

УДК 530.18+532.59+534.0+621.37

НЕЛИНЕЙНОЕ ПОДМЕШИВАНИЕ РАДИО- И ВИДЕОСИГНАЛОВ В СИСТЕМЕ СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ДИНАМИЧЕСКОГО ХАОСА

И.В. Романов, И.В. Измайлов, А.П. Коханенко, Б.Н. Пойзнер

Томский государственный университет

E-mail: roil@elefot.tsu.ru

Экспериментально показана возможность передачи и приёма сигналов методом нелинейного подмешивания и хаотического отклика на основе динамической системы с нелинейностью, обладающей тремя минимумами.

Ключевые слова:

Генератор хаотических колебаний, связь, хаотическая маскировка, нелинейное подмешивание, синхронный хаотический отклик.

Key words:

Chaos generator, communication, chaotic masking, nonlinear admixing, synchronous chaotic response.

В радиофизике, радиотехнике и в оптике сформулирован ряд важных практических задач, для решения которых требуются источники сигналов, занимающих широкий частотный диапазон и имеющих высокую спектральную плотность. Потребность в источниках широкополосных колебаний обусловлена возможностью построения на их основе систем: радиопротиводействия, радиомаскировки, шумовой радиолокации, конфиденциальной связи, сверхбыстродействующей радиосвязи, криптографических структур, приборов нетрадиционного воздействия на биологические объекты, различного рода устройств специального назначения [1].

Использование методов нелинейной динамики и детерминированного хаоса в задаче защиты информации было показано, например, в работах [1–7]. К настоящему времени накоплен значительный опыт в разработке схем передачи и алгоритмов кодирования информации с использованием динамического хаоса. Следует отметить, что существует достаточно большое число различных вариантов систем связи, использующих хаотические сигналы. Это связано с тем, что модуляция и манипуляция хаотическими колебаниями при передаче и методы селекции полезного сигнала при приеме значительно разнообразнее по сравнению с традиционными

системами связи с амплитудной, частотной и фазовой модуляцией и манипуляцией. По этой же причине возможности, принципы построения и пути реализации хаотических систем связи изучены далеко не полностью. В литературе предложены различные варианты введения информационного сигнала в хаотический сигнал на передающей стороне и его восстановления на приёмной стороне. Вторая задача является более сложной.

В настоящее время коммуникационные системы с хаотической несущей используют два типа приёмников: когерентные и некогерентные [5, 7]. *Некогерентные* приёмники используют статистические свойства приходящего из канала связи сигнала для извлечения информации. *Когерентные* приёмники представляют собой системы, аналогичные генераторам хаотических сигналов в передатчиках, либо их фрагментам. Они способны синхронизоваться с передатчиком, а потому позволяют извлекать сообщение из принимаемого хаотического сигнала.

Примером использования когерентных приёмников является метод нелинейного подмешивания. Принцип работы схемы с нелинейным подмешиванием следующий (рис. 1). В ведущей системе информационный сигнал $m(t)$ подмешивается к собственному сигналу системы $x(t)$. Информацион-

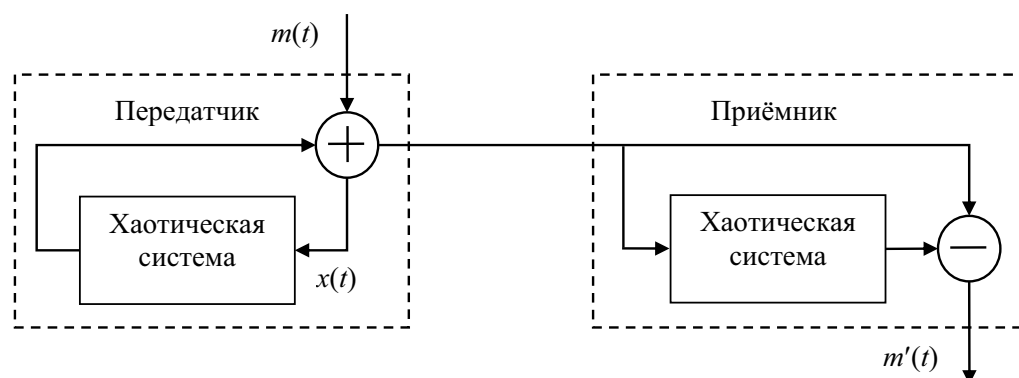


Рис. 1. Схема связи с нелинейным подмешиванием в передатчике и синхронным хаотическим откликом в приёмнике

ный сигнал изменяет режим работы передающего устройства, однако режим остаётся хаотическим. Сформированная смесь $x_m(t) = x(t) + m(t)$ передаётся по каналу связи.

Существует ряд достоинств и недостатков способа, основанного на нелинейном вводе информационного сигнала и на синхронном хаотическом отклике для извлечения сообщения. К достоинствам можно отнести: 1) возможность точного (без искажений) восстановления информационного сигнала при отсутствии помех в канале связи; 2) сложность выделения информационного сигнала посторонним лицом методом адаптивной фильтрации, так как информационный сигнал участвует в формировании хаотического поведения передающей системы. К недостаткам этого способа можно отнести: 1) опасность частичной или полной потери хаотической синхронизации между передающей и приёмной системами из-за присутствия шумов, линейных и нелинейных искажений сигнала в канале связи; 2) ограничение на уровень информационного сигнала, задаваемое величиной хаотического сигнала: превышение первого над вторым чревато срывом хаотических колебаний или демаскировкой сообщения.

В контексте защиты информации важным параметром, обуславливающим устойчивость криптосистемы к «взлому», служит количество ключей. Последнее связано здесь с разнообразием хаотических режимов. В свою очередь, оно обеспечивается числом независимых параметров системы и шириной диапазона их допустимых значений. Важной частью таких систем является нелинейный элемент, свойства которого отражает нелинейная многомерная передаточная характеристика $F(x, \mu)$, фигурирующая, например, в уравнении вида:

$$\tau \frac{dx(t)}{dt} + x(t) = F(x(t - t_e), \mu), \quad (1)$$

где x – вектор динамических переменных; μ – вектор параметров ДС. Очевидно, чем богаче характеристика $F(x, \mu)$ особенностями (например, экстремумами), тем больше параметров она потенциально содержит. Значит, тем больше количество ключей. Судя по литературе [1, 8–10], большой популярностью у исследователей на практике пользуются системы, имеющие характеристику $F(x, \mu)$ с одним экстремумом, либо с двумя, например, схема Чуа. Хорошо изучена сложная динамика в кусочно-линейном «пилообразном» отображении с числом ветвей $N \geq 2$ вплоть до $N=5$ [11. С. 28–38].

В связи с этим целесообразно выяснить условия, при которых возможно экспериментально осуществить защиту информации при использовании в качестве передатчика генератора детерминированного хаоса с нелинейной характеристикой $F(x, \mu)$. При этом нетривиальной задачей оказывается выполнение требований к идентичности формы характеристики $F(x, \mu)$ передатчика и приёмника, а также к ее воспроизводимости при изготовлении приёмно-передающего устройства. То есть пе-

ред разработчиком стоит проблема минимизации отличия $|\delta F(x, \mu)| = |F_r(x, \mu) - F_t(x, \mu)|$ в форме характеристик приёмника $F_r(x, \mu)$ и передатчика $F_t(x, \mu)$.

В соответствии с такой постановкой задачи ниже приводятся математическая модель, результаты вычислительных и лабораторных экспериментов, полученных при создании генератора хаоса с нелинейной функцией $F(x, \mu)$, рис. 3.

Математическая модель и результаты вычислительного эксперимента

Общая структура генератора хаоса (ГХ) представлена на рис. 2, а. Она содержит регулируемый усилитель со схемой смещения $(D+kU)$ и линию задержки. Последняя обеспечивает высокую размерность фазового пространства и хаотический режим динамической системы (подобно тому, как это делает колебательный контур, например, в работах [1, 8–10]). Нелинейный элемент (рис. 2, б) включает блок преобразования сигнала U с «перевёрнутой» N -образной передаточной характеристикой $g(U)$ и умножитель, формирующий характеристику $g^2(U)$. В экспериментальной установке нелинейное преобразование $g(U)$ реализовано на диодах Шоттки, операционных усилителях, а умножение осуществляется четырёхквadrантным перемножителем AD835.

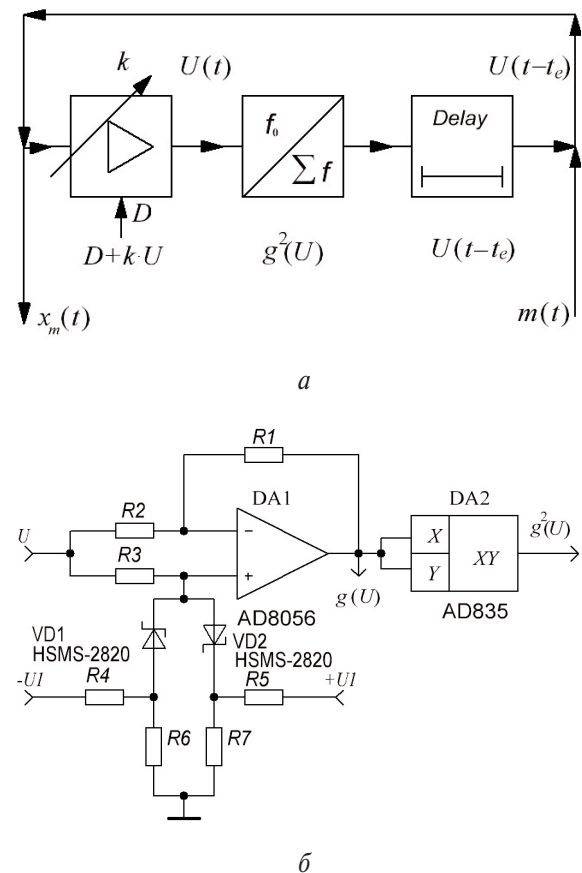


Рис. 2. Схема: а) структурная генератора хаоса; б) электрическая нелинейного элемента $g^2(U)$

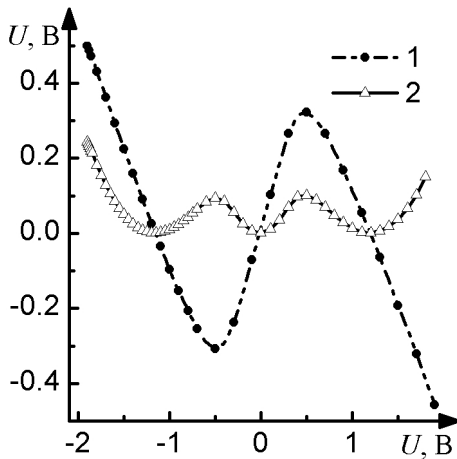


Рис. 3. Функции $g(U)$ (кривая 1) и $g^2(U)$ (кривая 2) нелинейного преобразования: экспериментально полученные точки соединены отрезками

С учётом описания конструкции ГХ можно построить его математическую модель в достаточно абстрактном виде. Пусть $U_{\text{out}} = U = g^2(U_{\text{in}})$ — статическая передаточная характеристика цепи из нелинейного элемента и регулируемого усилителя. Инерционность её учтём феноменологически, введя время релаксации τ . Будем полагать, что инерционность остальных элементов генератора пренебрежимо мала по сравнению с τ . Тогда модель динамики в генераторе хаоса с учётом следующих предположений: $F(x, \mu) \equiv F(U, D, k, t_e) \equiv D + kg^2(U(t - t_e))$, $x = U$, $\mu = (D, k, t_e)$ принимает вид

$$\tau \frac{dU(t)}{dt} + U(t) = D + kg^2(U(t - t_e)), \quad (2)$$

где k — коэффициент нелинейности в модели, соответствующий коэффициенту усиления в радиотехнической схеме; $U(t)$ — сигнал на входе элемента $g(U)$ в момент времени t (пропорциональный сигналу на выходе $g(U)$ в момент $t - t_e$), D — напряжение постоянного смещения, $g(U) = M(af(U) - U)$, $f(U) = \text{sgn}(U)[1 - \exp(-|U/V|)]$. В расчётах — с ориентацией на данные эксперимента (рис. 3) — полагалось, что $V_i = 0,472$ В, $a = 1,31$, $M = 1,0$. В приближении мгновенного отклика модель можно переписать в виде дискретного отображения $U_{i+1} = F(U_i)$. Уравнение динамики (2) решалось методом Рунге–Кутты четвёртого порядка с помощью программы, написанной на языке C++.

Решение дифференциального уравнения (2) показывает наличие сложных квазипериодических и хаотических колебаний [12, 13]. Одним из простых методов изучения многообразия динамических режимов в модели является построение бифуркационных диаграмм. На рис. 4 приведена бифуркационная диаграмма решений уравнения (2). Точки на ней соответствуют экстремумам решений (первая производная равна нулю), поэтому количество и взаимное отображение точек однозначно определяет режим. Широкие затемнённые области свидетельствуют о хаотических режимах.

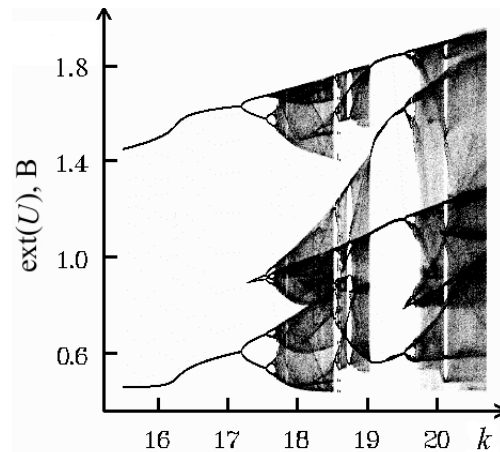


Рис. 4. Бифуркационная диаграмма для (1) при $D = -0,17$ В

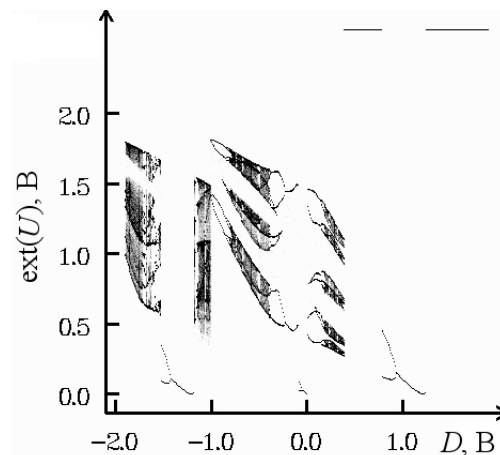


Рис. 5. Бифуркационная диаграмма для (1) при $k = 15,5$

Наблюдаемое на диаграмме характерное [8, 9, 14] «раздвоение» кривых (при переходе от периодических к хаотическим движениям динамической системы) свидетельствует о каскаде бифуркаций удвоений периода. Это влечёт появление субгармоник и расширение спектра $U(t)$ в направлении низких частот. Напротив, на рис. 4 при $k \approx 17,3$ и $k \approx 19,5$, а также на рис. 5 при $D \approx -0,7$ и $D \approx 0$ различимы вновь рождающиеся «клювообразные» ветви. Они свидетельствуют о появлении пары экстремумов, что неизбежно должно приводить к уширению спектра $U(t)$ в сторону высоких частот. В интервале изменения значений параметра усиления $k \approx 18 \dots 20$ при $D = -0,17$ В области хаоса перемежаются окнами периодичности.

Очевидно, что наличие детерминированного хаоса и обогащение спектра (суб)гармониками создаёт предпосылки для практического применения ГХ в системе конфиденциальной связи.

Эксперименты по шифрации и дешифрации радио- и видеосигналов

Для демонстрации возможностей передачи сигналов $m(t)$ различной формы проводились лабораторные эксперименты по их маскировке в режиме

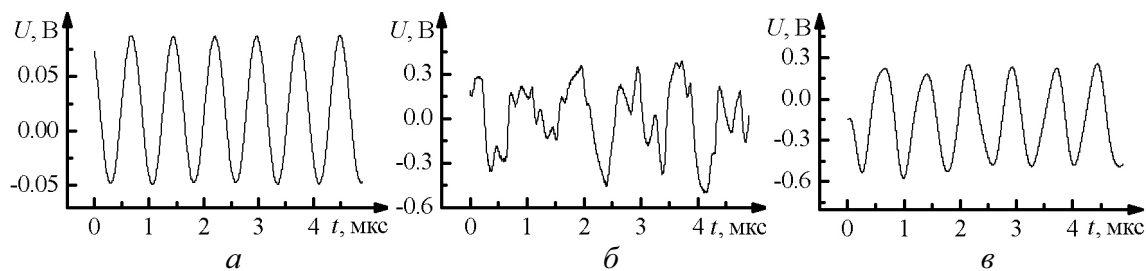


Рис. 6. Сигналы: а) на входе передатчика, б) в канале связи, в) на выходе приёмника

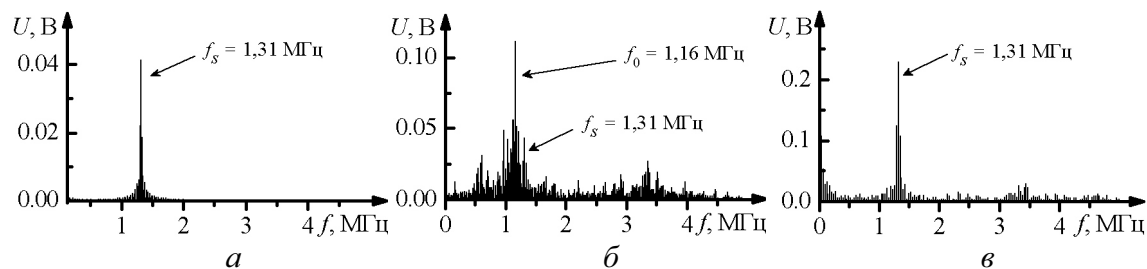


Рис. 7. Спектры Фурье при нелинейном подмешивании гармонического сигнала: а) до передатчика, б) в канале связи, в) после приёмника; f_s – частота сигнала на входе передатчика, f_0 – основная частота колебаний динамической системы

нелинейного подмешивания. На рис. 6 и 7 изображены сигналы и их фурье-спектры соответственно для случая гармонического сигнала $m(t)$ с частотой $f_s = 1,31$ МГц на входе передатчика. Запись сигналов проводилась в следующих узлах лабораторной установки: на входе передатчика (рис. 6, а, и рис. 7, а), в линии передачи (рис. 6, б, и рис. 7, б), на выходе приёмника (рис. 6, в, и рис. 7, в).

Судя по рис. 6, б, гармонический сигнал трудно распознать на фоне хаотической «помехи». Согласно рис. 7, б, спектр полезного сигнала «спрятан» в спектре хаотических колебаний $U(t)$ (или $x(t)$ согласно рис. 1), поскольку последний богат спектральными компонентами с амплитудой, большей, чем у компонент спектра $m(t)$. Спектральный компонент с максимальной амплитудой имеет частоту $f_0 = 1,16$ МГц, близкую к значению $1/t_c$. В спектре дешифрованного (восстановленного) сигнала (рис. 6, в, и рис. 7, в) наблюдаются высокочастотные искажения, о причинах которых будет сказано ниже.

В отличие от гармонического сигнала, используемые для передачи информации сигналы характеризуются конечной по ширине полосой частот. Возьмём в качестве тестового сигнал в виде последовательности прямоугольных импульсов. Он привлекателен для этой цели, поскольку имеет «лепестковый» спектр, который тем шире, чем короче импульсы. Чтобы выяснить, как ведёт себя исследуемая система связи под воздействием таких сигналов, подадим на передатчик, работающий в хаотическом режиме, периодическую последовательность импульсов длительностью 1 мкс со скважностью 10. Рис. 8 и 9 аналогичны по содержанию рис. 6 и 7. Нетрудно видеть, что общие выводы, которые были сделаны при анализе рис. 6 и 7, справедливы и здесь.

Пусть m' и $m'_{m=0}$, m и $x_{m=0}$ – среднеквадратичные значения напряжения $m'(t)$ на выходе приёмника при наличии и в отсутствие информационного сигнала $m(t)$ на входе передатчика, входного сигнала $m(t)$ передатчика и хаотического сигнала $x(t)$ в нём при $m(t) = 0$. Тогда, измерив их, можно построить (рис. 10) зависимости отношения S_n величины $[(m')^2 - (m'_{m=0})^2]$ информационного сигнала на выходе приёмника к уровню $(m'_{m=0})^2$ ошибки дешифрации $S_n = 10 \log[-1 + (m')^2 / (m'_{m=0})^2]$ от отношения $\alpha = m / x_{m=0}$ среднеквадратичных значений напряжения: входного сигнала $m(t)$ передатчика и хаотического сигнала $x_{m=0}(t)$ в нём.

В электрических цепях шумы присутствуют всегда. Например, тепловой шум и шум Джонсона неустранимы, поскольку связаны с фундаментальными свойствами материала и элементной базы устройства. При измерении шумов в приёмнике и передатчике показано, что шумы в системе не превышают ~ 2 мВ. Из этого следует, что низкое соотношение сигнал/шум (рис. 10) на выходе передатчика связано с конструктивными особенностями схемы передатчика и приёмника.

Действительно, известно, что точность восстановления сигнала зависит как от разбалансировки параметров динамической системы, так и от их среднего значения и режима динамической системы. В осуществлённом нами устройстве отличие функции $F(U)$ в приёмнике и передатчике вызвано разбросом величин напряжений смещения операционных усилителей (для AD8056 – 3 мВ), различием коэффициентов ослабления синфазного сигнала, выраженной зависимостью вольтамперной характеристики диодов-ограничителей (HSMS-2820) от температуры, а также разницей их рабочих температур.

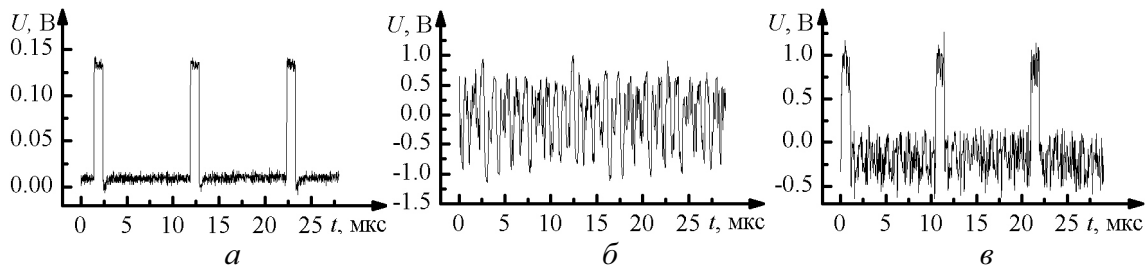


Рис. 8. Сигналы: а) на входе передатчика, б) в канале связи, в) на выходе приёмника

Р

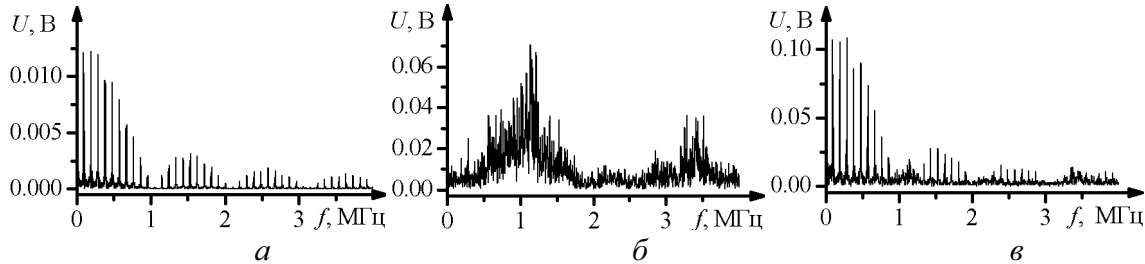


Рис. 9. Спектры Фурье при нелинейном подмешивании последовательности прямоугольных импульсов: а) до передатчика, б) в канале связи, в) после приёмника

Снижение ошибки дешифрации возможно путём замены операционного усилителя AD8056 на более точный OP37 (типичное значение входного напряжения смещения равно 10 мкВ). Это должно уменьшить погрешность $|m'_{m=0}|$ восстановления сигнала m' .

Предположим, что напряжение ошибки $m'_{m=0}$ пропорционально произведению некоторой суммарной ошибки δF (например, $\delta F = \langle \delta F(U) \rangle_U = \langle |F_A(U) - F_i(U)| \rangle_U$ либо $\delta F = \langle \delta F(U(t)) \rangle_t = \langle |F_A(U(t)) - F_i(U(t))| \rangle_t$) функции $F(U)$ на коэффициент k ($m'_{m=0} \sim k \delta F$). Пусть $k=10$, тогда рост величины δF в 10 раз приведёт к увеличению $m'_{m=0}$ в 100 раз. То же самое справедливо для случая уменьшения δF и, соответственно, ошибки восстановления $m'_{m=0}$. Из этих соображений следует, что для увеличения значения отношения сигнал/шум S_n в 4 раза для $k=10$ достаточно уменьшить $\delta F(U)$ примерно в 10 раз.

Данные оценки качественно подтверждаются взаимным расположением кривых 1–3 (рис. 10): чем больше коэффициент усиления k , тем ниже качество дешифрации. Действительно, кривые 1–3 (построенные для $k=15$, $k=19$ и $k=22$) показывают, что в диапазоне изменения $0 \dots 1$ параметра $\alpha = m/x_{m=0}$ отношение $S_n = 10 \log[-1 + (m')^2/(m'_{m=0})^2]$ достигает максимальных значений при $\alpha=1$. Эти значения равны 25, 19 и 16,7 дБ, соответственно.

Другой путь борьбы за качество восстановленного сигнала — фильтрация нелинейных помех $m'_{m=0}$. Особенностью функции $F(U)$ является её высокий порядок аппроксимации. Сигнал, преобразованный $F(U)$, искажается, и в его спектре появляются компоненты высоких порядков (рис. 7, в, 9, в). В дешифрованном сигнале именно высокочастотные составляющие спектра вносят значительную ошибку, возможно, из-за неудовлетворительной «работы» функции $F(U)$ на высоких частотах.

Тогда, естественно, потребуются ограничения на спектр информационного сигнала.

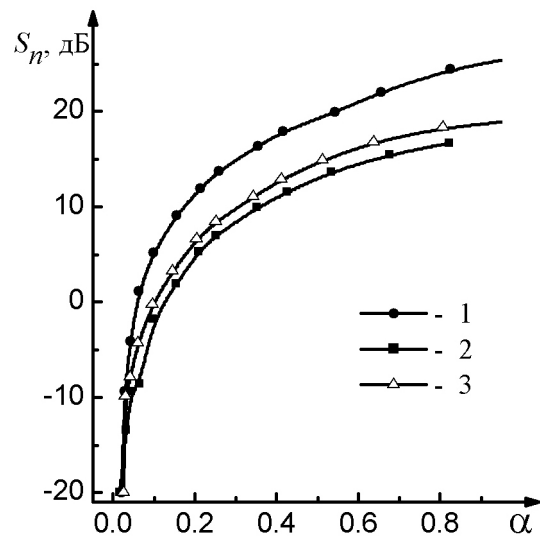


Рис. 10. Зависимость отношения сигнал/шум S_n на выходе приёмника от отношения среднеквадратичных значений напряжения входного сигнала и хаотического сигнала в передатчике α при $k=15$ (1), $k=19$ (2), $k=22$ (3), $D=-0,4$ В

На рис. 11 приведены результаты шифрации и дешифрации видеосигнала с применением описанного метода нелинейного подмешивания сигнала в передатчике и хаотического отклика в приёмнике (рис. 1). Исходный сигнал с полосой частот до 6 МГц (рис. 11, а) создавался стандартной видеокамерой. Визуализатором сигнала служил компьютер со стандартным устройством захвата видеосигнала с приёмника. Восстановленное изображение хорошо различимо на рис. 11, в. Наблюдаемые высокочастотные искажения объясняются неболь-

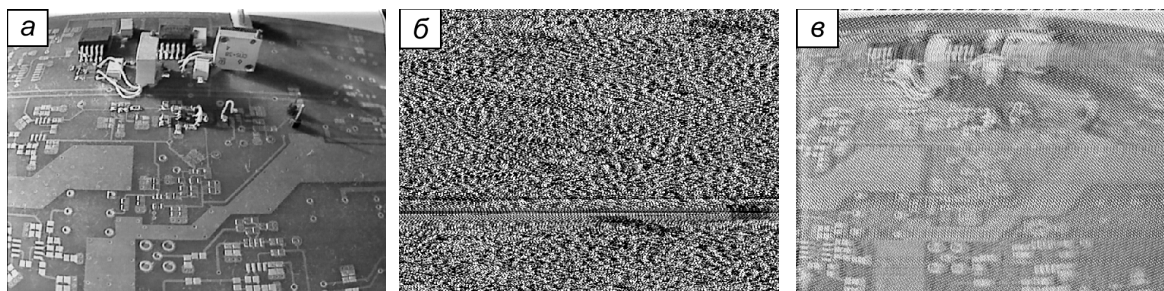


Рис. 11. Опыт передачи изображения (а) видеосигналом, хаотизированным в передатчике (б), и результат восстановления изображения в приёмнике (в)

шим расхождением параметров приёмника и передатчика за счёт больших входных напряжений смещений операционного усилителя в схеме нелинейного элемента. Тем не менее, авторы полагают, что модернизация и более тонкая настройка узлов схем устранят данную проблему.

Выводы

Экспериментально доказана возможность передачи и приёма сигналов методом нелинейного подмешивания и хаотического отклика на основе динамической системы с нелинейным элементом. Проведены эксперименты по шифрованию и дешифрованию гармонического сигнала, периодической последовательности прямоугольных импуль-

сов и видеосигнала. Получена зависимость качества дешифрации (отношение сигнал/шум на выходе приёмника) от относительного уровня информационного сигнала. Установлено, что отношение сигнал/шум на выходе дешифратора ограничивается сверху разбросом параметров в элементе схемы нелинейного преобразования передатчика и приёмника. Влияние этого фактора растёт с увеличением значения коэффициента усиления.

Предложена математическая модель поведения динамической системы. Рассчитаны бифуркационные диаграммы режимов. Характер и расположение точек на них свидетельствуют о наличии как статических, периодических, так и хаотических аттракторов в модели.

СПИСОК ЛИТЕРАТУРЫ

1. Дмитриев А.С., Панас А.И. Динамический хаос: новые носители информации для систем связи. – М.: Изд-во физ.-мат. лит-ры, 2002. – 252 с.
2. Владимиров С.Н., Золотов С.В., Негруль В.В., Перфильев В.И. Детерминированный хаос в СВЧ электронике // Электронная промышленность. – 2002. – № 2. – С. 87–90.
3. Дмитриев А.С. Беспроводная связь с хаотическими носителями: состояние и перспективы // Будущее прикладной математики: лекции для молодых исследователей. Поиски и открытия / под ред. Г.Г. Малинецкого. – М.: Книжный дом «ЛИБРОКОМ», 2009. – С. 511–529.
4. Кислов В.Я. Динамический хаос и его использование в радиоэлектронике для генерирования, приема и обработки колебаний и информации // Радиотехника и электроника. – 1993. – Т. 38. – № 10. – С. 1783–1815.
5. Хаслер М. Достижения в области передачи информации с использованием хаоса // Успехи современной радиоэлектроники. – 1998. – № 11. – С. 33–43.
6. Дмитриев А.С., Кузьмин Л.В., Лактюшкин А.М. Амплитудная модуляция и демодуляция хаотических сигналов // Вопросы прикладной физики: Межвуз. науч. сб. / под ред. Ю.В. Гуляева, Н.И. Синицына и В.М. Аникина. – Саратов: Изд-во Саратов. ун-та, 2004. – Вып. 11. – С. 185–191.
7. Владимиров С.Н., Измайлов И.В., Пойзнер Б.Н. Нелинейно-динамическая криптология: радиофизические и оптические системы / под ред. С.Н. Владимирова. – М.: Физматлит, 2009. – 208 с.
8. Кузнецов С.П. Динамический хаос (курс лекций). – М.: Изд-во физ. мат. лит-ры, 2001. – 296 с.
9. 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.
10. Владимиров С.Н. Динамические неустойчивости потоков и отображений. Взгляд радиофизика. – Томск: Изд-во Том. ун-та, 2008. – 352 с.
11. Аникин В.М., Голубенцев А.Ф. Аналитические модели детерминированного хаоса. – М.: Физматлит, 2007. – 328 с.
12. Измайлов И.В., Коханенко А.П., Пойзнер Б.Н., Романов И.В. Генератор детерминированного хаоса радиодиапазона с линейной задержки на оптическом волокне // Известия вузов. Сер. Физика. – 2008. – Т. 51. – № 9/2. – С. 178–179.
13. Романов И.В., Измайлов И.В. Генератор хаоса с нелинейностью N-типа и удвоителем частоты // Материаловедение, технологии и экология в 3-м тысячелетии: Матер. IV Всерос. конф. молодых ученых. – г. Томск, 19–21 октября 2009. – Томск: Изд-во Института оптики атмосферы СО РАН, 2009. – С. 628–631.
14. Карлов Н.В., Кириченко Н.А. Колебания, волны, структуры. – М.: Физматлит, 2003. – 496 с.

Поступила 15.07.2010 г.