ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

на диссертацию
Кульминского Данила Дмитриевича
«АНСАМБЛИ ХАОТИЧЕСКИХ ГЕНЕРАТОРОВ С ЗАПАЗДЫВАЮЩЕЙ ОБРАТНОЙ СВЯЗЬЮ (РЕКОНСТРУКЦИЯ, КОЛЛЕКТИВНАЯ ДИНАМИКА И ПРИЛОЖЕНИЯ)»,
представленную на соискание учёной степени
кандидата физико-математических наук
по специальности 01.04.03 — радиофизика.

Исследование ансамблей нелинейных систем — это одна из ключевых задач современной радиофизики. По этой теме выходит много журнальных статей и монографий. Интерес к этой теме вызван как высоким потенциалом практического применения получаемых знаний о свойствах сложноструктурированных нелинейных систем так и возможностью открытия новых, ранее неизвестных типов динамики. В качестве примера можно привести сравнительно недавно обнаруженные химеры — это режимы наблюдаемые в ансамблях нелинейных систем, когда возникают изолированные области с разными типами поведения. Из-за конечного времени распространения сигналов, одной из типичных моделей нелинейных систем являются системы с запаздыванием. Такие системы отличает сравнительная простота математической записи и физической реализации и очень богатая и сложная феноменология. Ещё больше сложностью отличаются ансамбли таких систем. На сегодняшний день они исследованы не достаточно хорошо. Существует большое число важных и пока недостаточно хорошо проработанных направлений исследований таких систем и их приложений. Сюда, например, можно отнести задачи о восстановлении модельных уравнений по заданному сигналу, полученному от ансамбля систем с запаздыванием. Очень перспективными выглядят также исследования в области конфиденциальной передачи информации, где в качестве несущей используется хаотический сигнал, генерируемый системами с запаздыванием. Таким образом, тема диссертации, которая посвящена изучению ансамблей нелинейных систем с запаздыванием, является актуальной.

При изучении сложной динамики нелинейных систем, большое зна-

чение имеет построение их математических моделей в ситуации, когда необходимая информация о внутреннем устройстве системы отсутствует и поэтому традиционный способ построения модели на основе выделения существенных функциональных элементов и значимых связей между ними не может быть применим. В этом случае применяют подход, получивший название динамическим моделированием. В его рамках изучаемая система рассматривается как чёрный ящик, сигнал которого регистрируется. На его основе конструируется динамическая система таким образом, что бы она максимально точно воспроизводила необходимые характеристики этого сигнал на как можно более длинном интервале времени. Эта задача очень сложна и не имеет формализованного алгоритма решения. Ещё более сложной она становится, когда восстановлению подлежит модель ансамбля взаимодействующих систем с запаздыванием. Известные в литературе методы построения таких моделей требуют достаточно ресурсоёмких вычислений. В диссертации предложен подход, позволяющий более эффективно строить такие модели. Подход основан на минимизации специально подобранной целевой функции. Существенным является то, что минимизация осуществляются независимо для каждого узла ансамбля, а следовательно её сравнительно легко можно выполнять в параллельном режиме на многопроцессорных вычислительных системах.

Очень интересные результаты представлены в части построения систем шифрования на основе хаотической синхронизации. В диссертации предложены эффективные конструкции приёмо-передающих систем, в которых информация кодируется при помощи хаотического сигнала, а декодирование осуществляется на основе эффекта хаотической синхронизации. Сами по себе такие системы известны достаточно давно. Однако до сих пор существует целый ряд проблем, которые затрудняют их широкое использование. В диссертации предложены несколько интересных идей, позволяющих преодолеть известные недостатки таких схем шифрования. Немаловажно, что наряду теоретическим исследованием была выполнена и экспериментальная реализация. Также нужно отметить, что кроме анализа надёжности передачи информации к помехам и затуханию, показана также устойчивость предлагаемых схем шифрования к известным методом неавторизованного дешифрования.

Интересные результаты получены при изучении ансамблей систем с

запаздыванием и бистабильностью. Продемонстрировано, что в таких ансамблях, связь внутри которых осуществляется через среднее поле, могут возникать химеры, когда часть элементов демонстрирует синхронные колебания с некоторой основной частотой, а другие элементы не синхронны с ними и совершают колебания с другой основной частотой.

Научные положения, выводы и рекомендации, сформулированные в диссертации, обоснованы в достаточной мере и достоверны. Они получены с применением хорошо обоснованных численных и теоретических методов, выполнена также их экспериментальная проверка. Исследования и результаты, к которым они привели, являются новыми, они прошли апробацию на российских и международных конференциях, опубликованы в авторитетных российских и международных журналах. Представленные в диссертации результаты имеют высокую значимость. Результаты работы могут быть использованы в работе научных групп, занимающихся радиофизикой, в работе таких организаций как ИРЭ РАН, СГУ, СГТУ, а также в учебном процессе. Автореферат точно отражает содержание работы.

Замечания.

1. Значительная часть формул и математических символов в диссертации набраны очень не качественно. Типичный и далеко не единственный пример — уравнение (1.12), в котором для одного и того же символа V, который встречается в формуле несколько раз, задействовано три разных начертания. Символ, используемый в качестве индекса у этой величины в двух случаях вообще нельзя идентифицировать. Также следует отметить общее низкое качество оформления работы. Не проведено никакой работы по аккуратному размещению рисунков в тексте. Типичной и не единственный пример — стр. 75 где есть только три строчки текста, а на следующей странице находится рисунок. Очевидно, что рисунок можно было бы сдвинуть так, чтобы не оставлять таких больших пустых мест в тексте. В описании рис. 3.3(в) упоминаются цвета линий, хотя рисунок чёрно-белый. В результате нельзя понять, чему отвечает каждая из показанных на рисунке кривых.

2. В первой главе предложен метод восстановления модели ансамбля систем с запаздыванием. В качестве базового выбрано уравнение в форме (1.1). Метод состоит в том, что для заданных временных рядов вычисляются параметры этого уравнения. Уравнение (1.1) это только один из

возможных примеров моделей с запаздыванием. Однако в диссертации не обсуждается чем мотивирован выбор именно такой формы базовой модели.

3. В диссертации показано, что метод реконструкции, предложенный в главе 1, эффективно работает когда мы заранее знаем, что система описывается уравнениями в форме (1.1) и требуется определить только числовые значения параметров. Однако, очевидно, что возможна ситуация, когда заранее неизвестна даже форма модельных уравнений. В такой ситуации применимость предложенного метода будет под вопросом. В этой связи было бы полезным в диссертации проанализировать возможность выявления ситуации, когда метод не работает. Например, можно было бы привести контрпример и показать как ведут себя целевые функции когда сигнал сгенерирован ансамблем, описываемым уравнениями, отличными от (1.1).

4. В главе 2 рассматривается ансамбль систем с запаздыванием и бистабильностью. В начале параграфа 2.2 на стр. 38 говорится, что у парциальной системы возможны колебания на двух частотах, ν_1 и ν_2. Отсюда можно сделать вывод, что оба режима являются периодическими. Однако затем выясняется, что один из этих режимов на самом деле хаотический. Такую организацию материала нельзя признать удачной. В параграфе 2.2 стоило бы привести более подробное обсуждение одиночной системы вида (2.1), (2.2).

5. В главе 2 обсуждается синхронизация в ансамбле идентичных осцилляторов. Такой подход, хотя и с оговоркой о невозможности его точной экспериментальной реализации, приемлем в случае синхронизации хаотических осцилляций. Несмотря на идентичность, в таких системах действительно могут наблюдаться синхронные и не синхронные режимы. Однако говорить о синхронизации предельных циклов в математически идентичных системах не вполне корректно. Два цикла в таких системах будут синхронны всегда, даже при отсутствии связи, в том смысле, что разность их фаза будет всегда постоянной. Кроме того, результаты численного моделирования сопоставляются с экспериментом в котором принципиально невозможно получить идентичные системы. Поэтому более правильным было бы внести небольшой случайный разброс по параметрам в модельные уравнения.

6. Главные результаты главы 2 получены на основе того, что кластер осцилляторов синхронизируется при условии, что сдвиг по фазе между средним полем $G(t)$ и каждым осциллятором по модулю меньше $\pi/2$. Этот критерий не очевиден и правомерность его применения требует специального обсуждения. Хотя в диссертации даны ссылки на работы [43] и [83], но этого не достаточно, так как в указанных работах данный критерий рассматривается на примере других уравнений.

7. Для рассматриваемых в главе 2 различных способов формирования среднего поля приводятся формулы для фазовых сдвигов $\Delta\varphi_1$ и $\Delta\varphi_2$, см. например (2.8), (2.11), (2.12), (2.13), (2.14). Вывод формул для $\Delta\varphi_{1,2}$ стоило бы объяснить более подробно и привести ссылки на соответствующую литературу.

8. В главе 3 рассматривается система скрытой передачи информации на основе хаотической синхронизации и обсуждается экспериментальная реализация такой системы с использованием 16-ти разрядных микроконтроллеров. По всей видимости, применение цифровых устройств вообще, а таких низкоразрядных в частности, является неудачным решением и может быть оправдано только для предварительной «обкатки» идей. Как известно, если смешать информацию с настоящей случайной последовательностью, сгенерированной, например, в результате бросков монеты, то зашифрованный таким образом сигнал будет принципиально невозможно дешифровать, не зная эту последовательность. Эта идея реализуется в виде пар идентичных шифроблокнотов: один используют для шифрования, второй для дешифрования. Каждую пару можно использовать только один раз. Но если зашифровать сообщения, используя несколько раз один и тот же блокнот, то стойкость такого шифрования падает и возникает возможность его взлома. Шифрование на основе хаотической синхронизации реализует парадигму шифроблокнотов, где идентичность блокнотов достигается за счёт синхронизации. Но если вместо полноценного хаоса генерируется периодическая последовательность, то возникает дополнительная возможность для атаки на шифр. Поэтому предлагая в качестве генератора хаоса в схемах шифрования цифровой генератор, который в силу конечной разрядности может генерировать только периодические последовательности, следует иметь ввиду такую возможность. Низкая разрядность используемого в диссертации генератора даёт осно-

вания предполагать, что на самом деле он генерирует не достаточно качественную с точки зрения стохастических свойств последовательность, что даёт дополнительную возможность для атаки на шифр. Кроме того, низкоразрядные параметры генератора, контролирующие его хаотический режим, вероятно, можно найти простым перебором.

Указанные недостатки не снижают впечатления о работе, которая свидетельствует о высокой квалификации автора. В диссертационной работе Кульминского Д. Д. содержится новое решение актуальной научной задачи радиофизики. Она представляет собой законченное исследование, выполненное автором самостоятельно. Диссертация Кульминского Д. Д. удовлетворяет критериям, установленными «Положением о присуждении ученых степеней» и соответствует специальности 01.04.03 — радиофизика. Ее автор, Кульминский Данил Дмитриевич, заслуживает присуждения учёной степени кандидата физико-математических наук по специальности 01.04.03 — радиофизика.

Профессор кафедры «Приборостроение» Федерального государственного бюджетного образовательного учреждения высшего образования «Саратовский государственный технический университет имени Гагарина Ю. А.» (Россия, 410054, Саратов, ул. Политехническая, 77, Эл. почта: p.kuptsov@sstu.ru, Телефон: 8452-99-88-14), д. ф.-м. н., доцент

15.01.2018

Купцов Павел Владимирович

Подпись П. В. Купцова заверяю, Учёный секретарь Учёного совета Федерального государственного бюджетного образовательного учреждения высшего образования «Саратовский государственный технический университет имени Гагарина Ю. А.», к. и. н., доцент

Малова Наталия Анатольевна