альтернативу* классической связи [18, 19] между дифференциальными уравнениями для динамического режима и отображениями на основе сечений Пуанкаре. Поэтому номер транспозиционной точки в цепочке логично трактовать как дискретную эволюционную переменную.

В динамическом режиме значения динамической переменной ($U(\mathbf{r}, t)$ либо $A_{\text{НС}}(\mathbf{r}, t)$) в точках ЦТТ также можно трактовать как ее значения в точках дискретного отображения. Но при этом у отображения помимо традиционной дискретной эволюционной переменной (номера транспозиционной точки в цепочке) имеется непрерывная эволюционная переменная (время t в модели (1) или (2)), отвечающая

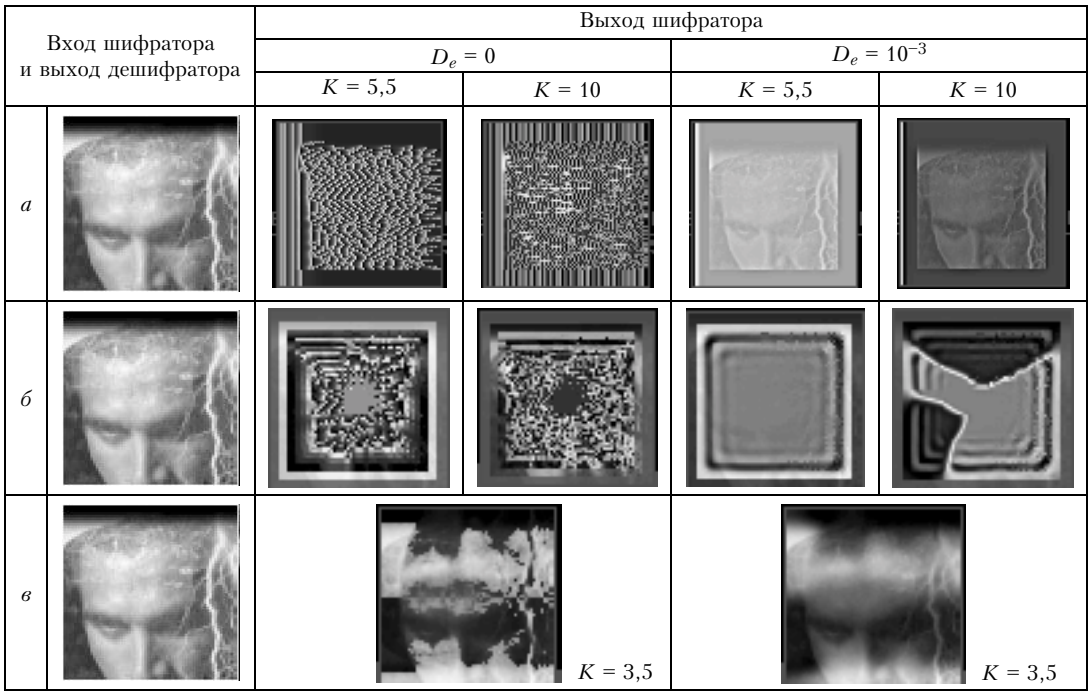


Рис. 8. Имитация (де)шифрации изображения в статическом режиме НКИ при различных значениях коэффициента нелинейности K и нормированного коэффициента диффузии D_e. Лазерный пучок в контуре обратной связи НКИ подвержен: сдвигу вдоль оси Ox, равному 1/80 (*а*); сжатию $\sigma = 0{,}9$ (*б*); зеркальному отображению относительно оси Ox (*в*)

за трансформацию ЦТТ как единого целого. Очевидно, что связь между значениями динамической переменной в точках такого дискретного отображения становится не столь тривиальной, как в случае статического режима. Применительно к НКИ эта связь латентно присутствует в модели (1) и явно в (2). Тем самым задачу изучения процессов в НКИ в пределах одной ЦТТ можно переформулировать как *задачу исследования эволюции дискретных отображений*.

Если ЦТТ замкнута, то дискретное отображение оказывается периодичным, а его период равен числу точек в ЦТТ. Незамкнутость ЦТТ предполагает четыре возможности: 1) конечное число m точек в ЦТТ; 2) бесконечное число точек ($m = \infty$) в ЦТТ, причем цепочка имеет такую нумерацию точек, что: а) номер начальной точки равен 1, а номер последней равен ∞; б) номер последней точки равен 1, а номер начальной равен $-\infty$; в) номера начальной и последней точек равны соответственно $-\infty$ и ∞. Насколько могут судить авторы, в случаях «б» и «в», когда неизвестна первая точка, приходится иметь дело с весьма специфической задачей, например в рамках модели (1), (2): если нас интересует эволюция хотя бы одной точки в цепочке, то необходимо учесть влияние *бесконечного* числа предшествующих ей точек в ЦТТ.

Из физических соображений ясно, что функционирование шифратора можно характеризовать временем разогрева τ_h (в режиме пространственно-временного хаоса) и временем установления τ_r (в статическом режиме), а дешифратора – временем установления синхронизации τ_s. Коснемся оценки эффективности этих устройств в указанных режимах, когда требуется передать одно изображение либо их серию.

Если требуется передать одно изображение, то в статическом режиме время, необходимое для шифрования, определяется временем установления τ_r процессов в шифраторе (НКИ), которое, в частности, зависит от длины ЦТТ. В этом случае принимающей стороне для дешифрации необходимо получить лишь установившееся изображение на выходе шифратора (криптограмму). Поэтому если в составе дешифратора предусмотрено устройство запоминания криптограммы, то длительность сообщения τ_m определяется его быстродействием. Если же такого устройства нет, то $\tau_m = \tau_s$. Время, необходимое для дешифрации, определяется временем установления синхронизации τ_s.

В режиме пространственно-временного хаоса возможны два варианта. Если шифратор и дешифратор предварительно синхронизованы, т.е. в обоих установлены соответствующие начальные условия, то время, необходимое для шифрации, для дешифрации, и τ_m определяются временем разогрева τ_h. В противном случае время дешифрации и τ_m определяются временем τ_s, а время шифрации равно наибольшему из значений τ_h, τ_s.

Если требуется передать серию изображений, то в статическом режиме процесс передачи каждого из сообщений ничем не будет отличаться от передачи одиночного изображения. В режиме пространственно-временного хаоса передача первого сообщения также не будет отличаться от передачи одиночного изображения. Последующие же изображения можно передавать настолько быстро, насколько это позволяют делать технические устройства смены и регистрации изображений (возможное снижение или повышение криптостойкости при столь быстрой передаче здесь не рассматривается).

Разумно считать, что выполняется следующее неравенство: $\tau_s < \tau_h < \tau_r$. Тогда получается, что статический режим *предпочтительнее*, если лимитирующим фактором выступают пропускная способность канала связи либо его цена, а также если стоит задача хранения информации в зашифрованном виде.

Очевидно, опыт моделирования оптического устройства нелинейно-динамической криптографии приводит к задаче многопараметрической оптимизации этого устройства, его возможных аналогов и вариантов.

Заключение

В статье обоснована возможность и намечены пути создания устройств нелинейно-динамической криптографии оптического диапазона на примере нелинейного кольцевого интерферометра.

Осуществлен лизинг методов описания и организации систем нелинейно-динамической криптографии радио- и оптического диапазонов. В частности, нелинейный кольцевой интерферометр (см. рис. 1) интерпретирован как обобщенная структурная модель шифраторов. Основу для такого обобщения дает маршрутно-операторное описание. Развитие этого подхода позволило предложить новые основания классификации и варианты реализации скрытой передачи информации на базе устройств нелинейно-динамической криптографии.

Оперирование понятием цепочек транспозиционных точек послужило основанием для обращения к элементам теории графов. В результате удалось сконструировать язык описания ЦТТ. На его основе построен «маршрутно-операторный формализм», ориентированный на изучение систем, физические взаимодействия в которых имеют структуру графа, в том числе кольцевых систем. На языке этого формализма описана модель [«маршрутно-операторное» уравнение (2)] процессов в шифраторе на базе НКИ. Трактовка подобных моделей как уравнения относительно неизвестного входного сигнала шифратора способна служить методологией синтеза «маршрутно-операторной» модели дешифратора, использующего хаотический отклик. Применение указанной методологии привело к модели дешифратора (3) и, в свою очередь, к оптической схеме устройства нелинейно-динамической криптографии (см. рис. 2).

Проведено сравнение варианта модели дешифратора (см. рис. 3) со схемой пространственно-временной связи в режиме синхронизации хаоса (см. рис. 4) [8], указаны недостатки последней и пути превращения ее в схему рис. 3.

Сделана оценка эффективности работы шифратора в режиме пространственно-временного хаоса и в статическом режиме.

Для статического и динамического режимов выявлена связь ЦТТ с дискретными отображениями. Показана возможность постановки задачи об эволюции

дискретных отображений как инструменте изучения процессов в НКИ в пределах одной ЦТТ.

Выдвинуто понятие детерминированного пространственного хаоса, возникающего в статическом режиме динамической системы, например НКИ.

Приведены примеры компьютерной имитации (де)шифрации двумерных изображений в режимах пространственно-временного и пространственного хаоса (см. рис. 5, 8). Влияние нелинейности на степень конфиденциальности связи в режиме пространственно-временного хаоса раскрывается с помощью Фурье-спектров и фазовых портретов (см. рис. 6, 7).

В целом продемонстрирован эвристический потенциал «маршрутно-операторного формализма» на примере изучения переноса сигналов в нелинейных кольцевых системах оптического диапазона.

Авторы признательны С.Н. Владимирову, В.В. Негрулю за указание на обзор [3] и А.А. Рыбаку – за указание на статью [8].

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект № 01-02-06175) и Министерства образования РФ (проект № 99 06 75 в рамках программы «Фундаментальные исследования высшей школы в области естественных и гуманитарных наук. Университеты России»).

1. *Новые* физические принципы оптической обработки информации / Под ред. С.А. Ахманова, М.А. Воронцова. М.: Наука, 1990. С. 263–326.
2. *Дойч Д.* Структура реальности. Ижевск: НИЦ «РиХД», 2001. 400 с.
3. *Хаслер М.* Достижения в области передачи информации с использованием хаоса // Успехи современной радиоэлектроники. 1998. № 11. С. 33–43.
4. *Владимиров С.Н., Негруль В.В.* Системы связи с пассивной хаотической синхронизацией // Тр. 5-й Международной конференции «Актуальные проблемы электронного приборостроения (АПЭП-2000)» (26–29 сентября 2000 г., г. Новосибирск). В 7 т. Т. 7. Новосибирск, 2000. С. 39–41.
5. *Измайлов И.В., Пойзнер Б.Н., Шулепов М.А.* Управление дехаотизацией колебательно-волнового процесса, сформированного в нелинейной системе с обратной связью // Тезисы Четвертой Междунар. конф. «Математические модели нелинейных возбуждений, переноса, динамики, управления в конденсированных системах и других средах» (27 июня – 1 июля 2000 г., Москва). М.: Изд-во Станкин, 2000. С. 50.
6. *Измайлов И.В., Пойзнер Б.Н., Шулепов М.А.* Модуляция и демодуляция оптических сигналов с использованием нелинейного кольцевого интерферометра. Ред. Ж. Изв. вузов. Физ. Томск, 2000. 6 с. Деп. в ВИНИТИ 04.07.00. № 1865-В00.
7. *Измайлов И.В., Пойзнер Б.Н., Шулепов М.А.* Опыт моделирования оптического устройства нелинейно-динамической криптографии // Сб. трудов. Международного оптического конгресса «Оптика XXI века» (16–20 октября 2000 г., г. Санкт-Петербург). Конференция «Фундаментальные проблемы оптики» (17 – 19 октября 2000 г., Санкт-Петербург). С. 30–31.
8. *Garcia-Ojalvo J., Roy R.* Spatiotemporal communication with Synchronized Optical Chaos // http://xxx.lanl.gov/abs/nlin.CD/0011012.
9. *Izmailov I.V., Shulepov M.A.* Simulation of signal enciphering by means of nonlinear ring interferometer and decoding // Proc. SPIE. 2001. V. 4513. P. 46–51.
10. *Измайлов И.В.* Модель процессов в нелинейном кольцевом интерферометре, учитывающая запаздывание, потери, преобразование плотности энергии и многопроходовость немонохроматического поля. Ред. Ж. Изв. вузов. Физ. Томск, 1997. 15 с. Деп. в ВИНИТИ 31.12.97. № 3865-В97.
11. *Измайлов И.В., Магазинников А.Л., Пойзнер Б.Н.* Идентификация винтовой дислокации волнового фронта и компенсация ее влияния на структурообразование в моделях кольцевого интерферометра // Оптика атмосф. и океана. 2000. Т. 13. № 9. С. 805–812.
12. *Chesnokov S.S., Rybak A.A.* Spatiotemporal Chaotic Behavor of Time-Delayed Nonlinear Optical Systems // Laser Phys. 2000. V. 10. № 5. P. 1–8.
13. *Соснин Э.А., Пойзнер Б.Н.* Исследовательская деятельность в университетах и лизинг методологий // Интеграция учебного процесса и фундаментальных исследований в университетах: инновационные стратегии и технологии: Первая Всерос. конф. (20–21 апреля 2000 г., г. Томск). Т. 1. Томск: Изд-во ТГУ, 2000. С. 115–118.
14. *Розанов Н.Н.* Оптическая бистабильность и гистерезис в распределенных нелинейных системах. М.: Наука, 1997. 336 с.
15. *Евтушенко Г.С., Пойзнер Б.Н., Соснин Э.А., Тарасенко В.Ф.* Как начать работать в научном сообществе: Уч. пособие. Томск: Изд-во Том. ун-та, 1998. 140 с.
16. *Математический* энциклопедический словарь / Под ред. Ю.В. Прохорова. М.: Сов. энциклопедия, 1988. 847 с.
17. *Владимиров С.Н., Негруль В.В.* Сравнительный анализ некоторых систем хаотической синхронной связи // Изв. вузов. Прикл. нелинейн. динам. 2000. Т. 8. № 6. С. 53–64.
18. *Анищенко В.С., Вадивасова Т.Е., Астахов В.В.* Нелинейная динамика хаотических и стохастических систем. Фундаментальные основы и избранные проблемы. Саратов: Изд-во Саратов. ун-та, 1999. 368 с.
19. *Кузнецов А.П.* Наглядные образы хаоса // Сорос. образ. ж. 2000. № 11. С. 104–110.

I.V. Izmailov, B.N. Poizner. **Nonlinear optical device of information hidden transmission: realization variants.**

The nonlinear ring interferometer (NRI) is chosen as a generalized structural model of ciphering devices in nonlinear-dynamic cryptology. The suggested concept of chains of «transpositional points» (CTP) allows one to present NRI as a system in which the optical-physical interactions have a structure of a graph. For analysis and synthesis of similar systems, a «route-operator formalism» is constructed. The processes in NRI are described and a model of decoder using the chaotic response is synthesized by means of the formalism. The possible foundations for classification of nonlinear dynamic cryptography devices and following realization variants of the devices are stated. The examples of computer imitation of ciphering/deciphering in dynamical chaos and static regimes of functioning are presented and also the influence of parameters of the model on confidentiality degree of communication is illustrated. The concept of determined spatial chaos originating in a static regime of dynamic system is considered. The relation of CTP with discrete maps is detected.