Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

УДК 004.056.5

ПОЛОВЕНЯ
Сергей Иванович

АЛГОРИТМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ОТКРЫТЫХ КАНАЛАХ С ПОМЕХАМИ МЕТОДАМИ НЕЛИНЕЙНОЙ ДИНАМИКИ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

по специальностям 05.13.19 – Методы и системы защиты информации, информационная безопасность и 05.12.04 – Радиотехника, в том числе системы и устройства телевидения

Минск 2014

Работа выполнена в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники»

Чердынцев Валерий Аркадьевич, доктор технических наук, профессор, профессор кафедры радиотехнических систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Сидоренко Алевтина Васильевна, доктор технических наук, профессор, профессор кафедры физики и аэрокосмических технологий
Белорусского государственного университета,
Хижняк Александр Вячеславович, кандидат технических наук, доцент, начальник кафедры автоматизированных систем управления войсками учреждения образования «Военная академия Республики Беларусь»

Оппонирующая организация: учреждение образования «Полоцкий государственный университет»

Защита состоится «9» октября 2014 г. в 14.00 часов на заседании совета по защите диссертаций Д 02.15.06 при учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, Минск, ул. П. Бровки, 6, корп. 1, ауд. 232, тел. 293-89-89, e-mail: dissovet@bsuir.by

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радио-

КРАТКОЕ ВВЕДЕНИЕ

Возрастающие требования к защищённости информации от перехвата при её передаче по открытым каналам технически удовлетворяются двумя подходами: 1) усовершенствованием алгоритмов криптографической защиты информации; 2) созданием и адаптацией новых сигнально-кодовых конструкций и методов информационной модуляции. Второе направление связано с системами, в которых имеется существенно нелинейная обратная связь.

Интерес к хаотическим процессам в системах передачи и обработки обусловлен объективными тенденциями: повышающимися требованиями к защищённости и скрытности передачи информации.

На текущий момент времени показана возможность передачи полезных сигналов на основе динамического хаоса по проводным каналам. Однако использование хаоса в радиоканале является нерешённой задачей: уверенная обработка возможна при длине радиолинии в несколько десятков метров или менее. Хаос-генераторы обладают сверхчувствительностью к отклонениям собственных параметров и искажениям сигнала в канале. Указанный недостаток существенно снижает возмож ость использования динамического хаоса при передаче информации по реальному радиоканалу с помехами.

В диссертационной работе предлагается комплексный подход к решению проблемы устойчивости хаос-сигналов к воздействию помех, базирующийся на использовании теории сигналов, теории динамических систем и марковской теории нелинейной фильтрации.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами и темами

Результаты диссертационной использовались в госбюджетных НИР, выполнявшихся на кафедре радиотехнических систем БГУИР: «Разработка алгоритмов, структурно-функциональных схем и устройств передачи и приема информации в системах пожарной сигнализации» (ГБ 08-3046, ГР № 20081282).

Тема диссертационной работы соответствует следующим приоритетным направлениям научных исследований и научно-технической деятельности в Республике Беларусь.

1. Системные решения, архитектура, методологическое и аппаратно-программное обеспечение высокопроизводительных параллельных и распределенных информационно-коммуникационных процессов, сетей и

систем, их информационная безопасность (п. 5.2 Постановления Совета Министров Республики Беларусь от 19 апреля 2010 г. № 585 «Об утверждении перечня приоритетных направлений научных исследований Республики Беларусь на 2011–2015 годы»).

2. Макротехнология «Производство средств связи, вычислительных средств и программного продукта; высокопроизводительные системы, технологии передачи и обработки информации», критические технологии: «обработка, передача, хранение и защита информации» (п. 34 Указа Президента Республики Беларусь от 22 июля 2010 г. № 378 «Об утверждении приоритетных направлений научно-технической деятельности в Республике Беларусь на 2011–2015 годы»).

Цель и задачи исследования

Целью диссертационной работы является создание методов и алгоритмов генерации и оптимальной обработки сигналов на основе систем с нелинейной динамикой для обеспечения защищенной передачи информации по открытым каналам связи в условиях действия помех.

Для достижения поставленной цели необходимо решить следующие задачи:

1) синтезировать алгоритмы генерации хаотических сигналов на основе нелинейных динамических систем и их характеристик, обеспечивающих заданное стохастическое поведение системы;

2) провести анализ статистических, спектральных и корреляционных свойств хаотических сигналов, формируемых нелинейной динамической системой с одномерным отображением;

3) решить задачи нелинейной фильтрации радиосигналов с дискретно-непрерывными случайными и хаотическими параметрами в условиях действия помех, тем самым обеспечить помехоустойчивую синхронизацию и демодуляцию радиосигнала;

4) конкретизировать общие уравнения фильтрации для различных видов функциональной связи между информационным сообщением и хаотическим сигналом;

5) провести анализ помехоустойчивости приёма радиосигналов с хаотической модуляцией по неэнергетическим параметрам; широкополосных сигналов с псевдослучайной перестройкой радиочастоты; кодовой конструкции на основе сигналов с параллельно-составной структурой;

6) разработать численные модели устройств генерации и фильтрации сигналов, максимально приближенных к реальным условиям работы защищенных систем передачи информации.

Объектом исследования является защищенная система передачи информации в условиях действия мультипликативных и аддитивных помех.

Предметом исследования являются методы генерирования, модуляции, синхронизации и демодуляции радиосигналов с хаотическими компонентами в защищенных системах передачи информации при воздействии помех.

Положения, выносимые на защиту

1. Метод генерации хаоса в одно- и многокольцевых динамических системах с локализацией фазовых состояний, позволяющий обеспечить практически реализуемое использование хаос-сигналов для защиты информации в системах передачи дискретных сообщений.

2. Метод и алгоритм информационной модуляции динамического хаоса на основе кодирования по областям n-мерного фазового пространства состояний в системах защиты информации, позволяющие обеспечить структурную скрытность сложного сигнала при реализации кодера в вычислительных системах разрядностью от 8 бит и выше.

3. Метод и алгоритм генерации и информационной модуляции динамического хаоса для обеспечения информационной безопасности на основе распределённых отображений, позволяющие повысить помехоустойчивость сигнально-кодовой конструкции на 15–18 дБ для вероятности ошибки не хуже 10^{-4} в условиях действия помех.

4. Уравнения обобщённой синхронизации демодуляции радиосигналов с хаотическими и дискретно-непрерывными марковскими параметрами в условиях действия помех, основанные на совместной оценке информативных и неинформативных параметров сложного сигнала и повышающие энергетическую эффективность системы передачи информации на 9–12 дБ по сравнению с известными.

Личный вклад соискателя

Подход к повышению качественных показателей информационных систем на основе динамического хаоса, цель и задачи диссертационной работы определены научным руководителем доктором технических наук, профессором В. А. Чердынцевым. Личным вкладом соискателя являются разработка методов генерации и информационной модуляции хаос-сигналов, синтез алгоритмов обработки применительно к разработанным сигнально-кодовым конструкциям, а также численное моделирование исследуемых алгоритмов.

Апробация результатов диссертации

Основные научные положения и результаты диссертации докладывались и обсуждались на следующих научных конференциях: IV Международная молодежная научно – техническая конференция «Современные проблемы радиотехники и телекоммуникаций» РТ-2008 (г. Севастополь, 2008), V Международная молодежная научно – техническая конференция «Современные проблемы радиотехники и телекоммуникаций» РТ-2009 (г. Севастополь, 2009), XIV Международная научно – техническая конференция «Современные средства связи» (г. Минск, 2009), VII Белорусско – российская научно – техническая конференция «Технические средства защиты информации» (г. Минск, 2009), 45-ая научная конференция аспирантов, магистрантов и студентов «Радиотехника и электроника» (г. Минск, 2009), VI Международная молодежная научно – техническая конференция «Современные проблемы радиотехники и телекоммуникаций» РТ-2010 (г. Севастополь, 2010), VII Международная молодежная научно – техническая конференция «Современные проблемы радиотехники и телекоммуникаций» РТ-2011 (г. Севастополь, 2011), IX Международная молодежная научно – техническая конференция «Современные проблемы радиотехники и телекоммуникаций» РТ-2013 (г. Севастополь, 2013).

Опубликованность результатов диссертации

Результаты исследований по теме диссертации опубликованы в 21 научной работе. Из них 5 статей в научных журналах в соответствии с пунктом 18 Положения о присуждении ученых степеней и присвоении ученых званий в Республике Беларусь (общим объёмом 2,3 авторских листа), 12 докладов и 2 тезиса в сборниках материалов научных конференций.

Результаты диссертационного исследования реализованы в полезной модели: патент Республики Беларусь «Система передачи дискретной информации на основе составного динамического хаоса», №7489.

Структура и объём диссертации

Диссертационная работа состоит из введения, общей характеристики работы, четырех глав, заключения, библиографического списка и трех приложений.

Общий объем диссертации составляет 126 страниц. Диссертация включает 90 рисунков на 60 страницах, 2 таблицы на 2 страницах,

библиографический список из 81 наименования на 6 страницах, список собственных публикаций из 21 наименования на 3 страницах и приложения на 2 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во ***введении*** показано использование особенностей генерации хаотических последовательностей, указаны основные недостатки методов и определено направление диссертационной работы.

Первая глава рассматривает предпосылки постановки задачи основного исследования диссертационной работы. Анализ тенденций развития систем передачи сообщений и применяемых при этом сигнальных конструкций показал, что важнейшими аспектами при создании перспективных радиоинформационных систем являются:

– повышение пропускной способности канала связи за счёт строго обоснованного подхода в создании и выборе сигнально-кодовых конструкций;

– возможность эффективного уплотнения информационных потоков от разных источников в одном канале связи;

– повышение энергетической и структурной скрытности сигнала;

– оправданные по сложности цифровые методы генерации, приёма и обработки сложных сигналов.

Сравнительный анализ известных ансамблей сигналов и хаотических последовательностей, формируемых нелинейными динамическими системами, позволяет утверждать, что величина ансамбля последних приближается к полному коду при малых уровнях выбросов боковых лепестков АКФ.

В работе показано, что для целей конфиденциальной передачи информации по каналам с помехами необходимо усложнять структуру нелинейных систем, формирующих квазислучайные последовательности (рисунок 1).

Метод генерации полезного сигнала на основе двухступенчатого перехода из хаос-процесса в хаос-сигнал и из хаос-сигнала в хаотический радиосигнал позволяет получить совершенно новые подходы к передаче информации с использованием хаоса.

Применение динамического хаоса для передачи конфиденциальной информации возможно за счёт создания новых типов сигналов и методов их генерации. Следует различать три класса схем генерации хаос-процессов:

1) схемы на основе так называемого «чистого» хаоса, фазовое пространство которых представляет континуум значений;

2) схемы, формирующие континуальный хаос-процесс в фиксированные промежутки времени;

3) схемы, формирующие значения процесса в фиксированные моменты времени и квантованные по уровню.

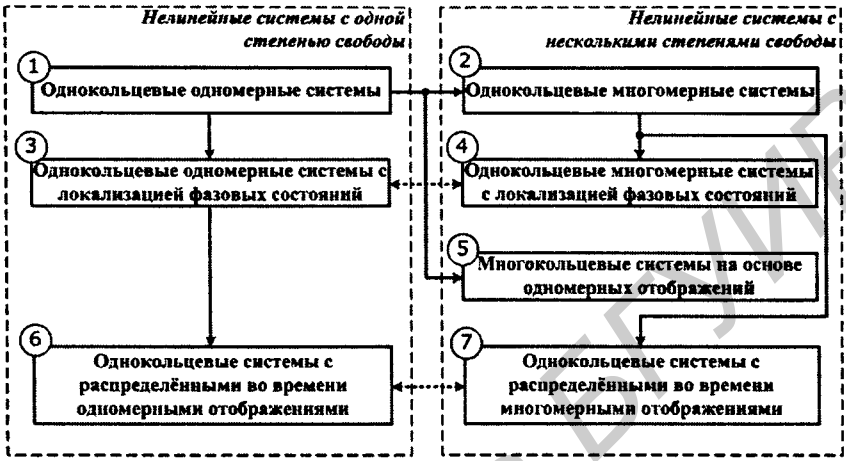

Рисунок 1 – Иерархия исследуемых динамических систем

Вторая глава посвящена вопросам генерации сигналов на основе динамического хаоса, а также условиям выбора нелинейной формирующей функции.

В случае применения нелинейных формирующих функций (НФФ) двух, трёх, …, n переменных отображение ХС будет представлять собой трёх-, четырёх-, ..., $(n+1)$-мерное пространство фазовых состояний. Для генерации ХС подходит не любая функция. Сформулируем несколько базовых требований, налагаемых на НФФ. Функция должна иметь ограниченную область допустимых значений (ОДЗ). Условие следует из необходимости конечного динамического диапазона формируемого ХС. Определённый интеграл от НФФ по области её определения должен быть равен нулю. В этом случае хаос-сигнал будет сбалансированным. Скорость изменения НФФ вблизи точек пересечения с осью абсцисс для одномерных отображений, или плоскостью (x, y) – для двумерных, должна быть максимальна. В этом случае значения ХС будут с большей вероятностью находиться у границ ОДЗ НФФ. С учётом собственных шумов аналоговой части приёмного устройства и в условиях передачи ХС по каналу с аддитивным шумом выполнение указанного требования позволит повысить помехоустойчивость приёма и обработки.

Нелинейную формирующую хаос-функцию (НФФ), или просто «формирующую функцию», обозначим как $f(x)$. Для генерации хаотических процессов подходит не любая нелинейная функция. Сформулируем необходимые требования, которым она должна удовлетворять.

1. Функция должна определяться на некотором отрезке аргумента $[-x_{max}\ x_{max}]$. В связи с тем, что во всех случаях при генерации хаоса задействованы один или несколько предыдущих его состояний, такому же отрезку должны принадлежать и значения функции. Наиболее удобным является значение $x_{max}=1$.

$$\begin{cases} x \in [-1;1]; \\ f(x) \in [-1;1]. \end{cases}$$

Условия следуют из необходимости ограничения динамического диапазона генерируемого хаотического процесса.

2. Интеграл от формирующей функции на области её определения должен быть приблизительно равен либо равен нулю. С учётом требования 1:

$$\int_{-1}^{1} f(x)dx \cong 0.$$

Условие следует из необходимости получения сбалансированной последовательности значений.

3. Формирующую функцию желательно выбирать из класса кусочно-линейных функций. В этом случае одномерная плотность распределения вероятностей сгенерированного хаотического процесса будет равномерной. Известно, что в строго ограниченном динамическом диапазоне наиболее энтропийным будет процесс с равномерным распределением значений.

4. Значения второй производной формирующей функции по возможности должны быть равны нулю в точках пересечения $f(x)$ с осью абсцисс.

$$f''(x_i) = 0,$$

где $x_i \in [x_1, ..., x_n]$ – корни уравнения $f(x) = 0$.

Требование следует из необходимости генерации хаотического процесса, в котором уровни отсчётов находятся вблизи границ ОДЗ формирующей функции. Это позволяет уменьшить влияние шума на качество выделения информации. Отметим, что требование 4 вступает в противоречие с требованием 3.

При модуляции хаос-процесса путём нелинейного подмешивания мощность информационного сигнала должна составлять малую часть мощности хаотического сигнала, иначе возможно выделение полезного сигнала из хаотического путём линейной фильтрации.

Подход реализуется, если вместо кусочно-линейных в качестве нелинейных формирующих функций (НФФ) использовать некоторые поверхности в трёхмерном пространстве.

Алгоритм формирования ХП можно записать в виде:

$$\begin{cases} h_k'' = c(1 - h_{k-1}/a - h_{k-2}/b); \\ h_k' = 2\,\mathrm{sign}(h_k'') - h_k'', \ \text{если} \ |h_k''| > 1; \ \text{иначе} \ h_k' = h_k''; \\ h_k = (1-\alpha)h_k' + \alpha\lambda_k. \end{cases}$$

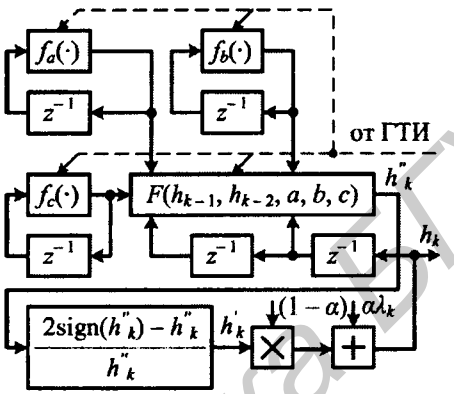

Рисунок 2 – Структурная схема формирователя хаотического колебания

Структура формирователя хаос-сигнала представляется собой систему связанных кольцевых подсистем, в каждой из которых введена нелинейная обратная связь. Основной подсистемой, формирующей сигнал, является вычислитель функции $F(\cdot)$ вместе с двумя регистрами задержки z^{-1}. Функция $F(\cdot)$ реализует отображение в виде некоторой плоскости в трёхмерном пространстве фазовых состояний. Нормаль к плоскости, проведённая из начала координат, близка к вертикальной. Это обеспечивает нечувствительность НФФ к возмущениям. НФФ, кроме двух аргументов, имеет три параметра: a, b и c, определяющие характер изменения фазовых состояний хаос-процесса. Каждый из параметров определяется собственным хаос-генератором, тактируемым генератором тактовых импульсов (ГТИ).

По причине того, что достаточно сложно обеспечить ограниченность динамического диапазона (ДД) хаос-процесса значениями ± 1, то в алгоритме предлагается использовать метод ограничения значений в виде «зеркального преобразования», реализуемого на рисунке 2 блоком $2\mathrm{sign}(h_k'') - h_k''$. Запись h_k'' внизу означает, что если ХП не выходит за границы ДД, то на выход передаётся входное значение. Перемножитель и сумматор на схеме

осуществляет нелинейное подмешивание информационного процесса λ_k к ХП $h_k^{'}$.

Последовательность отсчётов ХП h_k подаётся на радиочастотный модулятор.

Применение динамического хаоса для передачи конфиденциальной информации возможно за счёт создания новых типов сигналов и методов их генерации. Следует различать три класса схем генерации хаос-процессов:

1. Схемы на основе так называемого «чистого» хаоса, фазовое пространство которых представляет континуум значений.

2. Схемы, формирующие континуальный хаос-процесс в фиксированные промежутки времени.

3. Схемы, формирующие значения процесса в фиксированные моменты времени и квантованные по уровню.

Применение первого типа хаос-процесса предполагает создание на приёмной стороне строго идентичного генератора ХП, что с учётом континуальности значений процесса затрудняет надёжный приём в условиях радиоканала. Однако в этом случае разбегание фазовых траекторий играет позитивную роль в смысле информационной защищённости канала связи.

Второй тип хаос-процесса предполагает обработку его абсолютных значений, основная идея которой состоит в анализе текущего и нескольких предыдущих состояний системы. Эти значения взаимосвязаны детерминированной функцией, которая определяет характеристики сигнала. Использование различных нелинейных функций в формирователе ХП позволяет управлять типом сигнала, его корреляционными и статистическими свойствами. Однако если в качестве формирующей функции берётся функция одной переменной, то в случае относительно мало зашумлённого канала появляется возможность проанализировать одну реализацию принимаемого процесса и определить вид нелинейности, что негативно сказывается на защищённости канала от перехвата. Поэтому в целях улучшения эффективности системы предпочтительнее в качестве формирующих выбирать более сложные функциональные зависимости. При наличии в канале Рэлеевских замираний необходима нормировка сигнала.

Третий тип хаос-процессов наиболее приемлем для сильно зашумлённых каналов, так как воздействие помехи будет нивелироваться защитным интервалом, равным половине уровня квантования хаос-процесса.

Особенность предлагаемых схем – это возможность построения ГХП как в виде аналоговой, так и в виде цифровой схемы. Это не характерно для предлагавшихся ранее алгоритмов и обусловлено особенностями обработки сигнала на приёмной стороне.

Бинарный информационный поток воздействует на один или несколько параметров нелинейности $f(\cdot)$, элемента, включенного в цепь обратной связи формирователя хаос-процесса. С приходом очередного тактового импульса, например, по его фронту, из задержанного h_{k-n} отсчета формируется следующий h_{k+1}. В диссертационной работе в качестве аргумента $F(\cdot)$ взято значение h_{k-1}. Если $\theta = \pm 1$, то допустимо использовать два различных ГХП с последующей коммутацией выходных сигналов согласно подаваемой информации. Такая схема обладает большей гибкостью в выборе типа используемых хаотических мод. Схема кроме простой реализации имеет еще одно неоспоримое достоинство: выходной сигнал имеет высокую структурную скрытность. Последнее обусловлено тем, что при смене информационного символа и соответственно параметра a начальным условием при формировании последующего отсчёта хаотического сигнала выступает последнее значение на выходе ГХП для предыдущего бита информации.

Для обеспечения структурной скрытности сигнала ставится задача подбора оптимальных пар функций $f(\cdot)$, которые в то же время должны обеспечивать требуемую помехоустойчивость. Подбор нелинейностей определяется плотностью распределения вероятностей (ПРВ) порождаемых ими хаос-процессов. Желательно, чтобы значения процесса на выходе ИХП чаще находились у границ области значений функций и реже около нуля. Если это условие выполняется, то энергетика системы связи будет выше, более эффективно будет использоваться динамический диапазон аппаратуры, следовательно, возрастет помехоустойчивость.

Перспективным является формирование состояний ХП на основе многокомпонентного отображения. Это позволяет сохранить положительные качества континуального хаос-процесса и осуществлять передачу сигнала в условиях значительных помех при сохранении структурной скрытности сигнала. При генерации хаос-сигналов, адаптированных для передачи сообщений по радиоканалу, возможны следующие методы подмешивания хаотического процесса к радиочастотному колебанию:

– на основе амплитудной модуляции колебания хаотическим процессом;

– на основе угловой (фазовой, частотной) модуляции колебания хаотическим процессом;

– на основе модуляции задержки комплексной огибающей колебания хаотическим процессом.

Метод зонального декодирования хаос-процесса с информационной манипуляцией отображений позволяет обеспечить высокую криптостойкость сообщений. В сочетании с модуляцией гармонического колебания по одному

из параметров удаётся построить помехоустойчивые информационные системы. Методы корреляционной и зональной обработки хаос-процессов применимы не только для передачи бинарных сообщений, но и сообщений с алфавитом $A > 2$, при этом увеличивается количество каналов нелинейной обработки, и решающее устройство будет находить максимальный сигнал на выходе A каналов.

В отличие от известных подходов в рассматриваемых случаях носителем сообщений хаос-процесса может являться радиосигнал. Таким образом, в главе определены основные направления практически реализуемого использования хаос-сигналов в системах связи. Предложены новые методы генерации хаос-сигналов, основанные на перемежении и нелинейной модуляции гармонического сигнала хаос-процессом.

В ***третьей главе*** рассмотрены методы информационной модуляции и декодирования. Метод кодирования по пространству фазовых состояний сигнала предлагает особым образом задавать характер нелинейных функций, включаемых в цепь обратной связи динамической системы, тем самым отображая тот или иной информационный символ на некоторый известный переход системы из одного фазового состояния в другое. При соответствующем подборе нелинейных функций такие переходы однозначно идентифицируют состояние информационного процесса.

Показано, что базовым подходом к реализации помехоустойчивых систем передачи информации является распределение во времени относительно медленно меняющихся нелинейных формирующих функций.

В пространстве фазовых состояний определяется некоторая плоскость: $Ax + By + Cz + D = 0$, где A, B, C определяют проекции нормали к плоскости на оси координат; D – некоторый произвольный коэффициент. Для нечувствительности НФФ к возмущениям необходимо, чтобы $A \cong 0$, $B \cong 0$. Параметры D и C можно найти из второй формы уравнения для плоскости: $x/a + y/b + z/c = 1$. Плоскость пересекает оси координат в точках $(a; 0; 0)$, $(0; b; 0)$ и $(0; 0; c)$, где $c = -D/C$. Таким образом, параметры C и D могут быть произвольными, но значения $|C|$ и $|D|$ должны быть соразмерными. Такое требование следует из необходимости пересечения плоскостью оси Oz в точке, находящейся внутри или в непосредственной близости от интервала $(-1; 1)$.

Для случая нелинейного подмешивания алгоритм декодирования хаос-сигнала описывается следующим выражением:

$$\begin{cases} \lambda_k = [h_k - (1-\alpha)h_k^{'}]/\alpha; \\ h_k^{''} = c(1 - h_k/a - h_{k-1}/b); \\ h_k^{'} = 2\,\mathrm{sign}(h_k^{''}) - h_k^{''}, \text{ если } |h_k^{''}| > 1; \text{ иначе } h_k^{'} = h_k^{''}. \end{cases}$$

На рисунке 3 представлена схема, реализующая алгоритм.

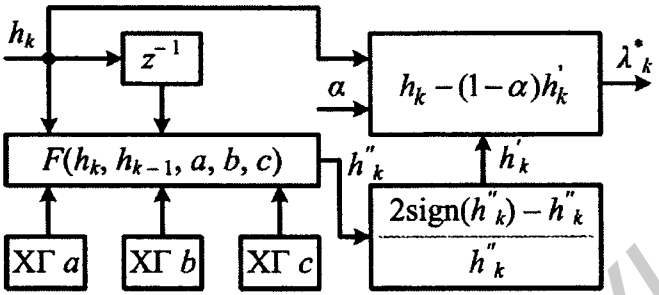

Рисунок 3 – Структурная схема декодера сигнала

Структурная схема обработки хаос-сигнала представляет собой нелинейный фильтр, реализуемый функцией $F(\cdot)$, аргументами которого являются два последовательных входных отсчёта, а три параметра определяют характер изменения отображения, известный на приёмной стороне.

Общей отличительной чертой методов является весьма эффективное извлечение пользы из особенностей механизмов генерации сигналов в нелинейных динамических системах для кодирования информации, что является несомненным достоинством. Распределённые во времени отображения позволяют формировать структурно сложные хаотические процессы, выгодно отличающиеся от классических последовательностей. Основное преимущество таких процессов – энергетическая эффективность систем передачи информации на их основе при простоте реализации сигнально-кодовых конструкций.

Также рассмотрен метод формирования динамического хаоса на основе нелинейного подмешивания с кодированием блока информационных символов. Предложено подмешивать не некоторый аналоговый сигнал, а многоуровневую последовательность, каждое состояние которой кодирует блок информационных бит. В результате формируется хаотический процесс со сложной структурой фазовых переходов даже при простейших нелинейностях в цепи обратной связи нелинейной динамической системы.

Метод открывает ещё один подход к использованию случайно-подобных последовательностей в скрытных и защищённых от перехвата системах передачи информации.

При синтезе алгоритмов передачи дискретной информации, базирующихся на свойствах нелинейной динамики, приходится сталкиваться с противоречивыми требованиями, налагаемыми на характер НФФ. Простые

кусочно-линейные функции придают системам связи приемлемую помехоустойчивость, однако затрудняют стохастизацию колебаний, а значит, уменьшают структурную скрытность сигналов. Для решения данной проблемы можно предложить метод расщепления нелинейных формирующих функций на L распределённых во времени сегментов.

Сущность подхода состоит в том, что в пределах некоторого временного окна конечной длительности фазовые переходы хаоса из состояния в состояние определяются различными простейшими функциями из множества L.

Пусть $L \in N$ – объём функционального множества $F(h)$, а N – некоторое натуральное число:

$$F(h) \equiv f_0(h); f_1(h); ...; f_{L-1}(h) .$$

Тогда алгоритм формирования хаотического сигнала для случая одномерного отображения определяется следующим выражением:

$$h_{k+1} = f_{(k \bmod L)}(h_k),$$

где $k \bmod L$ – операция нахождения значения k по модулю L; $k = 0, 1, 2, ...$ – индекс элемента хаотической последовательности.

Данный метод генерации в качестве информационной модуляции допускает как нелинейное подмешивание, так и манипуляцию хаотических режимов. В последнем случае имеем:

$$h_{k+1} = \begin{cases} f_{1,(k \bmod L)}(h_k), & \text{если } x_k = 0; \\ f_{2,(k \bmod L)}(h_k), & \text{если } x_k = 1. \end{cases}$$

Здесь $f_{1,i}$ и $f_{2,i}$ – одна из L функций, принадлежащих множеству F_1 и F_2 соответственно; x_k – значение информационного символа на k-м такте.

Особенностью метода является то, что хаотичность колебаний зависит не от характера НФФ, а от объёма функционального множества. Кроме того, объём функционального множества может быть любым натуральным числом и на него не накладываются никакие дополнительные требования.

Четвертая глава посвящена задаче фильтрации дискретно-непрерывных хаос-сигналов на фоне белого шума. Показано решение задачи нелинейной фильтрации хаос-сигналов на фоне негауссовской марковской помехи.

Приведены алгоритмы совместной фильтрации, которые в отличие от известных позволяют осуществлять синтез устройств квазикогерентного приёма и обработки цифровых сигналов для каналов с негауссовскими марковскими помехами.

В *заключении* сформулированы основные научные результаты диссертации и рекомендации по их практическому использованию.

Приложение содержит акты внедрения.

ЗАКЛЮЧЕНИЕ

В диссертационной работе показана принципиальная возможность сохранения конфиденциальности и защищённости передачи информации в системах на основе динамического хаоса с нелинейным подмешиванием при существенном улучшении энергетической эффективности радиолинии. При этом динамический хаос может формироваться в системах на основе простейших одномерных отображений, а также многомерных отображений, реализуемых гладкими функциями.

Основные научные результаты диссертации

1. Метод генерации хаоса в одно- и многокольцевых динамических системах с локализацией фазовых состояний, позволяющий обеспечить практически реализуемое использование хаос-сигналов для защиты информации в системах передачи дискретных сообщений. Отличительной особенностью предлагаемого метода является то, что сигнал, описываемый не менее чем тремя параметрами, формируется в одно- или многокольцевой нелинейной системе с обратной связью, использующей в качестве нелинейных формирующих функций кусочно-линейные поверхности в N-мерном пространстве фазовых состояний. Предлагаемая сигнально-кодовая конструкция устойчива к длительным замираниям, аддитивным шумовым помехам, а также к преднамеренным помехам в канале связи. Ансамбль формируемых сигналов составляет величину от 2^{16} до 2^{80} в зависимости от разрядности вычислительной системы и количества степеней свободы фазового пространства, что обеспечивает высокую структурную скрытность передаваемой информации, определяемую некоррелированностью двух последовательных отсчетов хаотического сигнала на уровне $1/\sqrt{N}$, где N – количество элементов последовательности. Повышенная защищённость системы от несанкционированного доступа и более высокая её энергетическая эффективность в сравнении с известными системами аналогового и дискретного типов обеспечивается за счёт подмешивания нелинейным образом информационного потока в сигнал-переносчик [3, 4, 10–12, 17].

2. Метод и алгоритм информационной модуляции динамического хаоса на основе кодирования по областям n-мерного фазового пространства состояний в системах защиты информации, позволяющий обеспечить

структурную скрытность сложного сигнала при реализации кодера в вычислительных системах разрядностью от 8 бит и выше.

Метод обеспечивает увеличение степени конфиденциальности передачи информации с нелинейным подмешиванием при условии, когда динамический хаос формируется на основе простейших одномерных отображений. По сравнению с манипуляцией хаотических режимов отсутствует необходимость в тщательном выборе НФФ. В предлагаемом методе основным требованием к НФФ является простота и удобство её вычисления в реальном устройстве, так как лишь одна формирующая функция задаёт структуру и характеристики динамического хаоса вне зависимости от длины информационного блока.

Аналитические расчёты и результаты численного моделирования показали следующие достоинства предлагаемого метода: 1) исключается влияние распределения нелинейной последовательности на распределение кодированного сигнала, что улучшает структурную скрытность сигнала; 2) величина динамического диапазона ограничена фиксированными значениями и контролируема; 3) при кодировании информационного символа несколькими отсчетами хаотической последовательности ослабляется влияние сосредоточенных по частоте помех на вероятность ошибочного приёма за счёт декорреляции помехи при обработке сигналов [2–4, 15, 16].

3. Метод и алгоритм генерации и информационной модуляции динамического хаоса для обеспечения информационной безопасности на основе распределённых отображений, позволяющий повысить помехоустойчивость сигнально-кодовой конструкции на 15–18 дБ при вероятности ошибки не хуже 10^{-4} в условиях действия помех и получить более высокую степень достоверности передаваемой информации в условиях сложной помеховой обстановки при рациональном использовании частотного ресурса [4, 5, 13, 14].

4. Уравнения обобщённой синхронизации демодуляции радиосигналов с хаотическими и дискретно-непрерывными марковскими параметрами в условиях действия помех, основанные на совместной оценке информативных и неинформативных параметров сложного сигнала и повышающие энергетическую эффективность системы передачи информации на 9–12 дБ по сравнению с известными.

Полученные уравнения фильтрации дискретно-непрерывных сообщений содержащихся в радиосигнале с хаотической модуляцией, отличаются от известных тем, что фильтрации подвергается объединённый процесс $\mathbf{X}(t) = \mathbf{h}, \lambda$, включающий наряду с сообщением $\lambda(t)$ хаотические компоненты $\mathbf{h}(t)$. Дискретный параметр θ оценивается на основании

апостериорной вероятности состояния $P_i(\cdot)$. При этом компонента $\mathbf{F}(\cdot)$, содержащая наблюдаемый процесс, усредняется с учётом апостериорных вероятностей состояний дискретного процесса, а в качестве текущих значений вектора $\mathbf{X}(t)$ берутся его оценки $\mathbf{X}^*(t)$. Такой алгоритм предполагает постоянство процесса $\mathbf{X}(t)$ на интервале формирования процесса $P_i(\cdot)$ [1, 6, 7].

Рекомендации по практическому использованию результатов

Практическая значимость результатов диссертационной работы заключается в том, что разработанный метод формирования сигнала и кодирования информации на основе распределённых во времени отображений может быть использован для передачи информации как в гражданских службах (для осуществления высокоскоростной защищённой пакетной радиосвязи), так и специальных (например, для передачи команд управления).

Разработанные подходы, методы и алгоритмы позволят обеспечить энергетическую (отношение сигнал/шум на входе приёмника 15 дБ и выше), спектральную (система может работать без расширения спектра сигнала) и стоимостную эффективность функционирования любых систем передачи дискретной информации в открытых каналах связи. К ним можно отнести радиорелейные линии связи, системы подвижной связи общего и специального назначения, спутниковые радиолинии, высокоскоростные точки доступа в Интернет. Все предложенные алгоритмы хорошо адаптированы к цифровым методам формирования и обработки сигнала, в том числе в системах с невысокой разрядностью целочисленных регистров.

Совокупность задач, решённых в диссертационной работе, расширяет класс сигналов с хаотической модуляцией и методов их приёма и обработки на фоне шумов, что обеспечивает создание помехозащищённых и скрытных телекоммуникационных систем нового типа.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в научных журналах

1. Половеня, С.И. Фильтрация параметров сигналов, содержащих случайные начальные фазы / С.И. Половеня, В.А. Чердынцев, В.В. Дубровский, Исса И.Скиб // Доклады БГУИР. – 2009. – № 2(40). – С. 5–11.

2. Половеня, С.И. Обработка информации, кодированной по пространству фазовых состояний сигнала / С.И. Половеня, В.А. Чердынцев, В.В. Дубровский // Доклады БГУИР. – Минск, 2010. – № 4. – С.11–18.

3. Половеня, С.И. Динамический хаос на основе нелинейного подмешивания с кодированием блока информационных символов / С.И. Половеня // Доклады БГУИР. – Минск, 2010.– № 5.– С.100–104.

4. Половеня, С. И. Обеспечение скрытности информации хаотическими сигналами на основе отображений, распределенных во времени / С.И. Половеня, В.В. Дубровский // Вестник БГУ. Сер. 1. – Минск, 2012. – № 3. – С. 50–55.

5. Половеня, С. И. Генерация и обработка хаотических сигналов на основе трехмерных функций в пространстве состояний / С.И. Половеня, В.А. Чердынцев, В.В. Дубровский // Доклады БГУИР. – Минск, 2014. – № 4(82).– С.23–28.

Статьи материалов конференций

6. Половеня, С.И. Генерация и обработка сигналов с псевдослучайной перестройкой рабочей частоты / С. И. Половеня, В. В. Дубровский // Современные проблемы радиотехники и телекоммуникаций: материалы IV международной молодежной научно-технической конференции, Севастополь, апрель, 2008 г. / Севастополь, 2008. – С.76.

7. Половеня, С.И. Синхронизация сложного фазоманипулированного сигнала с хаотической модуляцией задержки / С. И. Половеня, В. В. Дубровский // Современные проблемы радиотехники и телекоммуникаций: материалы IV международной молодежной научно-технической конференции, Севастополь, апрель, 2008 г. / Севастополь, 2008. – С.75.

8. Половеня, С.И. Обработка хаос-сигналов, формируемых на основе составных отображений / С. И. Половеня, В. А. Чердынцев // Современные проблемы радиотехники и телекоммуникаций: материалы V международной молодежной научно-технической конференции, Севастополь, апрель, 2009 г. / Севастополь, 2009. – С.74.

9. Половеня, С.И. Система передачи информации на основе составных хаос-сигналов / С.И. Половеня, В.А. Чердынцев, Исса И.Скиб // Современные средства связи: материалы XIV международной научно-технической конференции, Минск, октябрь, 2009 г. / Минск, 2009. – С.43.

10. Половеня, С.И. Динамический хаос на основе нелинейного подмешивания с кодированием блока информационных символов / С.И. Половеня // Современные средства связи: материалы XV международной научно-технической конференции, Минск, октябрь, 2010 г. / Минск, 2010. – С.100.

11. Половеня, С.И. Формирование хаотических сигналов, кодированных системой ортогональных функций / С.И. Половеня, В.В. Дубровский, О.И. Королькова // Современные проблемы радиотехники и телекоммуникаций: материалы VI международной молодежной научно-технической конференции, Севастополь, апрель, 2010 г. / Севастополь, 2010. – С.100.

12. Половеня, С.И. Обработка хаотических сигналов, кодированных системой ортогональных функций / С.И. Половеня, В.В. Дубровский, О.И. Королькова // Современные проблемы радиотехники и телекоммуникаций: материалы VI международной молодежной научно-технической конференции, Севастополь, апрель, 2010 г. / Севастополь, 2010. – С.101.

13. Половеня, С.И. Генерация хаотических сигналов на основе распределенных во времени отображений / С.И. Половеня, В.В. Дубровский, // Современные проблемы радиотехники и телекоммуникаций: материалы VII международной молодежной научно-технической конференции, Севастополь, апрель, 2011 г. / Севастополь, 2011. – С.66.

14. Половеня, С.И. Обработка хаотических сигналов на основе распределенных во времени отображений / С.И. Половеня, В.В. Дубровский, // Современные проблемы радиотехники и телекоммуникаций: материалы VII международной молодежной научно-технической конференции, Севастополь, апрель, 2011 г. / Севастополь, 2011. – С.67.

15. Половеня, С.И. Модуляция хаотических процессов на основе отображений в трехмерном пространстве фазовых состояний / С.И. Половеня, В.В. Дубровский, // Современные проблемы радиотехники и телекоммуникаций: материалы VIII международной молодежной научно-технической конференции, Севастополь, апрель, 2012 г. / Севастополь, 2012. – С.88.

16. Половеня, С.И. Обработка хаотических процессов на основе отображений в трехмерном пространстве фазовых состояний / С.И. Половеня, В.В. Дубровский, // Современные проблемы радиотехники и телекоммуникаций: материалы VIII международной молодежной научно-

технической конференции, Севастополь, апрель, 2012 г. / Севастополь, 2012. – С.89.

17. Половеня, С.И. Защита информации в системах на основе нелинейно формируемых последовательностей / С.И. Половеня, В.В. Дубровский, А.К. Стефанович // Современные проблемы радиотехники и телекоммуникаций: материалы IX международной молодежной научно-технической конференции, Севастополь, апрель, 2013 г. / Севастополь, 2013. – С.63.

Тезисы материалов конференций

18. Половеня, С.И. Формирование составных хаос-сигналов / С.И. Половеня, В.А. Чердынцев, Исса И.Скиб // Технические средства защиты информации: материалы VII Белорусско-российской научно-технической конференции, Минск, июнь, 2009 г. / Минск 2009.

19. Половеня, С.И. Формирование хаос-сигналов на основе составных отображений / С.И. Половеня, В.А. Чердынцев, Исса И.Скиб // Технические средства защиты информации: материалы VII Белорусско-российской научно-технической конференции, Минск, июнь, 2009 г. / Минск 2009.

Патент

20. Система передачи дискретной информации на основе составного динамического хаоса:патент 7489 Респ. Беларусь, МПК 11 H03M 9/00 / С.И. Половеня, В.А. Чердынцев, А.В. Мартинович, Исаа И. Скиб; заявитель УО БГУИР № u 20101011, заявл. 03.12.10; опубл. 30.08.2011.

РЭЗЮМЭ

Палавеня Сяргей Іванавіч

Алгарытмы абароны інфармацыі ў адкрытых каналах з перашкодамі метадамі нелінейнай дынамікі

Ключавыя словы: нелінейная дынамічная сістэма, дынамічны хаос, нелінейная фармуючая функцыя, размеркаванае ў часе адлюстраванне, крыптаграфічная абарона інфармацыі, перамешванне фазавых траекторый, лічбавая сувязь, алгарытм аптымальнай апрацоўкі, рабастнасць, памехаўстойлівасць.

Мэта працы: павелічэнне памехаўстойлівасці сістэм перадачы дыскрэтнай інфармацыі на аснове дынамічнага хаоса ў каналах з інтэнсіўнымі перашкодамі і забеспячэнне абароны інфармацыі ад несанкцыянаванага доступу.

Асноўныя вынікі працы: праведзены аналіз патэнцыйных магчымасцяў нелінейных адно- і многакальцавых дынамічных сістэм з больш за адной ступенню свабоды. Вызначаны патрабаванні да нелінейных фармуючых функцый, уключаным у ланцуг зваротнай сувязідынамічнай сістэмы. Выяўлена магчымасць захавання высокай ступені стахастызацыі ваганняў пры выкарыстанні простыхкавалкава-лінейных і гладкіх функцый, а таксама фрагментаў плоскасцяў у трохмернай фазавай прасторы пры ўмове псеўдавыпадковага размеркавання параметраў нелінейнай фармуючай функцыі на працягу канчатковага ці бясконцага інтэрвала часу. Паказана што на працягу аднаго ці больш такта працы дынамічнай сістэмы можна выкарыстоўваць параўнальна простыя фарміруючыя функцыі, вытворная якіх ваўсёй вобласці іх вызначэння мае малыя па модулі значэнні. Пры гэтым складаны нерэгулярны характар вагальнага працэсу на выхадзе дынамічнай сістэмы захоўваецца за кошт змены аднаго ці некалькіх параметраў фарміруючай функцыі, а паказчык экспаненцыяльнай разбежнасці траекторый А. М. Ляпунова блізкі да нуля. Улічваючы, што памехаўстойлівасць нелінейнага фільтра, які здзяйсняе дэкадаванне сігнала, вызначаецца ступенню разбежнасці фазавых траекторый хаатычнага працэса, алгарытм становіцца істотна менеў адчувальным да ўзбурэнняў. Прапанаваныя алгарытмы генерацыі, інфармацыйнай мадуляцыі хаатычнага працэсу. На аснове маркаўскай тэорыі нелінейнай фільтрацыі сінтэзаваныя алгарытмы квазіаптымальнай апрацоўкі складанага сігналу на фоне негаусаўскіх маркаўскіх памех. Паказаны шлях і практычнай рэалізацыі алгарытмаў, метадаў і падыходаў.

Вобласць прымянення: сістэмы тэлекамунікацый з высокай ступенню абароны канала перадачы ад несанкцыянаванага доступа да інфармацыі.

РЕЗЮМЕ

Половеня Сергей Иванович

Алгоритмы защиты информации в открытых каналах с помехами методами нелинейной динамики

Ключевые слова: нелинейная динамическая система, динамический хаос, нелинейная формирующая функция, распределенное во времени отображение, криптографическая защита информации, перемешивание фазовых траекторий, цифровая связь, алгоритм оптимальной обработки, помехоустойчивость.

Цель работы: увеличение помехоустойчивости систем передачи дискретной информации на основе динамического хаоса в каналах с интенсивными помехами и обеспечение защиты информации от несанкционированного доступа.

Основные результаты работы: проведен анализ потенциальных возможностей нелинейных одно- и многокольцевых динамических систем с более чем одной степенью свободы. Определены требования к нелинейным формирующим функциям, включенным в цепь обратной связи динамической системы. Выявлена возможность сохранения высокой степени стохастизации колебаний при использовании простых кусочно-линейных и гладких функций, при условии псевдослучайного распределения параметров нелинейной формирующей функции в течение конечного или бесконечного интервала времени. Показано что в течение одного или более такта работы динамической системы можно использовать сравнительно простые формирующие функции, производная которых во всей области их определения имеет малые по модулю значения. При этом сложный нерегулярный характер колебательного процесса на выходе динамической системы сохраняется за счёт изменения одного или нескольких параметров формирующей функции, а показатель экспоненциальной расходимости траекторий А. М. Ляпунова близок к нулю. Учитывая, что помехоустойчивость нелинейного фильтра, осуществляющего декодирование сигнала, определяется степенью расходимости фазовых траекторий хаотического процесса, алгоритм становится существенно менее чувствительным к возмущениям. Предложены алгоритмы генерации, информационной модуляции хаотического процесса. На основе марковской теории нелинейной фильтрации синтезированы алгоритмы квазиоптимальной обработки сложного сигнала на фоне негауссовских марковских помех.

Область применения: системы телекоммуникаций с высокой степенью защиты канала передачи от несанкционированного доступа к информации.

ABSTRACT

Polovenya Sergey Ivanovich

Algorithms for information security in open channels with interference by means of methods of nonlinear dynamics

Key words: nonlinear dynamic system, dynamic chaos, nonlinear forming function, distributed in time mapping, cryptographic protection of the information, agitating of phase trajectories, digital communication, algorithm of optimum processing, robustness, noise immunity.

The purpose of this work: increase of a noise stability of transmitting systems of the discrete information on the basis of dynamic chaos in channels with intensive hindrances and maintenance of protection of the information from unapproved access.

Main results: The analysis of potentialities of nonlinear one- and multiring dynamic systems with more than one degree of freedom is carried out. Requirements to the nonlinear forming functions included in a chain of feedback of dynamic system are defined. Possibility of conservation of high degree stochastic fluctuations at use of simple piece-linear and smooth functions, and also fragments of planes in tridimensional phase space, under condition of pseudo-random distribution of parameters of nonlinear forming function during a final or infinite time slice is revealed. According to a method during one or more step of work of dynamic system it is possible to use rather simple forming functions which derivative in all area of their definition has small values on the module. Thus complex irregular character of oscillatory process on a yield of dynamic system is conserved for the account of change of one or several parameters of forming function, and the index of exponential divergence of trajectories of A. M. Lyapunov is close to zero. Considering that the noise stability of the nonlinear filter which is carrying out decoding of a signal, is defined by degree of divergence of phase trajectories of chaotic process, algorithm it becomes essential less sensitive to perturbation. Algorithms of generationand information modulation of chaotic process are offered. On a basis of the Markov theory of a nonlinear filtration are synthesized algorithms of quasioptimum processing of a complex signal against non-Gaussian Markov hindrances. Numerical modeling proves expediency of application of methods of nonlinear dynamics in digital communication systems on open canals. Paths of practical realization of algorithms, methods and approaches are specified.

Area of application: telecommunication systems with high degree of protection of the transmission channel from unapproved access to the information.

Научное издание

Половеня Сергей Иванович

АЛГОРИТМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ОТКРЫТЫХ КАНАЛАХ С ПОМЕХАМИ МЕТОДАМИ НЕЛИНЕЙНОЙ ДИНАМИКИ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

по специальностям 05.13.19 – Методы и системы защиты информации, информационная безопасность и 05.12.04 – Радиотехника, в том числе системы и устройства телевидения

Подписано в печать 18.08.2014.	Формат 60x84 $^{1}/_{16}$.	Бумага офсетная.
Гарнитура «Таймс».	Отпечатано на ризографе.	Усл. печ. л. 1,63.
Уч.-изд. л. 1,4.	Тираж 60 экз.	Заказ 352.

Издатель и полиграфическое исполнение: учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя, распространителя печатных изданий №1/238 от 24.03.2014, №2/113 от 07.04.2014, №3/615 от 07.04.2014
ЛП №02330/264 от 14.04.2014.
220013, Минск, П. Бровки, 6