МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний політехнічний університет

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Том 6, № 2

Volume 6, No. 2

Одеса – 2016
Odesa – 2016

Журнал внесений до переліку наукових фахових видань України
(технічні науки)
згідно наказу Міністерства освіти і науки України № 463 від 25.04.2013 р.

Виходить 4 рази на рік

Заснований Одеським національним політехнічним університетом у 2011 році

Свідоцтво про державну реєстрацію КВ № 17610 - 6460Р від 04.04.2011р.

Published 4 times a year

Founded by Odessa National Polytechnic University in 2011

Certificate of State Registration KB № 17610 - 6460P of 04.04.2011

Друкується за рішенням редакційної колегії та Вченої ради Одеського національного політехнічного університету

Оригінал-макет виготовлено редакцією журналу

Адреса редакції: просп. Шевченка, 1, Одеса, 65044, Україна
Телефон: +38 048 705 8506
Web: http://immm.opu.ua E-mail: immm.ukraine@gmail.com

Editorial address: 1 Shevchenko Ave., Odessa, 65044, Ukraine
Tel.: +38 048 705 8506
Web: http://immm.opu.ua E-mail: immm.ukraine@gmail.com

ЗМІСТ / CONTENTS

УДК 621. 317.799. 297 + 681.849

Informatics and Mathematical Methods in Simulation
Vol. 6 (2016), No. 2, pp. 105-115

МЕТОДОЛОГИЯ ПОСТРОЕНИЯ СИСТЕМЫ ЭКСПЕРТНОЙ ПРОВЕРКИ ЦИФРОВЫХ ФОНОГРАММ И ИДЕНТИФИКАЦИИ АППАРАТУРЫ ЦИФРОВОЙ ЗВУКОЗАПИСИ С ПРИМЕНЕНИЕМ ПРОГРАММЫ «ФРАКТАЛ»

О.В. Рыбальский, В.И. Соловьев, В.В. Журавель

Национальная академия внутренних дел,
пл. Соломянская, 1, Киев, 03056, Украина; e-mail: rybalsky_ol@mail.ru

Рассмотрена методология построения экспертного инструментария, предназначенного для проверки целостности информации, содержащейся в цифровых фонограммах. Показано, что методология разработки инструментария для экспертной проверки целостности информации, содержащейся в цифровых фонограммах, качественно отличается от применявшейся методологии разработки инструментария, предназначавшегося для проверки целостности информации, содержащейся в аналоговых фонограммах. Показано, что «классический» трассологический подход, использовавшийся при создании инструментария для проверки аналоговых фонограмм, не удовлетворяет требованиям экспертизы; для проверки цифровой информации требуется применение новых технологий, основанных на фрактальном подходе к информации, содержащейся в цифровых фонограммах. Показано, что предложенная методология создания инструментария для проверки целостности информации, содержащейся в цифровых фонограммах, и идентификации аппаратуры цифровой звукозаписи, обеспечила разработку программы «Фрактал» и методики ее применения при проведении экспертиз материалов и средств цифровой звукозаписи.

Ключевые слова: аппаратура цифровой звукозаписи, методика проведения экспертизы, методология, мультифрактальные структуры, цифровые фонограммы, фрактальные технологии, экспертиза

Введение

Развитие цифровой техники записи звука настоятельно потребовало создания нового инструментария, обеспечивающего надежность проверки целостности информации, зафиксированной в цифровых фонограммах (ЦФ) и идентификации аппаратуры цифровой звукозаписи (АЦЗЗ).

Такая проверка проводится специализированными экспертными подразделениями, входящими в системы МВД и СБ Украины и институтами судебной экспертизы Министерства юстиции Украины и называется технической экспертизой материалов и средств видеозвукозаписи. С криминалистической точки зрения проверка целостности информации в ЦФ относится к диагностическим исследованием фонограмм, а идентификация АЦЗЗ – к идентификационным исследованиям аппаратуры записи.

Построение системы проверки целостности информации в ЦФ и идентификации АЦЗЗ подразумевает создание инструментария, содержащего два взаимосвязанных блока: специализированного программного продукта и методики проведения

экспертизы. Успешность, как и сама возможность, их создания определяется правильностью выбора методологического подхода к решению этой задачи. Для ее решения была разработана программа «Фрактал» и методика ее применения при экспертизе ЦФ и АЦЗЗ [1]. Создание программы и методики потребовали применения новой методологии, ранее нигде не рассматриваемой. Ее основа – глубокая теоретическая проработка тонких процессов, происходящих при записи и обработке звуковой информации в цифровой форме, с условием представления этой информации в свете фрактального подхода.

Цель статьи – раскрытие основных аспектов методологии, использованной при создании программы «Фрактал» и методики проведения экспертизы с ее использованием.

Основная часть

В основе методик проведения технической экспертизы материалов и средств видеозвукозаписи всегда лежал принцип сравнительных исследований образцовых и спорных фонограмм. И это вполне естественно, поскольку фонограмма являются тем идентифицирующим объектом, в котором отображаются индивидуальные особенности аппаратуры записи, вне зависимости от ее вида или типа [2]. На этом же общем принципе основана методика проверки целостности информации, содержащейся в ЦФ, и идентификации АЦЗЗ. Однако в методологии построения инструментария для проверки материалов и средств цифровой звукозаписи, имеются существенные отличия от «классической» криминалистической методологии, основанной на трассологии, принятой для материалов и средств аналоговой звукозаписи. Это обусловлено особенностями цифровой записи звука. К таким особенностям следует, например, отнести очень малый уровень сигналов паразитных параметров АЦЗЗ, фиксируемых в ЦФ. Эти особенности потребовали разработки новой теоретической базы, основанной на структурном анализе АЦЗЗ и процессов, происходящих при цифровой записи, воспроизведении и обработке ЦФ [2; 3]. Были установлены идентификационные признаки и определены требования к их выделению из ЦФ и последующей обработке. При этом был установлен фрактальный характер сигналов идентификационных признаков и, как следствие этого, была выбрана концепция использования фрактальности собственных шумов АЦЗЗ, зафиксированных в ЦФ, для построения необходимого инструментария для проведения экспертизы [4]. В результате изменилась методология как построения программы для проверки целостности ЦФ и идентификации АЦЗЗ, так и построения методики проведения исследований с использованием такой программы.

Рассматривая строение программы «Фрактал» с методологической точки зрения, следует отметить, что она является совокупностью фрактальных технологий, учитывающих свойства исследуемых сигналов. Действительно, сегментация информации в ЦФ производится программой на измерении фрактальной меры Хаусдорфа и основана на различии этой меры для сигналов речи и сигналов пауз [5; 6]. Заслуживает особого внимания тот факт, что фрактальная мера сигналов пауз меньше фрактальной меры речевых сигналов, что свидетельствует о значительно большей степени самоупорядоченности сигналов шумов АЦЗЗ, чем сигналов речи.

Сигнал после обработки, например, методом вырезания и перестановки фрагментов изменяет свой фрактальный состав, что также свидетельствует об изменениях в самоупорядоченности сигналов шумов [7; 8].

Выделение самоподобных структур производится с использованием вейвлета Морле, что является наилучшим способом решения для поставленной задачи [9; 10]. При этом следует отметить, что применение фрактальных технологий всегда

подразумевает нахождение наилучшей аппроксимации самоподобных структур под решение конкретной задачи.

Таким образом, использование фрактальных свойств исследуемых сигналов привело к применению комплекса новых технологий при построении программы «Фрактал».

Появились и новые методологические требования к построению программы «Фрактал» при разработке методики ее применения. Вследствие этого была поставлена и решена задача автоматического расчета величины фрактальных масштабов (меры близости фрактальных характеристик) при сравнении двух ЦФ [11; 12]. При отработке методики и программы была установлена, во-первых, зависимость результата исследований от величины фрактального масштаба самоподобных структур, что обусловлено наличием отдельной области этих масштабов в распределении меры близости самоподобных структур двух ЦФ, при которых проявляются индивидуальные особенности АЦЗЗ (см. рис. 1 и рис. 2); во-вторых, выявлена необходимость при проведении проверки ЦФ установления области фрактальных размеров, соответствующей той области их распределения, где проявляются индивидуальные особенности каждой конкретной АЦЗЗ, на которой были записаны исследуемые ЦФ. И, в-третьих, установления такого значения фрактального размера в установленной области, при котором ошибка I рода имеет наименьшее значение.

Понимание необходимости учета этих особенностей появилась в процессе отработки версий программы, поскольку при использовании ее первых версий эксперт был вынужден устанавливать эту область в ручном режиме, что, во-первых, требовало значительной квалификации и, во-вторых, огромных трудозатрат. При этом правильность принятия экспертного решения носила субъективный характер и могла вызывать обоснованные сомнения.

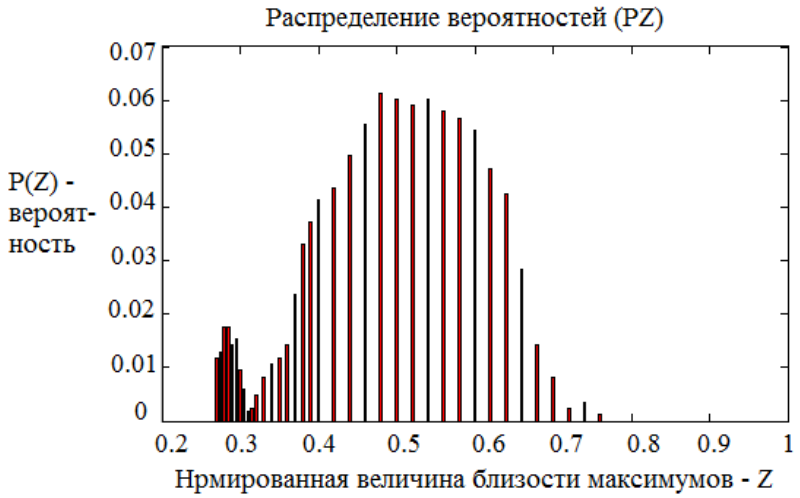


Рис. 1. Плотность вероятности меры близости Z для записи двух ЦФ на одной АЦЗЗ

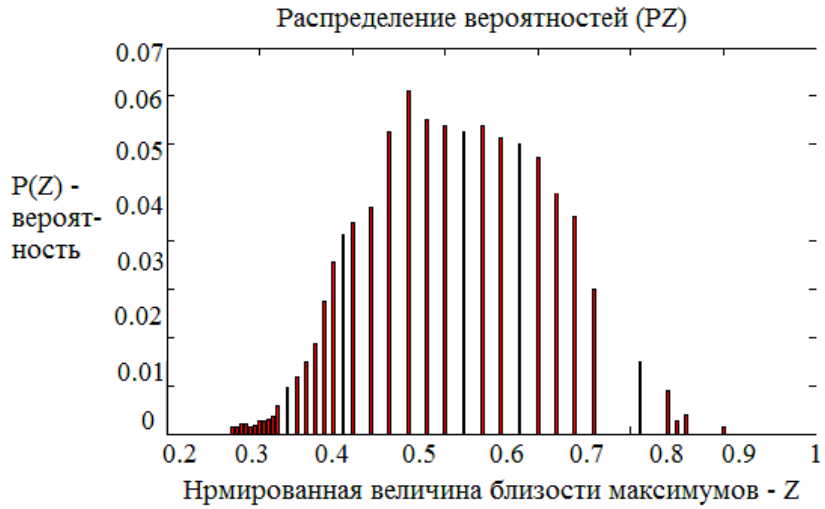


Рис. 2. Плотность вероятности меры близости Z для записи двух ЦФ, на разной АЦЗЗ

На рис. 1 и рис. 2 приведены плотности вероятности меры близости P(Z) для двух ЦФ, записанных на одной и различной АЦЗЗ. Фонограммы в каждой паре ЦФ записывалась при различных условиях звуковой среды.

Многочисленные экспериментальные исследования статистических характеристик пауз различных ЦФ при записи в различных условиях звуковой среды показали устойчивую особенность плотности вероятности P(Z) величины меры близости Z [13].

Мера близости Z является множеством минимальных расстояний для каждого из локальных максимумов, выделенных из пауз одной из ЦФ по отношению к ближайшему локальному максимуму, выделенному из пауз второй ЦФ [13]. Выделение этих структур иллюстрируется скейлограммой, приведенной на рис. 3 [10].

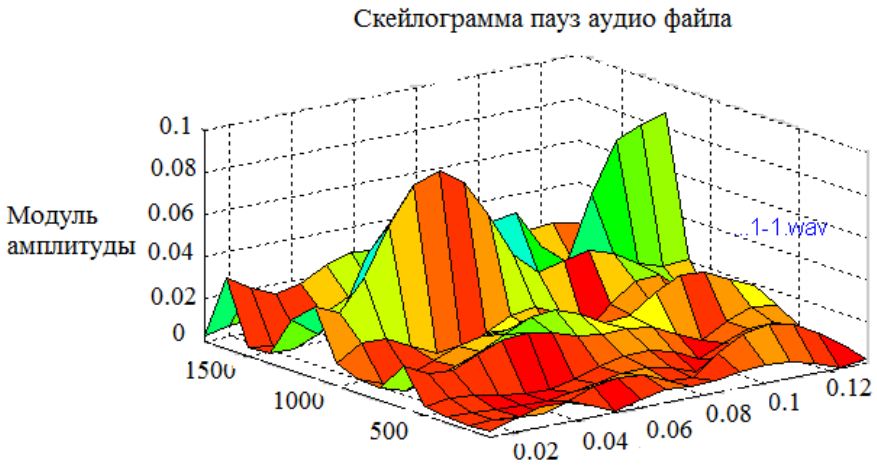


Рис. 3. Скейлограмма пауз ЦФ

Решение задачи автоматического расчета фрактальных масштабов во всей области их применения полностью изменило методологический подход к экспертизе и позволило осмыслить и уточнить построение методики проведения диагностических исследований ЦФ и идентификационных исследований АЦЗЗ. Стало ясно, что при сравнении двух ЦФ всегда будут существовать две области фрактальных масштабов: область близких параметров (совпадения) двух ЦФ и область различия параметров двух ЦФ. Между ними существует четкая граница. Это поясняется тем, что как в случае близости параметров, так и в случае их различия обязательно существует область

фрактальных масштабов, где проявляются индивидуальные параметры аппаратуры [10; 13]. И именно в этой области лежит правильное решение. Но как при этом определить, в какой области – близости или различия параметров лежит область масштабов, в которой проявляется индивидуальность АЦЗЗ? Разрешение этой двойственной ситуации лежит в методике проведения диагностических исследований ЦФ.

Методика их проведения основана на записи нескольких (не менее трех) образцовых фонограмм на аппаратуре, представленной на экспертизу. Запись образцов производится экспертом и, поскольку очевидно, что эти записи проведены на одной АЦЗЗ, то фрактальные масштабы, при которых проявляются индивидуальные характеристики АЦЗЗ, лежат в области близких параметров (характеристик). Поэтому сначала проводятся сравнительные исследования образцовых фонограмм, при которых они сравниваются между собой. При этом определяются значения крайних левых точек границы раздела между областями близких и различных характеристик при сравнении каждой пары образцовых ЦФ (точки пересечения границы раздела с прямой предельной вероятности ошибки I рода, равной 0,15). Устанавливается степень расхождения этих точек, полученных при сравнении разных пар, и определяются минимальное и максимальное значения расположения точек пересечения (контрольных точек) для границ между разными парами.

После этого проводятся попарные сравнительные исследования между образцовыми и спорной (исследуемой) фонограммами. Если значение контрольной точки при сравнении спорной и образцовых фонограмм совпадает с точностью до 25 % со значением минимального или максимального положения этой точки при попарной проверке образцовых фонограмм (при выходе за интервал) либо лежит внутри этого интервала, то принимается решение о близости характеристик этих фонограмм. Таким образом, в силу близости характеристик самоподобных структур, выделенных из образцовой и спорной фонограмм, принимается гипотеза о том, что обе фонограммы записаны на одной аппаратуре, т.е. о том, что спорная фонограмма является оригинальной. В противном случае принимается гипотеза о различии характеристик самоподобных структур, выделенных из образцовой и спорной фонограмм. В этом случае возможны три варианта оценки этого факта: фонограмма является копией, что равносильно тому, что она подвергалась цифровой обработке, либо записи образцовой и спорной фонограмм проводились на различной аппаратуре. Эксперт в таких случаях указывает в выводах, что фонограмма не являет оригиналом, а окончательное принятие решения в этом случае производится следствием и судом, поскольку налицо факт попытки обмануть экспертизу (либо предоставили копию, либо подделку, либо другой аппарат записи, что само по себе является преступлением).

Очевидно, что для принятия двух различных гипотез необходимо представить эксперту обе области фрактальных масштабов – для близких и раздельных характеристик, поскольку гипотезы являются взаимоисключающими. В зависимости от принятой гипотезы выбирается соответствующая область масштабов (каждая из них в своем окне). В выбранной области выбирается фрактальный масштаб, при котором величина ошибки I рода для выбранной гипотезы минимальна, и при этом масштабе строятся кривые плотности вероятности самоподобных структур для каждой из двух фонограмм.

Представленная методика иллюстрируется рис. 4 – рис. 9, где показан процесс проведения экспертизы.

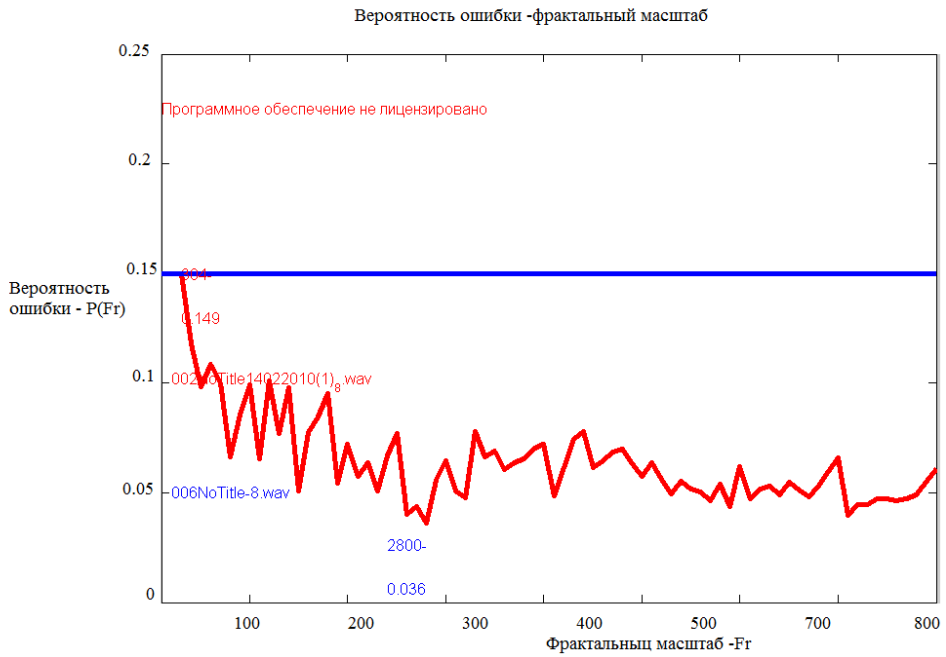


Рис. 4. Результат расчета фрактальных масштабов для области близких характеристик фонограмм № 2 и № 6, записанных на одной АЦЗЗ

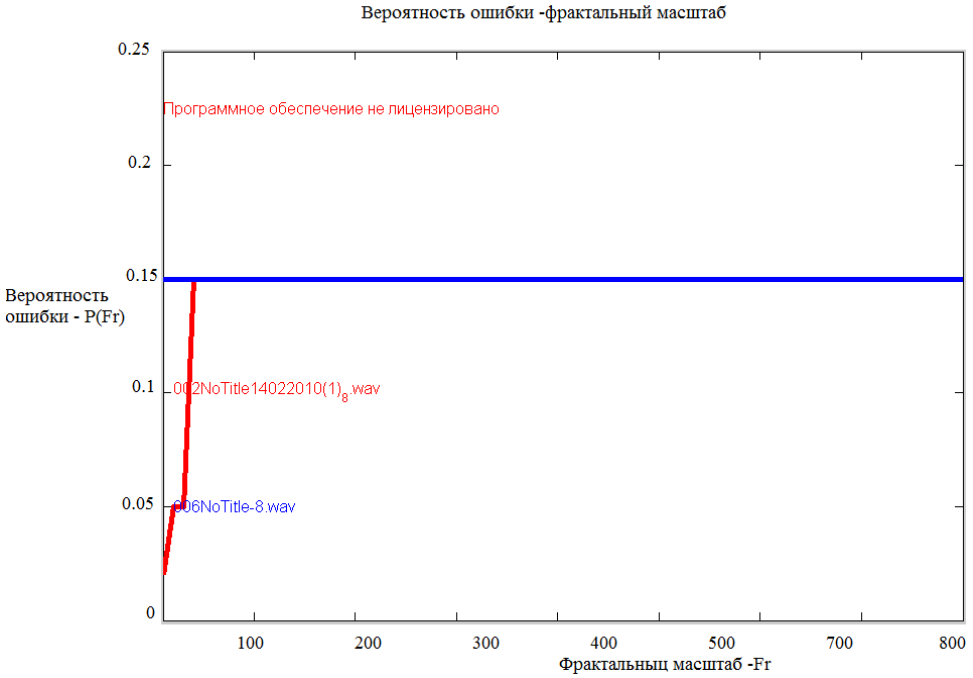


Рис. 5. Результат расчет фрактальных масштабов для области различающихся характеристик фонограмм № 2 и № 6, записанных на той же АЦЗЗ

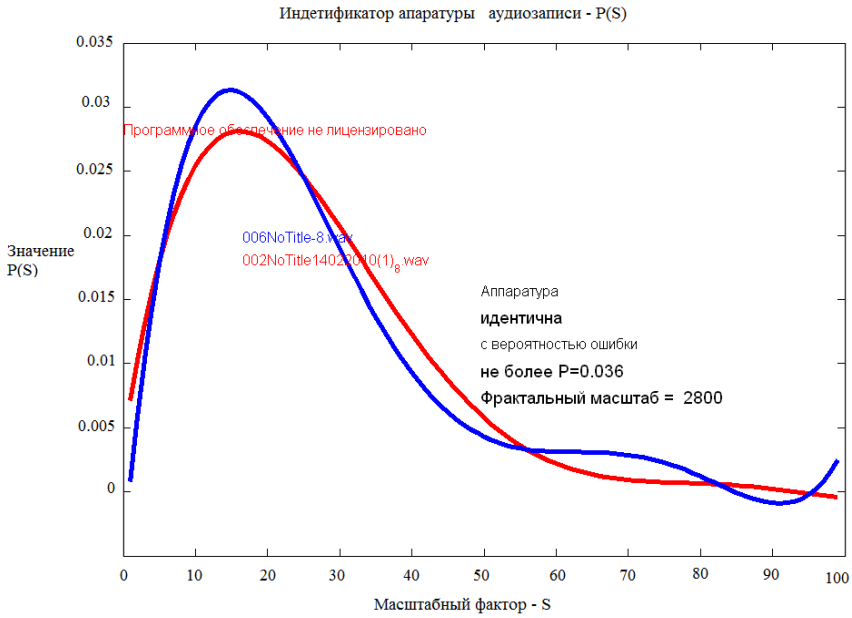


Рис. 6. Плотность вероятностей самоподобных структур для фонограмм № 2 и № 6, записанных на одной АЦЗЗ ул. коблевская 65023 0800506508

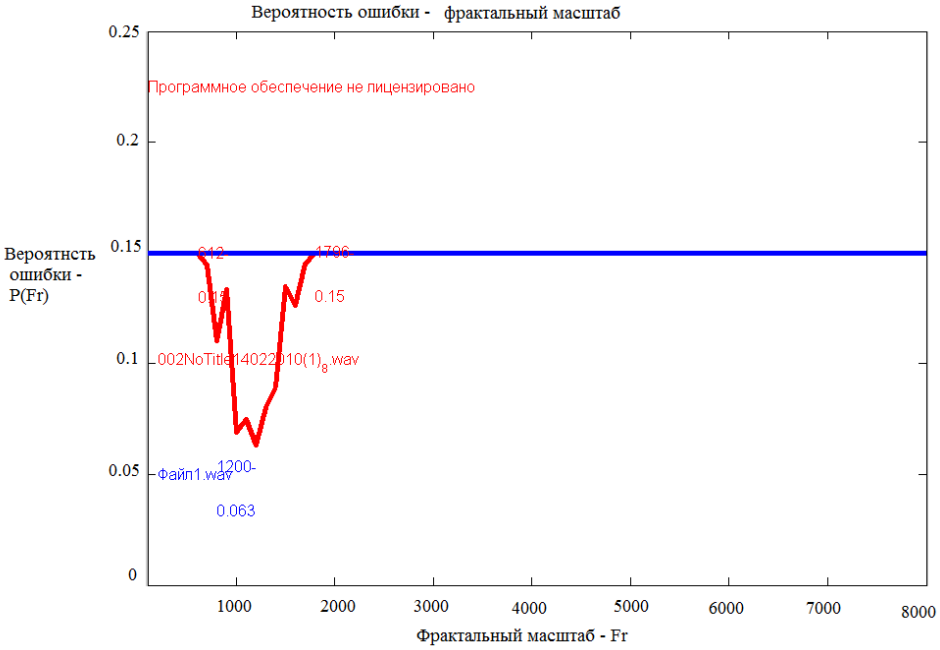


Рис. 7. Результат расчета фрактальных масштабов для области близких характеристик фонограмм № 2 и № 1, записанных на разной АЦЗЗ

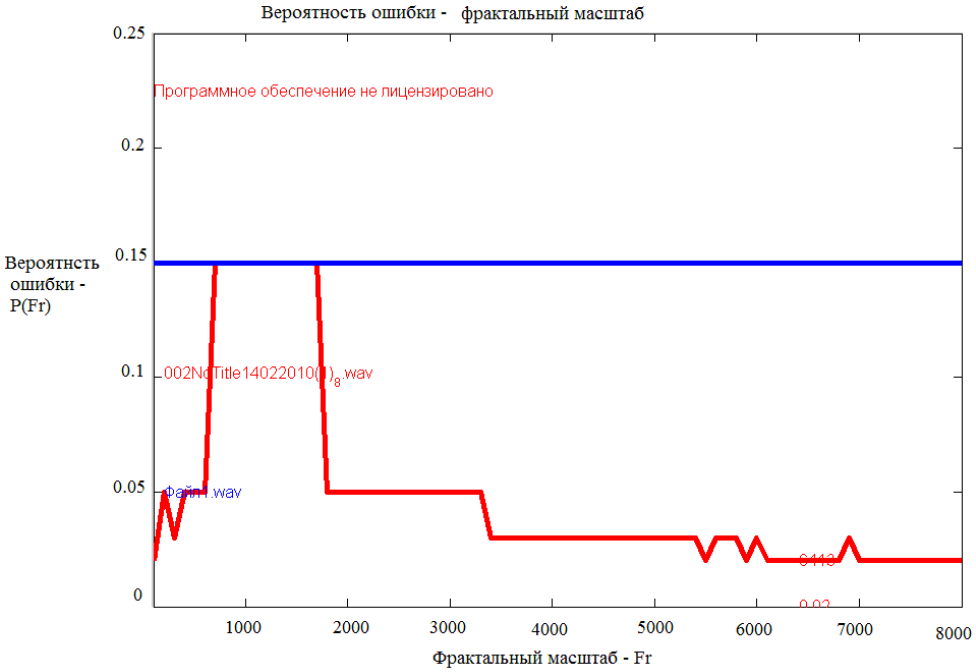


Рис. 8. Результат расчет фрактальных масштабов для области различающихся характеристик фонограмм № 3 и № 1, записанных на разной АЦЗЗ

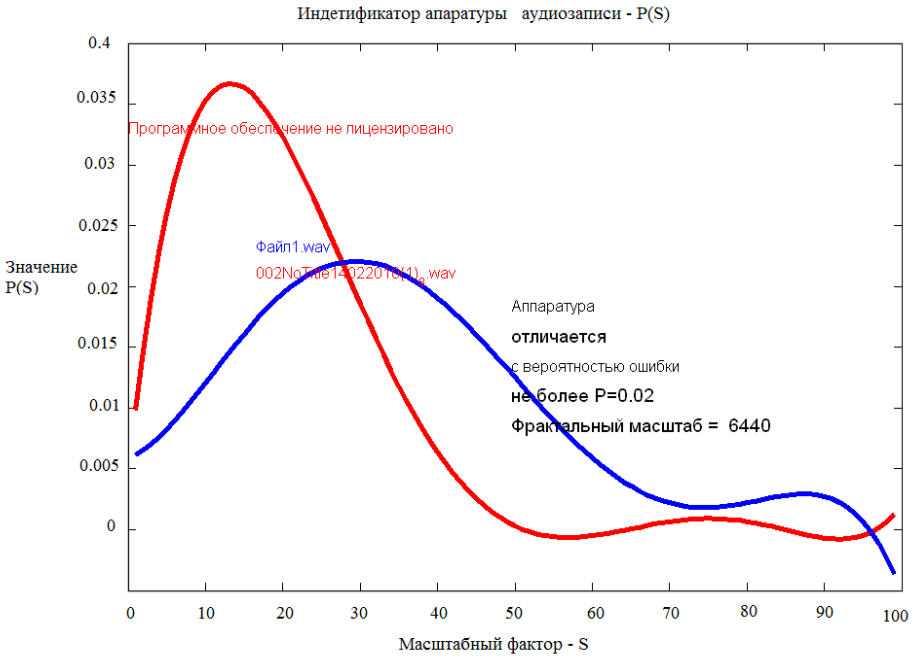


Рис. 9. Плотность вероятностей самоподобных структур для фонограмм № 2 и № 1, записанных на разной АЦЗЗ

Из сравнения положения контрольных точек по шкале фрактальных масштабов на рис. 4 и рис. 7 видно, что их значения расходятся более чем на 100 %. Поэтому выбрана область несовпадения статистических характеристик шумов, зафиксированных на сравниваемых фонограммах.

При этом из рассмотрения рис. 4, рис. 5, рис. 7 и рис. 8 видно, что пороговая вероятность ошибки первого рода принята на уровне 0,15. Это поясняется, во-первых, плотностью вероятности меры близости Z для ЦФ, записанных на одной АЦЗЗ [13],

(см. рис. 1), и, во-вторых, определением этой величины эмпирическим путем на различных видах и типах АЦЗЗ в качестве оптимальной.

Следует отметить, что программа «Фрактал» и методика ее применения прошли апробацию в экспертных учреждениях Украины, внедрены в экспертную практику и используется при проведении экспертиз материалов и средств цифровой звукозаписи

Выводы

Показано, что методология разработки инструментария для экспертной проверки целостности информации, содержащейся в цифровых фонограммах, качественно отличается от применявшейся методологии разработки инструментария, предназначавшегося для проверки целостности информации, содержащейся в аналоговых фонограммах.

Показано, что трассологический подход, использовавшийся при создании инструментария для проверки аналоговых фонограмм, не удовлетворяет требованиям экспертизы.

Показано, что для проверки цифровой информации требуется применение новых технологий, основанных на фрактальном подходе к информации, содержащейся в цифровых фонограммах.

Показано, что предложенная методология создания инструментария для проверки целостности информации, содержащейся в ЦФ и идентификации АЦЗЗ, обеспечила разработку программы «Фрактал» и методики ее применения при проведении экспертиз материалов и средств цифровой звукозаписи.

Список литературы

1. Рибальський, О.В. Методика ідентифікаційних і діагностичних досліджень матеріалів та апаратури цифрового й аналогового звукозапису зі застосуванням програмного забезпечення «Фрактал» при проведенні експертиз матеріалів та засобів відео та звукозапису: наук.-метод. посіб. / О.В. Рибальський, В. І. Соловйов, В. В. Журавель, Т. О. Татарнікова. – К. : ДУІКТ, 2013. – 75 с.
2. Рыбальский, О.В. Современные методы проверки аутентичности магнитных фонограмм в судебно-акустической экспертизе / О.В. Рыбальский, Ю.Ф. Жариков. – К.: Нац. акад. внутр. справ України, 2003. – 300 с.
3. Рибальський, О.В. Застосування вейвлет-аналізу для виявлення слідів цифрової обробки аналогових і цифрових фонограм у судово-акустичній експертизі / О.В. Рибальський. – К.: Нац. акад. внутр. справ України, 2004. – 167 с.
4. Рибальський, О.В. Новий напрям рішення комплексу проблем фоноскопії / О.В. Рибальський, В.І. Соловйов, О.М. Шабля, В.В. Журавель // Захист інформації і безпека інформаційних систем : зб наук. пр. 2-ої міжнар. наук.-техн. конф., 30 травня – 01 червня 2013 р. – Львів: УАД. – С. 122 – 123.
5. Соловьев, В.И. Сегментация речи в задачах выявления монтажа аудиофайлов / В. И. Соловьев, О. В. Рыбальский, В. В. Журавель, Т. В. Командина // Інформаційна безпека. – 2012. – № 1 (7). – С. 35 – 42.
6. Соловьев, В.И. Сегментация звукового сигнала в задачах выявления монтажа в аудиофайлах / В.И. Соловьев // Збірник наукових праць військового інституту Київського національного університету ім. Т Шевченко. – 2013. –. № 39. – С. 210 – 216.
7. Рыбальский, О.В. Следы монтажа в цифровых фонограммах, выполненного способом вырезания и перестановки фрагментов / О.В. Рыбальский, В.И. Соловьев, В. В. Журавель // Реєстрація, зберігання і обробка даних. – 2016. – Т.18. – №1. – С. 32 – 41.
8. Рыбальский, О.В. Экспериментальное подтверждение результатов моделирования механизма возникновения идентификационных признаков монтажа в цифровых фонограммах / О.В. Рыбальский, В.В. Журавель // Сучасні інформаційні та електронні технології : зб. наук. пр. 17 Міжнародної науково-практичної конференції, 23 – 27 травня 2016 р. – Одеса. – С. 124 – 125.

9. Рыбальский, О. В. Обобщенная модель выделения фрактальных структур из цифровых сигналов методом максимумов вейвлет преобразования / О. В. Рыбальский, В. В. Журавель, В. И. Соловьев, В. К. Железняк // Вестник Полоцкого государственного университета. – Серия С. – 2015. – № 4. – С. 13 – 16.
10. Рыбальский, О. Выделение самоподобных структур из шумов цифровых фонограмм / О. Рыбальский, В. Журавель, В. Соловьев, Л. Тимошенко, А. Шабля // Захист інформації і безпека інформаційних систем: зб. наук. пр. V Міжнар. наук.-техн. конф., 02 – 03 червня 2016 р. – Львів. – С. 130 – 131.
11. Рыбальский, О.В. Автоматизация подбора коэффициента фрактального масштаба в программе “Фрактал” / О.В. Рыбальский, В.И. Соловьев, В.В. Журавель, А. Н. Шабля, Т. А. Татарникова // Сучасна спеціальна техніка. – 2013. – № 3 (34), 2013. – С. 5 – 8.
12. Рыбальский, О.В. Автоматизированный расчет коэффициентов фрактального масштаба в программе “Фрактал” / О.В. Рыбальский, В.И. Соловьев, В.В. Журавель, А.Н. Шабля, Т.А. Татарникова // Сучасна спеціальна техніка. – 2014. – № 4 (39). – С. 5 – 11.
13. Соловьев, В.И. Идентификация аппаратуры аудиозаписи по статистическим характеристикам аудиофайлов / В.И. Соловьев // Реєстрація, зберігання і обробка даних. – 2013. – Т.14. – № 1. – С. 59 – 70.

МЕТОДОЛОГІЯ ПОБУДОВИ СИСТЕМИ ЕКСПЕРТНОЇ ПЕРЕВІРКИ ЦИФРОВИХ ФОНОГРАМ І ІДЕНТИФІКАЦІЇ АПАРАТУРИ ЦИФРОВОГО ЗВУКОЗАПИСУ ІЗ ЗАСТОСУВАННЯМ ПРОГРАМИ «ФРАКТАЛ»

О.В. Рибальський, В.І. Соловйов, В.В. Журавель

Національна академія внутрішніх справ,
пл. Солом'янська, 1, Київ, 03056, Україна; e-mail: rybalsky_ol@mail.ru

Розглянута методологія побудови експертного інструментарію, призначеного для перевірки цілісності інформації, що міститься в цифрових фонограмах.
Показано, що методологія розробки інструментарію для експертної перевірки цілісності інформації, що міститься в цифрових фонограмах, якісно відрізняється від методології розробки інструментарію, що призначався для перевірки цілісності інформації, що міститься в аналогових фонограмах, що застосовувалася.
Показано, що «класичний» трасологічний підхід, що використався при створенні інструментарію для перевірки аналогових фонограм, не задовольняє вимогам експертизи.
Показано, що для перевірки цифрової інформації потрібно застосування нових технологій, заснованих на фрактальному підході до інформації, що міститься в цифрових фонограмах.
Показано, що запропонована методологія створення інструментарію для перевірки цілісності інформації, що міститься в цифрових фонограмах, і ідентифікації апаратури цифрового звукозапису, забезпечила розробку програми «Фрактал» і методики її застосування при проведенні експертиз матеріалів і засобів цифрового звукозапису.
Ключові слова: апаратура цифрового звукозапису, методика проведення експертизи, методологія, мультифрактальні структури, цифрові фонограми, фрактальні технології, експертиза.

METHODOLOGY OF CONSTRUCTION OF SYSTEM OF EXPERT VERIFICATION OF DIGITAL PHONOGRAMS AND AUTHENTICATION OF APPARATUS OF DIGITAL AUDIO RECORDING WITH THE USE OF PROGRAM «FRACTAL»

O.V. Rybalsky, V.I. Solovyov, V.V. Zhuravel

National Academy of Internal Affairs,
1, Solomenskaya Sq., Kiev, 03056, Ukraine; e-mail: rybalsky_ol@mail.ru

Methodology of construction of the expert tool, intended for verification of integrity of the information contained in digital phonograms, is considered.

It is shown that methodology of development of tool for expert verification of integrity of the information contained in digital phonograms, high-quality differs from being used methodology of development of tool, targeting at verification of integrity of the information contained in analog phonograms.

It is shown that the «classic» approach used for creation of tool for verification of analog phonograms dissatisfies to the requirements of examination.

It is shown that for verification of digital information application of the new technologies, based on the fractal going near the information contained in digital phonograms, is required.

It is shown that the offered methodology of creation of tool for verification of integrity of the information contained in digital phonograms and authentication of apparatus of the digital audio recording, provided development of the program «Fractal» and methodology of her application during realization of examinations of materials and facilities of the digital audio recording.

Keywords: apparatus of the digital audio recording, methodology of examining, methodology, multifractal structures, digital phonograms, fractal technologies, examination.

УДК 003.26:004.7:053.072:519.876.5

Informatics and Mathematical Methods in Simulation
Vol. 6 (2016), No. 2, pp. 116-126

МЕТОДИ ЗМЕНШЕННЯ ТУРБУЛЕНТНИХ ТА СИНГУЛЯРНИХ ЯВИЩ У МОДЕЛІ ДИНАМІКИ ІНЦИДЕНТІВ КІБЕРБЕЗПЕКИ

І.В. Кононович

Одеська національна академія харчових технологій,
вул. Канатна, 112, Одеса, 65039, Україна; e-mail: kononovich@mail.ru

Розглядаються шляхи вирішення проблеми гіперболічного зростання кількості інцидентів кібербезпеки. Процес росту кількості інцидентів кібербезпеки представляється як перехідний процес, який описується математичною моделлю циклічної багатоетапної обробки інформаційних потоків із позитивними зворотними зв'язками. В моделі можуть виникати регулярні, квазіперіодичні коливання та динамічний хаос. У перехідний період можливі турбулентність та сингулярність. Запропоновано метод управління перехідним процесом, який підвищує стійкість системи, знижує ризик виникнення сингулярності та зменшують, у середньому вдвічі, викиди в зоні турбулентності. Як доповнення до математичної моделі, представлена логіко-лінгвістична модель процесів росту інцидентів. Пояснюються внутрішньо та зовнішньо системні причини недостатності застосовуваних сьогодні засобів забезпечення кібербезпеки. Для кардинального вирішення проблеми інцидентів інформаційної безпеки запропоновані позасистемні заходи, що забезпечують функціональну повноту засобів контролю доступів. Одним із засобів є технологія визначення ідентичності.

Ключові слова: кібернетична безпека, модель динамічної системи, турбулентність, сингулярність, біфуркації, управління безпекою, соціальна природа кібербезпеки

Вступ

Слідом за прискореним розвитком інфокомунікацій та інформаційних технологій швидко зростає кількість інцидентів кібербезпеки (КБ). Постає проблема моделювання таких явищ та пошук методів зупинки чи уповільнення росту інцидентів КБ.

Аналіз існуючих досліджень. Проблемі росту кількості і якості загроз, кількості інцидентів КБ присвячена величезний обсяг наукових і практичних робіт. Ці досягнення викладені, наприклад, в [1, 2]. Добре вивчені процеси розповсюдження і засоби боротьби з вірусами та іншими шкодоносними програмами [3, 4]. Для моделювання процесів боротьби з порушниками застосовані біологічні моделі [5, 6]. Статистика динаміки кількості інцидентів КБ видається регулярно, наприклад, [1, 7]. Але перехідні динамічні процеси досліджені недостатньо. Неясними залишаються питання, як зупинити гіперболічне зростання кількості інцидентів КБ, статистика яких залишається невтішною. Така ситуація схожа на аналогічну кризу інформаційних технологій внаслідок сингулярного переходу в процесі їх бурхливого розвитку [8]. Раніше автор приймав участь в обґрунтовуванні гіпотези щодо сингулярного характеру динаміки кількості інцидентів КБ. Представляє інтерес дослідження цієї динаміки окіл точок сингулярності. Стало ясно, що попередження сингулярних явищ не можливо без управління перехідними процесами.

В управлінні виробництвом, бізнесом, в державному управлінні, у військовій сфері, сфері кібернетичної безпеки широко застосовуються циклічні системи

управління. Такі циклічні управління реалізуються послідовністю мінімум із чотирьох етапів: планування, дії, перевірки, впливання. У стандарті ISO 9001:2008 рекомендується процесно-орієнтований підхід [9]. У військовій сфері будь-яку діяльність, із певною мірою наближення, представляють у вигляді типової кібернетичної моделі OODA, яка має такі її компоненти: Observe – спостерігай, Orient – орієнтуйся, Decide – вирішуй, Act – дій [10]. Подібні логігіко-лінгвістичні моделі застосовують у сфері інформаційної безпеки в системах виявлення кібератак [11]. Вказані моделі передбачають безперервне повторення циклу, який складається із чотирьох послідовних взаємодіючих процесів. На кожному витку такого циклу здійснюється взаємодія із зовнішнім середовищем, оцінка стану і ефективний вплив на нього. У той же час стала приділятись увага нелінійним моделям в соціально-економічній сфері та управлінні [12]. Проте, нелінійні фактори при циклічному управлінні також досліджені ще недостатньо. Особливо це стосується проблеми аналізу перехідних процесів і, стосовно КБ, ставить задачу управління деструктивними явищами у перехідний період.

Мета роботи. Спираючись на гіпотезу щодо сингулярного характеру динаміки кількості інцидентів КБ, на математичну і логіко-лінгвістичну модель, пояснити причини і фактори, що приводять до сингулярності та швидкого росту кількості інцидентів й виробити системні та позасистемні методи, засоби і механізми протидії росту кількості інцидентів КБ та запобіганню чи обходу сингулярностей.

Математична модель динаміки узагальненого циклічного інформаційного процесу

Забезпечення інформаційної безпеки, управління інформаційною безпекою, обробка та використання інформаційних потоків, розвиток інформаційних технологій являються інформаційними процесами. Створимо формальне описання певного узагальненого інформаційного процесу, який буде відображати основні характерні риси перелічених процесів. До типового представника узагальненого інформаційного процесу можна віднести процес, який реалізується організаційною структурою підготовки і реалізації інформаційного управління. «Управлінські рішення приймаються у різноманітних обставинах, включаючи кризові, і тим не менш вони повинні бути прийняті своєчасно, бути максимально обґрунтованими та забезпечувати найбільш повне і ефективне використовування наявних можливостей. … Основними складовими цього складного процесу являються: збирання та підготовка вхідних даних, побудова моделі розвитку ситуації, формулювання (прийняття) рішення керівником, конкретизація і деталізація рішення у плані реалізації інформаційного управління, доведення даного рішення до виконавців , а також організація, оперативне управління і контроль за його реалізацією [13]».

В сфері державного управління, де реалізуються сучасні світові стандарти інформаційної та організаційної культури, цикловий принцип управління отримав важливий розвиток. «На відміну від традиційних інформаційних служб, згадані фахівці виконують завдання якісно-змістовного перетворення інформації, функціонально поєднаного із науковою (виробництво нового знання) і управлінською (розробка варіантів рішень, сценаріїв) діяльністю. При цьому спостерігається організаційне відокремлення такої інформаційно-аналітичної діяльності від управлінської [14]». Виділений процес інформаційно-аналітичної діяльності, у свою чергу, складається з чотирьох кроків: виявлення вхідних вимог та даних; формування інформаційних ресурсів; витяг, придбання та генерація нових знань; доведення інформації, яка придатна для прийняття рішень щодо виконання конкретного завдання.

До характерних рис перелічених інформаційних процесів віднесемо мультиетапність процесів, циклічність процесів і наявність зворотних позитивних

зв'язків між сусідніми етапами обробки і використання інформації. Тоді динаміка цих процесів може бути описана єдиною математичною моделлю. Пропонується скористатись математичною моделлю циклічного управління КБ, у розробці якої автор приймав участь [15], яка формалізує дані моделі. Цикл перетворення даних в знання, рішення і управлінські дії можна представити як на рис. 1.

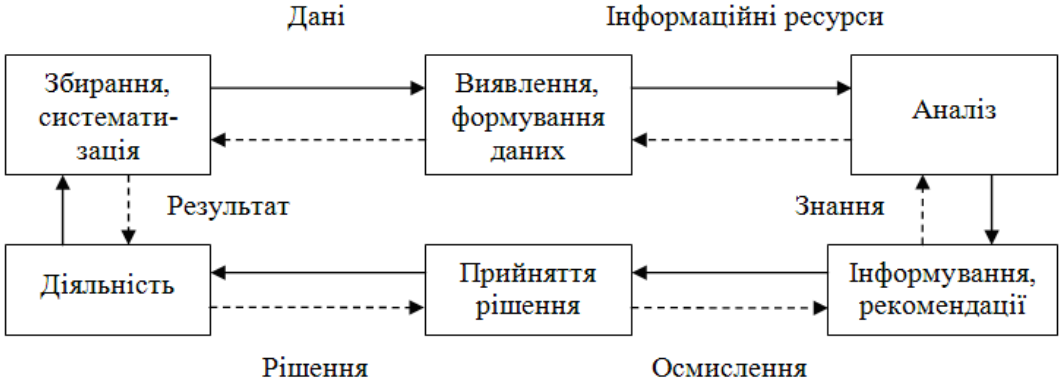


Рис. 1. Цикл перетворення даних у знання та рішення

Не всі цикли управління є чисто послідовними. Наприклад, у циклах Бойда є взаємодія несуміжних процесів циклу. При цьому ніде не враховується зворотний вплив суміжних процесів. Вдосконалення моделі полягає у тому, що в математичній моделі передбачається двостороння взаємодія між суміжними процесами. Генеровані процесом елементи інформації, знання чи рішення можуть повертатись до попереднього процесу для уточнення або доповнення. Ці «зворотні» взаємодії показані на рис. 1 пунктиром.

Математична модель циклічної системи управління пропонується у такому загальному вигляді наступного відображення.

$$\Phi(x,y,z,v,w)=\begin{cases} x_{n+1}=x_n-k_{xy}px_n^2+k_{yx}qy_n^2+x_{in} \\ y_{n+1}=y_n+k_{xy}px_n^2-\left(k_{yx}+k_{yz}\right)qy_n^2+k_{zy}rz_n^2 \\ \dots \\ w_{n+1}=w_n+k_{vw}sv_n^2-\left(k_{wv}+k_{out}\right)tw_n^2 \end{cases} \quad (1)$$

де x, y, …, w являються динамічними змінними; k_{ij}, p, q, r, s, ..., t є перехідні та, відповідно, розподільні коефіцієнти, які за Герегою мають чітке тлумачення у залежності від фізичної чи інформаційної природи системи; x_{in} – кількісна характеристика інформаційного вхідного потоку даних щодо середовища. При цьому, $\{k_{ij}\}$ и $\{p, q, r, s,..., t\} \in (0,1)$, $\{x, y, ..., w\} \in R$, $x_{in}= const \in R^+$.

У попередній роботі автора показано, що «наявність у системі двох груп коефіцієнтів (k_{ij} и p, q, r, s, ..., t) має конкретну фізичну інтерпретацію: коефіцієнти k_{ij} описують відносну величину редукції і консолідації інформації та задають долю інформаційного потоку, який переходить з одного етапу на сусідній. Частина інформаційного потоку повертається на попередній етап обробки для виправлення неточностей, врахування зауважень тощо. Коефіцієнти p, q, r, s ..., t описують розподіл елементів інформаційного потоку за їх видами. Перехід між етапами обробки визначається добутком коефіцієнтів обох груп [16]».

Аналіз моделі проводився при наступних умовах. На початку моделювання на всіх етапах обробки інформації руху нема і здійснюється включення вхідного потоку заданої інтенсивності. Для відображення рівнянь руху чисельно вирішувалась система рівнянь (1) при початкових умовах: x_0=0; y_0=0; ...; w_0=0. Приклад графіку рівнянь руху

у вигляді проекцій на площину 0_{yz} при певних значеннях коефіцієнтів системи рівнянь (1) [16], інтенсивності вхідного потоку x_{in} = 4,94 показано на рис. 2. Графік відтворює у часі значення змінної y_n другого рівняння системи (1).

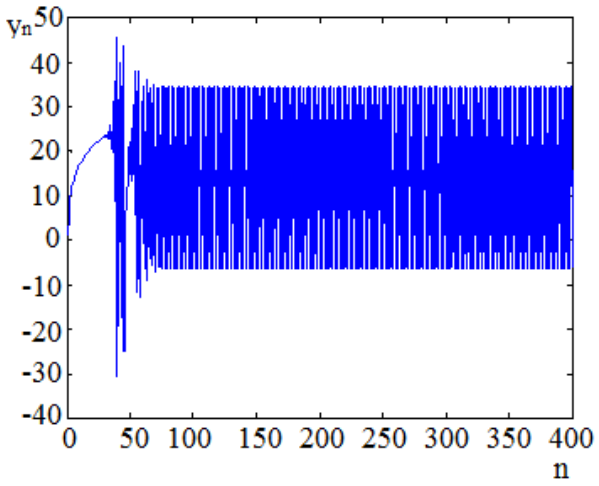


Рис. 2. Графік рівняння руху в проекції на площину 0_{xt}

На графіку виділяються три характерні ділянки: початкова, турбулентна і усталена (при заданих значеннях параметрів – квазіперіодична). Початкова ділянка відрізняється плавним зростанням величини інтенсивності потоку від нуля до максимального значення. Потік не може вирости миттєво і наростає плавно.

Турбулентна ділянка характеризується хаотичними коливаннями, викиди досягають великих значень і при збільшенні інтенсивності вхідного потоку прямують до нескінченності. Сингулярності у даній моделі, за певних параметрах виникають при $x_{in} > 4{,}94$. Причиною виникнення коливань і турбулентності являються зворотні зв'язки між етапами обробки інформації та перехідні процеси при включенні потоку. Наявність інерційних ефектів сприяє виникненню коливань.

Якщо сингулярність не досягається, то поступово хаотичні коливання затухають і замінюються стаціонарними квазіперіодичними коливаннями. В усталеній ділянці, в залежності від величин параметрів системи, відбуваються біфуркації подвоєння періоду Фейгенбаума. Періодичні коливання змінюються на квазіперіодичні, а потім – динамічним хаосом [17]. Коливання являються повздовжніми. З результатів моделювання витікає, що в стаціонарному режимі всі змінні коливаються з однаковою частотою і фазою, представляючи собою єдину хвилю. Турбулентну і стаціонарну ділянки наглядно видно на фазовому портреті системи у перехідному і стаціонарному режимах. На рис. 3 представлена проекція багатомірного фазового портрета на трьохмірний простір 0_{xyt}. Останнє дозволяє прослідкувати еволюцію траєкторії до атрактору.

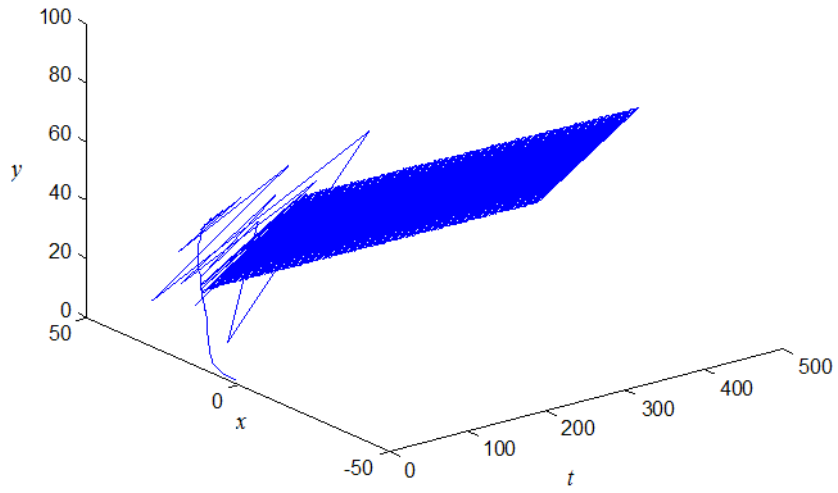


Рис. 3. Перехідний процес і атрактор системи (1)

У турбулентному режимі спостерігаються хаотичні траєкторії. У стаціонарному режимі маємо атрактор у вигляді тонкого сильно витягнутого еліпсоїдного тора.

Таким чином, турбулентність і сингулярність динамічних систем типу (1), для яких характерна наявність позитивних зворотних зв'язків, визначаються природними властивостями цих систем. Турбулентність виникає як при включенні вхідного інформаційного потоку, так і при його виключенні.

Тривіальний метод зменшення турбулентності у моделі динаміки узагальненого циклічного інформаційного процесу

Постає питання, чи можна у рамках даної моделі змінити якісний характер турбулентності або усунути саму турбулентність. Це можливо двома способами: за допомогою управління вхідним потоком у зоні перехідного процесу; та обмеженням інтенсивності вхідного потоку не досягаючи біфуркацій. Розглянемо перший спосіб.

У даному випадку ми доводимо саму можливість зменшення розмаху турбулентності у моделі динаміки циклічного інформаційного процесу. Задача полягає у тому, щоб безпечно провести систему через ділянку турбулентності, виключивши попадання траєкторії в окіл, де можливі сингулярності. Таку задачу можна вирішити синергетичними методами управління складними системами, що описані Колесниковим [18]. Проте у даній роботі розглянемо тривіальний метод. Із фізичних міркувань слідує, що причиною турбулентності може бути велика швидкість перехідного процесу у ті моменти, коли виникають умови для коливань. Моменти поблизу біфуркації являються такими умовами. По інерції траєкторії можуть вибігати на великі відхилення. Щоб зменшити ці явища, досить уповільнити перехідні процеси в районі біфуркацій. В моделі вхідний потік включається стрибком, що зумовлює велику початкову швидкість перехідного процесу. У найпростішому випадку розглянемо управління вхідним потоком за допомогою функції, вираженою у неперервній та дискретній формах:

$$U(t)=1-e^{-\lambda t}, t>0; U_n=1-e^{-\lambda n}, n>0, \qquad (2)$$

де λ – управляючий параметр.

Змінюючи управляючий параметр, можна регулювати швидкість за рахунок тривалості перехідного процесу. При цьому, перше рівняння системи (1) набуває такого вигляду

$$x_{n+1} = x_n - k_{xy} p x_n^2 + k_{yx} q y_n^2 + x_{in}\left(1 - e^{-\lambda n}\right), \qquad (3)$$

На рис. 4 показана часова діаграма змінної $y(t)$ при експоненціальному управлінні вхідним потоком згідно з виразом (3) і величиною $\lambda = 0{,}003$.

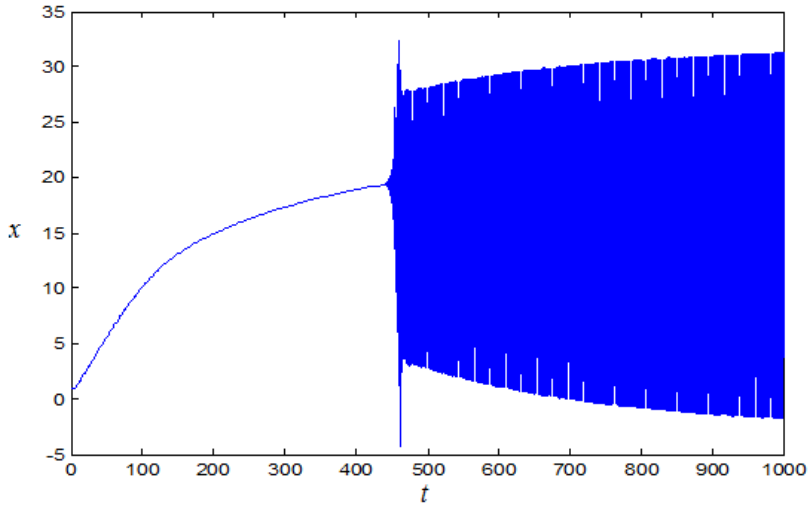


Рис. 4. Рівняння руху системи (1) при експоненціальному управлінні вхідним потоком

Управління вхідним потоком, як і управління параметрами системи (1) не змінює якісний характер турбулентності, який визначається властивостями системи (1), але дозволяє зменшити величину викидів та сингулярності. Сингулярність є природною властивістю такого роду систем. Внутрішньо системними засобами повністю позбутись сингулярності не можливо. До того ж, практична реалізація такого управління здається не здійсненною. Мова йдеться про управління «усталеним розвитком» інформаційних технологій (ІТ) шляхом уповільнення його початкової прискореної стадії, яка згідно із Законом Мура, ще не закінчилась. Уповільнення усталеного розвитку ІТ могло б дати можливість випереджаючого його розвиток засобів забезпечення кібербезпеки.

Тому є сенс звернутись до другого способу зменшення інтенсивності вхідного потоку позасистемними засобами. Позасистемні засоби мають впливати на параметри вхідного потоку утримуючи його в рамках до біфуркаційного (до турбулентного) режиму роботи системи (1).

Логіко-лінгвістична модель позасистемного впливу на динаміку узагальненого циклічного інформаційного процесу

Розглянемо логіко-лінгвістичну модель гіперболічного зростання кількості інцидентів КБ. Причинами гіперболічного зростання кількості інцидентів КБ на сучасному етапі являється зростання степені вразливості інформації та відповідних систем і ресурсів. Це пояснюється комплексом основних факторів. З одного боку, бурхливо розвиваються інформаційні технології, комунікаційні мережі, швидкими темпами зростають валові обсяги інформації в глобальних і місцевих інформаційних мережах, а також пропускна здатність інформаційно-комунікаційних мереж. Це різко розширює поле деструктивної діяльності. З іншого боку, «відбувається зосередження у єдиних базах даних великих обсягів інформації різного призначення, розвиток систем колективного користування, що приводить до розширення кола користувачів, які мають до обчислювальним ресурсам і даних, широке впровадження режимів розділення часу і реального часу, висока степінь автоматизації обміну інформації між ЕОТ [13]». Крім того, на зростання кількості інцидентів КБ впливають розвиток технологій кібератак,

недостатність ресурсів, що виділяються на КБ, легкість і малі витрати реалізації атак, не досконаліть задіяних засобів і заходів забезпечення КБ. Недостатність задіяних засобів і заходів забезпечення КБ мають внутрішньо та зовнішньо системні причини і фактори. До внутрішньо системних причин відносяться:

- поки що відсутні розробки превентивних методів забезпечення КБ, які мають протистояти всім загрозам, що виникли і що можуть виникнути у майбутньому;
- не розроблені операційні системи, що мали б високий стандартний рівень інформаційної захищеності;
- комунікаційні мережі залишаються не довіреною ланкою інформаційно-комунікаційних систем;
- є певне об'єктивне протиріччя між багатофункціональністю, масштабованістю, гнучкістю інформаційних систем та їх захищеністю. Засоби захисту знижують продуктивність систем, зменшують зручність їх використання. Є широкий діапазон у виборі величини витрат на захист: від захисту будь-якою ціною, навіть ціною людського життя; до оптимального відношення між витратами і можливим ризиком.

У череді не вирішуваних проблем КБ є такі:

- проблема керівника. Керівник відповідає за стан безпеки своєї організації, установи, підприємства. Але керівник організації не має права суміщати свою посаду із посадою керівника служби безпеки, Це часто порушується, особливо, у невеликих фірмах, організаціях, підприємствах;
- проблема системного адміністратора. Не можливо при розмежуванні прав доступу суттєво обмежити права доступу системного адміністратора до системи. Інакше він не зможе повністю відповідати за правильну роботу комп'ютерної системи. Необхідно удосконалювати підбір кадрів, мотивації і методи контролю;
- проблема головного криптографа. Цю проблему іноді формулюють так: «Головний криптограф ні за яких умов не повинен пересікати лінію фронту». У будь-якій системі захисту є частина ядра захисту чи персоналу, якому доводиться довіряти безумовно, не маючи можливості її абсолютного контролю. Звідси неможливість досягнення абсолютного захисту, абсолютної безпеки;
- соціально-психологічна проблема. Знаходячись на перехідному періоді переходу від індустріального суспільства до високотехнологічного суспільства ми маємо ситуацію відставання соціально-психологічного розвитку від високих темпів технологічного розвитку, а також посилення «цифрової нерівності». Члени суспільства з «індустріальною» психологією і менталітетом, опинившись у високотехнологічному інтелектуальному середовищі повільно адаптуються до його вимог і умов існування. Звідси походить девіантна, з точки зору нового суспільства, поведінка як мас, так і еліти. В результаті ті прошарки суспільства, з якого рекрутуються хакери та інші зловмисники, часто не усвідомлюють свої дії як злочинні;
- стратегічна проблема. Стратегії КБ і військові оборонні стратегії все більше стають схожими. На сьогодні сфера КБ, по її значимості для стану та розвитку людства і особливостях ситуації, що склалася у сучасному світі, в значній мірі можна віднести до військової сфери. Стратегія КБ базується на інтелекті та психології й пов'язана з усіма проблемами впливу одного розуму на інший. Сфера КБ вимагає застосування нешаблонних і ефективних управлінських рішень. В програми навчання менеджменту включається вивчення військової стратегії. Ймовірно, що у віддаленому майбутньому, буде комплементація політичних, ділових та етичних стандартів поведінки і ера інформаційних та корпоративних воєн відійде у минуле, тоді будуть створені умови для чесного законного застосування принципів і методик конкуренції та КБ;
- поки що має місце різне відношення до кіберзлокинців і кіберпорушників на територіях різних країн. З позицій місця, на яке направлена кібератака, кіберпорушник є злочинцем. З позицій місця, з якого кібератака здійснюється, кіберпорушник може

бути героєм. Інакше кажучи, поки відсутній єдиний міжнародний підхід до проблеми відповідальності за порушення КБ;

- нерозуміння керівництвом, користувачами і пересічним громадянинм важливості дотримання заходів КБ;
- не розвиненість правових і юридичних норм, невідповідність цих норм новим умовам функціонування постіндустріального високотехнологічного суспільства, та елементарна комп'ютерна неграмотність персоналу правоохоронних органів.

Мають також місце наступні тенденції розвитку сфери безпеки, які заслуговують підвищеної уваги. Це тенденції інтеграції та конвергенції різних видів безпеки в межах одного об'єкта: інформаційної, фізичної та економічної безпеки, охорони та відео спостереження; кібернетичної та національної безпеки й енергетичної та економічної безпеки. Переваги конвергенції та уніфікації практично доведені в багатьох сферах. Важливо вияснити умови, за яких можлива конвергенція в сфері безпеки.

«Наприклад, в сфері телекомунікації вона стала можлива за таких умов: цифровізація і наступна комп'ютеризація телекомунікаційних систем передачі сигналів різної природи (телеграфних, телефонних, телевізійних тощо); ієрархічна блочно-модульна архітектура систем на базі семирівневої моделі взаємодії систем, яка дозволила легко замінювати та удосконалювати будь-які модулі незалежно від інших; вирішальна умова, універсальний пакетний спосіб передачі і розподілу сигналів; винайдення функціонально повної системи функціональних елементів (функцій), із яких можна будувати функціональні схеми будь-якої складності [19]».

«У сфері безпеки друга та третя умови виконується легко. Перша умова набирає широти свого впровадження – розповсюджуються цифрові камери відео спостереження, роботизація у виробничій, енергетичній, побутовій сферах, інтелектуалізація управління, автоматичне розпізнавання образів та аналізу критичних ситуацій, тощо. Що стосується четвертої умови, тут ще потрібні теоретичні і практичні дослідження. Одна з ідей, яка може привести до замкнутої функціонально повної системи елементів безпеки, це впровадження техніки (технології) визначення ідентичності [19]».

Ще одна тенденція полягає в усвідомленні соціальної природи КБ. Є «взаємозалежність інформації та безпеки як стійкості та соціальної упорядкованості, безпеки суб'єкта в умовах наростання інтенсивності інформаційних потоків та особливостей соціальних практик забезпечення інформаційної безпеки; ролі кіберпростору у забезпеченні безпеки суб'єкта та аналізом основних груп загроз в Інтернеті [20]».

Сукупність розглянутих проблем та причин недостатності засовів забезпечення КБ дозволяє дійти до висновку, що на даному етапі суттєве значення мають позасистемні, зовнішні засоби забезпечення КБ. Враховуючи соціальну природу КБ, може бути ефективним розвиток соціальних аспектів теорії і технології КБ, підкріплений поглибленням інтеграції видів безпеки та організаційними й технічними заходами контролю за допомогою категорії й технологій визначення ідентичності.

Категорія технологій визначення ідентичності та управління визначенням ідентичності

Дана категорія ІБ введена Рекомендаціями МСЕ X.1250 – X.1279, Y.2720 – Y.2739 і пропонується автором для тотального впровадження в телекомунікаційних мережах України та кіберпросторі. Суть застосування технології викладена автором в [21].

«У мережному середовищі менеджмент визначення ідентичності (MBI – identify management) має забезпечувати можливості, які забезпечують гарантування безпечного обміну інформацією між об'єктами. Обмін інформацією засновується на розробленій

політиці та довірі, що встановлюється між цими об'єктами у середовищі з участю багатьох постачальників послуг. МВІ надає можливості захисту конфіденційності інформації об'єктів та забезпечує, щоб у телекомунікаціях розповсюджувалась лише авторизована інформація. Ідентичність – це інформація щодо об'єкта, якої досить для ідентифікації цього об'єкта у тому чи іншому контексті. Менеджмент визначенням ідентичності – МВІ – це набір функцій та можливостей (наприклад, адміністрування, управління та технічне обслуговування, виявлення, обмін повідомленнями, співставлення та ув'язування, забезпечення реалізації політики, автентифікація та затвердження), які використовуються для: гарантування інформації, що підтверджує ідентичність (наприклад, ідентифікаторів, реєстраційних даних, атрибутів); гарантування ідентичності об'єкта; забезпечення комерційних застосувань та застосувань безпеки [21]».

Багато сучасних інформаційних послуг, таких як електронна торгівля, електронній уряд, вимагають від телекомунікаційного середовища посиленої спостережності. Необхідне забезпечення визначення ідентичності всіх об'єктів та їх інформаційних потоків, на всіх рівнях та на всіх компонентах телекомунікаційної мережі при максимальному сприянні вільному, але контрольованому обертанні інформації. Поряд з іншими механізмами захисту, міжмережними екранами, системами виявлення вторгнень, захистом від вірусів, МВІ відіграє важливу роль у захисті інфраструктури, послуг та застосування телекомунікацій від кіберзлочинності, таких як шахрайство та крадіжка даних ідентичності. Трансакції у телекомунікаціях будуть захищеними та надійними.

Корисним ефектом визначення ідентичності є те, що вона частково відтворює властивості безпосередніх контактів між людьми. Люди безпосередньо сприймають (за допомогою усіх органів почуттів) один одного і мають можливість пізнавати фізичні, психологічні та індивідуальні особливості, притаманні кожній стороні. Співрозмовники у процесі контактів мають змогу скласти більш-менш об'єктивне враження про те, що становить собою партнер по спілкуванню, проникнути в його внутрішній світ, зрозуміти мотиви поведінки, звички, оцінити ставлення до фактів дійсності. Бажано, щоб телекомунікації надавали хоча б частину цих можливостей.

З теоретичної точки зору, технологія визначення ідентичності є елементом функціонально повного набору технологій КБ. У сфері КБ принцип функціональної повноти повинен поєднуватись із принципом безперервності захисту (принципом «кругової оборони»). Захищеність об'єкта визначається рівнем захищеності найслабшої ланки. Системи контролю доступу, як правило, є лише на вході у систему, або при доступах до ресурсу і не контролюють подальші дії суб'єкта. Технологія визначення ідентичності застосовується для кожної транзакції, замикаючи функціональну повноту технологій захисту. А у розподілених системах КБ технологія визначення ідентичності є не замінимою. Універсальна техніка визначення ідентичності значно полегшує вирішення проблем КБ. У повсякденному житті є стійка тенденція до зменшення анонімності. Повсюдно встановлюється камери спостереження, вживлюються чіпи для автоматичної ідентифікації тощо. Заборона анонімності не означає обмеження нашої свободи. Ми діємо там, де нам потрібно та дозволено і робимо те законне, що є нашим інтересом. Але робимо це відкрито, так як це роблять інші люди.

Висновки

Проведене математичного моделювання перехідних процесів забезпечення КБ показало, що в них можуть виникати стаціонарні квазіперіодичні коливання, біфуркації, а в перехідний період можливі турбулентність і сингулярність. Запропоновано метод управління перехідним процесом, який підвищує стійкість інформаційної системи, знижує ризик впливу сингулярностей і в середньому вдвічі

знижує величину викидів у зоні турбулентності. Отримано висновок, щодо необхідності застосування позасистемних заходів захисту. Логіко-лінгвістична модель перехідних процесів забезпечення КБ дала можливість виробити позасистемні засоби захисту шляхом застосування технік і технологій, які замикають систему захисту до функціонально повної. Доведена ефективність категорії і технології визначення ідентичності. Напрямок подальшої роботи полягає у виконанні повної програми досліджень нелінійних турбулентних властивостей системи забезпечення КБ.

Список літератури

1. Бурячок, В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В.Л. Бурячок, В.Б. Толубко, В. О. Хорошко, С. В. Толюпа за заг. ред. д-ра техн. наук, професора В.Б. Толубка. – К.: ДУТ, 2015. – 288 с.
2. Обзор кибербезопасности / Рекомендация МСЭ-Т X.1205 // Безопасность электросвязи. – Женева: 2008. – 56 с.
3. Котенко, И.В. Аналитические модели распространения сетевых червей / И.В. Котенко, В.В. Воронцов // Труды СПИИРАН. Вып. 4. – СПб.: Наука. – 2007. – С. 208-224.
4. Захарченко, А.А. Черводинамика: причины и следствия / А.А. Захарченко // Защита информации. Конфидент. – 2004. – № 2. – С. 50–55.
5. Кононович, І. В. Динаміка кількості інцидентів інформаційної безпеки / І. В. Кононович // Інформатика та математичні методи в моделюванні. – 2014. – Т. 3. – № 3. – С. 35-43.
6. Кононович, В. Г. Вплив затримки прийняття заходів із захисту інформації на ризики інформаційної безпеки / В. Г. Кононович, І. В. Кононович, Ю.В. Копитін, С.В. Стайкуца // Безпека інформації. – Київ: НАУ. – 2014. – Том 20, № 1. – С. 83 - 91.
7. The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world. – November 2011. – 43 p.
8. Кононович, І. В. Інформаційні революції. Ієрархічна класифікація інформації / І.В. Кононович // Цифрові технології: Збірник / Кол. Авт: – Вип. 8. Одес. нац. академія зв'язку. – Одеса, 2010. – С. 88 - 96.
9. ДСТУ ISO 9001:2009 Системи менеджменту якості. Вимоги [Аналог ISO 9001:2008]. – 32 с.
10. Ивлев, А.А. Основы теории Джона Бойда. Принципы, применение и реализация / А.А. Ивлев [Электронный ресурс]. – 2009. – 21 с. Режим доступа: http://www.milresource.ru/Boyd.html.
11. Кононович, В.Г. Технічна експлуатація систем захисту інформації. Частина 4 – Інформаційна безпека комунікаційних мереж та. Реагування на атаки: навч. посібник / В.Г. Кононович, С.В. Гладиш; За ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2009. – 208 с.
12. Милованов, В.П. Неравновесные социально-экономические системы: синергетика и самоорганизация // В.П. Милованов. – М.: Эдиториал УРСС, 2001. – 264 с.
13. Кузнецов, Н.А. Информационная безопасность системы организационного управления. Теоретические основы : в 2 т. / Н.А. Кузнецов, В.В. Кульба, Е.А. Микрин и др.; [отв. ред. Н.А. Кузнецов, В.В. Кульба] ; Ин-т проблем передачи информ. РАН. – М.: Наука, 2006. – Т.1 – 495 с.
14. Бондаренко, М.Ф. Підготовка професіоналів у галузі інформації для державної служби України / М.Ф. Бондаренко, С.І. Маторін, К.А. Соловйова // Навчання державних службовців [Електронний ресурс]. – 7 с. Режим доступу: http://nadoest.com/navchannya-derjavnih-slujbovciv-m-bondarenko.
15. Кононович, В.Г. Нелінійні моделі циклічного управління кібербезпекою / В.Г. Кононович, І.В. Кононович, А.І. Міхова // «ІНФОРМАЦІЙНІ УПРАВЛЯЮЧІ СИСТЕМИ ТА ТЕХНОЛОГІЇ» (ІУСТ – ОДЕСА – 2015) [Електронний ресурс]. Матеріали Міжнародної науково-практичної конференції, 22 – 24 вересня 2015 р., Одеса / відп. ред. В.В. Вичужанін. –, 2015. (– 336 .с). – С. 171 – 173.
16. Герега, О.М. Гіпотеза і формальна модель сингулярної динаміки інцидентів кібернетичної безпеки / О.М. Герега, С.О. Гнатюк, В.Г. Кононович, І.В Кононович // Інформатика та математичні методи в моделюванні. – Одеса, 2016. – Т. 6. – № 1. – С. 35-43.
17. Табор, М. Хаос и интегрируемость в нелинейных системах / М. Табор // М.: Эдиториал УРСС. – 2001. – 320 с.
18. Колесников, А.А. Синергетического управления сложными системами: Теория системного синтеза / А.А. Колесников. – М.: КомКнига, 2006. – 240 с.

19. Кононович, В.Г. Метастратегія інформації та управління захистом інформації / В.Г. Кононович // Перспективні напрями захисту інформації : матеріали першої всеукраїнської наук.-пр. конф. м. Одеса 7 – 9 вересня 2015 р. – Одеса: ОНАЗ, 2015. – С. 49-53.
20. Владимирова, Т.В. Социальная природа информационной безопасности [Текст] : монография / Т.В. Владимирова // АНО содействия развитию соврем. отечеств. науки. Изд. Дом «Науч. обозрение». – 2014. – 239 с.
21. Кононович, В.Г. Визначення ідентичності об'єктів у системі соціальної та інформаційної безпеки / В. Г. Кононович, І. В. Кононович, С.В. Стайкуца, О.О. Цвілій // Сучасний захист інформації. – 2015. – № 1. – С. 19-27.

МЕТОДЫ УМЕНЬШЕНИЯ ТУРБУЛЕНТНЫХ И СИНГУЛЯРНЫХ ЯВЛЕНИЙ В МОДЕЛИ ДИНАМИКИ ИНЦИДЕНТОВ КИБЕРБЕЗОПАСНОСТИ

И.В. Кононович

Одесская национальная академия пищевых технологий,
ул. Канатная, 112, м. Одесса, 65039, Украина; e-mail: kononovich@mail.ru

Рассматриваются пути решения проблемы гиперболичного роста количества инцидентов кибербезопасности. Процесс роста количества инцидентов кибербезопасности представлен в виде переходного процесса, который описывается математической моделью циклической многоэтапной обработки информационных потоков с положительными обратными связями. В модели могут возникать регулярные, квазипериодические колебания и динамический хаос. В переходный период возможны турбулентность и сингулярность. Предложен метод управления переходным процессом, который повышает стойкость системы, снижает риск возникновения сингулярности и уменьшает, в среднем вдвое, выбросы в зоне турбулентности. Как дополнение к математической модели, представлена логико-лингвистическая модель процессов роста количества инцидентов. Поясняются внутренне внешне системные причины недостаточности использованных сегодня средств обеспечения кибербезопасности. Для кардинального решения проблемы инцидентов кибербезопасности предложены внесистемные меры, которые обеспечивают функциональную полноту средств контроля доступов. Одним из таких средств является технология определения идентичности.
Ключевые слова: кибернетическая безопасность, модель динамической системы, турбулентность, сингулярность, управление безопасностью, социальная природа кибербезопасности.

METHOD TO REDUCE TURBULENCE AND SINGULAR EFFECTS IN DYNAMICS MODELS INCIDENTS CIBERSECURITY

I.V. Kononovich

Odessa National Academy of Food Technologies,
112, Kanatnaja str, Odessa, 65039, Ukraine; e-mail: kononovich@mail.ru

Discusses ways solving the problem of hyperbolic growth in the number of incidents of cybersecurity. The process of growth in the number of incidents of cyber security presented in the form of the transition process, which is described by a mathematical model of a multi-stage cyclic processing of information flows from the positive feedback. In the model, there may be regular, quasi-periodic oscillations and dynamic chaos. During the transition period may be turbulence and singularity. A method for management transition process, which increases the stability of the system, reduces the risk of singularity and reduces, on average twice the emissions in the zone of turbulence. As an addition to the mathematical model presented logical-linguistic model of growth the number of incidents. Describes the internal and external system causes of insufficiency of cybersecurity tools. For a radical solution to the problem of cybersecurity incidents out of system proposed measures, which provide functional completeness access controls. One such tool is the technology determining the identity.
Keywords: cyber security model dynamic systems, turbulence, singularity, bifurcation, safety management, social nature of cybersecurity.

УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 6 (2016), No. 2, pp. 127-132

INCREASE THE CLARITY OF DIGITAL IMAGE

V. Zorilo, A. Matveeva, O. Lebedeva, M. Kozina

Odessa national polytechnic university,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: Jyzel@ramble.ru

Photos are an integral and certainly an important part of our lives. Often we are faced with a need to increase the clarity of digital image, for example, solving pattern recognition problems, or for other reasons. Methods of increasing the clarity of digital images are very diverse, each has its own range of applicability. However, there may be often artifacts by processing of digital image. The aim of this paper is to increase clarity of digital image with the possibility of avoiding artifacts. To achieve this aim the researchers used digital image processing algorithms, based on using different convolution matrix types. There are shown in typical images with increasing clarity of digital image what advantages is the use of combinations of these algorithms in a specific sequence. A comparative analysis of the impact of different filters to increase the clarity of digital images was conducted and gives recommendations by using them.

Keywords: digital image, clarity image, matrix of filter, the convolution, image processing

Introduction

Photos taken by most digital cameras, are not sufficiently clear (may have low sharpness). This happens even with the images created by high-end cameras with high resolution display. Increased clarity - a highlight and underline the contours of objects, lines and borders to make them more distinct and noticeable. Improve the clarity of digital images - is to make sharper the edges of objects.

Clarity - is one of the main parameters that characterize the quality of the image and shows the completeness playing small objects on it. Clarity also characterizes the degree of blurring boundaries around image objects [1]. Setting clarity (sharpness) is getting by increasing the contrast on the image contours to improve detail.

However, the application field of sharpness filters is to avoid redundancy. Excessive sharpening create a very "rough" texture of the image, and "torn" outlines and shadows. That may be artifacts of sharpness field [2]. Artifacts are a wide range of micro-defects on the image. Noise can also be attributed to artifacts. Usually artifacts appear in tricky situations or with incorrect camera settings. Number artifacts significantly increases with the wrong or excessive computer processing.

The aim of this scientific work is to improve clarity of digital images with the ability to avoid artifacts.

Main part

Modern graphics editors provide a wide range of filters to increase the clarity (sharpness) of digital images. But sometimes increase the clarity can cause to artifacts.

The basis of most known methods of digital images sharpening is the use of spatial filters. The core or matrix filter – a coefficient matrix of 3 × 3, 5 × 5, 7 × 7, etc., which identified certain function [3]. The core filter used for the image using convolution operations. Convolution – a linear combination of elements values of the image (1).

$$\begin{bmatrix} p_1 & p_2 & p_3 \\ p_4 & p_5 & p_6 \\ p_7 & p_8 & p_9 \end{bmatrix} \begin{bmatrix} k_1 & k_2 & k_3 \\ k_4 & k_5 & k_6 \\ k_7 & k_8 & k_9 \end{bmatrix} = \sum_{i=1}^{9} p_i k_i = p_5^{'} \quad (1)$$

p_i – elements of the image area; k_i – core filter; $p_5^{'}$ – new pixel value.

Most use a matrix of 3 × 3, allowing for more image processing [2]. During brightness filtration pixels of the original image are processed one after other and is determined by the color of the pixel through its values and pixel values that surround it. The core filter shows which value extends to each of the surrounding pixels and affect to the final result. [3] Filtration filter made moving windows on the image.

The core filter to increase the clarity formed as follows: the central rate should be greater than 1, and surround it with not positive numbers whose sum in absolute is less than the central one, for example: next we will use in our experiments the following core filter (2), as the experiments have shown that it works very well with images made by shallow depth of represented space field.

$$\begin{bmatrix} -1 & -1 & -1 \\ -1 & 9 & -1 \\ -1 & -1 & -1 \end{bmatrix}, \quad (2)$$

Experimentally, it was found that increase the clarity leads to many artifacts when the image is made of shallow depth of represented space field (Fig. 1).

Fig. 1. Example of images with shallow depth of represented space field

These images have as clear and blurred areas. If the object on the image is sharp (is in focus), the increase of its sharp causes to artifacts on it. At the same time, the blurred areas of the digital image are more clearer. That's why it would be advisable to slightly reduce the sharpness of your own digital image that is to say blur it.

The assumption that the previous blurred digital image (when the clear objects will become more blurred) further sharpening filter application will give the best results without artifacts, was confirmed in experiments, a typical example of which is shown on Fig. 2.

а

б

в

Fig. 2. Application of increase the clarity algorithm: a – original image; b – without preliminary blurring; c – after blurring

Fig. 2 shows an example of using the increase the clarity filter without preliminary blurring. As we can see in the area, which was clear, there were artifacts. Blurry area became clearer. Fig. 2,c shows the result of using the increase the clarity filter to image that was previously blurred.

Even the subjective ranking shows that the area that was in focus, almost no sharpness artifacts, and the area that is out of focus, has also become clearer. However, conduct a quantitative assessment of improved clarity of digital images.

Reliability perceptions will evaluate the classic way with a typical signal to noise ratio (PSNR), as measured by a scale in decibels (dB). The easiest way to define it by the standard deviation (SCR or MSE), for two monochrome or color images I and K size $m \times n$, one of which is original and the processed one, calculated using the formula:

$$MSE = \frac{2}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} | I(i, j) - K(i, j) |^2$$

PSNR is defined as:

$$PSNR = 10 \log_{10} (\frac{MAX_I^2}{MSE}) = 20 \log_{10} (\frac{MAX_1}{\sqrt{MSE}})$$

MAX_I – a maximum value that is accepted image pixel; MSE – standard deviation; I, K – monochrome image; i, j – pixels.

The experiment we will use a variety of matrix filters (3) - (5) for blur digital image and define the use of which matrix is the most successful in terms of increasing PSNR compared

with the case where the image before increase the clarity not blurred. Matrix filters to blur images taken with a digital resource [2].

$$\frac{1}{8}\times\begin{bmatrix}0 & 1 & 0\\ 1 & 4 & 1\\ 0 & 1 & 0\end{bmatrix} \quad (3)$$

$$\begin{bmatrix}1/9 & 1/9 & 1/9\\ 1/9 & 1/9 & 1/9\\ 1/9 & 1/9 & 1/9\end{bmatrix} \quad (4)$$

$$\frac{1}{6}\times\begin{bmatrix}0.5 & 0.75 & 0.5\\ 0.75 & 1 & 0.75\\ 0.5 & 0.75 & 0.5\end{bmatrix} \quad (5)$$

The experiment is as follows. We have the original image I_1 and get the following image:

- image $I_2 - I_1$ processed by increase the clarity filter (2);
- image $I_3 - I_1$ blurred by Gauss window of 5 × 5 filter and blur radius 2 with further application of increase the clarity filter (2);
- image $I_4 - I_1$ blurred using a filter matrix (3) with further application of increase the clarity filter (2);
- image $I_5 - I_1$ blurred using a filter matrix of 5 × 5 (1/25 × E, where E - the identity matrix) with further application of increase the clarity filter (2);
- image $I_6 - I_1$ blurred using a filter matrix (4) of 3 × 3 with further application of increase the clarity filter (2);
- image $I_7 - I_1$ blurred using a filter matrix (5) of 3×3 with further application of increase the clarity filter (2);.

Compare the original image with each of the received tested images are presented in Table 1.

Table 1.

Result of comparison definition digital images after processing

Pairs of images	PSNR, dB	Improved results compared to PSNR(I1,I2), %
(I1, I2)	19.6470	—
(I1, I3)	9.0490	54%
(I1, I4)	37.0109	88%
(I1, I5)	30.7402	56%
(I1, I6)	34.2050	74%
(I1, I7)	34.6821	77%

As we can see from the table 1, the best results were obtained with matrix filter to blur, represented by (3).

Based on the experiments, the authors of this scientific work give next recommendations. If the aim of image processing is to improve clarity of details that are out of focus, and does not matter possibility of artifacts to clear objects, it is best not to use the previous blur, so not clear elements become more expressive. But if you want all the image details become clearer, and they were no visible artifacts on it, it should be used blur with the filter above to the digital image before increase its sharpness.

Conclusions

It was proposed in this paper, the way of increase of clarity the digital images, which avoids the sharpness artifacts by blurring previous processed file. It was conducted a comparative analysis of the impact of different filters for blur to improve the clarity of digital images and recommendations to use them.

Further work the authors focused on a detailed study of the process sharpening a digital image. The results will be used to create a method of increase the clarity of digital image.

References

1. Четкость изображения [Электронный ресурс] // Режим доступу: http://foto-kan.ru/chetkost-izobrazheniya.html (Дата звернення 27.05.2016).
2. Матричные фильтры обработки изображений [Электронный ресурс]// Режим доступу: https://habrahabr.ru/post/142818/ (Дата звернення 27.05.2016).
3. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа. – М. : Техносфера, 2006. – 1070 с.
4. Фильтрация изображений методом свертки [Электронный ресурс]// Режим доступу: https://habrahabr.ru/post/62738/ (Дата звернення 27.05.2016).

ПІДВИЩЕННЯ ЧІТКОСТІ ЦИФРОВОГО ЗОБРАЖЕННЯ

В.В. Зоріло, А.С. Матвєєва, О.Ю. Лебедєва, М.О. Козіна

Одеський національний політехнічний університет,
Просп. Шевченко, 1, Одеса, 65044, Україна; e-mail: Jyzel@ramble.ru

Фотографії є невід'ємною і, безумовно, важливою складовою нашого життя. Часто ми стикаємось з необхідністю підвищити чіткість цифрового зображення, наприклад, під час вирішення задач розпізнавання образів або з інших причин. Методи підвищення чіткості цифрових зображень дуже різноманітні, кожен має свою область застосування. Проте часто при обробці цифрового зображення тим чи іншим методом можуть виникати артефакти. Метою даної роботи є підвищення чіткості цифрового зображення з урахуванням необхідності уникнення артефактів. Для досягнення даної мети в роботі застосовано алгоритми обробки цифрового зображення, засновані на використанні матриць згортки різних типів. На прикладі типових зображень показано, які переваги при підвищенні чіткості цифрового зображення дає використання комбінації цих алгоритмів у певній послідовності. Проведено порівняльний аналіз впливу різних фільтрів на покращення чіткості цифрового зображення та дано рекомендації щодо їх використання.

Ключові слова: цифрове зображення, чіткість зображення, матриця фільтра, згортка, обробка зображень.

ПОВЫШЕНИЕ ЧЕТКОСТИ ЦИФРОВОГО ИЗОБРАЖЕНИЯ

В.В. Зорило, А.С. Матвеева, Е.Ю. Лебедева, М.А. Козина

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: Jyzel@ramble.ru

Фотографии являются неотъемлемой и, безусловно, важной составляющей нашей жизни. Часто мы сталкиваемся с необходимостью повысить четкость цифрового изображения, например, при решении задач распознавания образов или по другим причинам. Методы повышения четкости цифровых изображений очень разнообразны, каждый имеет свою область применимости. Однако часто при обработке цифрового изображения тем или иным методом могут возникать артефакты. Целью данной работы является повышение четкости цифрового изображения с учетом необходимости избежать артефактов. Для достижения данной цели в работе использованы алгоритмы обработки цифрового изображения, основанные на использовании матриц свертки разных типов. На примере типичных изображений показано, какие преимущества при повышении четкости цифрового изображения дает использование комбинации этих алгоритмов в определенной последовательности. Проведен сравнительный анализ влияния различных фильтров на улучшение четкости цифрового изображения и даны рекомендации относительно их использования.

Ключевые слова: цифровое изображение, четкость изображения, матрица фильтра, свертка, обработка изображений.

УДК 004.732.629.5-52

Informatics and Mathematical Methods in Simulation
Vol. 6 (2016), No. 2, pp. 133-141

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСТАНЦИОННОЙ ОЦЕНКИ РИСКОВ СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ

Н.О. Шибаева, В.В. Вычужанин

Одесский национальный морской университет,
ул. Мечникова, 34, Одесса, 65404, Украина; e-mail: vint532@yandex.ru

Статья посвящена дистанционной диагностике технического состояния сложных технических систем, их взаимосвязанных, взаимодействующих подсистем и элементов по оценкам рисков. Проведен анализ используемых методов дистанционного мониторинга, диагностики сложных технических систем. Описан метод дистанционного мониторинга, диагностики, основывающийся на учете взаимосвязанности и взаимодействия подсистем сложных технических систем и их элементов, а также количественного и качественного информационно-энергетического взаимообмена. Применение разработанного метода и его информатизация позволяет оценить работоспособность сложной технической системы в различных условиях и режимах ее эксплуатации, а также прогнозировать состояние системы в аварийных экстремальных ситуациях и осуществлять последующую автоматизацию принятия решений.

Ключевые слова: сложная техническая система, информационно-энергетический взаимообмен, мониторинг, диагностика, прогнозирование

Введение

Своевременная и качественная диагностика, в том числе дистанционная, сложных технических систем (СТС) при их эксплуатации позволяет повысить надежность систем, а значит и эффективность их эксплуатации. Одним их важнейших показателей надежности СТС является оценка рисков систем. В работах [1-9] для обеспечения безопасности СТС рекомендуется пользоваться данными, полученными сочетанием качественных и количественных методов оценок рисков, что позволяет осуществить анализ рисков при использовании меньшего объема информации и затрат труда. Однако многообразие методов оценки рисков СТС базируется на инженерных, модельных, экспертных и других подходах, связанных со сложными и дорогостоящими расчетами, определяющими значения оценок рисков с точностью не выше первого порядка.

Проведенный анализ публикаций показал, что сегодня вопросом исследования дистанционного мониторинга и диагностики (ДМД) СТС уделяется существенное внимание. Однако авторы оценки рисков при ДМД СТС для автоматизации принятия решений не в полной мере используют комплексный подход, основанный на учете взаимосвязанности и взаимодействия подсистем СТС, а также количественного и качественного информационно-энергетического взаимообмена [10,11].

При оценках надежности СТС наиболее важным является учет влияния взаимосвязанных, взаимодействующих подсистем и их элементов на технические риски систем в целом. Поэтому для эффективной эксплуатации, прогнозирования и борьбы с аварийными ситуациями следует определять «вклад» каждой подсистемы и ее элементов на надежность СТС, оценивая технические риски с учетом взаимосвязанности и взаимодействия компонентов системы.

Учитывая специфику СТС, технологии передачи данных в них, задача повышения эффективности систем на стадии их эксплуатации путем оценки рисков при ДМД СТС актуальна.

Цель статьи и постановка задачи исследования

Целью статьи является информационное обеспечение дистанционного мониторинга и диагностирования технического состояния СТС для автоматизации принятия решений в аварийных ситуациях.

Задача исследования - оценки технических рисков СТС в аварийных ситуациях с учетом взаимосвязанности и взаимодействия их компонентов.

Основная часть

Для обеспечения надежности необходимо рассматривать СТС и их компоненты с учетом взаимосвязанности и взаимодействия, количественного и качественного информационно-энергетического взаимообмена. Такой подход позволяет оптимизировать время поиска возникшей неисправности в реальной аварийной ситуации и выявить взаимозависимость всех компонентов СТС от конкретного ее критичного элемента.

Определяющим фактором надежности СТС является наличие своевременной, полной и достоверной информации для оценки риска систем. Она может формироваться системой менеджмента качества проектирования и эксплуатации СТС в соответствии со стандартом ISO 9000 [12], предусматривающего мероприятия по обеспечению надежности СТС при условии развития коммуникаций и умения управления информацией. Своевременное и регулярное поступление информации о состоянии оборудования СТС позволяет обслуживающему персоналу отслеживать аварийные ситуации, выявлять причины отказов и вырабатывать меры, направленные на повышение надежности СТС.

Следует отметить, что известны СТС, устанавливаемые на судах, для которых привычные методы резервирования агрегатов, мониторинг технического состояния для повышения надежности СТС не всегда возможно реализовать из-за ограниченного судового пространства и высокой стоимости оборудования. Для таких систем актуальным является дистанционное определение наиболее уязвимых (критичных) агрегатов СТС в различных аварийных ситуациях эксплуатации систем.

Дистанционное диагностирование технического состояния СТС включают этапы [13].

1. Выявление взаимосвязанности и взаимодействия компонентов в иерархии и топологии СТС с учетом используемого ресурса ЭВИ (энергия, вещество, информация).
2. Построение и исследование когнитивной имитационной модели (КИМ) СТС.
3. Оценки ущербов и рисков СТС.

Задача дистанционного мониторинга и диагностики состояния СТС предусматривает распознавание его текущего состояния в условиях ограниченной информации и может быть представлена в виде составляющих рис. 1.

Для исследования модели системы ДМД и СТС среди множества существующих методов моделирования надежности выбрана относительно развитая технология когнитивного имитационного моделирования надежности, живучести, безопасности, эффективности и риска функционирования СТС [14-17], позволяющая реализовать формализованное с разной степенью описание оборудования, учитывающее эволюцию

технической системы во времени.

Рис. 1. Структура задачи технического мониторинга СТС

В рамках когнитивного подхода основой когнитивной модели является когнитивная карта, представленная в виде ориентированного графа, включающего в себя элементы СТС судна, представленные вершинами, и их взаимосвязи, представленные направленными дугами. В зависимости от уровня моделирования, когнитивная карта с разной точностью и достоверностью может отражать взаимодействие элементов системы в нескольких различных аспектах, в частности дуги могут рассматриваться как взаимовлияние объектов системы, либо как связь элементов по ресурсу («энергия» – «информация» – «вещество»).

В качестве объекта исследования СТС выбрана судовая энергетическая установка (СЭУ), представляющая собой либо функциональный комплекс подсистем, либо взаимосвязь этих комплексов. СЭУ является особо важным элементом энергетической установки судна и влияет на работоспособность всех ее остальных элементов. Поэтому функционирование СЭУ с позиций надежности необходимо рассматривать во взаимной связи со всеми ее элементами. Эксплуатационная готовность СЭУ имеет решающее значение для эффективного использования судна как транспортного средства. Следует отметить, что одной и той же эксплуатационной готовности можно достичь при разной величине затрат, поэтому необходимо нормировать величину показателей надежности. Решение такой задачи с помощью натурного эксперимента затруднительно. Единственно возможный на данном этапе путь ее решения – с помощью аналитических методов, а именно методом моделирования процесса функционирования СЭУ. Решая задачу аналитически, можно исключить заведомо нереальные варианты и, таким образом, снизить степень технического риска. Технический риск представляет собой комплексный показатель надежности элементов СТС, а именно комбинацию вероятностей возникновения опасностей определенного класса и ущербов от нежелательных событий из-за несовершенства, нарушения правил эксплуатации технических систем. Технические риски при КИМ определяются как произведение вероятности возникновения опасности и ущерба от пораженных компонентов СТС в соответствии с алгоритмом, приведенным на рис. 2. В качестве источника статистических значений вероятностей выхода из строя элементов СЭУ, используется база данных офшорных судовых компаний [18].

Агрегаты СТС СЭУ взаимодействуют между собой по межагрегатным связям – трубопроводам, линиям передачи энергии и информации. Для математического описания и оценок рисков СТС с учетом выявленной взаимосвязанности и взаимодействия их элементов используется КИМ, представленная в виде орграфа, в котором направленные дуги (ребра графа) выполняют функции межэлементных связей. Каждому агрегату СТС соответствует узел орграфа, каждой межэлементной связи – направленная дуга, направление которой совпадает с направлением передачи ЭВИ.

Основной задачей предлагаемого метода является оценка влияния состояния отдельного элемента на общую надежность СТС. Для оценки рисков элементов СТС введем коэффициенты рисков, численно выражающие степень рисков на интервале 0-1. Для значения коэффициента «0» состояние межэлементной связи не сказывается на надежности СТС, а для значения «1» надежность СТС определяется состоянием межэлементной связи.

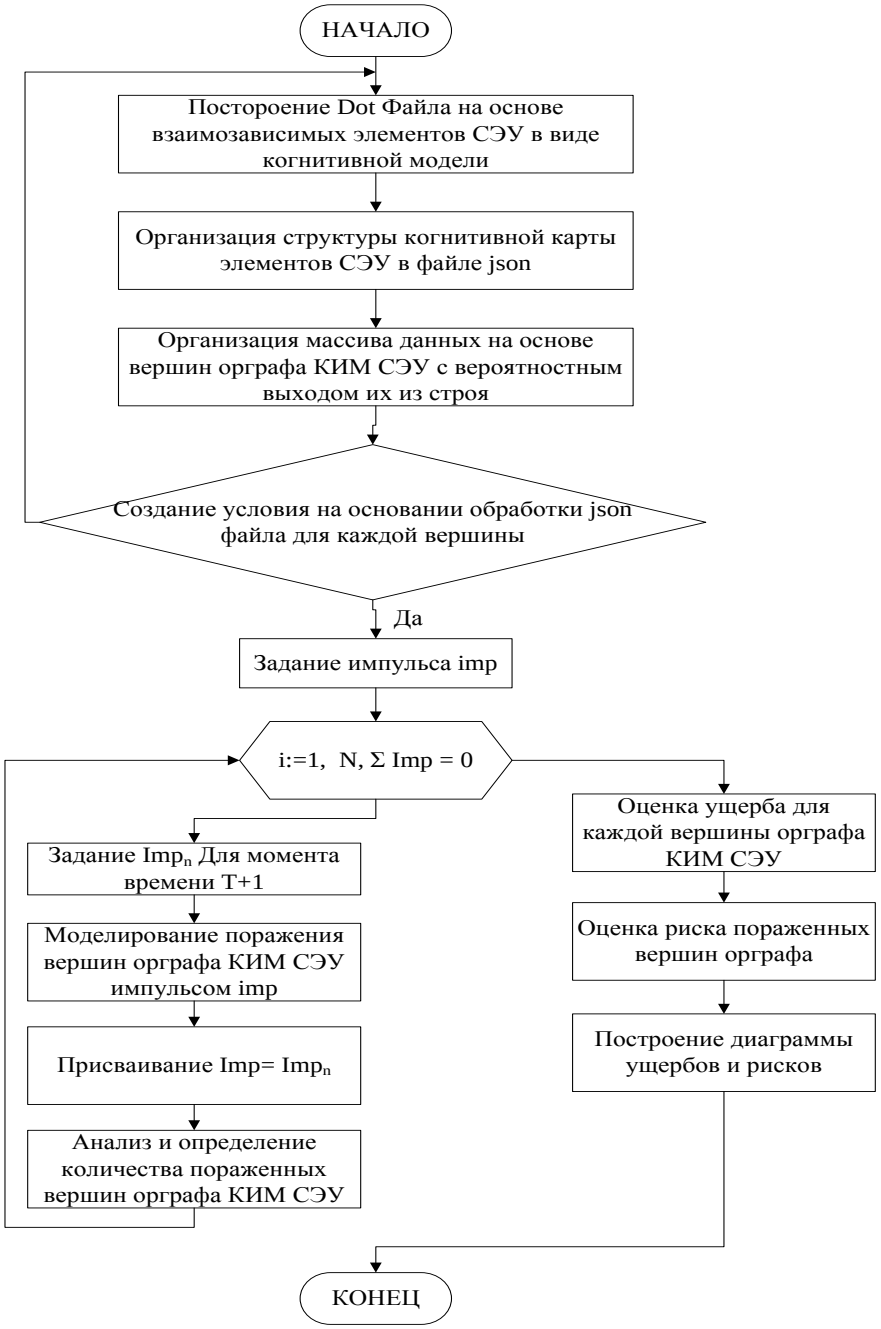


Рис. 2. Алгоритм реализации метода оценок ущерба и риска вершин орграфа КИМ СЭУ

Когнитивное имитационное моделирование выполняется путем воздействия на орграф модели имитационных моделирующих импульсов (ИМИ). Суть такого моделирования состоит в том, что в одной из вершин графа задается определенное изменение. Эта вершина актуализирует всю систему показателей, т.е. связанных с ней вершин, в большей или меньшей степени. Таких вершин может быть несколько, однако в данной методике рассмотрено воздействие только единичных импульсов. Проходя по вершинам и дугам орграфа, импульс изменяет их значения, изменяется сам. При оценке структурных угроз используется воздействие поражающего не изменяющегося МИ (ПМИ), распространяющегося по орграфу и модифицирующего состояние его отдельных узлов [19]

$$I(t) = (imp_{ij}(t)),\ i = 1,..., t = t_1,..., t_d$$

где $imp_{ij}(t)$ – набор значений модулей ПМИ, соответствующих направленным дугам орграфа; t – момент дискретного времени; t_1 – начальный момент дискретного времени; t_d – конечный момент дискретного времени.

ПМИ последовательно распространяется по орграфу, выводя из строя смежные узлы и дуги на каждом очередном шаге дискретного времени. Дуга и узел меняют свое значение с 1 («исправен») на 0 («не исправен»), а значения модулей вектора I(t) отражают прохождение ПМИ по узлам на каждый дискретный момент времени, вдоль направленных ребер графа. При распространении по системе импульс ослабляется в зависимости от весов дуг орграфа СТС. В рассматриваемом случае веса дуг принимают бинарные значения (0 либо 1) в зависимости от исправности дуги. С целью моделирования промежуточных состояний частичной исправности МС алгоритм ПМИ предусматривает использование широкого диапазона весов.

Исследуемая СЭУ при ДМД в виде КИМ, основанная на оценке рисков, состоит из функциональных элементов СЭУ и ДМД, где элементы подсистем СЭУ образуют вершины орграфа, а проводные элементы подсистемы выступают в качестве межэлементных связей и образуют ребра орграфа.

На рис. 3 приведен орграф СЭУ при ДМД, вершинами которого являются: ручное управление главным двигателем (РУГД); система сжатого воздуха (ССВ); котельная установка (КУ); судовая электростанция (СЭ); противопожарная система (ПС); аварийный привод ДРК (АП); главный двигатель (ГД); система дистанционно-автоматизированного управления (ДАУ) главного двигателя; система управления ДРК; передача мощности от главного двигателя к движителю (ПМ); система санитарной водоподготовки (ССВП); балластно-осушительная система (БОС); движительно-рулевой комплекс (ДРК). Кроме того на рис.3 приведены элементы вершины орграфа СДМ: ИУ – измерительное устройство контроля параметров СЭУ; КО – контроллер; С – сервер; АРМ – автоматизированное рабочее место; К и Д – кодер и декодер; ПП – приемо-передающее устройство; ППС – подвижная спутниковая связь; СТ – стационарная станция; ГР – грид- облако; Ш – шлюз; ЛС – локальная сеть.

С использованием программного продукта graphwiz, осуществляется построение и отображение графа. В файле json задаются параметры графа, такие как вершины и переходы между вершинами, и указываются веса вершин и ребер. При помощи автоматизированного пакетного файла, написанного на языке python, выполняется расчет ущербов, и результаты заносятся в файл с расширением .csv.

Орграф функционирования СЭУ и системы ДМД описывает их реальный состав. Связи вершин орграфа функционирования СЭУ с позиций обеспечения системы ДМД представлены матрицей функционирования на рис. 4.

На рис. 5 приведены зависимости ущерба (Y) наносимого СЭУ, вероятности (P) того, что ущерб нанесет весомые повреждения СЭУ при ДМД и риска (R) возникновения ущерба.

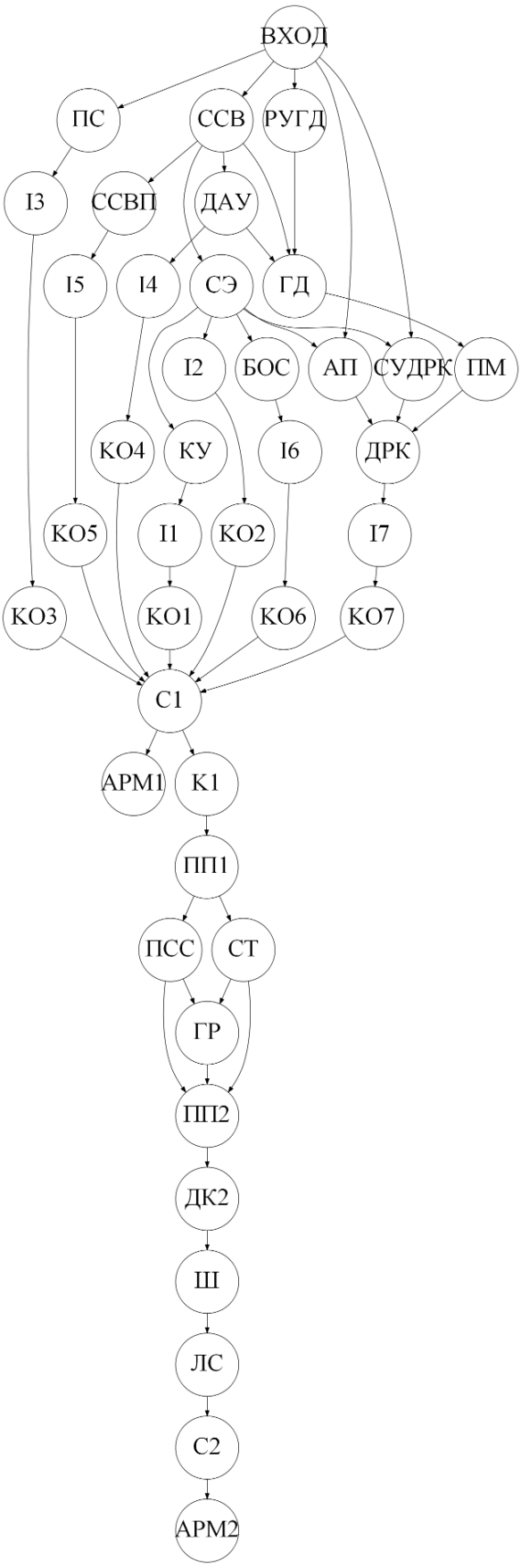


Рис. 3. Орграф функционирования СЭУ и системы ДМД

$\|a_{nk}\| =$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1														
2	$a_{1;2}$													
3	$a_{1;3}$				$a_{5;3}$									
4														
5			$a_{3;5}$											
6	$a_{1;6}$				$a_{5;6}$									
7					$a_{5;7}$									
8		$a_{2;8}$	$a_{3;8}$						$a_{9;8}$					
9			$a_{3;9}$											
10														
11								$a_{8;11}$						
12			$a_{3;12}$		$a_{5;12}$									
13														
14							$a_{7;14}$			$a_{10;14}$	$a_{11;14}$			

Рис. 4. Матрица функционирования СЭУ

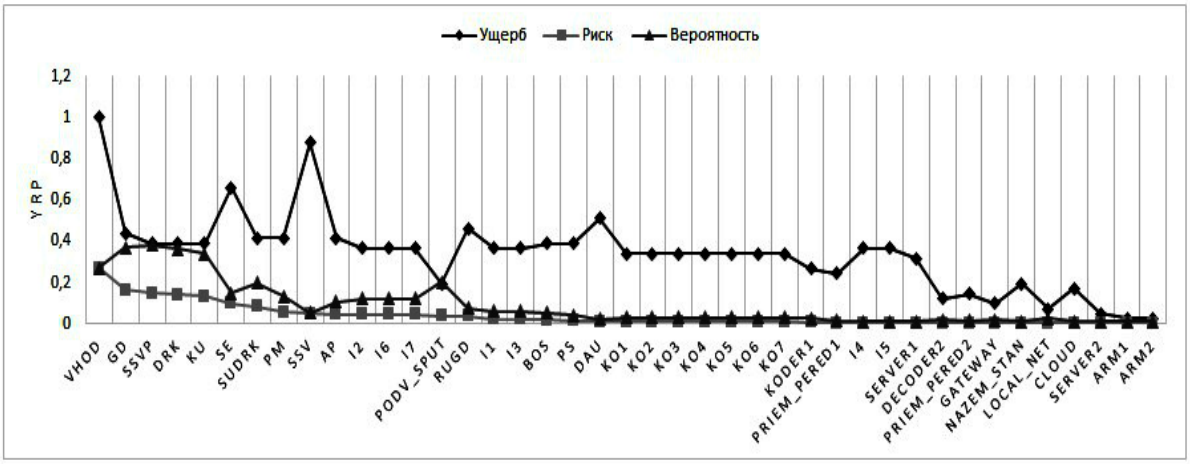


Рис. 5. Зависимости ущерба, вероятности и риска для функциональной схемы СЭУ

Для упрощения математического описания обобщенная модель ДМД СЭУ разработана на уровне подсистем СЭУ, механизмов и устройств. При необходимости детального исследования модели СЭУ и системы ДМД модель может дополняться отдельными моделями (орграфами) подсистем СЭУ. В этом случае сохраняется разработанный принцип моделирования.

Из результатов полученных оценок рисков следует, что наиболее уязвимыми подсистемами СЭУ являются: главный двигатель (ГД) (0,16), система санитарной водоподготовки (ССВП) (0,14), движительно-рулевой комплекс ДРК (0,14), котельная установка КУ (0,13). К менее уязвимым элементам СЭУ относятся следующие элементы системы: система дистанционного автоматизированного управления (ДАУ) главного двигателя (ДАУ) (0,010), Противопожарная система (ПС) (0,016), Балластно-осушительная система (БОС) (0,019), ручное управление главным двигателем РУГД (0,035).

Выводы

Впервые разработаны методологические основы обеспечения дистанционного мониторинга и диагностирования состояния судовых СТС на основе оценки технических рисков систем в аварийных ситуациях с учетом взаимосвязанности и взаимодействия их компонентов, количественного и качественного информационно – энергетического взаимообмена.

Технические риски систем, определяемые по предлагаемой методике для аварийной ситуации позволяют прогнозировать тенденцию изменения технического состояния СТС во времени (в зависимости от изменения работоспособности и надежности отдельных ее элементов, с учетом разной скорости изменения этих параметров).

Предлагаемая методика оценки рисков судовых СТС позволяет: определить значимость действующих в системе взаимосвязей м взаимодействий компонентов систем; моделировать распространения различных уровней тяжести неблагоприятных внешних воздействий и поражающих факторов по структуре системы.

Список литературы

1. Бакланов, А.И. Системы наблюдения и мониторинга / А.И.Бакланов // М.: Бином. – 2009.– 234 с.
2. Кончаков, Е. И. Техническая диагностика судовых энергетических установок / Е. И. Кончаков. – Владивосток: ДВГТУ, 2007. – 112 с.
3. Головко, С.В. Диагностика технического состояния судового электрооборудования на основе интеллектуального анализа данных / С.В. Головко. // Вестник АГТУ. Сер.: Управление, вычислительная техника и информатика, 2009. – С. 90 – 95.
4. Рябинин, И. А. Надежность и безопасность структурно-сложных систем / И. А. Рябинин. – СПб.: Изд-во С.-Петерб. ун-та, 2007. – 276 с.
5. Andersen, B. A Diagnostic System for Remote Real-Time Monitoring of Marine Diesel-Electric Propulsion Systems / B. Andersen. – Leipzig, 2011. – 45 p.
6. Минаков, А.А. Диагностирование оборудования с использованием параметров технологического контроля / А.А. Минаков, Д.В. Федосеев. // Известия Самарского научного центра Российской академии наук, 2009. – С. 305 – 309.
7. Klein, J. H. An approach to technical risk assessment / J. H. Klein, R. B. Cork // International Journal of Project Management. – 1998. – 16 (6). – Pp. 345-351
8. O'Neill, J. Technical Risk Assessment: a Practitioner's Guide] / J. O'Neill, N. Thakur, A. Duus. – Australia, 2007. – 29 p.
9. Kertzner, P. Process Control System Security Technical Risk Assessment Methodology & Technical Implementation / P. Kertzner, J. Watters, D. Bodeau // Research Report. – 2008. – № 13. – 47 p.
10. Вычужанин, В.В. Метод управления рисками судовых сложных технических систем / В.В. Вычужанин, Н.Д. Рудниченко // Проблеми техніки. – 2014. – №2. – С. 138 – 142.
11. Вычужанин, В.В. Технические риски сложных комплексов функционально взаимосвязанных структурных компонентов судовых энергетических установок/ В.В. Вычужанин, Н.Д. Рудниченко // Вісник Одеського національного морського університету, збірник наукових праць. – 2014. – Вып. 2(40) . – С. 68 – 77.
12. ISO 9000:2015 Quality management systems -- Fundamentals and vocabulary, 2015. – 51 p.
13. Вычужанин, В.В. Оценки структурного и функционального рисков сложных технических систем[Текст] / В.В. Вычужанин, Н.Д. Рудниченко // Восточно-Европейский журнал передовых технологий. – 2014. –1/2 (67) . – С. 18 – 22.
14. LangIcy, P. Automated cognitive modeling / P. LangIcy, S. Ohlsson // Automated cognitive modeling. – 1984. – 112 p.
15. Frank, A.. Spatial and cognitive simulation with multi-agent systems / A. Frank, S. Bittner, M. Raubal // Spatial Information Theory. – 2001. – Pp. 124 – 139.
16. Beetz, M. Cognitive technical systems—what is the role of artificial intelligence / M. Beetz, M. Buss, D. Wollherr // KI 2007: Advances in Artificial Intelligence. – 2007. – Pp. 19 – 42.
17. Schwenk, C.R. The cognitive perspective on strategic decision making / C.R. Schwenk // Journal of Management Studies. – 2007. – Т. 25. – № 1. – Pp. 41 – 55.

18. OREDA. OREDA – Offshore Reliability Data Handbook 2015. – 6th Edition / OREDA 2015 6TII EDITION, 2015. – 783 p.
19. Вычужанин, В.В. Взаимодействие технических средств СЭУ на основе когнитивного моделирования / В.В. Вычужанин, Н.Д. Рудниченко// Матеріали VI Міжнародної науково–технічної конференції Суднова енергетика: стан та проблеми. – 2013. – С. 58 – 60.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСТАНЦІЙНОЇ ОЦІНКИ РИЗИКІВ СКЛАДНИХ ТЕХНІЧНИХ СИСТЕМ

Н.О. Шибаєва, В.В. Вичужанін

Одеський національний морський університет,
Мечникова, 34, Одеса, 65404, Україна; e-mail: vint532@yandex.ru

Стаття присвячена дистанційній діагностиці технічного стану складних технічних систем, їх взаємопов'язаних, взаємодіючих підсистем і елементів за оцінками ризиків. Проведено аналіз використовуваних методів дистанційного моніторингу, діагностики складних технічних систем. Описано метод дистанційного моніторингу, діагностики, який базується на обліку взаємозв'язку і взаємодії підсистем складних технічних систем і їх елементів, а також кількісного та якісного інформаційно – енергетичного взаємообміну. Застосування розробленого методу і його інформатизація дозволяє оцінити працездатність складної технічної системи в різних умовах і режимах її експлуатації, а також прогнозувати стан системи в аварійних екстремальних ситуаціях і здійснювати подальшу автоматизацію прийняття рішень.
Ключові слова: складна технічна система, інформаційно – енергетичний взаємообмін, моніторинг, діагностика, прогнозування.

INFORMATIVE PROVIDING OF THE CONTROLLED FROM DISTANCE ESTIMATION OF RISKS OF THE DIFFICULT TECHNICAL SYSTEMS

N.O. Shibaeva, V.V. Vychuzhanin

Odessa National Maritime University,
34, Mechnikov str., Odessa, 65404, Ukraine; e-mail: vint532@yandex.ru

The article is sanctified to the controlled from distance diagnostics of the technical state of the difficult technical systems, their associate, interactive subsystems and elements on the estimations of risks. The analysis of the used methods of remote monitoring, diagnostics of the difficult technical systems is conducted. The method of remote monitoring, diagnostics, being base on account of associateness and co-operation of subsystems of the difficult technical systems and their elements, is described, and also quantitative and quality informatively - power trade-out. Application of the worked out method and his informatization allow to estimate the capacity of the difficult technical system under various conditions and modes of her exploitation, and also to forecast the state of the system in an emergency
Keywords: difficult technical system, informatively is a power trade-out, monitoring, diagnostics, prognostication.

УДК 004.056.55

Informatics and Mathematical Methods in Simulation
Vol. 6 (2016), No. 2, pp. 142-148

ПОЛУТОРАБАЙТНЫЕ НЕЛИНЕЙНЫЕ ПРЕОБРАЗОВАНИЯ КОНСТРУКЦИИ НИБЕРГ

Д.А. Юровских, А.В. Соколов, Б.С. Троицкий

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: radiosquid@gmail.com

Статья посвящена актуальным вопросам конструирования полуторабайтных S-блоков подстановки для повышения эффективности современных шифров. Построены полуторабайтные S-блоки конструкции Ниберг над всеми изоморфными представлениями поля $GF(2^{12})$, проведено их выборочное тестирование на соответствие основным критериям криптографического качества, которое показало, что полуторабайтные S-блоки обладают значительно лучшими криптографическими характеристиками, нежели однобайтные или полубайтные. Введен удобный для длинных S-блоков критерий удельного расстояния нелинейности, характеризующий «количество нелинейности» в элементе Q-последовательности либо значении булевой функции. Результаты работы позволяют утверждать, что построенные S-блоки могут быть эффективно использованы для модернизации современных шифров и построения новых перспективных криптоалгоритмов.

Ключевые слова: S-блок, конструкция Ниберг, поле Галуа, изоморфизм

Введение

Повсеместное внедрение компьютерной техники во все сферы человеческой деятельности приводит к постоянному росту количества обрабатываемой, передаваемой и хранимой информации. Данное обстоятельство приводит к дальнейшей актуализации вопросов совершенствования методов защиты информации, в том числе, дальнейшего развития криптографических алгоритмов. В последнее время существенное распространение получили блочные криптоалгоритмы, что объясняется тем, что на сегодняшний день они обладают простой технической реализацией и высокими показателями криптографического качества.

Одним из важнейших этапов разработки любого современного симметричного блочного алгоритма шифрования является построение нелинейного преобразования — S-блока подстановки, характеристики которого во многом определяют характеристики конструируемого шифра. Так, в литературе достаточно много внимания уделяется проблеме построения высококачественных S-блоков, тем не менее, все они характеризуются длиной входного слова $k \le 10$ [1].

С другой стороны, результаты экспериментов [2] показывают, что криптографическое качество S-блоков подстановки и их способность противостоять атакам криптоанализа значительно улучшаются с ростом их длины $N = 2^k$. Данное обстоятельство четко прослеживается исторически в виде роста длины применяемых в криптоалгоритмах S-блоков. Так, на смену алгоритму DES, который использовал полубайтные S-блоки, пришел криптоалгоритм Rijndael (AES), который является ныне действующим стандартом шифрования США и использует S-блоки конструкции Ниберг с длиной входного слова $k = 8$ бит и, соответственно, с длиной Q-последовательности $N = 2^8 = 256$ (однобайтные). Исходя из этого, становится очевидно, что следующим шагом в конструировании новых криптоалгоритмов будет синтез и использование полуторабайтных S-блоков подстановки.

Процесс выбора S-блока является весьма трудоемким с вычислительной точки зрения, поэтому в современной криптографии принят подход, основанный на построении регулярных методов синтеза S-блоков с заранее определенными криптографическими характеристиками. Одним из таких методов является предложенная К. Нибергом конструкция, основанная на обращении элементов поля Галуа по модулю неприводимого полинома [3]. Тем не менее, в литературе S-блоки конструкции Ниберг синтезированы лишь для значений длины входного слова $k \le 10$, в то время как исследование характеристик более длинных S-блоков в литературе отсутствует.

Целью настоящей работы является построение S-блоков подстановки конструкции Ниберг с длиной входного слова $k = 12$ (полуторабайтных) над всеми изоморфными представлениями поля $GF(2^{12})$.

Основная часть

Конструкция S-блоков подстановки классических блочных криптографических алгоритмов (например, ГОСТ 28147-89, Магма, Калина, BelT, DES, AES и др.) состоит из дешифратора, который преобразует *k*-разрядный двоичный сигнал в одноразрядный сигнал по модулю 2^k, системы внутренних связей (всего связей должно быть 2^k) и шифратора, который преобразует сигнал из одноразрядного 2^k -ичного в *k*-разрядный двоичный. Схема полуторабайтного S-блока представлена на рис. 1.

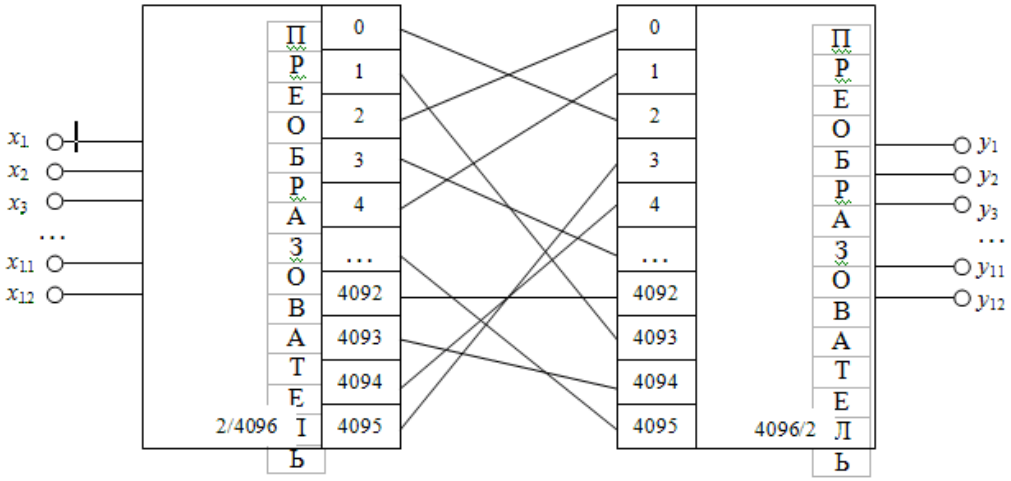


Рис. 1. Конструкция полуторабайтного S-блока подстановки

Очевидно, что S-блок подстановки определяет однозначное соответствие между электродами дешифратора и электродами шифратора или соответствующими ячейками памяти, которые реализуют блок программно. Данное правило часто записывают в виде кодирующей Q-последовательности, которая в свою очередь может быть представлена в виде k компонентных булевых функций. Криптографические свойства последних полностью определяют качество конструируемого S-блока.

S-блок называют биективным, если его кодирующая Q-последовательность содержит в своем составе все элементы тривиальной входной последовательности $\{0,1,...,2^{k-1}\}$, а все линейные комбинации компонентных булевых функций, соответственно, являются сбалансированными. Ясно, что всего биективных полуторабайтных S-блоков существует $J_{4096} = 2^k! = 4096!$, что является астрономической величиной. Данное обстоятельство полностью исключает

возможность поиска оптимальных структур Q-последовательностей переборными методами и диктует необходимость применения регулярных методов синтеза, одним из которых является ранее используемая для небольших длин S-блоков конструкция Ниберг [3].

Конструкция Ниберг, которая представляет собой отображение, задаваемое мультипликативно обратными элементами поля Галуа $GF(2^k)$ определяется следующим соотношением

$$y = x^{-1} \bmod d[f(z), p],\ y,\ x \in GF(2^k), \tag{1}$$

скомбинированным вместе с аффинным преобразованием

$$b = A \cdot y + a, a, b \in GF(2^k), \tag{2}$$

где $f(z)$ – неприводимый над полем $GF(2^k)$ полином; A – невырожденная матрица аффинного преобразования; a – вектор сдвига; $p = 2$ – характеристика расширенного поля Галуа, $0^{-1} \equiv 0$ – принято; a, b, x, y – элементы расширенного поля Галуа $GF(2^k)$, рассматриваются как десятичные числа, либо двоичные векторы, либо полиномы степени $k-1$.

S-блоки, построенные в соответствии с выражениями (1) и (2) обладают высоким уровнем криптографического качества [4, 5]: высокой алгебраической степенью нелинейности, высоким расстоянием нелинейности, равномерной минимизацией коэффициентов корреляции. Существенным недостатком конструкции Ниберг является то, что количество различных структур высококачественных S-блоков равно количеству неприводимых полиномов над полем $GF(2^k)$, которое является весьма небольшим и определяется как [6]

$$|w_k| = \frac{1}{k} \sum_{\substack{d \\ d/k}} \mu(d) q^{(k/d)}, \tag{3}$$

где d – делители степени k; $\mu(d)$ – функция Мёбиуса; запись d/k означает, что d делит k нацело.

В случае небольших S-блоков подстановки данный недостаток удалось преодолеть за счет рассмотрения всех изоморфных представлений основного поля [1], однако, как показывают эксперименты, данный подход применим и для полуторабайтных S-блоков.

Так, основополагающая теорема полей Галуа гласит, что для каждого простого числа p и натурального k существует конечное алгебраическое поле порядка p^k, единственное с точностью до изоморфизма. Однако, оказывается, что свойства криптографических конструкций, ровно как и корректирующих кодов и шумоподобных сигналов, существенно зависят от выбора вида представления поля. Поэтому с прикладной точки зрения целесообразно различные представления поля порядка p^k рассматривать как различные поля.

Основное, рассматриваемое в данной работе поле $GF(2^{12})$, имеет следующие свои изоморфные представления

$$GF(q^k) \Rightarrow GF(2^{12}) \Rightarrow GF(4^6) \Rightarrow GF(8^4) \Rightarrow GF(16^{13}) \Rightarrow GF(64^2). \tag{4}$$

Таким образом, исходя из (3) выражение (1) принимает вид

$$y = x^{-1} \bmod dd\left[f_1(z), f_2(z), p\right], \quad y, x \in GF\left(q^k\right), \tag{5}$$

где $f_1(z)$ – неприводимый полином, определяющий операцию умножения в поле «нижнего уровня» $GF(q)$, $f_2(z)$ – в поле «верхнего уровня», т.е. расширении расширенного поля $GF(q^k)$.

Количества различных неприводимых полиномов [3] над различными представлениями основного поля (4), и соответственно, количества различных структур S-блоков подстановки, рассчитанные в соответствии с (3), приведены в табл. 1.

Таблица 1.

Количества различных неприводимых полиномов

Поле $GF(q^k)$	$GF(2^{12})$	$GF(4^6)$	$GF(8^4)$	$GF(16^3)$	$GF(64^2)$
Кол-во неприв. полиномов $f_1(z)$ в поле $GF(q)$	1	1	2	2	6
Кол-во неприв. полиномов $f_2(z)$ в поле $GF(q^k)$ для выбранного $f_1(z)$	335	670	1008	1360	2016
Общее кол-во неприв. полиномов в поле $GF(q^k)$	335	670	2016	2720	12096

Таким образом, общее количество S-блоков подстановки конструкции Ниберг, которые могут быть построены над всеми изоморфными представлениями поля $GF(2^{12})$, составляет J=17837, что является достаточным для использования данных высококачественных подстановочных конструкций в качестве долговременного ключа, а также для реализации концепции оперативной смены ключа.

В настоящей статье полученные полуторабайтные S-блоки были подвергнуты тестированию по следующим общепринятым критериям криптографического качества [4, 5]:

- алгебраическая степень нелинейности, определяемая как максимальная степень (наибольшее из количеств конъюнкций в терме) алгебраической нормальной формы представления компонентных булевых функций S-блока (минимум среди компонентных булевых функций);
- расстояние нелинейности, определяемое как минимальное расстояния Хэмминга от компонентных булевых функций S-блока до кодовых слов аффинного кода (минимум среди компонентных булевых функций);
- матрица коэффициентов корреляция, показывающая корреляционную взаимосвязь векторов выхода S-блока и векторов его входа.

Анализ криптографических свойств S-блоков большой длины, например, полуторабайтных представляет собой весьма сложную вычислительную задачу, что диктует необходимость проведения выборочного анализа на полном множестве построенных S-блоков. Результаты выборочного анализа криптографических свойств S-блоков подстановки на основе различных изоморфных представлений основных полей $GF(2^4)$, $GF(2^8)$, $GF(2^{12})$ приведены в табл. 2, где данные записаны в следующем порядке: алгебраическая степень нелинейности (расстояние нелинейности) максимум среди модулей коэффициентов корреляции.

Таблица 2.

Криптографические характеристики S-блоков подстановки

Поле	$GF(2^k)$	$GF(4^k)$	$GF(8^k)$	$GF(16^k)$	$GF(32^k)$	$GF(64^k)$
Полубайтные	3 / 4 / 0.25	3 / 4 /0.5	—	—	—	—
Однобайтные	7 / 112 / 0.125	7 / 112 / 0.125	—	7 / 112 / 0.125	—	—
Полуторабайтные	11 / 1984 / 0.0293	11 / 1984 / 0.0293	11 / 1984 / 0.0283	11 / 1984 / 0.0313	—	11 / 1984 / 0.0313

Анализ данных табл. 2 показывает существенный прирост в качестве построенных S-блоков, причем их качество является стабильным для различных изоморфных представлений основного поля.

Одним из наиболее показательных и практически ценных критериев является расстояние нелинейности. Так, расстояние нелинейности для конструкции Ниберг показывает значительный рост с увеличением их длины, что делает сравнительный анализ подстановочных конструкций неочевидным и затрудненным. Впервые, проведя оценку криптографических свойств S-блоков конструкции Ниберг столь большой длины $N = 2^k = 4096$, в настоящей работе авторами предлагается введение показателя удельного расстояния нелинейности

$$\eta_s = \frac{2 \cdot N_s}{N}, \eta_f = \frac{2 \cdot N_f}{N}, \tag{6}$$

где η_S — удельное расстояние нелинейности S-блока; η_f — удельное расстояние нелинейности булевой функции; N_s — расстояние нелинейности исследуемого S-блока; N_f — расстояние нелинейности исследуемой булевой функции; N — длина исследуемого S-блока или булевой функции.

Таким образом, по построению, удельное расстояние нелинейности показывает «количество нелинейности», содержащееся в одном элементе кодирующей *Q*-последовательности или в одном значении булевой функции. Так, нетрудно видеть, что для аффинных булевых функций $\eta = 0$, в то время как для бент-функций $\eta = \frac{2\left(2^{k-1} - 2^{(k/2)-1}\right)}{N} = \frac{2\left(2^{k-1} - 2^{(k/2)-1}\right)}{2^k}$ [7]. Нетрудно показать, что $\lim\limits_{k\to\infty} = \frac{2\left(2^{k-1} - 2^{(k/2)-1}\right)}{2^k} = \frac{2}{2} = 1$, таким образом удельное расстояние нелинейности бесконечно длинной булевой бент-функции достигает значения 1, в то время как $0 \le \eta_S < 1$, $0 \le \eta_f < 1$.

В виду схожести криптографических свойств S-блоков конструкции Ниберг над различными изоморфными представлениями основного поля $GF(2^k)$, а также с учетом результатов [8] построим на рис. 2 график эволюции удельного расстояния нелинейности

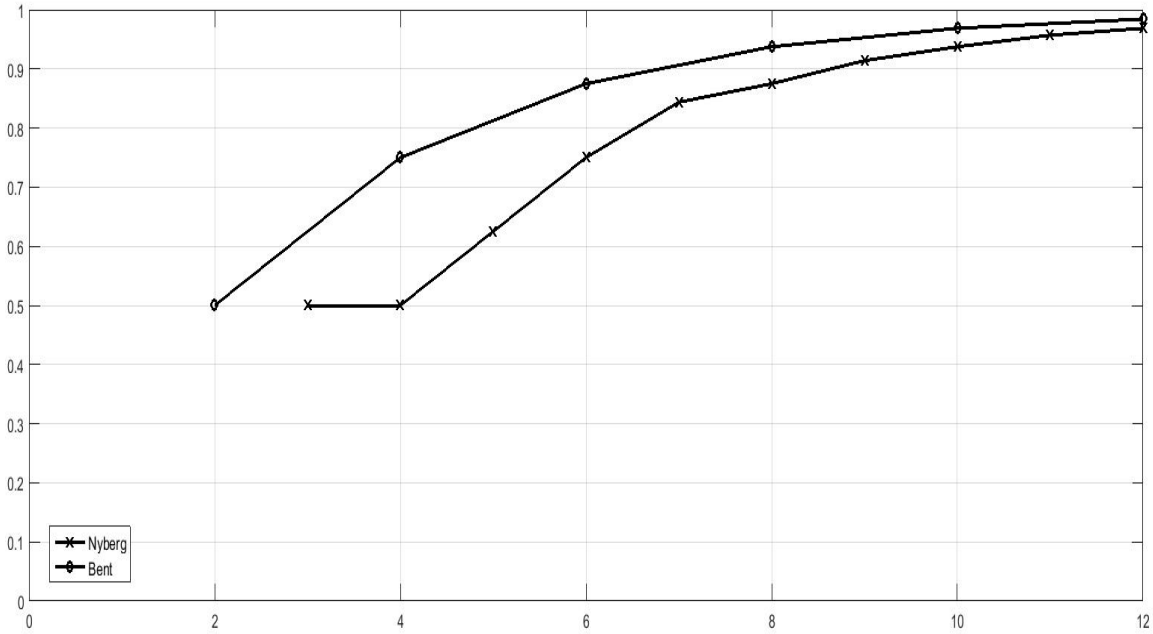


Рис. 2. Эволюция удельного расстояния нелинейности конструкции Ниберг и бент-функций

Детальный анализ данных рис. 2 показывает, что с увеличением длины S-блоков конструкции Ниберг их удельное расстояние нелинейности стремится к расстоянию нелинейности бент-функций. Так, для полуторабайтных S-блоков, отставание расстояния нелинейности S-блоков конструкции Нибрег от бент-функций составляет всего $\Delta_{12} = 0{,}0156{=}1{,}56\%$, в то время как для однобайтных S-блоков эта величина составляет $\Delta_8 = 0.0625 = 6.25\%$.

Выводы

1. Построен полный класс мощности $J{=}17837$ полуторабайтных S-блоков конструкции Ниберг над всеми изоморфными представлениями основного поля $GF(2^{12})$. Проведен выборочный анализ криптографического качества построенных S-блоков, который показал, что полуторабайтные S-блоки подстановки обладают значительно лучшим качеством, чем при длине входного слова полбайта или байт. При этом криптографическое качество является относительно стабильным в различных изоморфных представлениях основного поля.

2. Введен удобный для исследования длинных S-блоков критерий удельного расстояния нелинейности, показывающий «количество нелинейности», содержащееся в одном элементе кодирующей *Q*-последовательности или в одном значении булевой функции. Проведенный сравнительный анализ S-блоков конструкции Ниберг и бент-функций показал, что удельное расстояние нелинейности конструкции Ниберг приближается к удельному расстоянию нелинейности бент-функций с увеличением длины, при этом для полуторабайтных S-блоков величина отставания составляет $\Delta_{12} = 0{,}0156{=}1{,}56\%$.

3. Проведенные исследования подтверждают высокую перспективность применения полуторабайтных S-блоков подстановки конструкции Ниберг как для модернизации существующих криптоалгоритмов, так и для разработки новых криптоалгоритмов с большóй длиной блока.

Список литературы

1. Мазурков, М.И. Нелинейные S-блоки конструкции Ниберг с максимальным лавинным эффектом / М.И. Мазурков, А.В. Соколов // Известия высших учебных заведений. Радиоэлектроника. – 2014. – Т. 57. – N 6. – С. 47 – 55.
2. Ростовцев, А. Г. Большие подстановки для программных шифров / А.Г. Ростовцев // Проблемы инф. безопасности. Компьютерные системы. – СПб. – 2000. – № 3. – С. 31 – 34.
3. Nyberg, K. Differentially uniform mappings for cryptography. I Advances in cryptology / K. Nyberg // Proc. of EUROCRYPT'93. – Berlin, Heidelberg, New York. – 1994. – Vol.765. – Pp. 55 – 65.
4. Горбенко, І.Д. Дослідження аналітичних і статистичних властивостей булевих функцій криптоалгоритму RIJNDAEL (FIPS 197) / І.Д. Горбенко, О.В. Потій, Ю.А. Ізбенко // Радіотехніка: всеукр. міжвідом. наук.-техн. зб. – Харків, 2004 . – Т. 126. – С. 132 – 138.
5. Мазурков, М.И. Алгебраические свойства криптографических таблиц замен шифра Rijndael и шифра ГОСТ 28147-89 / М.И. Мазурков, А.В. Соколов. – Одесса: Труды СИЭТ. – 2012. – С. 149.
6. Берлекэмп, Э. Алгебраическая теория кодирования / Э. Берлекэмп // М: МИР. – 1971. – 477 с.
7. Токарева, Н.Н. Бент-функции: результаты и приложения. Обзор работ / Н.Н. Токарева // Приклад. дискрет. математика. – Томск, 2009. — №1(3). – С. 15–37.
8. Sokolov, A.V. Nyberg construction nonlinear transforms based on all isomorphic representations of the Galois field GF(512) [Электронный ресурс] / A.V. Sokolov // Проблеми телекомунікацій. – 2015. – № 2 (17). – С. 68 – 75. – Режим доступу: http://pt.journal.kh.ua/2015/2/1/152_sokolov_gf.pdf .

ПІВТОРАБАЙТНІ НЕЛІНІЙНІ ПЕРЕТВОРЕННЯ КОНСТРУКЦІЇ НІБЕРГ.

Д.А. Юровських, А.В. Соколов, Б.С. Троїцький

Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна; e-mail: radiosquid@gmail.com

Стаття присвячена актуальним питанням конструювання півторабайтних S-блоків підстановки для підвищення ефективності сучасних шифрів. Побудовано півторабайтні S-блоки конструкції Ніберг над усіма ізоморфними уявленнями поля $GF(2^{12})$, проведено їх вибіркове тестування на відповідність основним критеріям криптографічної якості, яке показало, що півторабайтні S-блоки мають значно кращі криптографічні характеристики у порівнянні з однобайтними або полубайтними. Введено зручний для довгих S-блоків критерій питомої відстані нелінійності, що характеризує «кількість нелінійності» в елементі Q-послідовності або значенні булевої функції. Результати роботи дозволяють стверджувати, що побудовані S-блоки можуть бути ефективно використані як для модернізації сучасних шифрів, так і для побудови нових перспективних криптоалгоритмів.

Ключові слова: S-блок підстановки, конструкція Ніберг, поле Галуа, ізоморфізм.

NIBERG CONSTRUCTION 12 BIT NONLINEAR TRANSFORMS.

D.A. Yurovsky, A.V. Sokolov, B.S. Troitsky

Odessa National Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: radiosquid@gmail.com

The article is devoted to the actual issues of the construction of 12 bit S-boxes in order to improve the effectiveness of modern ciphers. We built the full class of 12 bit S-boxes of Nyberg construction over all isomorphic representations of the field $GF(2^{12})$, performed their sample testing for compliance to the basic criteria of cryptographic quality, which showed that 12 bit S-boxes have much better cryptographic properties than 8 bit or 4 bit ones. We introduced new criterion of specific distance of nonlinearity for long S-boxes which characterizes "the number of non-linearity" in item of Q-sequence or single value of a Boolean function. The results suggest that the constructed S-boxes can be effectively used for the modernization of existing chipers and construction of modern promising cryptographic algorithms.

Keywords: S-box, Nyberg's construction, Galois field, isomorphism.

УДК 681.3:681.5

Informatics and Mathematical Methods in Simulation
Vol. 6 (2016), No. 2, pp. 149-157

ОБ ОДНОМ МЕТОДЕ ОРГАНИЗАЦИИ ВЫЧИСЛИТЕЛЬНОГО ПРОЦЕССА ПРИ РЕШЕНИИ СИСТЕМЫ ЛИНЕЙНЫХ АЛГЕБРАИЧЕСКИХ УРАВНЕНИЙ МЕТОДОМ ПРОСТОЙ ИТЕРАЦИИ

С. А. Положаенко, А.Г. Кисель, И.Ю. Голиков

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: polozhaenko@mail.ru

Выполнен анализ численного решения системы линейных алгебраических уравнений (СЛАУ) на вычислителях с фиксированной запятой. Показано, что точность результата вычислений зависит от процедуры организации вычислительного процесса. Приведена аналитическая оценка точности вычислений известных вычислительных процедур, совпадающая с результатами практического исследования последних. Предложен алгоритм вычислений, позволяющий ограничить накопление ошибок округлений на заданном уровне. Выполнен аналитический анализ результирующих ошибок округления предложенного алгоритма. Приведены условия, обеспечивающие ограничение накопления указанных ошибок на заданном уровне.

Ключевые слова: СЛАУ, метод простой итерации, вычислительный алгоритм, ошибки округления, максимальные вероятностные оценки

Введение

Одним из центральных разделов современной теории управления является теория управления системами с распределенными параметрами (РП-системы), принципиальной особенностью которых является пространственная распределенность управляемых величин и управляющих воздействий. Для управления такими объектами используются современные методы модального управления и синтеза наблюдающих устройств [1].

Методы синтеза наблюдающих устройств, подробно исследованные в рамках автоматического управления системами с сосредоточенными параметрами (СП-системы), а в теории управления РП-системами – разработаны гораздо хуже.

Кроме того, часто при решении практических задач модального управления РП-системами бывают доступны для измерения не все переменные состояния объекта, а только некоторые входы и выходы.

Известен подход к решению таких задач при неполной наблюдаемости объекта, связанный с использованием в качестве наблюдателя модели объекта управления. Для объектов с РП-параметрами такая модель содержит распределенные по пространственным координатам переменные состояния и в общем случае является трансцендентной. Действенным из возможных методов является дискретизация по пространству исходной модели РП-системы моделью с СП-параметрами в виде системы обыкновенных дифференциальных уравнений (ОДУ) [2]. Для достижения хорошей управляемости, степень дискретизации должна быть достаточной. Однако полученная модель будет иметь большую размерность и поэтому, для ее реализации, целесообразно использовать параллельные вычислительные структуры. При

реализации таких моделей в реальных объектах управления для упрощения аппаратных и алгоритмических затрат целесообразно использовать более простые алгоритмы вычисления, а в качестве аппаратной части использовать более простые и быстродействующие вычислители с фиксированной запятой.

Среди объектов управления с РП-параметрами большую долю составляют объекты, описываемые уравнениями теплопроводности. При использовании метода дискретизации таких моделей по пространственным переменным, исходному дифференциальному уравнению в частных производных (ДУЧП) на каждом временном слое ставится в соответствие некоторая система алгебраических уравнений (СЛАУ) [3] вида

$$\hat{\mathrm{A}} \cdot \vec{\varphi} = \vec{f}\,, \tag{1}$$

где $\vec{\varphi}$ м пространственный вектор решения на данном временном слое, $\vec{f}$ – вектор правых частей, определяемый граничными и задающими воздействиями, $\hat{\mathrm{A}}$ – матрица коэффициентов, определяемая физическими свойствами РП-объекта и параметрами дискретизации.

Среди наиболее простых алгоритмов вычислений, ориентированных на решение задач вида (1) с помощью параллельных сеточных процессоров, наиболее хорошей распараллеливаемостью и максимальной простотой реализации отличается метод простой итерации.

Цель работы

Исследование вычислительных погрешностей при решении систем линейный алгебраических уравнений методом простой итерации на вычислителях с фиксированной запятой.

Основная часть

Решение СЛАУ вида (1) методом простой итерации сводится к построению итерационной процедуры вида

$$\vec{\varphi}^{(k+1)} = \vec{\varphi}^{(k)} + \tau\left(\hat{\mathrm{A}} \cdot \vec{\varphi}^{(k)} - \vec{f}\right). \tag{2}$$

Здесь: $\hat{\mathrm{A}} = \left(a_{ij}\right)_{p\times p}$ – вещественная симметрическая отрицательно определенная матрица; p – ее размерность; $k = 1,2,\ldots,L$ – число шагов итераций; $\vec{\varphi}^{(0)}$ – вектор известных начальных условий.

Следует заметить, что к зависимости вида (2) приводятся также системы линейных дифференциальных уравнений (СЛДУ) вида

$$\frac{d\vec{\varphi}}{dt} = \hat{\mathrm{A}} \cdot \vec{\varphi} = \vec{f} \tag{3}$$

при решении их методом Эйлера. В этом случае параметр τ выступает уже как шаг интегрирования по времени, а каждый вектор $\vec{\varphi}^{(k)}$, $k = 1,2,\ldots,L$ является решением (3) для данного момента времени.

В скалярном виде процедура (2) запишется следующим образом:

$$\vec{\varphi}_i^{(k+1)} = \vec{\varphi}_i^{(k)} + \tau\left(\sum_{j=1}^{p} a_{ij} \cdot \vec{\varphi}_j^{(k)} - f_i\right); \quad (4)$$

$$i = 1,2,\ldots,p.$$

При вычислении зависимостей (4) на вычислителях с ограниченной разрядностью на каждой итерации возникают погрешности округления [3]. В зависимости от последовательности выполнения операций указанные ошибки могут накапливаться с разной скоростью и привести к потере точности. Возникает задача исследования вычислительных ошибок решения СЛАУ методом простой итерации, которая включает в себя две подзадачи:

- поскольку реальные ошибки округления – случайные величины, то необходимо проанализировать вероятностные характеристики последних;
- поскольку алгоритм вычисления зависимости (4) может быть построен не единственным образом, то необходимо рассмотреть вопрос выбора алгоритма, обеспечивающего наименьшие ошибки округления.

При вычислениях в формате с фиксированной запятой наиболее удобной является фиксация запятой перед старшим разрядом [4, 5]. При этом все машинные числа являются правильными двоичными дробями. Поэтому, в дальнейшем, полагаем все машинные числа нормализованными, то есть принадлежащими интервалу [-1, 1]. Интервал возможных значений чисел с фиксированной запятой будет равен: $-\left(1-2^{-M}\right) \le b \le 1-2^{-M}$. Здесь M – разрядность машинных чисел. Очевидно, что необходимость округления возникает после выполнения операций умножения, деления или сдвига вправо. Будем считать, что результаты выше указанных операций представляют некоторое множество действительных чисел B, а множество двоичных чисел, представляемых в машине, является подмножеством $B_i \in B$. Пусть результат арифметической операции $b \in B$ удовлетворяет условию $b_i < b < b_{i+1}$, где $b_i, b_{i+1} \in B_i$ – следующие друг за другом машинные числа. Расстояние между соседними машинными числами b_i и b_{i+1} обозначим ε_0. Очевидно, оно будет равно $\varepsilon_0 = 2^{-M}$. Под округлением будем понимать замену по определенному правилу числа b приближенным значением b_i или b_{i+1}. Погрешность округления будет представлять собой разность

$$\varepsilon_j = b_j - b, \quad \text{где} \quad b_j = \{b_i, b_{i+1}\}. \quad (5)$$

Замена числа его приближенным значением меньшей разрядности может выполняться по разным правилам (способам) округления. Различают следующие виды округления [4].

1. Т-округление (или усечение). При этом округлении младшие разряды отбрасывают, а сохраняемые разряды не изменяются.
2. А-округление. При этом округлении добавляется единица в младший из сохраняемых разрядов, если он содержит нуль, или данный разряд сохраняется неизменным, в случае записи в нем единицы.
3. R-округление. При этом округлении добавляется единица в младший сохраняемый разряд, если старший из отбрасываемых разрядов содержит единицу. Если старший отбрасываемый разряд равен нулю, то младший сохраняемый разряд не изменяется.

Проведенный на основании методики, предложенной в [4], анализ показал, что распределение ошибок округления при использовании Т-, А- и R-округления к результатам умножения, деления и сдвига вправо аппроксимируется равномерным законом при достаточной длине исходных неокругленных двоичных чисел. При этом,

как показано в [6], уже при $M \geq 6$ и $m \geq 6$ закон распределения ошибок округления с достаточно высокой точностью можно полагать равномерным, а при $M \geq 8$ и $m \geq 8$ он практически совпадает с равномерным. Здесь M и m – длина соответственно сохраняемых и отбрасываемых разрядов.

Для проведения анализа вычислительных ошибок рассмотрим некоторые аспекты вычисления зависимости (4). С точки зрения последовательности выполнения операций могут быть построены несколько алгоритмов, отличающихся друг от друга количеством и последовательностью выполняемых операций. Так, например, выражение (4) можно реализовать различной последовательностью вычислительных процедур (6).

$$a)\ \begin{cases} \varphi_i^{(k+1)} = \varphi_i^{(k)} + \Delta\varphi_i^{(k+1)}; \\ \Delta\varphi_i^{(k+1)} = \tau \cdot F_i^{(k)}; \\ F_i^{(k)} = S_i^{(k)} - f_i; \\ S_i^{(k)} = \sum_{j=1}^{p} a_{ij} \varphi_j^{(k)}; \\ i = 1,2,\ldots,p \end{cases} \qquad b)\ \begin{cases} \varphi_i^{(k+1)} = \varphi_i^{(k)} + \Delta\varphi_i^{(k+1)}; \\ \Delta\varphi_i^{(k+1)} = F_{i1}^{(k)} + F_{i2}^{(k)}; \\ F_{i1}^{(k)} = -\tau \cdot f_i; \quad F_{i2}^{(k)} = \tau \cdot S_i^{(k)} \\ S_i^{(k)} = \sum_{j=1}^{p} a_{ij} \varphi_j^{(k)}; \\ i = 1,2,\ldots,p \end{cases} \qquad (6)$$

Как видно из анализа (6*a*) и (6*b*), эти выражения эквивалентны с точки зрения математики, но не равноценны по количеству операций. В (6*b*) количество операций умножения больше, а это может привести к дополнительным ошибкам округления.

Поэтому при построении вычислительного алгоритма любого вычисления целесообразно строить такой алгоритм, который содержит минимальное количество операций умножения, а также деления и сдвига.

Учитывая сказанное, в качестве базового алгоритма будем использовать алгоритм (6*a*). Следует отметить, что в указанном алгоритме вычисление $S_i^{(k)}$ может быть организовано последовательно, параллельно или последовательно-параллельно. Однако, поскольку это не изменяет общее количество операций умножения и не приводит к перестановке сомножителей, то последовательность вычислений не будет влиять на величину возможной ошибки округления.

Учитывая вышесказанное, в качестве базового алгоритма будем использовать вычислительный алгоритм 6*a*, графическое представление которого (в соответствии с методикой, предложенной в [4]), изображено на рис.1.

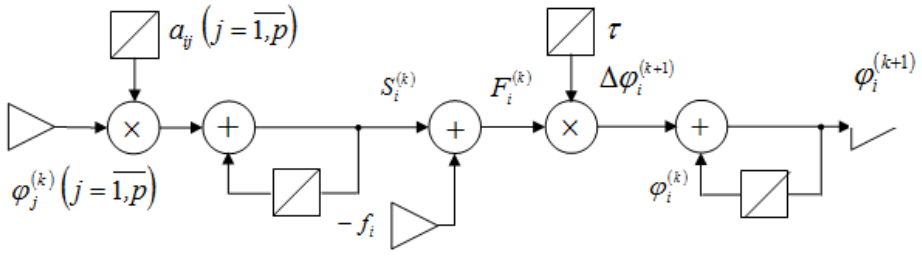


Рис. 1. Графическое представление вычислительного алгоритма

Алгоритм, представленный на рис. 1, описывает последовательность выполнения операций на одном шаге вычислений. Однако представленный алгоритм является идеализированным, так как не учитывает операции округления. Реальный алгоритм будет содержать на каждом шаге операции округления, необходимые для ограничения разрядности выходной величины.

Известен [7, 8] алгоритм вычислений зависимостей вида (4), в котором на каждой итерации операция округления осуществляется после вычисления невязки $\Delta\varphi_i^{(k)}$, то есть на выходе алгоритма. Графическое изображение алгоритма представлено на рис. 2.

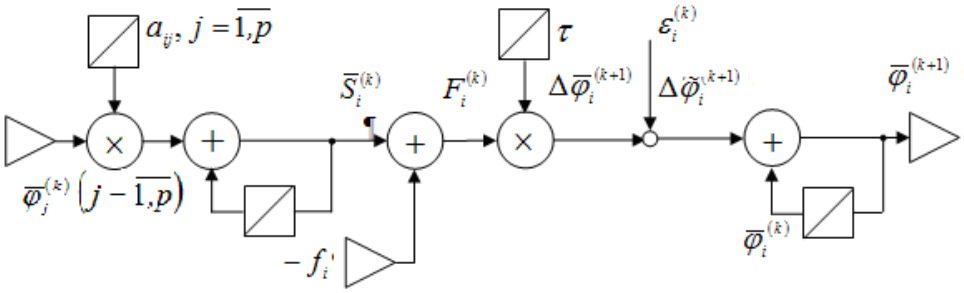


Рис. 2. Вычислительный алгоритм с округлением выходной величины

Результаты практического использования указанного алгоритма показали, что результирующие накопившиеся ошибки округления ведут себя пропорционально k при использовании Т-округления, и пропорционально $\sqrt{k}$ – при R-округлении. Здесь k – число шагов вычисления.

В результате теоретических исследований были получены аналитические оценки накопления ошибок для данного вычислительного алгоритма. Согласно полученным результатам, максимальное вероятностное значение результирующих ошибок округления подчиняется следующему неравенству

$$\left|r_i^{(k)}\right|_{\max} \le 3\sigma_\varepsilon\sqrt{\Omega_{2M}(k)} + \left|\xi_\varepsilon\right|\cdot p\cdot\Omega_{1M}(k), \tag{7}$$

где

$$\Omega_{1M}(k) = \max_{1\le j\le p}\frac{1-\left|1-\tau\lambda_j\right|^k}{1-\left|1-\tau\lambda_j\right|}; \tag{8}$$

$$\Omega_{2M}(k) = \max_{1\le j\le p}\frac{1-\left(1-\tau\lambda_j\right)^{2k}}{\tau\lambda_j\left(2-\tau\lambda_j\right)}. \tag{9}$$

Здесь: λ_j, $j=1,2,...,p$ – собственные числа матрицы $\hat{A}$; ξ_ε – математическое ожидание локальных ошибок округления $\varepsilon_i^{(k)}$; σ_ε – среднеквадратическое отклонение локальных ошибок округления.

Анализ выражений (7) – (9), показывает, что результирующие ошибки округления:

- растут с ростом числа обусловленности матрицы $\hat{A}$;
- определяются выбором параметра τ, при этом для случая не центрированных локальных ошибок округления (Т-округление) они растут пропорционально $1/\tau$, то есть пропорционально k, а при центрированных локальных ошибках округления (*R*-округление) – пропорционально $\sqrt{1/\tau}$, то есть пропорционально $\sqrt{k}$.

Таким образом, результаты теоретического анализа полностью совпадают с приведенными в [7, 8] результатами практического исследования, что подтверждает достоверность полученных аналитических оценок.

Вместе с тем, при численном решении тестовых задач с применением данного алгоритма был выявлен существенный недостаток, заключающийся в том, что при относительно небольшой разрядности M округляемых двоичных чисел (при этом $M \geq 8$), а также при малых значениях τ возникает явление глобального вырождения решения, при котором накопившаяся ошибка полностью искажает результаты счета. Это не позволяет использовать данный вычислительный алгоритм для решения СЛАУ большой размерности с плохо обусловленной матрицей, а также для решения «жестких» СЛДУ [3] первого порядка методом Эйлера с малым шагом, определяющим методическую погрешность решения.

Для устранения указанных недостатков предложен вычислительный алгоритм, в котором на каждой итерации операция округления осуществляется перед вычислением невязки $\Delta\varphi_i^{(k)}$, то есть на входе алгоритма. Графическое изображение алгоритма представлено на рис. 3.

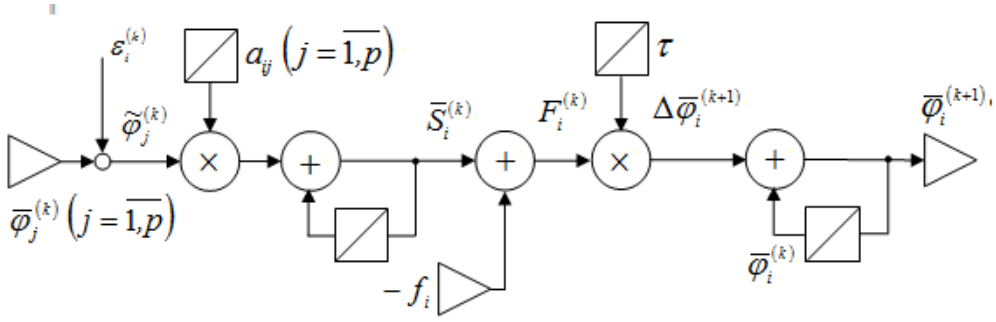


Рис. 3. Вычислительный алгоритм с округлением входной величины

Для данного вычислительного алгоритма также были получены аналитические оценки накопления ошибок. Согласно полученным результатам, максимальное вероятностное значение результирующих ошибок округления подчиняется следующему неравенству

$$\left|r_i^{(k)}\right|_{\max} \leq 3\sigma_\varepsilon \sqrt{\Omega_{4M}(k)} + \left|\xi_\varepsilon\right| \cdot p \cdot \Omega_{3M}(k), \tag{10}$$

где

$$\Omega_{3M}(k) = \max_{1\leq j\leq p}\left|\tau\lambda_j\right| \cdot \frac{1-\left|1-\tau\lambda_j\right|^k}{1-\left|1-\tau\lambda_j\right|}; \tag{11}$$

$$\Omega_{4M}(k) = \max_{1\leq j\leq p}\frac{\tau\lambda_j \cdot \left[1-\left(1-\tau\lambda_j\right)^{2k}\right]}{2-\tau\lambda_j}. \tag{11}$$

Анализируя (11), видим, что функция $\Omega_{3M}(k)$ (в отличие от (7)) – монотонна и максимальна только при $\tau\lambda \to 2$. Кроме того, при $\tau\lambda < 2$ эта функция ограничена при любых k и, в пределе, равна

$$\lim_{k\to\infty}\Omega_{3M}(k)=\frac{\tau\lambda}{1-|1-\tau\lambda|}. \tag{13}$$

Более того, в диапазоне $\tau\lambda=0-1$ данная функция не превышает значения единицы при любых k, то есть

$$\Omega_{3M}(k)\le 1,\quad 0\le\tau\lambda\le 1,\quad 1\le k\le\infty. \tag{14}$$

Для каждой конкретной матрицы $\hat{A}$ функция $\Omega_{3M}(k)$ максимальна при $\tau\lambda=\tau\lambda_M$, где λ_M – максимальное собственное число матрицы.

Из анализа (12), видим, что $\Omega_{4M}(k)$ также монотонна и максимальна только при $\tau\lambda\to 2$. При $\tau\lambda<2$ функция $\Omega_{4M}(k)$ ограничена для любых k и, в пределе, равна

$$\lim_{k\to\infty}\Omega_{4M}(k)=\frac{\tau\lambda}{2-\tau\lambda}. \tag{15}$$

Аналогично выше рассмотренной $\Omega_{3M}(k)$ функция $\Omega_{4M}(k)$ в диапазоне $\tau\lambda=0-1$ не превышает значения единицы при любых k, то есть

$$\Omega_{4M}(k)\le 1,\quad 0\le\tau\lambda\le 1,\quad 1\le k\le\infty. \tag{16}$$

Для каждой конкретной матрицы $\hat{A}$ функция $\Omega_{4M}(k)$ так же максимальна при $\tau\lambda=\tau\lambda_M$.

Таким образом, выбирая параметр τ из условия $\tau\lambda_M\le 1$, получим следующую максимальную оценку для результирующей ошибки округления (10)

$$\left|r_i^{(k)}\right|_{\max}\le 3\sigma_\varepsilon+|\xi_\varepsilon|\cdot p. \tag{17}$$

Более того, применение типов округления, дающих центрированные локальные ошибки $(\xi_\varepsilon=0)$, позволяет значительно уменьшить величину результирующих ошибок округления.

В таблице 1 приведены вероятностные характеристики результирующих ошибок округления, полученных для различных видов округления и представления двоичных чисел в различных кодах (прямом, обратном и дополнительном).

Таблица 1.

Вероятностные характеристики результирующих ошибок округления для вычислительного алгоритма с округлением входной величины

		$b>0$		
		$T(b^n), T(b^o), T(b^\partial)$	$A(b^n), A(b^o), A(b^\partial)$	$R(b^n), R(b^o), R(b^\partial)$
$\left\|r_i^{(k)}\right\| \le$ $i=\overline{1,p}$	$\tau\lambda_M \le 2$	$\left(\sqrt{3\Omega_{4M}} + p\cdot\Omega_{3M}\right)\frac{\varepsilon_0}{2}$	$\sqrt{3\Omega_{4M}}\cdot\varepsilon_0$	$\sqrt{3\Omega_{4M}}\cdot\frac{\varepsilon_0}{2}$
	$\tau\lambda_M \le 1$	$\left(\sqrt{3}+p\right)\frac{\varepsilon_0}{2}$	$\sqrt{3}\cdot\varepsilon_0$	$\frac{\sqrt{3}}{2}\cdot\varepsilon_0$
	$\tau\lambda_M \le \frac{1}{2}$	$(1+p)\frac{\varepsilon_0}{2}$	ε_0	$\frac{\varepsilon_0}{2}$

		$b<0$				
		$T(b^n), T(b^o),$ $T(b^\partial)$	$A(b^n),$ $A(b^\partial)$	$A(b^o)$	$R(b^n),$ $R(b^\partial)$	$R(b^o)$
$\left\|r_i^{(k)}\right\| \le$ $i=\overline{1,p}$	$\tau\lambda_M \le 1$	$\left(\sqrt{3}+p\right)\frac{\varepsilon_0}{2}$	$\sqrt{3}\cdot\varepsilon_0$	$\left(\sqrt{3}+p\right)\cdot\varepsilon_0$	$\frac{\sqrt{3}}{2}\cdot\varepsilon_0$	$\left(\sqrt{3}+2p\right)\frac{\varepsilon_0}{2}$
	$\tau\lambda_M \le \frac{1}{2}$	$(1+p)\frac{\varepsilon_0}{2}$	ε_0	$(1+p)\cdot\varepsilon_0$	$\frac{\varepsilon_0}{2}$	$(1+p)\cdot\varepsilon_0$

Анализ полученных в табл. 1 оценок позволяет сделать следующие выводы:

- предложенный вычислительный алгоритм позволяет для всех типов округления соответствующим выбором шага итерации ограничить величину результирующих ошибок округления на заданном уровне;
- применение в алгоритме округлений, дающих центрированные локальные ошибки округления $(\xi_\varepsilon = 0)$, позволяет значительно уменьшить величину результирующих ошибок округлений;
- наименьшую результирующую ошибку округления дает применение R-округления в прямом и дополнительном кодах, дающего центрированные локальные ошибки округления с наименьшей дисперсией. При этом если задать τ из условия $\tau\lambda_M \le \frac{1}{2}$, то величина результирующей ошибки округления не будет превышать значения локальной ошибки округления $\frac{\varepsilon_0}{2}$ для любого числа шагов вычисления.

Выводы

Предложен метод аналитического выделения результирующих ошибок округления при решении методом простой итерации СЛАУ, к которым сводится решение многих задач. На основании предложенного метода проведен теоретический анализ известных вычислительных алгоритмов, а также показана малая их пригодность для решения плохо обусловленных СЛАУ на вычислителях с фиксированной запятой и с ограниченной разрядностью. Предложен и теоретически исследован вычислительный алгоритм с округлением входной величины, позволяющий ограничить накопление результирующих ошибок округления на заданном уровне путем выбора соответствующего значения параметра τ. Показана возможность ограничения (с помощью предложенного вычислительного алгоритма) результирующих ошибок

округления на уровне локальной ошибки округления, соответствующей значению единицы младшего разряда округляемого двоичного числа.

Список литературы

1. Рапопорт, Э.Я. Анализ и синтез систем управления с распределенными параметрами: Учебн. пособие / Э.Я. Рапопорт // М.: Высш. шк. – 2005. – 292 с.
2. Рапопорт, Э.Я. Оптимальное управление системами с распределенными параметрами / Я.Э. Рапопорт // М.: Высшая школа. – 2009. – 680 с.
3. Самарский, А.А Численные методы математической физики / А.А. Самарский, А.В. Гулин // М.: «Научный мир». –2003. — 316 с.
4. Желнов, Ю.А. Точностные характеристики управляющих вычислительных машин / Ю.А. Желнов // М.: Энергоатомиздат. – 1983. – 136 с.
5. Тарасенко, В.П. Основы компьютерной арифметики / В.П. Тарасенко, В.И. Корнейчук. – К.: Корнейчук, 2002. – 176 с.
6. Соренков, Э.И. Точность вычислительных устройств и алгоритмов / Э.И. Соренков, А.И. Телига, А.С. Шаталов // М.: Машиностроение. –1976. – 200 с.
7. Приклонский, В. И. Численные методы / В.И. Приклонский. – МГУ.: Физфак, 1999. – 146 с.
8. Амосов, А.А. Вычислительные методы для инженеров / А.А. Амосов, Ю.А. Дубинский, Н.В. Копченов. – Издательство МЭИ, 2003. – 544 с.

ПРО ОДИН МЕТОД ОРГАНІЗАЦІЇ ОБЧИСЛЮВАЛЬНОГО ПРОЦЕСУ ПРИ РІШЕННІ СИСТЕМ ЛІНІЙНИХ АЛГЕБРАЇЧНИХ РІВНЯНЬ МЕТОДОМ ПРОСТОЇ ІТЕРАЦІЇ

С.А. Положаєнко, А.Г. Кісєль, І.Ю. Голіков

Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна; e-mail: polozhaenko@mail.ru

Виконано аналіз чисельного рішення СЛАУ на обчислювачах з фіксованою комою. Показано, що точність результату обчислень залежить від процедури організації обчислювального процесу. Наведено аналітичну оцінку точності обчислень відомих обчислювальних процедур, що збігається з результатами практичного дослідження останніх. Запропоновано алгоритм обчислень, що дозволяє обмежити нагромадження помилок округлень на заданому рівні. Виконано аналітичний аналіз результуючих помилок округлення запропонованого алгоритму. Наведено умови, що забезпечують обмеження нагромадження зазначених помилок на заданому рівні.

Ключові слова: СЛАР, метод простої ітерації, обчислювальний алгоритм, помилки округлення, максимальні імовірнісні оцінки.

ABOUT ONE METHOD OF COMPUTING PROCESS IN SOLVING SYSTEM OF LINEAR EQUATIONS BY FIXED-POINT ITERATION

S.A. Polozhaenko, A.G. Kisel, I.Yu. Golikov

Odessa national polytechnic university,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: polozhaenko@mail.ru

The analysis of the numerical solution of SLAE in the fixed-point calculators was done. There is shown that the accuracy of calculation results depend on procedure of the organization of the computing process. The article gives an analytical estimation of accuracy of calculations known computational procedures, which coincides with the results of practical research of the latter. Proposed the computing algorithm allows to limit the accumulation of the rounding errors at specified level. Was performed analytical analysis of the rounding errors of the proposed algorithm. It is given conditions that provides limiting accumulation of indicated errors at a given level.

Keywords: SLAE, fixed-point iteration, computing algorithm, rounding errors, maximum probabilistic estimation.

УДК 621.311:656.212.4

Informatics and Mathematical Methods in Simulation
Vol. 6 (2016), No. 2, pp. 155-163

МАТЕМАТИЧНА МОДЕЛЬ СПОЖИВАННЯ ПАЛИВА МОДЕРНІЗОВАНИМ МАНЕВРОВИМ ТЕПЛОВОЗОМ

О.В. Рудковський

Український державний університет залізничного транспорту,
вул. Фейербаха, 7, Харків, 61050, Україна; e-mail: Od.is@rambler.ru

Наведено результати статистичної обробки експлуатаційних даних споживання палива для «гарячого» простою та виконання маневрової роботи модернізованим маневровим тепловозом ЧМЕ3М. Розроблено математичну модель витрати палива маневровим тепловозом. Запропонована математична модель може бути застосована для оцінки життєвого циклу модернізованого маневрового тепловоза ЧМЕ3М в частині споживання палива для виконання експлуатаційної роботи.

Ключові слова: маневровий тепловоз, експлуатація, маневрова робота, витрата палива, математична модель

Актуальність теми

Вирішення проблеми оновлення тягового рухомого складу залізниць України повинно носити комплексний характер та включати як його повну заміну (переважно зразками нового покоління), так і його модернізацію з подовженням терміну експлуатації [1]. Такий підхід дозволяє планово та практично без болю ліквідувати кризи залізничної галузі.

Одним з рішень щодо оновлення парку маневрових тепловозів стала комплексна модернізація тепловоза ЧМЕ3 з установкою дизеля Caterpillar потужністю на номінальному режимі 970 кВт.

Ключовим питанням при виборі варіанту оновлення тепловозів за цих обставин є фактична витрата палива для виконання експлуатаційної роботи.

Огляд досліджень

В роботах [2, 3] для визначення питомої витрати дизельного палива (кг/год) тепловозом ЧМЕ3 при виконанні маневрової роботи в якості математичної моделі пропонується поліном другого ступеня, застосування якого ґрунтується на обробці статистичних даних експлуатації.

В роботі [4] наведено багатофакторну математичну модель витрати палива тепловозом ЧМЕ3 при роботі на маневровій горці при різних умовах експлуатації, а саме: структурою потягу за кількістю та типами вантажних вагонів і рівнем їх завантаженості.

Визначення таким чином витрати дизельного палива не становить складності і може, дійсно, використовуватися для орієнтовних підрахунків, як це пропонується авторами, але такий підхід не достатньо точно враховує особливості маневрового тепловоза, що пройшов комплексну модернізацію за рахунок оснащення сучасним силовим енергетичним обладнанням.

Мета роботи

Метою статті є виклад результатів обробки статистичних даних витрати палива маневровим тепловозом ЧМЕ3, який було комплексно модернізовано сучасним силовим енергетичним обладнанням, та подальшим складанням математичної моделі споживання палива з урахуванням виконаної статистичної обробки.

Основна частина

Тепловоз ЧМЕ3М є продуктом комплексної модернізації тепловоза серії ЧМЕ3, від якого перейнято головну раму та ходову частину тепловоза. Зміни в цих вузлах пов'язано з встановленням на тепловозі нових агрегатів так, що, по суті, вище головної рами тепловоз повністю відновлено.

На тепловозі розташовано привідний агрегат, який складається із двигуна внутрішнього згоряння, тягового та допоміжного генератора змінного струму. На локомотиві встановлено двигун внутрішнього згоряння CAT 3508B з заданою потужністю 970 кВт. Регулювання потужності здійснюється за допомогою електронного регулятора.

Спостереження за споживанням палива модернізованим маневровим тепловозом ЧМЕ3М здійснювалось протягом 80 робочих змін. Протягом окремої і-ої робочої зміни тепловоз знаходився у наступних характерних експлуатаційних станах:

- холодний простій;
- гарячий простій;
- виконання маневрової роботи.

Тривалість знаходження у стані протягом і-ої робочої зміни складав відповідно $\tau_i^{x.n.}$, $\tau_i^{г.n.}$, $\tau_i^{м.р.}$ годин. Загальний час робочих змін за період спостереження споживання палива локомотивом складав $\sum_{i=1}^{i=80}(\tau_i^{x.n.}+\tau_i^{г.n.}+\tau_i^{м.р.})=1015,4$ годин. Протягом цього періоду модернізований маневровий тепловоз 56,22 % часу знаходився у стані холодного простою, 4,62 % – у стані гарячого простою, 39,16 % – у стані виконання маневрової роботи. Слід також відзначити, що окремі робочі зміни за період спостереження складалися з трьох вказаних станів локомотива (кількість таких робочих змін 37), а окремі – з двох, а саме: холодний простій та виконання маневрової роботи (кількість таких робочих змін 43). Такі варіанти складу робочих змін склали відповідно 42,33% та 57,67 % робочого часу табл. 1.

Таблиця 1.

Розподіл тривалості стану локомотива протягом робочої зміни за період спостереження

Варіант складу робочої зміни за станами локомотива	Кількість робочих змін	Стан локомотива протягом робочої зміни, %			Разом
		холодний простій	гарячий простій	виконання маневрової роботи	
А	37	19,72	4,62	17,99	42,33
В	43	36,51	-	21,16	57,67
Разом	80	56,22	4,62	39,16	100,00

Зрозуміло, що протягом знаходження у холодному простої маневровий тепловоз паливо не використовує. Тому цей стан було виключено зі спостереження споживання палива тепловозом. Таким чином, протягом і-ої робочої зміни спостерігалась загальна

витрата палива маневровим тепловозом, яка складається з витрати палива для гарячого простою $G_i^{г.п.}$ та для виконання маневрової роботи $G_i^{м.р.}$ і визначається за формулою

$$G_i^{заг} = G_i^{г.п.} + G_i^{м.р.}. \quad (1)$$

Витрата палива локомотивом у гарячому простої визначається годинною витратою палива дизельною установкою на режимі холостого ходу $b_{x.x.}$ та тривалістю і-ої робочої зміни $\tau_i^{г.п.}$ і визначається за формулою

$$G_i^{г.п.} = b_{x.x} \cdot \tau_i^{г.п.}. \quad (2)$$

Підставляючи вираз (2) у формулу (1) отримаємо

$$G_i^{заг} = b_{x.x} \cdot \tau_i^{г.п.} + G_i^{м.р.}. \quad (3)$$

Витрату палива маневровим тепловозом для виконання маневрової роботи $G_i^{м.р.}$ можна дослідити за умови варіанту В складу робочої зміни (табл. 1), для якого характерним є відсутність гарячого простою.

Залежність витрати палива маневровим тепловозом ЧМЕ3М від тривалості виконання маневрової роботи протягом і-ої робочої зміни (за варіантом відсутності гарячого простою) наведено на рис. 1.

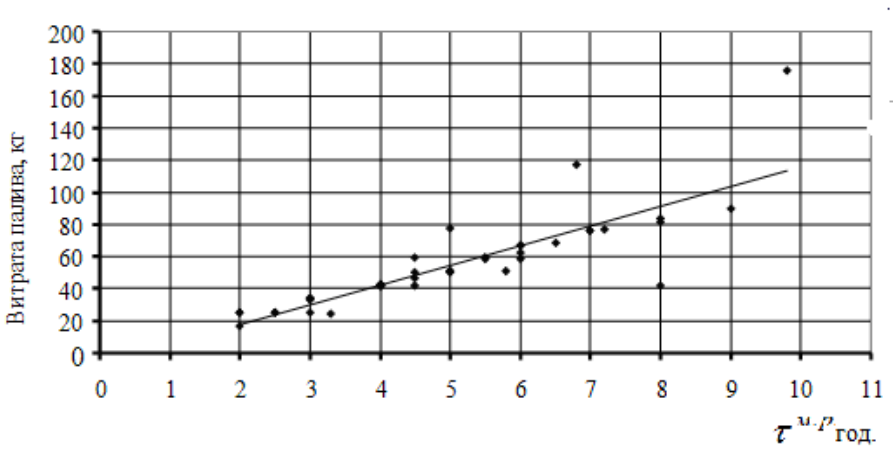


Рис. 1. Залежність витрати палива маневровим тепловозом ЧМЕ3М від тривалості виконання маневрової роботи протягом і-ої робочої зміни (за варіантом відсутності гарячого простою)

Наведена залежність витрати палива від тривалості виконання маневрової роботи модернізованим маневровим тепловозом ЧМЕ3М протягом і-ої робочої зміни (за варіантом відсутності гарячого простою) апроксимується наступною залежністю

$$G_i^{м.р.} = 12{,}29 \cdot \tau_i^{м.р.} - 6{,}766\ , \quad (4)$$

де $\tau_i^{м.р.}$ – тривалість виконання маневрової роботи модернізованим маневровим тепловозом ЧМЕ3М, яка знаходиться в межах $2 \le \tau_i^{м.р.} \ge 9{,}8$ годин протягом і-ої робочої зміни (за варіантом відсутності гарячого простою).

Тривалість виконання маневрової роботи модернізованим маневровим тепловозом ЧМЕ3 (за варіантом відсутності гарячого простою) за час дослідження (43 робочі зміни) склала $\sum_{i=1}^{i=43}\tau_i^{м.р.} = 214,9$ годин. За цей час модернізованим маневровим тепловозом ЧМЕ3М фактично було використано $\sum_{i=1}^{i=43}G_i^{м.р.} = 2350,14$ кг палива, тобто фактична середньо-експлуатаційна питома витрата палива для виконання маневрової роботи модернізованим маневровим тепловозом ЧМЕ3М складає $b_{м.р.}^{ф} = \frac{2350,14}{214,9} = 10,94$ кг/год. За розрахунком з використанням формули (4) за відповідний час тривалості маневрової роботи за робочими змінами модернізованим маневровим тепловозом ЧМЕ3М (за варіантом відсутності гарячого простою) було використано $\sum_{i=1}^{i=43}G_i^{м.р.} = \sum_{i=1}^{i=43}(12,29\cdot\tau_i^{м.р.} - 6,766) = 2350,18$ кг палива, тобто розрахункова середньо-експлуатаційна питома витрата палива для виконання маневрової роботи модернізованим маневровим тепловозом ЧМЕ3М складає $b_{м.р.}^{р} = \frac{2350,18}{214,9} = 10,94$ кг/год. Це вказує на достатню адекватність отриманої залежності витрати палива від тривалості виконання маневрової роботи модернізованим маневровим тепловозом ЧМЕ3М протягом і-ої робочої зміни (за варіантом відсутності гарячого простою).

З формули (3) та з урахуванням залежності (4) отримаємо вираз, який дозволяє визначити середньо-експлуатаційну годинну витрату палива тепловозом на режимі холостого ходу під час гарячого простою протягом:

- і-ої робочої зміни

$$b_{x.x_i}^{ф} = \frac{G_i^{заг} - G_i^{м.р.}}{\tau_i^{г.п.}} = \frac{G_i^{заг} - (12,29\cdot\tau_i^{м.р.} - 6,766)}{\tau_i^{г.п.}}; \qquad (5)$$

- всього періоду спостереження

$$b_{x.x}^{ф} = \frac{\sum_{i=1}^{i=37}(G_i^{заг} - (12,29\cdot\tau_i^{м.р.} - 6,766))}{\sum_{i=1}^{i=37}\tau_i^{г.п.}}. \qquad (6)$$

За результатами даних спостереження за формулою (6) було отримано середньо-експлуатаційну годинну витрату палива тепловозом на режимі холостого ходу під час гарячого простою $b_{x.x}^{ф} = 3,42$ кг/год. За технічним паспортом годинна витрата палива модернізованим тепловозом на режимі холостого ходу складає 4,2 л/год або 3,45 кг/год (густина зимового виду палива дорівнює 0,822 г/см^3 при середній температурі навколишнього середовища під час проведення спостережень $+8^0$ С), що, підтверджується фактичними даними спостереження в експлуатації.

Таким чином, остаточно отримаємо математичну модель споживання палива модернізованим маневровим тепловозом ЧМЕ3М протягом і-ої робочої зміни

$$G_i^{заг} = 3,42\cdot\tau_i^{г.п.} + 12,29\cdot\tau_i^{м.р.} - 6,766, \qquad (7)$$

при обмежені $\tau_i^{х.п.} + \tau_i^{г.п.} + \tau_i^{м.р.} \le 12$,

де $\tau_i^{x.n.}$ – тривалість холодного простою модернізованого маневрового тепловоза ЧМЕ3 протягом і-ої робочої зміни, год.; $\tau_i^{г.п.}$ – тривалість гарячого простою модернізованого маневрового тепловоза ЧМЕ3 протягом і-ої робочої зміни, знаходиться в межах $0{,}5 \le \tau_i^{г.п.} \ge 5{,}0$ годин; $\tau_i^{м.р.}$ – тривалість виконання маневрової роботи маневровим тепловозом протягом і-ої робочої зміни, знаходиться в межах $2 \le \tau_i^{м.р.} \ge 9{,}8$ годин; 12 – тривалість робочої зміни, год.

Рисунок 2 дає змогу оцінити адекватність отриманої математичної моделі споживання палива маневровим тепловозом ЧМЕ3М фактичним даним експлуатації.

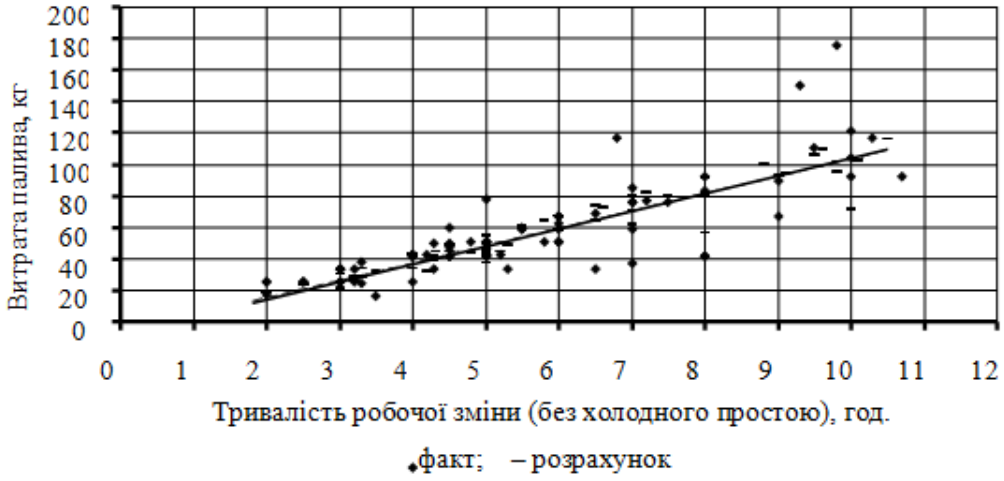


Рис. 2. Адекватність математичної моделі споживання палива маневровим тепловозом ЧМЕ3М фактичним даним експлуатації

Висновки

Загальна тривалість знаходження модернізованого маневрового тепловоза ЧМЕ3М у стані гарячого простою та виконання маневрової роботи за весь час спостереження склала 444,5 годин. За цей час тепловозом фактично було використано 4505,78 кг палива. За розрахунком з використанням математичної моделі (7) з урахуванням тривалості гарячого простою та виконання маневрової роботи за відповідними робочими змінами модернізованим маневровим тепловозом ЧМЕ3М було використано 4505,73 кг палива, Це вказує на достатню адекватність отриманої математичної моделі споживання палива маневровим тепловозом ЧМЕ3М фактичним даним експлуатації. Розроблену математичну модель може бути застосовано для оцінки життєвого циклу модернізованого маневрового тепловоза ЧМЕ3М в частині споживання палива для виконання експлуатаційної роботи.

Список літератури

1. Комплексна програма оновлення залізничного рухомого складу України на 2008-2020 роки: Наказ Міністерства транспорту та зв'язку України від 14 жовтня 2008 року № 1259.
2. Болжеларський, Я.В. Досвід і проблеми нормування палива на маневрову роботу в умовах Львівської залізниці / Я.В. Болжеларський, О.М. Гончаров // Залізничний транспорт України. – 2007. – №2. – С. 71 – 72.
3. Інструкція по технічному нормуванню витрат електричної енергії і палива локомотивами на тягу поїздів ЦТ-0059.: затверджено наказом Укрзалізниці від 5.03.2003 р. № 62-Ц. – Київ : Укрзалізниця, 2003. – 86 с.
4. Калабухін, Ю.Є. Застосування методології планування експерименту для математичного моделювання витрат палива маневровим тепловозом / Ю.Є. Калабухін // Інформаційно-керуючі системи на залізничному транспорті. Харків: УкрДАЗТ. – 2009. – №5-6. – С. 90-92.
5. Овчинников, В.М. О снижении расхода дизельного топлива в маневровой работе / В.М. Овчинников, С.А. Пожидаев, В.В., Скрежендевский // Энергоэффективность. – 2010. – №10 (134). – С. 147 . – 159.
6. Львовский, Е.Н. Статистические методы построения эмпирических формул: Учебное пособие для вузов / Е.Н. Львовский // М.: Высшая школа – 1982. – 224 с.
7. Закс, Л. Статистическое оценивание /Л. Закс // М.: Статистика. – 1976. – 598 с.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПОТРЕБЛЕНИЯ ТОПЛИВА МОДЕРНИЗИРОВАННЫМ МАНЕВРОВЫМ ТЕПЛОВОЗОМ

О.В. Рудковский

Украинский государственный университет железнодорожного транспорта,
ул. Фейербаха, 7, Харьков, Украина; e-mail: Od.ia@rambler.ru

Приведены результаты статистической обработки эксплуатационных данных потребления топлива для «горячего» простоя и выполнения маневровой работы модернизированным маневровым тепловозом ЧМЭ3М. Разработана математическая модель расхода топлива маневровым тепловозом. Предложенная математическая модель может быть использована для оценки жизненного цикла модернизированного маневрового тепловоза ЧМЭ3М в части потребления топлива для выполнения эксплуатационной работы.

Ключевые слова: маневровый тепловоз, эксплуатация, маневровая работа, расход топлива, математическая модель.

MATHEMATICAL MODEL OF FUEL CONSUMPTION BY THE MODERNIZED SHUNTING LOCOMOTIVE

O.V. Rudkovskiy

Ukrainian state university of railway transport,
Str. Feuerbach, 7, Kharkov, Ukraine; e-mail: Od.ia@rambler.ru

Results of statistical processing of operational data of fuel consumption for "hot" idle time and performance of shunting work as the modernized shunting locomotive ЧМЭ3М are given. The mathematical model of fuel consumption is developed by a shunting locomotive. The offered model can be used as the making mathematical model of life cycle of the modernized shunting locomotive ЧМЭ3М regarding of fuel consumption for operational work performance.

Keywords: shunting locomotive, operation, shunting work, fuel consumption, mathematical model.

УДК 519.71

Informatics and Mathematical Methods in Simulation
Vol. 6 (2016), No. 2, pp. 161-172

ПЕРЕМЕШИВАНИЕ И ЦИКЛЫ В НЕЛИНЕЙНЫХ ДИСКРЕТНЫХ СИСТЕМАХ С ХАОТИЧЕСКОЙ ДИНАМИКОЙ

И.М. Скринник

Одесский национальный политехнический университет,
пр. Шевченко, 1, Одесса, 65044, Украина; e-mail: anton_dora@mail.ru

В статье развивается метод перемешивания, сформулированный при участии автора ранее. Введено понятие уровней перемешивания. Показана возможность нахождения неизвестных наперед циклов заданной длины путем локальной стабилизации этих циклов. Приведены примеры.

Ключевые слова: нелинейные дискретные системы, управление хаосом

Введение

Впервые понятие управление хаосом было введено в работе [1], где также была сформулирована концепция стабилизации неустойчивых периодических орбит нелинейных систем малыми контролирующими воздействиями. Позднее были предложены другие методы управления, наиболее популярным из которых оказался метод Пирагаса [2]. Суть этого метода – введение линейной обратной связи с запаздыванием, величина которого равна периоду. Метод Пирагаса завоевал популярность, в первую очередь, из-за своей конструктивной простоты. В дальнейшем этот метод развивался и обобщался во многих работах, например в [3-6]. В [7, 8] для стабилизации периодических орбит было предложено использование нелинейной обратной связи с несколькими запаздываниями, величины которых пропорциональны периоду. Далее в [9] сформулирован метод перемешивания предыдущих состояний системы или функций этих состояний. Управление по принципу нелинейной запаздывающей обратной связи можно рассматривать как частный случай метода перемешивания.

Цель работы состоит в развитии алгоритмов, предложенных в [9], для определения неизвестных циклов путем их локальной стабилизации.

Задача*:* усовершенствовать алгоритмы выбора структуры и параметров системы управления для определения циклов заданной длины.

Постановка задачи и предварительные результаты

Пусть задана векторная нелинейная дискретная система вида

$$x_{n+1} = f(x_n),\ x_n \in R^H,\ n = 1, 2, \ldots, \tag{1}$$

у которой имеется один или несколько неустойчивых T - циклов $(\eta_1, \ldots, \eta_T)$, где все векторы $\eta_1, \ldots, \eta_T$ различны, и $\eta_{j+1} = f(\eta_j),\ j = 1, \ldots, T-1,\ \eta_1 = f(\eta_T)$.

Мультипликаторы $\mu_1,\ldots,\mu_H$ рассматриваемых неустойчивых циклов определяются, как собственные значения произведений матриц Якоби $\prod_{j=1}^{T} f'(\eta_j)$ размерностей H.

Требуется построить систему вида

$$x_{n+1} = \sum_{j=1}^{M} \gamma_j f\left(\sum_{i=1}^{N} \alpha_{ij} x_{n-iT+T} \right), \tag{2}$$

в которой все (или хотя бы некоторые) T- циклы будут локально асимптотически устойчивыми. Считается выполненными условия нормировки: $\sum_{j=1}^{M} \gamma_j = 1$, $\sum_{i=1}^{N} \alpha_{ij} = 1,\ j = 1,\ldots,N,\ \gamma_j \geq 0,\ \alpha_{ij} \geq 0$.

Коэффициенты оптимального перемешивания

Условие устойчивости T- цикла системы (2) состоит в том, что все корни уравнения

$$\prod_{j=1}^{H} \left(\lambda^{1+(N-1)T} - \mu_j \left(a_1 \lambda^{N-1} + \ldots + a_N \right)^T \right) = 0, \tag{3}$$

должны лежать в центральном единичном круге. Соответственно, задача управления хаосом в системе (1) путем перемешивания значений состояния системы и функций от этих значений в предшествующие моменты времени формулируется следующим образом:

- для заданной длины цикла T и заданного множества локализации мультипликаторов найти коэффициенты внутреннего перемешивания $\alpha_{ij},\ i = 1,\ldots,N,\ j = 1,\ldots,M$, и внешнего перемешивания $\gamma_j,\ j = 1,\ldots,M$, так, чтобы цикл длины T был бы локально асимптотически устойчивым; при этом величина используемой предыстории должна быть минимально возможной. Заметим, что решение поставленной задачи зависит от области локализации мультипликаторов $\{\mu_1,\ldots,\mu_H\}$. Повторим алгоритм нахождения минимального N и оптимальных коэффициентов $\{a_1,\ldots,a_N\}$, сформулированный в [9];
- вычисляются узлы: $\psi_j = \dfrac{\pi(\sigma + T(2j-1))}{\sigma + (N-1)T}$, $j = 1,2,\ldots,\dfrac{N-2}{2}$, если N – чётное, $j = 1,2,\ldots,\dfrac{N-1}{2}$, если – нечётное; при этом в случае $\{\mu_1,\ldots,\mu_H\} \in \{\mu \in R : \mu \in (-\mu^*, 1)\}$ следует полагать $\sigma = 2$, а в случае $\{\mu_1,\ldots,\mu_H\} \in \{\mu \in C : |\mu + R| < R\}$ – $\sigma = 1$;
- строятся полиномы $\eta_N(z) = z(z+1)\prod_{j=1}^{\frac{N-2}{2}} \left(z - e^{i\psi_j}\right)\left(z - e^{-i\psi_j}\right)$, если N – чётное, $\eta_N(z) = z\prod_{j=1}^{\frac{N-1}{2}} \left(z - e^{i\psi_j}\right)\left(z - e^{-i\psi_j}\right)$, если N – нечётное;
- вычисляются коэффициенты полинома $\eta_N(z) = \sum_{j=1}^{N} c_j z^j$;

- определяются оптимальные коэффициенты $a_j = \dfrac{\left(1-\dfrac{1+(j-1)T}{2+(N-1)T}\right)c_j}{\sum\limits_{j=1}^{N}\left(1-\dfrac{1+(j-1)T}{2+(N-1)T}\right)c_j}$, $j=1,\ldots,N$;
- в случае $\{\mu_1,\ldots,\mu_H\}\in\{\mu\in R:\mu\in(-\mu^*,1)\}$ вычисляются величины $I_N^{(T)}=\left[\dfrac{T}{2+(N-1)T}\prod\limits_{k=1}^{\frac{N-2}{2}}ctg^2\dfrac{\pi(2+T(2j-1))}{2(2+(N-1)T)}\right]^T$ при N – чётном, $I_N^{(T)}=\left[\prod\limits_{k=1}^{\frac{N-1}{2}}ctg^2\dfrac{\pi(2+T(2j-1))}{2(2+(N-1)T)}\right]^T$ при N – нечётном; оптимальное значение N вычисляется, как минимальное натуральное число, удовлетворяющее неравенству $\mu^*\le\dfrac{1}{\left|I_N^{(T)}\right|}$;
- в случае $\{\mu_1,\ldots,\mu_H\}\in\{\mu\in C:|\mu+R|<R\}$ вычисляются величины $I_N^{(T)}=\left[\dfrac{T}{1+(N-1)T}\prod\limits_{k=1}^{\frac{N-2}{2}}\cot^2\dfrac{\pi(1+T(2j-1))}{2(1+(N-1)T)}\right]^T$ при N – чётном, $I_N^{(T)}=\left[\prod\limits_{k=1}^{\frac{N-1}{2}}\cot^2\dfrac{\pi(1+T(2j-1))}{2(1+(N-1)T)}\right]^T$ при N – нечётном; оптимальное значение N вычисляется, как минимальное натуральное число, удовлетворяющее неравенству $R\le\dfrac{1}{2\left|I_N^{(T)}\right|}$.

Если оптимальные коэффициенты найдены, то коэффициенты перемешивания можно найти из системы

$$\begin{pmatrix}\alpha_{11} & \alpha_{12} & \ldots & \alpha_{1M}\\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2M}\\ \ldots & \ldots & \ldots & \ldots\\ \alpha_{N1} & \alpha_{N2} & \ldots & \alpha_{NM}\end{pmatrix}\begin{pmatrix}\gamma_1\\ \gamma_2\\ \ldots\\ \gamma_M\end{pmatrix}=\begin{pmatrix}a_1\\ a_2\\ \ldots\\ a_N\end{pmatrix}, \qquad (4)$$

К системе (4) необходимо добавить условия нормировки $\sum\limits_{j=1}^{M}\gamma_j=1$, $\sum\limits_{i=1}^{N}\alpha_{ij}=1,\ j=1,\ldots,N,\ \gamma_j\ge 0,\ \alpha_{ij}\ge 0$.

Примеры применения метода перемешивания

Рассмотрим несколько частных случаев.

Пусть $M = N$ и $\alpha_{ij} = \delta_{ij}$, где δ_{ij} – символ Кронекера. Тогда, из (4) получаем, что $\gamma_j = a_j$, $j = 1, \ldots, N$. Система (2) примет вид $x_{n+1} = \sum_{j=1}^{M} a_j f\left(x_{n-jT+T}\right)$. Система управляется с помощью внешнего перемешивания [8].

Пусть $M = 1$, тогда $\gamma_1 = 1$, и $\alpha_{i1} = a_i$, $i = 1, \ldots, N$. Система (2) примет вид $x_{n+1} = f\left(\sum_{i=1}^{N} a_i x_{n-iT+T}\right)$. Система управляется с помощью внутреннего перемешивания [9].

Пусть $M = N+1$; $\alpha_{i1} = a_i$, $i = 1, \ldots, N$; $\alpha_{i,i+1} = 1$, $i = 1, \ldots, N$; $\alpha_{ij} = 0$, при $j \neq 1,\ j \neq i+1,\ i = 1, \ldots, N,\ j = 1, \ldots, N+1$. Тогда система (2) примет вид

$$x_{n+1} = \gamma_1 f\left(\sum_{i=1}^{N} a_i x_{n-iT+T}\right) + \sum_{j=1}^{N} \gamma_{j+1} f\left(x_{n-jT+T}\right).$$

Определим оптимальные значения коэффициентов внешнего перемешивания $\gamma_1, \ldots, \gamma_{N+1}$. Система (9) в этом случае примет вид

$$\begin{pmatrix} a_1 & 1 & 0 & \ldots & 0 \\ a_2 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_N & 0 & \ldots & \ldots & 1 \end{pmatrix} \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \ldots \\ \gamma_{N+1} \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ \ldots \\ a_N \end{pmatrix}.$$

Общее решение этой системы представляется, как сумма частного решения неоднородной системы и общего решения однородной

$$\begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \ldots \\ \gamma_{N+1} \end{pmatrix} = \begin{pmatrix} 0 \\ a_1 \\ \ldots \\ a_N \end{pmatrix} + c \begin{pmatrix} 1 \\ -a_1 \\ \ldots \\ -a_N \end{pmatrix}.$$

С учетом того, что $\gamma_j \geq 0,\ j = 1, \ldots, N+1$, получаем $0 \leq c \leq 1$. Окончательно система (2) примет вид

$$x_{n+1} = c\, f\left(\sum_{i=1}^{N} a_i x_{n-iT+T}\right) + (1-c) \sum_{j=1}^{N} a_j f\left(x_{n-jT+T}\right), \tag{5}$$

где $0 \leq c \leq 1$. Система управляется с помощью смешенного перемешивания. При $c = 0$ переходим к внешнему перемешиванию, а при $c = 1$ – к внутреннему. Системы вида (5) возникают, например, при исследовании диффузионного хаоса [11].

Кратные циклы

В этом разделе речь пойдет о возможности управления хаосом путем стабилизации lT - циклов с помощью перемешивания, определяемого динамической системой (2), $l = 2, 3, \ldots$.

Каждая из точек T-цикла является неподвижной точкой T- итерации отображения f: $x_{n+1} = f^{(T)}(x_n)$, $f^{(T)}(x_n) = f(f^{(T-1)}(x_n))$, $f^{(0)}(x_n) = f(x_n)$.

Вопрос об устойчивости цикла сводится к вопросу об устойчивости неподвижных точек отображения $f^{(T)}$, которые составляют цикл длины T. Отметим, что величина мультипликатора цикла не зависит от выбора неподвижной точки, входящей в рассматриваемый цикл, и неподвижные точки отображения $f^{(T)}$ также являются неподвижными точками отображения $f^{(T_1)}$, если $T_1 = lT$ (l - целое число).

Таким образом, задачу стабилизации T_1- цикла системы (1) можно свести к задаче стабилизации T - цикла системы $x_{n+1} = f^{(l)}(x_n)$, $x_n \in R^H$, $n = 1, 2, \ldots$.

Перемешивание будем организовывать следующим образом:

- перемешивание первого уровня: $\sum_{i=1}^{N} \alpha_i x_{n-iT+T}$;
- перемешивание второго уровня: $\sum_{j=1}^{M} \beta_j f\left(\sum_{i=1}^{N} \alpha_{ij} x_{n-iT+T}\right)$;
- перемешивание третьего уровня: $\sum_{j_1=1}^{M_1} \gamma_{j_1} f\left(\sum_{j_2=1}^{M_2} \beta_{j_2} f\left(\sum_{i=1}^{N} \alpha_{i j_2 j_1} x_{n-iT+T}\right)\right)$.

Перемешивание более высоких уровней определяется аналогично.

Таким образом, система управления для стабилизации цикла длины $2T$ представима следующим образом

$$x_{n+1} = \sum_{j_1=1}^{M_1} \gamma_{j_1} f\left(\sum_{j_2=1}^{M_2} \beta_{j_2} f\left(\sum_{i=1}^{N} \alpha_{i j_2 j_1} x_{n-iT+T}\right)\right), \qquad (6)$$

В системе (6) все коэффициенты должны удовлетворять условиям нормировки, т.е. должны определять выпуклые комбинации.

Коэффициенты перемешивания можно рассматривать как компоненты тензоров. Для стабилизации циклов длины lT система управления должна состоять из $l+1$ уровня перемешивания, внешний уровень определяется вектором коэффициентов перемешивания размерности M_1, следующий l уровень определяется матрицей коэффициентов перемешивания размерности $M_2 \times M_1$, и т.д. каждый уровень определяется тензором коэффициентов соответствующего порядка. Все тензоры должны удовлетворять условиям свертки, при которых последовательное сворачивание тензоров коэффициентов от первого уровня перемешивания до $l+1$ уровня должно давать вектор оптимальных коэффициентов $\begin{pmatrix} a_1 \\ \ldots \\ a_N \end{pmatrix}$.

Ясно, что оптимальные коэффициенты перемешивания не всегда определяются единственным образом. Например, одной из возможных систем стабилизации цикла длины $2T$ может служить система

$x_{n+1} = c_1 \sum_{j=1}^{N} a_j f\left(f\left(x_{n-jT+T}\right)\right) + c_2 f\left(\sum_{j=1}^{N} a_j f\left(x_{n-jT+T}\right)\right) + c_3 f\left(f\left(\sum_{j=1}^{N} a_j x_{n-jT+T}\right)\right)$, где $c_1 \geq 0$, $c_2 \geq 0$. $c_3 \geq 0$, $c_1 + c_2 + c_3 = 1$.

Отметим важные отличия предложенного в статье метода стабилизации от большинства известных методов. Управление применяется во все моменты времени, а не только в окрестности желаемого цикла – сам цикл заранее знать нет необходимости! Более того, одно управление позволяет стабилизировать сразу ВСЕ циклы заданной

длины с мультипликаторами, лежащими в левой полуплоскости, вещественными или комплексными. Для стабилизации конкретного цикла достаточно, чтобы последовательность начальных точек оказалась в бассейне притяжения этого цикла. Разные начальные последовательности будут порождать последовательности решений, сходящиеся к разным циклам заданной длины.

Одним из возможных применений предлагаемого метода является проверка наличия периодических орбит заданного нелинейного отображения, неустойчивые орбиты можно обнаружить путем их стабилизации.

Определение циклов в системе «внезапного хаоса»

Рассмотрим отображение [10] $f(x)=(1+\sqrt{2})\left(\frac{1}{2}-\left|x-\frac{1}{2}\right|\right)+x$,

порождающее динамическую систему «внезапного возникновения хаоса» (SOC).

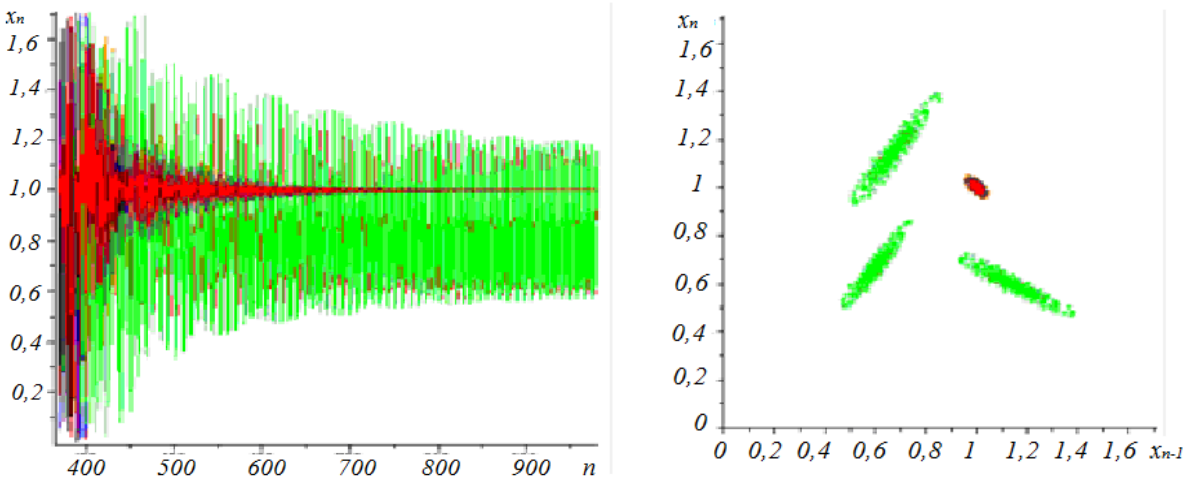
$$x_{n+1}=f(x_n), \tag{7}$$

Для системы (7) инвариантным является множество $\left[0,1+\frac{\sqrt{2}}{2}\right]$; положением равновесия – точка $z=1$.

Определим 9-цикл системы SOC. В системе управления

$$x_{n+1}=f\left(f\left(f\left(\sum_{j=1}^{N}a_j x_{n-jT+T}\right)\right)\right), \tag{8}$$

положим $T=3,\ N=11,$
$\{a_1,\ldots,a_{11}\}=\{0.276,0.168,0.127,0.102,0.084,0.070,0.058,0.046,0.036,0.024,0.009\}$.



а **б**

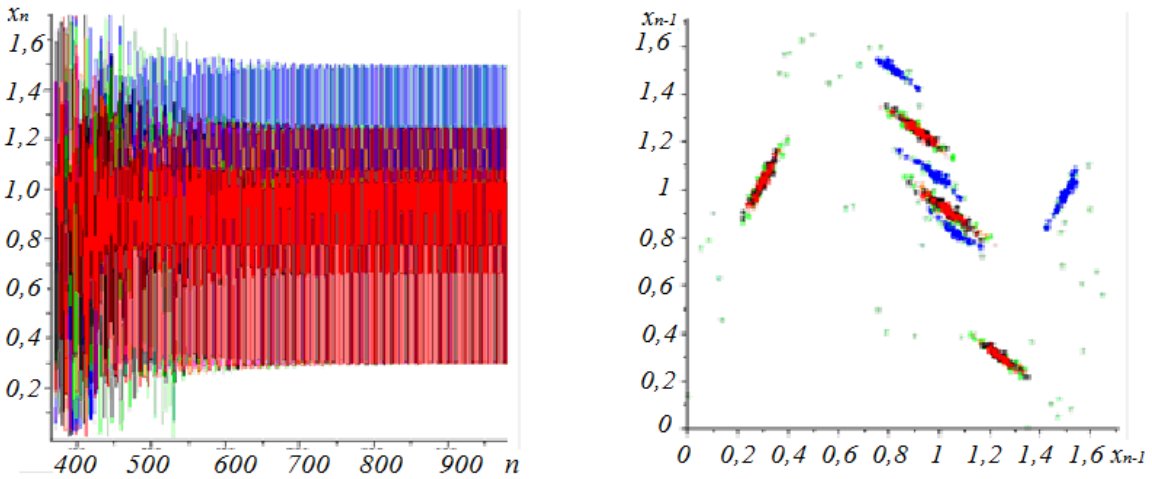
Рис. 1. Динамика решений системы (8) при $T=3,\ N=11$; а – в плоскости (n,x_n); б – в плоскости (x_{n-1},x_n)

В системе управления (8) наблюдается локально устойчивое положение равновесия, которое также является положением равновесия исходной системы (6), и локально устойчивый 3-цикл $\{1.142,0.598,0.667\}$. Этот 3-цикл определяет 9-цикл для системы (8): $\{1.142,0.799,1.285,0.598,1.570,0.194,0.667,1.478,0.326\}$.

Для определения 12-цикла системы (7) применим систему

$$x_{n+1} = f\left(f\left(\sum_{j=1}^{N} a_j f\left(x_{n-jT+T}\right)\right)\right), \tag{9}$$

при $T = 4,\ N = 11,$
$\{a_1,\ldots,a_{11}\} = \{0.361, 0.165, 0.113, 0.087, 0.069, 0.057, 0.047, 0.039, 0.031, 0.022, 0.009\}.$

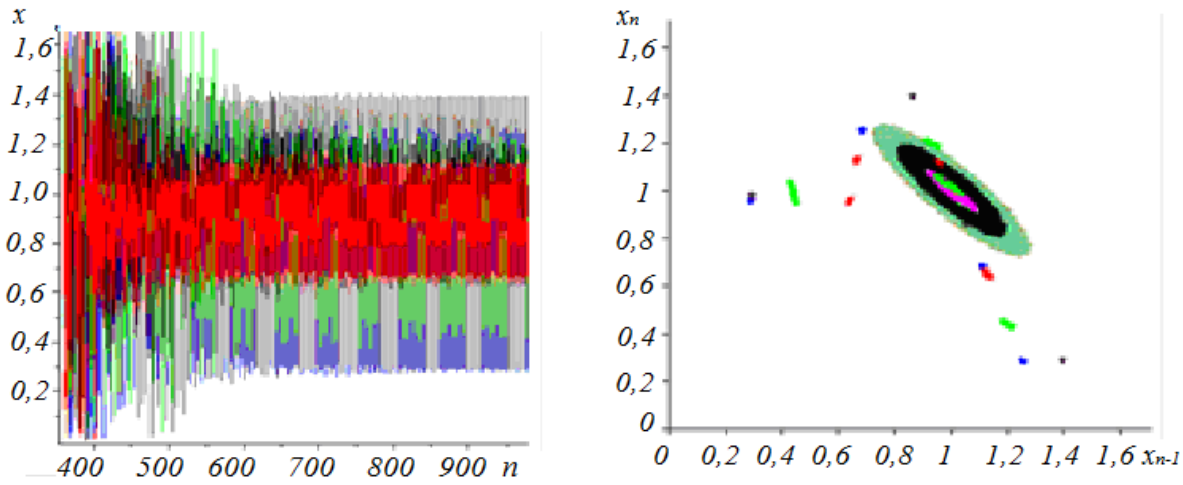


а **б**

Рис. 2. Динамика решений системы (9); а – в плоскости (n, x_n); б – в плоскости (x_{n-1}, x_n)

В системе (9) можно наблюдать два локально устойчивых 4-цикла. Они являются частью 12-цикла исходной системы (7):
$\{1.031, 0.956, 1.062, 0.912, 1.124, 0.824, 1.248, 0.649, 1.497, 0.297, 1.016, 0.978\}$.

Вообще говоря, с ростом длины цикла T, количество таких циклов увеличивается. Бассейны притяжения некоторых циклов могут оказаться настолько малыми, что практически такие циклы отыскать будет затруднительно. Пусть, например, необходимо отыскать циклы длины 15. Выберем несколько начальных точек и рассмотрим их динамику, происходящую в соответствие с уравнением $x_{n+1} = f\left(f\left(f\left(x_n\right)\right)\right)$. Возьмем 400 итераций этой системы, и на 401 шаге запустим процесс перемешивания. При этом положим $T = 5,\ N = 26,$ и коэффициенты перемешивания выберем в соответствие с формулами пункта 2. На рис. 3 изображена динамика решений системы при разных начальных значениях. При некоторых начальных значениях траектории будут притягиваться к циклам длины 5: при $x_0 = 0.99$ получаем цикл $\{0.989, 1.025, 0.929, 1.198, 0.440\}$; при $x_0 = 0.64$ получаем цикл $\{0.290, 0.982, 1.049, 0.860, 1.396\}$; при $x_0 = 0.5$ и $x_0 = 0.74$ получаем цикл $\{1.127, 0.640, 0.958, 1.119, 0.665\}$; при $x_0 = 0.21$ $\{0.960, 1.112, 0.683, 1.252, 0.287\}$. Эти четыре 5-циклов порождают четыре различных 15-циклов исходной системы (7). Приведем их:
$\{0.989, 1.509, 0.280, 1.025, 0.963, 1.052, 0.929, 1.100, 0.859, 1.198, 0.719, 1.397, 0.440, 1.501, 0.291\}$
$\{0.290, 0.991, 1.013, 0.982, 1.025, 0.965, 1.049, 0.930, 1.099, 0.860, 1.198, 0.720, 1.396, 0.440, 1.502\}$
$\{1.127, 0.820, 1.254, 0.640, 1.509, 0.281, 0.958, 1.059, 0.916, 1.119, 0.832, 1.237, 0.665, 1.474, 0.330\}$
$\{0.960, 1.056, 0.921, 1.112, 0.842, 1.224, 0.683, 1.448, 0.367, 1.252, 0.644, 1.504, 0.287, 0.981, 1.027\}$



а **б**

Рис. 3. Динамика решений системы (8): а – в плоскости (n, x_n); б – в плоскости (x_{n-1}, x_n)

Выводы

В статье предложен метод определения наперед неизвестных неустойчивых циклов дискретных систем с хаотической динамикой. Подход для решения задачи основан на локальной стабилизации циклов с использованием вспомогательной системы управления, построенной на перемешивании координат предыстории или функций этих координат, так что вспомогательная система может иметь несколько уровней перемешивания. Отметим, однако, что использование различных уровней перемешивания не позволяет уменьшить длину предыстории, необходимую для стабилизации цикла. Но, что важно, может увеличивать скорость сходимости к этому циклу. Кроме того, использование внутреннего перемешивания (перемешивания первого уровня) существенно сокращает объем вычислений, т.к. отпадает необходимость вычислять значение функции, которая задает динамическую систему, большее число раз, чем в системе без перемешивания. Также мы надеемся, что использование перемешивания первого уровня облегчит физическую реализацию предложенной схемы управления хаосом в нелинейных дискретных системах.

Список литературы

1. Ott, E. Controlling chaos. Phys. Rev / E. Ott , C. Grebodgi, J.A. Yorke. – 2000. – Lett. 64. – Pp. 1196 – 1199.
2. Pyragas, K. Continuous control of chaos by self-controlling feedback / K. Pyragas // Phys. – 1999. – Vol. 170. – 421 p.
3. Just, W. Control of chaos by time-delayed feedback: A survey of theoretical and experimental aspects / W. Just, H. Benner, E. Schoell // In: B. Kramer (Ed.), Advances in Solid State Physics. – 2003. – Vol. 43. – Springer, Berlin. – 589 p.
4. Hoevel, P. Control of unstable steady states by time-delayed feedback methods / P. Hoevel, E. Schoell // Phys. – 2005. – Rev. E. – Vol. 72.
5. Vieira, D.S. Controlling chaos using nonlinear feedback with delay / D.S. Vieira, A.J. Lichtenberg // Phys.Rev. – 2001. – E 54, Pp. 1200–1207.
6. Morgul, O. On the stability of delayed feedback controllers / O. Morgul. // Phys. – 2003. – Lett. A 314. –Pp. 278 – 285.

7. Dmitrishin, D. Methods of harmonic analysis in nonlinear dynamics / D. Dmitrishin, A. Khamitova // Comptes Rendus Mathematique. –2013. – Vol. 351. – Issues 9-10. – Pp. 367 –370.
8. Dmitrishin, D. Fejer polynomials and Chaos / D. Dmitrishin, A. Khamitova, A. Stokolos // Springer Proceedings in Mathematics and Statistics. – 2014. – Pp. 49 – 75.
9. Дмитиришин, Д. Перемешивание как способ управления хаосом / Д. Дмитиришин, И. Скринник // Информатика и математические методы моделирования. – 2016. –Т.1. – №1. – С. 11-18.
10. Tian, L. Predictive control of sudden occurrence of chaos/ L. Tian, G. Dong // Int. J. Nonlinear Science. – 2008 – 5(2), Pp. 99-105.
11. Oono, Y. Descret model of chemical turbulence. / Y. Oono, M. Kohmoto //Phys. Rev. Lett. – 2001. –Vol. 55. – No. 27. – Pp. 2927 – 2931.

ПЕРЕМІШУВАННЯ ТА ЦИКЛИ У НЕЛІНІЙНИХ ДИСКРЕТНИХ СИСТЕМАХ З ХАОТИЧНОЮ ДИНАМІКОЮ

І.М. Скринник

Одеський національний політехнічний університет,
пр. Шевченка, 1, Одеса, 65044, Україна; e-mail: anton_dora@mail.ru

У статті розвивається метод перемішування, сформульований за участю автора раніше. Введено поняття рівнів перемішування. Показана можливість знаходження невідомих наперед циклів заданої довжини шляхом локальної стабілізації цих циклів. Наведені приклади.
Ключові слова: нелінійні дискретні системи, управління хаосом.

MIXING AND CYCLES IN LINEAR DISCRETE SYSTEMS WITH CHAOTIC DYNAMICS

I.M. Skrinnik

Odessa national polytechnic university,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: anton_dora@mail.ru

The article develops the mixing method. The concept of mixing levels. The possibility of finding unknown prescribed lengths of cycles by the local stabilization of these cycles. Examples.
Keywords: linear discrete systems, chaos control.

УДК 004.9:371.261

Informatics and Mathematical Methods in Simulation
Vol. 6 (2016), No. 2, pp. 173-183

УЧЕТ МЕЖФРАЗОВЫХ СВЯЗЕЙ ПРИ АВТОМАТИЗИРОВАННОМ ПОСТРОЕНИИ ТОЛКОВОГО СЛОВАРЯ ПРЕДМЕТНОЙ ОБЛАСТИ

А.Б. Кунгурцев, А.И. Гаврилова, А.С. Леонгард, Я.В. Поточняк

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: abkun@te.net.ua

Предложены алгоритмы и информационная технология выявления межфразовых связей в процессе построения словарей предметной области. Разработанные решения позволяют повысить качество толкового словаря и сократить время на его формирование, что имеет большое значение для создания и развития информационных систем.

Ключевые слова: межфразовые связи, анафора, термин, словарь предметной области

Введение

В соответствии с [1] под толковым словарем предметной области (СПО) будем понимать специализированный словарь, дающий определение множеству понятий, связанных с деятельностью некоторой организационной структуры. Толковый словарь оказывается очень полезным при решении различных задач, связанных с созданием и развитием информационных систем, подготовкой кадров, созданием новой документации, четким распределением обязанностей между сотрудниками.

Каждая запись в словаре представляет одно слово или устойчивое для данной предметной области словосочетание («термин»), для которого приведено толкование, специфическое для данной предметной области, а также список синонимов.

Анализ литературных данных и формулировка задач исследования

Выбор терминов для толкового словаря происходит на основании частоты их появления в анализируемом тексте. При этом, в известных на данный момент работах [1-3] не учитывались межфразовые связи (МС). В качестве примера рассмотрим два предложения: Жесткий диск является основным запоминающим устройством для большинства персональных компьютеров. Обычно он содержит несколько пластин, покрытых слоем ферромагнитного материала, которые вращаются со скоростью в несколько тысяч оборотов в минуту. Здесь словосочетание «Жесткий диск» может быть определено как термин в рассматриваемой предметной области. Однако, без учета МС анализатор текста отметит только одно появление данного термина, тогда как фактически их два, поскольку во втором предложении местоимение «он» замещает термин «жесткий диск». Это может привести к ошибкам при решении вопроса о включении выявленного термина в словарь.

Подробное описание, подходы и особенности систем для разрешения анафоры на английском языке можно найти в работе [4], однако задача разрешения анафоры недостаточно исследована для русского языка, а также имеет свои особенности, ввиду

чего существует лишь небольшое количество систем, с различным успехом справляющимися с данной задачей.

В работе [5], сделана попытка построения алгоритма выделения МС в некотором тексте, однако представленный в работе подход нецелесообразен в рамках СПО, где требуется осуществить поиск анафоры при известном термине. Предложенная в [6] программа является коммерческой разработкой, которая в качестве синтаксического анализатора также использует коммерческий продукт. Поэтому отсутствует информация как об алгоритме выделения МС, так и об оценке эффективности программы. В работе [7] в методике разрешения кореференции рассмотрены только 3 группы местоимений – личные, возвратные и относительное, тогда как на практике часто используются также уточняющие прилагательные и порядковые числительные.

Система построения СПО выдвигает требования, которые ограничивают, и в то же время дополняют задачу учета МС, связанную с восстановлением частоты появления термина в тексте, что отличает данную систему разрешения кореференции от других ей аналогичных, делает ее более мобильной и быстрой.

На основании изложенного можно сформулировать следующие задачи исследования:

- анализ возможных типов МС и выделение тех, которые должны быть обнаружены при построении СПО;
- определение частот появления МС выделенных типов в текстах различного вида с целью обоснования целесообразности использования механизма выявления МС при построении СПО;
- создание формализованного описания процесса определения МС в текстах;
- разработка алгоритмов и программного обеспечения для выявления МС и соответствующей корректировки СПО.

Определение межфразовых связей, которые должны учитываться при построении словаря

Приведем определение некоторых понятий.

Межфразовая связь – это связь между предложениями, абзацами, главами и другими частями текста, организующая его смысловое и структурное единство. Для реализации межфразовой связи используются синтаксические повторы, синонимы, анафорические местоимения, слова с временным и пространственным значением и т.д.

Анафора – лингвистическое явление, когда интерпретация некоторого выражения (анафорическое выражение) зависит от другого выражения, которое, встречалось в тексте ранее анафорического выражения (антецедент), либо находится после него (постцедент).

Анафора считается частным случаем такого явления, как «дейксис». Согласно [8], дейктическим является такой элемент, который выражает идентификацию объекта – предмета, места, момента времени, свойства, ситуации – через его отношение к речевому акту, его участникам или контексту. В работе [9] говорится: «дейксис является базисным явлением, нежели анафора, а анафора в некотором смысле производна от дейксиса». Данное утверждение объясняется тем, что в то время, как дейксису характерно изменение фокуса внимания, анафоре характерно его сохранение.

Рассмотрим общую классификацию анафор для анализа возможности их использования при построении СПО, приведенную в работе [10].

1. По корреляционному расположению. Если в предыдущем предложении или ранее в рассматриваемом предложении найден 1 и более антецедентов, согласованных в роде, числе и падеже с анафорой, значит, анафора – ретроспективная.

Если антецедент найден в том же предложении, что и анафора, и следует после нее, значит, анафора – проспективная (катафора).

2. По позиции относительно предложения. Если в одном и том же предложении найден и антецедент, и анафора, значит, анафора – внутрисентенциальная. Если в предложении найдена только анафора, а антецедент – в предшествующих предложениях, значит, анафора – дискурсивная.

3. По формальной выраженности. Если в предложении анафора выражена в виде слова, значит, анафора имеет полную форму. Если в предложении нет слова, которое представляет анафору, и предложение – неполное (напр. отсутствует подлежащее, есть только сказуемое), а в предыдущем предложении есть антецедент (подлежащее), согласованный в роде и числе со сказуемым в последнем предложении, то перед нами нулевая анафора.

4. По наличию лексического компонента. Если анафора состоит только из анафорического местоимения, анафора – простая (я, это, они). Если анафора состоит из именной группы, содержащей местоимения в приименном употреблении (эта комната, такие сооружения и т.п.), анафора – составная.

5. По лексико-грамматическому классу. Если анафора выражена личным или указательным местоимением, значит, анафора – местоименная. Если анафора выражена именной группой или существительным, синонимичным по значению с антецедентом, значит, анафора – именная. Если анафора явно отсутствует, но исходя из контекста можно заключить, что она присутствует, и это выражается в виде неполного предложения, где отсутствует сказуемое, такая анафора – глагольная.

6. По вербальному описанию антецедента. Если антецедент явно указан в тексте, значит, анафора – эксплицитная. Если вербальное описание антецедента в тексте отсутствует или анафора представляет собой довольно значительные фрагменты текста различного синтаксического статуса, значит, анафора – имплицитная.

7. По степени полноты. Полная анафора означает прямой повтор наименования референта и служит для выражения отношения тождества между референтами двух наименований.

При частичной анафоре второе обозначение отличается от первого, представляя собой, например, согласованное в роде и числе местоимение, его синоним, или гипероним, соотносящийся с гипонимом.

Ассоциативная анафора предполагает наиболее широкие возможности выбора анафорического обозначения, поскольку логико-смысловые отношения, лежащие в её основе (метонимические, метафорические), могут быть чрезвычайно разнообразными. В следующем примере слова металлу и пластику являются отсылочными компонентами, ассоциирующимися с материалами изготовления антецедента жесткий диск.

Научные сотрудники института высшей математики и программирования Израиля заявили, что через 2 года жесткий диск превратится в мягкий накопитель информации. Носители будущего будут изготавливаться из материалов, противоположных металлу и пластику.

Конкретная анафора может относится одновременно к различным видам приведенной классификации. Рассмотрим два предложения.

Устройство позиционирования головок (жарг. актуатор) представляет из себя малоинерционный соленоидный двигатель. Он состоит из неподвижной пары сильных неодимовых постоянных магнитов, а также катушки (соленоид) на подвижном кронштейне блока головок.

Анафора он является ретроспективной (1), дискурсивной (2), эксплицитной (6), простой (4), местоименной (5), частичной выраженности (7) и имеет полную форму 0 (3).

Анализ различных видов МС с точки зрения их применимости при построении СПО предусматривает определение следующих характеристик МС:

- соответствие решаемой задаче;

- возможность формализации процесса определения анафоры в тексте;
- частота встречаемости в тексте, влияющая на качество СПО.

При определении соответствия МС решаемой задаче были удалены из дальнейшего рассмотрения следующие виды анафор:

- полная (предусматривает повторение ранее приведенного определения (возможно, термина из СПО); её учет не влияет на частоту использования термина);
- глагольная (термин в СПО непосредственно действие не обозначает);
- именная (в анафоре используется именная группа или существительное, которые могут быть ранее определенным термином или его синонимом);
- составная (то же, что и именная анафора, но с возможными сопутствующими ей указательными местоимениями);
- ассоциативная (при данном типе анафоры присутствует семантическая связь между словами и отсутствуют местоимения);
- проспективная (редко встречаемый вид, используется преимущественно в художественной литературе);

При определении возможности формализации следует исходить из следующего:

- имеется ли формальная возможность определить предложение, которое содержит анафору;
- имеется ли формальная возможность определить предложение, которое содержит антецедент или постцедент;
- имеется ли возможность связать анафору с термином путем использования морфологических атрибутов (часть речи, род, число, падеж) и синтаксических связей.

Используя указанные критерии из дальнейшего рассмотрения были удалены следующие типы анафоры:

- нулевая (нельзя точно выделить предложение, содержащее анафору);
- имплицитная (нельзя точно выделить предложение, содержащее антецедент или постцедент).

Таким образом, остались следующие типы МС, которые будут учтены при построении словаря предметной области:

1. Ретроспективная. Накопитель на жестком диске (HDD) относится к наиболее совершенным и сложным устройствам современных систем хранения цифровой информации, характеризующийся значимым объемом хранимой информации при низкой себестоимости. Однако, исходя из исследований доктора Бианки Шредер и Google, в силу своих конструктивных особенностей и элементов количество от- казов данного устройства после 3-го года работы стабильно увеличивается.
2. Полной формы. Операция дефрагментации должна быть отключена, так как она практически никак не влияет на производительность SSD-носителя и лишь дополнительно изнашивает его.
3. Местоименная (простая). Наследование — механизм языка, позволяющий описать новый класс на основе уже существующего (родительского, базового) класса или интерфейса. Оно является одним из основных принципов объектно-ориентированного программирования.
4. Эксплицитная. Все штрихкоды можно разделить на два типа: линейные и двухмерные. Первый – это код, который читается в одном направлении, характеризуется простой эксплуатацией и низкой себестоимостью.
5. Внутрисентенциальная. Функциональное программирование предполагает обходиться вычислением результатов функций от исходных данных и результатов других функций, и оно не предполагает явного хранения состояния программы.
6. Дискурсивная. Функциональное программирование предполагает обходиться вычислением результатов функций от исходных данных и результатов других функций, и не предполагает явного хранения состояния программы. Соответственно, не предполагает оно и изменяемость этого состояния.

Оценка частоты появления МС в текстах из различных предметных областей

Для определения влияния МС на качество СПО было проведено исследования 50 научно-популярных, публицистических и научных текстов объемом от 200 до 1500 слов на предмет выявления частоты появления МС.

В результате исследования установлено:

- различные виды анафор встречаются в текстах различной тематики в среднем 54,3 раз на 1000 слов;
- в публицистических и научно-популярных текстах – 54,1 раз на 1000 слов;
- в технических текстах – 35,6 раз на 1000 слов;
- в научно-технических текстах – 33,1 раз на 1000 слов.

При этом наиболее часто встречается местоименная анафора:

- в публицистических и научно-популярных текстах – 23,2 раз;

В научно-технических текстах местоименная анафора встречается 19,4 раза; в технических – 20,6 раз.

Учитывая, что при построении СПО слова и словосочетания, встречающиеся в анализируемых текстах в количестве 25 раз на 1000 слов, обычно принимаются в качестве терминов СПО, можно сделать вывод, что учет МС заметно изменит частотные характеристики терминов в СПО.

Результаты анализа видов МС и текстов приведены в табл. 1.

Таблица 1.

Оценка возможности использования МС при построении СПО

Классификация	Вид	Подлежит формализации	Высокая частота встречаемости	Соответствует решаемой задаче
По корреляционному расположению	Ретроспективная	+	+	+
	Проспективная	+	-	+
По позиции относительно предложения	Внутрисентен-циальная	+	+	+
	Дискурсивная	+	+	+
По формальной выраженности	Полная форма	+	+	+
	Нулевая	+	-	+
По наличию лексического компонента	Простая	+	+	+
	Составная	+	+	-
По лексико-грамматическому классу	Местоименная	+	+	+
	Именная	+	+	-
	Глагольная	-	-	-
По вербальному описанию антецедента	Эксплицитная	+	+	+
	Имплицитная	-	-	-
По степени полноты	Полная	+	+	-
	Частичная	+	+	+
	Ассоциативная	-	-	-

Формализация описания и выявления МС

Представим анализируемый текст S в виде множества предложений

$$S = \{S_i\} i = 1, n, \quad (1)$$

а каждое предложение – в виде последовательности элементов (слов и знаков препинания)

$$e_1, ..., e_l, .., e_m. \quad (2)$$

Каждый элемент будет характеризоваться текстом N и множеством атрибутов A

$e =< N, A >$

Определим некоторые из них. Пусть А1 представляет часть речи, А2 – число, А3 – род, А4 – лицо, А5 – падеж, А6 – время, А7 – залог, А8 – одушевленность.

Будем считать, что к началу процесса выявления МС завершился первый этап построения СПО. Представим каждую запись СПО в виде $d =< N, q >$,

где N – термин (слово или словосочетание); q - количество появления термина в тексте S.

В общем случае $N = \{e\}$.

Тогда СПО можно представить множеством записей:

$$D = \{d_j\} j = 1, k, \quad (3)$$

где k – количество терминов, обнаруженных в S (до процесса редактирования словаря).

Ведем определение принадлежности термина предложению $d_j \in_d S_i$.

Поскольку анализаторы текстов обычно не дают сведений о типе местоимения, то предложено ввести множество личных местоимений третьего лица, указательных и притяжательных местоимений, которые могут играть роль анафоры.

$M\,\mathrm{Pr} = \{он, она, оно, они, тот, этот, такой, таков, столько, свой, его, её, их\}$

Также необходимо ввести множество уточняющих прилагательных $MAdj$, порядковых числительных $MNum$

$$MAdj - \{указанный, данный, последний, ...\},$$

$$MNum = \{первый, второй, третий\},$$

В ходе анализа относительных местоимений, их изменяемости по введенным выше атрибутам, их было решено разделить на две группы, таким образом введем множество относительных местоимений, для которых условия проверок отличаются от условий проверок принадлежности $M\,\mathrm{Pr} - M\,\mathrm{Re}l\,\mathrm{Pr}$

$$M\,\mathrm{Re}l\,\mathrm{Pr} = \{кто, что, сколько\}.$$

Также дополним множество $M\,\mathrm{Pr}$ относительными местоимениями, проверки по атрибутам, для которых аналогичны элементам этого множества:

$M\,\mathrm{Pr} = \{он, она, оно, они, тот, этот, такой, таков, столько, свой, его, её, их,$

$который, какой, чей\}$

Рассмотрим ряд возможных ситуаций.

Ситуация 1. В предложении S_i обнаружен термин d_j, т. е.

$$\exists d_j \mid d_j \in_d S_i \wedge d_j \in D \tag{4}$$

Тогда следует искать МС сначала в данном предложении, а потом в следующем. Если предложение не содержит местоимений третьего лица, указательных и притяжательных местоимений, уточняющих прилагательных и порядковых числительных, то в нем нет анафор. Для этого осуществляем ряд проверок для каждого элемента предложения (2):

$$\begin{gathered} e_l \to A1 \neq pronoun \vee e_l \to A1 = pronoun \wedge e_l \to N \notin M\,\mathrm{Pr} \wedge N \notin M\,\mathrm{Re}\,l\,\mathrm{Pr} \\ e_l \to A1 \neq adjective \vee e_l \to A1 = adjective \wedge e_l \to N \notin MAdj \\ e_l \to A1 \neq numeral \vee e_l \to A1 = numeral \wedge e_l \to N \notin MNum \end{gathered} \tag{5}$$

Если в результате проверки каждого элемента предложения S_i результатом было только $true$, то делаем вывод, что это предложение S_i не содержит анафор. Аналогичный анализ производим для следующего предложения S_{i+1}. Если в этих предложениях в результате анализа также получен результат $true$, то можно сделать вывод об отсутствии МС между элементами предложений S_i и S_{i+1}. Тогда следует в соответствии с (4) проверить предложение S_{i+1} на вхождение в него термина из СПО.

Ситуация 2. В предложении S_i обнаружен термин (4), который в общем случае соответствует некоторой последовательности элементов предложения $d_j \to N = e_m e_{m+1} .... e_{m+k}$.

Также в этом предложении обнаружен некоторый элемент e_l, который может быть анафорой, т.е. результатом одной из проверок (5) было false.

Рассмотрим случай, когда термин является именной группой, содержащей опорное управляющее слово – имя существительное, которое нужно выявить. Пусть обнаружен элемент e_{nn}, такой что $e_{nn} \to A1 = noun \wedge e_{nn} \in \{e_m, e_{m+1}, \ldots, e_{m+k}\}$

Если антецедент и анафора находятся в одном предложении, то это предложение должно быть сложным. Антецедент будет находиться в одном простом предложении, а анафора в одном из следующих простых предложений. Записываем это условие. Существует $e_h \to punctuation \wedge h > (m+k) \wedge l > h$

Проверяем связь предполагаемых антецедента и анафоры. По результату проверок (8) получили $e_l \to A1 = pronoun \vee e_l \wedge e_l \notin M\,\mathrm{Re}\,l\,\mathrm{Pr} \to A1 = adjective \vee e_l \to A1 = numeral$.

Тогда условием выявления МС является

$$e_{nn} \to A2 = e_l \to A2 \wedge e_{nn} \to A3 = e_l \to A3 \tag{6}$$

Если $e_l \to A1 = pronoun \vee e_l \wedge e_l \in M\,\mathrm{Re}\,l\,\mathrm{Pr}$, тогда условиями для проверок являются

- e_l = 'кто', то для установления МС должно выполняться $e_{nn} \to A8 = animate$;
- e_l = 'что', то для установления МС должно выполняться $e_{nn} \to A8 = inanimate$;
- e_l = '*сколько*', то условие $e_{nn} \to A2 = e_l \to A2$.

(7)

Если термин состоит из одного слова, то это слово является элементом предложения e_{nn}.

Ситуация 3. В предложении S_i обнаружен термин (4) и не обнаружено кандидатов на анафору. В предложении S_{i+1} при отсутствии терминов обнаружены кандидаты на анафору, т.е такие элементы e_l, которые прошли проверки (5), и результат одной из проверок для каждого элемента оказался равным false.

Тогда соответствие между элементом – опорным словом термина e_{nn} и анафорой e_l нужно искать в соответствии с условиями проверок (6), (7). Кандидаты e_l, удовлетворившие данным условиям, считаем анафорами термина.

Ситуация 4. В предложении S_i обнаружено более одного термина (4) и обнаружен кандидат на анафору. Элемент e_l, являющийся кандидатом на анафору, проходит проверки на соответствие с каждым из терминов e_{nn} (6), (7). МС устанавливается с ближайшим e_{nn}, для которого e_l прошел проверку, после чего e_l уже не может быть анафорой для последующих терминов $e_{nn+1}, e_{nn+2}, \ldots$.

Ситуация 5. В предложении S_i обнаружено более одного термина (4) и обнаружено более одного кандидата на анафору. Каждый элемент e_l, являющийся кандидатом на анафору, проходит проверки на соответствие с каждым из терминов e_{nn} (6), (7). МС устанавливается между ближайшими $e_{nn} - e_l$, где e_l прошел проверки для e_{nn}, после чего e_l уже не может быть анафорой для последующих терминов $e_{nn+1}, e_{nn+2}, \ldots$, однако e_{nn} может далее рассматриваться как возможный референт для $e_{l+1}, e_{l+2}, \ldots$.

Ситуация 6. В предложении S_i обнаружено более одного термина (4) и обнаружено один или более одного кандидата на анафору. В предложении S_{i+1} обнаружен термин или более одного теримна и один или более кандидатов на анафору. В таком случае следует произвести проверки (6), (7) для элементов e_l из S_{i+1} – которые не прошли проверки на соответствие с терминами из S_{i+1} – на соответствие с терминами из S_i. МС устанавливается между ближайшими $e_{nn} - e_l$, где e_l прошел проверки для e_{nn}, аналогично ситуации 5.

Технология построения словаря с учетом МС

Технология предусматривает три основных этапа.

На первом этапе производится поиск терминов в некотором тексте. Поскольку число анафор в тексте значительно меньше числа терминов, то параллельно с их поиском определяется вхождение в текст слов из множеств:

$M\,\mathrm{Pr} = \{тот, этот, такой, таков, столько, свой, его, её, их\}$.

$MAdj - \{указанный, данный, последний, \ldots.\}$,

$MNum = \{первый, второй, третий\}$,

$M\,\mathrm{Re}l\,\mathrm{Pr} = \{кто, что, который, какой, чей, сколько\}$,

которые могут оказаться анафорами.

В анализируемый текст, представленный в формате .txt, перед каждой потенциальной анафорой вставляются метасимволы для её индексации.

На втором этапе после предварительного определения множества терминов выделяются предложения, которые предшествуют предложению с потенциальной

анафорой и предложения, которые содержат потенциальную анафору. В работе [5] для каждой анафоры текст просматривается в обратном направлении, в процессе чего составляется множество потенциальных антецедентов. Однако в виду того, что приоритетной задачей нашего алгоритма является не определение любого антецедента, а определения термина-антецедента, при разрешении анафоры в предложениях осуществляется поиск выделенных ранее терминов, и затем осуществляется поиск МС в соответствии с рассмотренными ранее ситуациями. Если анафора найдена, то производится корректировка частоты появления соответствующего термина в тексте.

На третьем этапе экспертом принимается решение об определении нижней частотной границы включения терминов в словарь.

Проведение экспериментов и анализ результатов

Для испытания предложенной технологии определения межфразовых связей была разработана методика определения эффективности выявления МС в текстах из различных предметных областей.

Методика предусматривает выполнение следующей последовательности действий:

- выбор текстов из некоторой предметной области;
- определение терминов (термин, количество вхождений в текст) в выбранных текстах;
- выявление МС с использованием предложенной технологии, определение ранее не учтенных вхождений терминов в текст;
- выявление МС в тех же текстах экспертом без использования предложенной технологии;
- определение ошибок при выявлении МС, которые были учтены в технологии;
- определение МС, которые не были учтены в технологии.

Результаты анализа изменения частотных характеристик терминов после учета МС с использованием предложенной технологии приведены в тал. 2.

Таблица 2.

Изменение частотных характеристик (числа вхождений) терминов

Тип текста и ссылки	Размер текстов (число слов)	Всего обнаружено МС	Термины	
			Всего (к-во)	Изменилось число вхождений на (%)
Электротехника [11], [12]	2500	69	61	11.6
Информатика [13]	2397	47	58	18.9
Энергетика [14]	4700	175	139	26.9
Экономика [15], [16]	5971	197	148	32.8
Юридические науки [17], [18]	3500	109	83	31.3

На основании анализа данных из табл. 2 можно сделать вывод, что учет МС существенно влияет на частотные характеристики терминов и должен быть реализован в технологии создания СПО.

Экспертом был проведен анализ текстов [11-18]. В результате было выявлено, что в автоматическом режиме не учтено 31 МС (учтенное количество МС равно 597), что составляет приблизительно 5% общего количества МС. Причинами ошибок являются синтаксические ошибки, опечатки, широкое использование слов на английском языке, сложная структура предложений с многочисленными вводными конструкциями. Учитывая особенности научных и технических текстов, такое количество ошибок допустимо.

Выводы

Показано, что существующие технологии построения СПО на основе анализа текстов не учитывают МС, что приводит к ошибкам в определении частотных характеристик терминов. Определены типы МС, которые должны быть выявлены при построении СПО. Дано математическое описание процесса определения МС. Разработана технология построения СПО с учетом МС и соответствующее программное обеспечение. Проведены эксперименты, которые подтвердили обоснованность теоретических положений и эффективность разработанной технологии и программного обеспечения.

Список литературы

1. Кунгурцев, А.Б. Метод автоматизированного построения толкового словаря предметной области/ А.Б. Кунгурцев, Я.В. Поточняк, Д.А. Силяев // Технологический аудит и резервы производства –2015. – № 2/2(22). – С. 58 – 63
2. Кунгурцев, А.Б. Застосування мереж фреймів для побудови моделі вилучення фактів з текстів на природній мові / А. Б. Кунгурцев, С. М. Бородавкін // Искусственный интеллект. – 2009. – №4.– С. 202 – 207.
3. Кунгурцев, А. Б. Метод построения словарей предметных областей для извлечения фактов из текстов на естественном языке/ А.Б. Кунгурцев, С.Н. Бородавкин, А.П. Голуб // Восточно-европейский журнал передовых технологий. – 2010. – № 1/4 (43). – С. 32 – 36.
4. Mitkov, R. Anaphora resolution: the state of the art / R. Mitkov // School of Languages and European Studies, University of Wolverhampton. – 1999. – С. 2 – 29
5. Malkovsky, M.G. A method for pronominal anaphora resolution in the course of syntactic analysis / M.G. Malkovsky, A.S. Starostin, I.A. Shilov // Proceedings of Sworld conference. – 2013. – С. 2 – 3
6. Bogdanov, A.V. Anaphora analysis based on ABBYY COMPRENO linguistic technologies / A.V. Bogdanov, S.S. Dzhumaev, D.A. Skorinkin, A.S. Starostin // Becasovo : 20th International Conference on Computational Linguistics "Dialog". – 2014. – С. 1 – 13
7. Ionov, M . The impact of morphology processing quality on automated anaphora resolution for Russian / M. Ionov, A. Kutuzov // Becasovo.: 20th International Conference on Computational Linguistics "Dialog". – 2014. – 3 с.
8. Падучева, Е.В. Семантические исследования/ Е.В. Падучева. // М.: Языки русской литературы. – 1996. – 464 с.
9. Кибрик, А.А. Человеческий фактор в языке: Коммуникация, модальность, дейксис / А.А. Кибрик // М.: Наука. – 1992. – 281 с.
10. Воронкова, А.В. Стратегии когнитивной обработки дискурсивной анафоры пропозитивно-именного типа / А.В. Воронкова. –2009. – С. 27 – 40
11. Зинченко, Е.Е. Методика расчета вентильных индукторно-реактивных двигателей / Е.Е. Зинченко, В.Б. Финкельштейн // Електротехніка і Електромеханіка. – 2009. – №4. – С. 24 – 29.
12. Мурашкин, С.И. Асинхронный частотный электропривод с векторным управление / С.И. Мурашкин // Вестник КрасГАУ. – 2012. – №9 – С. 189 – 196.

13. Проскуряков, Н.Е. Анализ и перспективы современных систем хранения цифровых данных / Н.Е. Проскуряков, А.Ю. Ануфриева // Известия Тульского государственного университета. Технические науки. – 2013. – №3 – С. 368 – 377.
14. Ушаков, В.Я. Основные проблемы энергетики и возможные способы их решения / В.Я. Ушаков // Известия Томского политехнического университета. – 2011 – Т. 319. – №4. – С. 5 – 13.
15. Оськина, Ю.Н. Обзор методик анализа финансовых результатов / Ю.Н. Оськина, Е.А. Баева // Социально-экономические явления и процессы. – 2013. - №4(050). – С.126 – 130.
16. Сысо, Т.Н. Оптимизация управления затратами предприятия / Т.Н. Сысо // Вестник Омского университета. Серия «Экономика». – 2011. – № 4. – С. 135 – 143.
17. Мальцева, Л.В. Преступность среди несовершеннолетних и ее предупреждение / Л.В.Мальцева // Общество: политика, экономика, право. – 2011. – № 4. – С.102 – 105.
18. Сафин, З.Ф. Понятие земель общего пользования и их правовой режим / З.Ф. Сафин, Э.Ф. Нигматуллина // Ученые записки Казанского государственного университета. – 2010. – Т. 152. – С. 141 – 148.
19. Kamenskaya, M.A. Data-driven methods for anaphora resolution of Russian texts // M. A. Kamenskaya, I.V. Khramoin, I.V. Smirnov // Becasovo: 20th International Conference on Computational Linguistics "Dialog". – 2014. – 8 с.
20. Protopopova, E.V Anaphoric annotation and corpus-based anaphora resolution: an experiment / E.V. Protopopova, A.A Bodrova, S.A. Volskaya et al. // Becasovo: 20th International Conference on Computational Linguistics "Dialog". – 2014. – 8 с.
21. Toldova, S.J. RU-EVAL-2014: Evaluating anaphora and coreference resolution for Russian / S. J. Toldova, A. Roytberg, A. A. Ladygina, M. D. Vasilyeva, I. L. Azerkovich, M. Kurzukov, G. Sim, D.V. Gorshkov, A. Ivanova, A. Nedoluzhko, Y. Grishina. – 2005. – 6 с.

ОБЛІК МІЖФРАЗОВИХ ЗВ'ЯЗКІВ ПРИ АВТОМАТИЗОВАНІЙ ПОБУДОВІ ТЛУМАЧНОГО СЛОВНИКА ПРЕДМЕТНОЇ ОБЛАСТІ

О.Б. Кунгурцев А.І. Гаврилова, А.С. Леонгард, Я.В. Поточняк

Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна; e-mail: abkun@te.net.ua

Запропоновано алгоритми та інформаційна технологія виявлення міжфразових зв'язків в процесі побудови словників предметної області. Розроблені рішення дозволяють підвищити якість тлумачного словника і скоротити час на його формування, що має велике значення для створення і розвитку інформаційних систем.

Ключові слова: міжфразовий зв'язкок, анафора, термін, словник предметної області.

ACCOUNTING OF INTER-PHRASE CONNECTIONS IN AUTOMATED DEVELOPMENT EXPLANATORY DICTIONARY OF SOME SUBJECT AREA

A. Kungurtsev, A. Gavrilova, A. Leonhard, Ia. Potochniak

Odessa national polytechnic university,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: abkun@te.net.ua

There was proposed an algorithm and information technology for detection of inter-phrase connections in a domain dictionary building process. Developed solution allows to increase quality of the dictionary and decrease it creation time. It has a big value for creation and development information systems.

Keywords: inter-phrase connections, anaphora, term, dictionary.

УДК 004.853

Informatics and Mathematical Methods in Simulation
Vol. 6 (2016), No. 2, pp. 184-192

АНАЛИЗ ЭВРИСТИЧЕСКОГО МЕТОДА ПОСТРОЕНИЯ БАЙЕСОВСКИХ СЕТЕЙ С ТОЧКИ ЗРЕНИЕ ПРОГРАММНОЙ РЕАЛИЗАЦИИ В РАМКАХ РАСШИРЯЕМОЙ АРХИТЕКТУРЫ

Е.Ю. Таран, В.Г. Пенко

Одесский национальный университет имени И.И.Мечникова,
ул. Дворянская, 2, Одесса, 65082, Украина; e-mail: e.taran@ukr.net

Данная статья содержит анализ одного из алгоритмов построения структуры байесовской сети (эвристический метод на основе данных) с точки зрения его программной реализации в рамках персональной мобильной экспертной системы. Алгоритм был реализован на платформе Android SDK. В статье предлагается подход к улучшению результатов рассмотренного алгоритма за счет взаимодействия с пользователем-экспертом. Применение этого подхода в ряде случаев приводит к улучшению структуры сети. В результате исследования разработана программная архитектура, реализующая рассмотренные алгоритмы и обладающая возможностью расширения для реализации других алгоритмов.

Ключевые слова: байесовская сеть, эвристический метод, взаимная информация, принцип описания минимальной длины, архитектура программной системы

Введение

Байесовская сеть – это вероятностная модель, представляющая собой множество переменных и их вероятностных зависимостей. Байесовские сети применяются для описания событий и процессов с неполной информацией и являются эффективным и быстроразвивающимся инструментом, используемым в интеллектуальном анализе данных. Вероятностный вывод на основе байесовской сети включает в себя множество различных алгоритмов. Но прежде, чем проводить соответствующие вычисления, необходимо вначале построить структуру байесовской сети, что представляет собой отдельную задачу, реализуемую нетривиальными алгоритмами. На данный момент существует немало подобных алгоритмов, большинство из которых описаны в виде формальных конструкций. Данная работа посвящена вопросам практической реализации таких алгоритмов в рамках программной системы, которая бы имела практическую пользу в широком диапазоне предметных областей. Практика разработки подобных систем свидетельствует о важности выработки общей архитектуры, которая бы позволила эффективно реализовать используемые алгоритмы в рамках текущих бизнес - ограничений, а также обеспечивала некоторую степень расширяемости.

Целью исследования является разработка программного обеспечения для мобильных устройств, обеспечивающего основные функции экспертной системы и использующей байесовские сети в качестве способа представления знаний и вероятностного вывода.

В данной статье рассматривается один из возможных алгоритмов построения байесовской сети на основе данных, а именно, эвристический метод, который описан в статье [1]. Основной задачей данной статьи является анализ этого алгоритма с той

степенью детализации, которая позволила бы осуществить его программную реализацию в рамках архитектуры, допускающей необходимую степень расширяемости и гибкости системы. Данный алгоритм планируется использовать для работы с байесовской сетью на мобильных устройствах планшетного типа, использующих ОС Android. В связи с этим далее будет рассматриваться различные аспекты реализации программы, с точки зрения языка реализации (Java), или более обобщенно, с точки зрения объектно-ориентированного подхода к разработке.

Архитектура программного обеспечения

Для возможности расширения архитектуры, а именно, добавления новых методов построения сети, изменения её структуры, подключения новых источников данных, повторного использования существующего кода, а также изменения интерфейса, была разработана архитектура, которая состоит из четырех основных модулей (рис. 1).

Модуль загрузки данных состоит из интерфейса AbstractDataSource, который имеет один метод – loadData, возвращающий поток данных. Этот интерфейс содержится в абстрактном классе структуры байесовской сети – AbstractBayesianNetwork. Для реализации конкретного источника данных, пользователю необходимо реализовать класс, имплементирующий этот метод, и потом добавить конкретную реализацию в структуру сети, после чего сеть будет получать данные из конкретного источника. Также в качестве источника данных могут выступать сенсоры мобильного устройства, которые после определенной обработки получаемых данных, могут быть основой для построения сети.

Модуль UI и взаимодействия с пользователем представляет различные реализации визуального пользовательского интерфейса, которые предоставляет Android SDK. Также в этом модуле содержатся классы, обеспечивающие необходимое для построения сети взаимодействие с пользователем.

В основе вершин лежат определенные события, между которыми строятся связи. Подготовленным для использования в сети набором данных является наблюдение – набор определенных событий, и их конкретных значений. Байесовская сеть в данной реализации работает с конкретным набором дискретных значений для каждого события. Основные концепции байесовских сетей были реализованы с помощью следующих базовых классов: BasicNode – вершина, Event – наблюдение, CaseTable – список наблюдений, EventWithNegation – событие с отрицанием и NodeProbabilityTable – таблица вероятностей вершин. Эти классы, которые могут использоваться для расчета вероятностей в процессе работы с сетью и на построение сети не влияют. Эти классы концептуально объединяет абстрактный класс байесовской сети – AbstractBayesianNetwork.

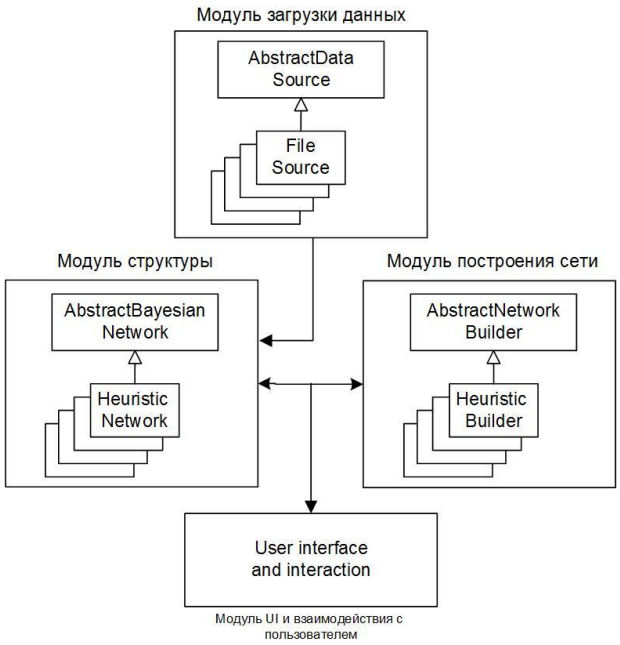


Рис. 1. Модульная диаграмма разработанного ПО

Для реализации различных методов построения сети используется интерфейс AbstractNetworkBuilder, который принимает на вход байесовсую сеть без определенной структуры и на основе наблюдений, которые представлены сети, возвращает сеть с установленными связями. На рис. 2 изображена диаграмма классов, составляющих основу приложения, и обеспечивающих возможность дополнения приложения конкретными реализациями.

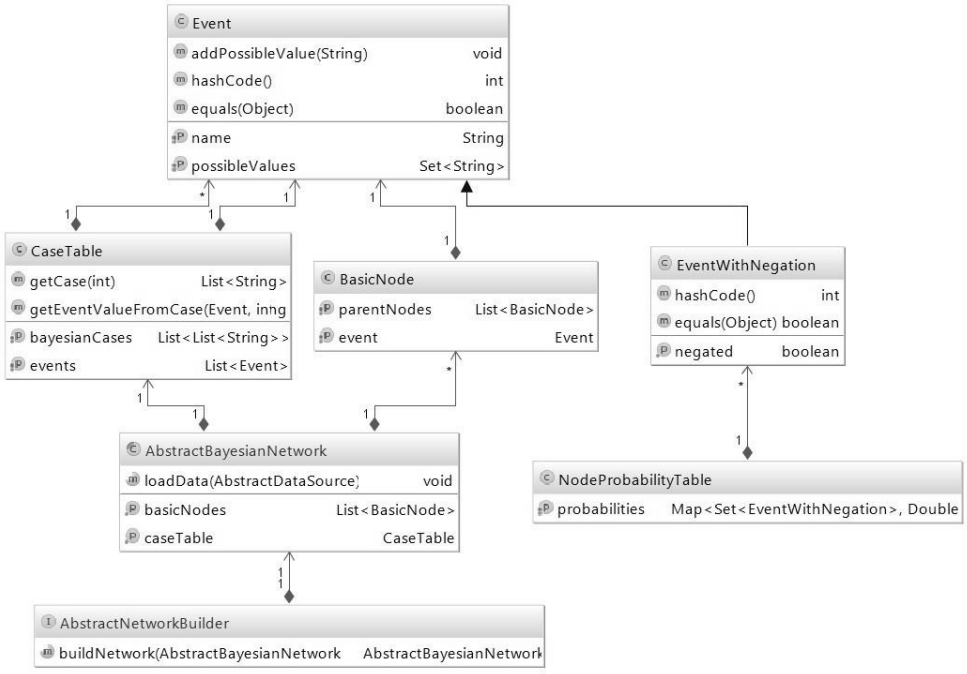


Рис. 2. Диаграмма базовых классов

Эвристический метод

Для реализации эвристического метода на основе ранее описанной архитектуры были разработанные классы, которые дополняют базовые и наследуются от них, для реализации конкретного алгоритма. Класс HeuristicBayesianNetwork унаследован от AbstractBayesianNetwork. В него включены реализации конкретных структур. Весь процесс построения сети реализуется в классе HeuristicNetworkBuilder, которые реализует метод buildNetwork.

Эвристический метод – итерационный алгоритм, который основан на таких понятиях как взаимная информация и принцип описания минимальной длины, который, в свою очередь, использует эмпирическую энтропию.

Входом алгоритма является множество обучающих данных: $D = \{x_1, ..., x_n\}$, которые являются наблюдениями. События, описываемые байесовской сетью, пронумеруем некоторым образом и будем обозначать как $x^{(j)}$. Каждое наблюдение x_i состоит из значений событий $x_i^{(j)}$, которые могут принимать значения из множества A^j: $A^j = \{0,1,...\alpha^{(j)} - 1\}, \alpha^{(j)} \in N, \alpha^{(j)} \geq 2$

Наблюдение будем записывать следующим образом: $x_i = \{ x_i^{(1)}, x_i^{(2)}, \ldots x_i^{N(}$, где $x_i^{(j)} \in A^j$.

На рис. 3 показана схема работы данного алгоритма. Далее будет рассмотрены подробно этапы построения структуры и их реализация.

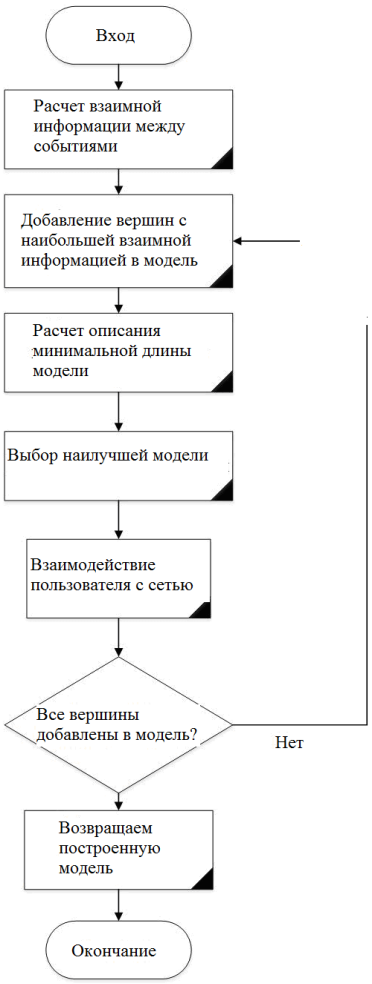


Рис. 3. Схема работы алгоритма

Взаимная информация

На первом этапе для всех пар вершин вычисляют значения взаимной информации $Set\_MI = \left\{ MI(x^{(i)}, x^{(j)});\ \forall i, j \right\}$. После этого элементы множества Set_MI упорядочивают по убыванию

$$Set\_MI = \{MI(x^{(m1)}, x^{(m2)}), MI(x^{(m3)}, x^{(m4)}), \ldots\}.$$

Этот этап выделяется отдельно, так как соответствующие вычисления необходимо выполнить один раз, а не выполнять в процессе итераций.

Взаимная информация является мерой близости между двумя переменными, или оценкой количества информации об одной переменной содержащейся в другой переменной[2]. Для её расчета используется следующее выражение:

$$MI(x^{(m1)}, x^{(m2)}) = \sum_{x_i^{(m1)} x_j^{(m2)} \in A^j} P(x_i^{(m1)}, x_j^{(m2)}) \cdot \ln\left(\frac{P(x_i^{(m1)}, x_j^{(m2)})}{P(x_i^{(m1)}) P(x_j^{(m2)})}\right) \qquad (1)$$

где $MI(x^{(m1)}, x^{(m2)})$ – взаимная информация между событиями $x^{(m1)}$ и $x^{(m2)}$; $P(x_i^{(m1)}, x_j^{(m2)})$ – вероятность одновременного наступления событий $x_i^{(m1)}$ и $x_j^{(m2)}$ для наблюдений из множества D; $P(x_i^{(m1)}), P(x_j^{(m2)})$ – вероятность наступления событий $x_i^{(m1)}, x_j^{(m2)}$ для наблюдений из множества D.

Для выполнения расчета взаимной информации между событиями в класс HeuristicCaseTable который наследуется от CaseTable, был добавлен список итераций, и при вызове пользователем метода buildNetwork, в первую очередь строится последовательность пар вершин упорядоченная по убыванию взаимной информации. Для этого был реализован метод calculateMutualInformation, который возвращает данный список. Для выполнения расчетов вызывается метод calculateTwoEventsMI для каждой пары вершин. В методе calculateTwoEventsMI, проводятся вычисления в соответствии с формулой (1). Результат хранится в виде упорядоченного списка объектов класса EventsMutualInformation, который указывает на два события, и хранит результат вышеописанных действий. После того как все значения взаимной информации найдены, они сортируются по убыванию взаимной информации.

Построение новых моделей

Вначале из множества значений взаимной информации Set_MI выбирают первые два максимальные значения $MI(x^{(m1)}, x^{(m2)})$ и $MI(x^{(m3)}, x^{(m4)})$. По полученным значениям $MI(x^{(m1)}, x^{(m2)})$ и $MI(x^{(m3)}, x^{(m4)})$ строится множество моделей G вида {($m_1 \rightarrow m_2$; $m_3 \rightarrow m_4$), ($m_1 \rightarrow m_2$; $m_3 \leftarrow m_4$), ($m_1 \leftarrow m_2$; $m_3 \leftarrow m_4$), ($m_1 \leftarrow m_2$; $m_3 \rightarrow m_4$), ($m_1 \leftarrow m_2$; m_3 не зависит от m_4), ($m_1 \rightarrow m_2$; m_3 не зависит от m_4), (m_1 не зависит от m_2 ; $m_3 \rightarrow m_4$), (m_1 не зависит от m_2 ; $m_3 \leftarrow m_4$), (m_1 не зависит от m_2 ; m_3 не зависит от m_4)}. Запись вида $m_i \rightarrow m_j$ означает, что вершина x^{m_i} является предком вершины x^{m_j}.

Для реализации данного этапа были введены классы NetworkStructure и Link. NetworkStructure является аналогом матрицы смежности, типы связей в которой задаются с помощью класса Link. Класс Link имеет 4 возможных состояния: unknown, child, no_link, parent. В начале построения сети, все связи инициализированы как unknown, и в процессе построения сети, значения заменяются на связь построенную

алгоритмом, который использует все возможные комбинации связей всех типов кроме unknown.

Описание минимальной длины

Процесс работы алгоритма описания минимальной длины (ОМД) следующий. Среди всех моделей множества G осуществляется поиск. В параметре g^* сохраняется оптимальная сетевая структура. Оптимальной структурой будет та, у которой наименьшее значение функции $L(g, x^n)$. $L(g, x^n)$ – ОМД структуры модели при заданной последовательности из n наблюдений $x^n = d_1 d_2 ... d_n$. Математически это может быть записано следующим образом.

1. $g^* \leftarrow g_0 (\in G)$.
2. $\forall g \in G - \{g_0\}$ если $L(g, x^n) < L(g^*, x^n)$, то $g^* \leftarrow g$.

На выход подаётся модель g^* в качестве решения.

Основная идея принципа ОМД в том что, необходимо использовать ту модель, которая позволяет наиболее кратко описать структуру байесовской сети, включая в это описание наибольшее количество информации. Этот принцип и его использование при работе с байесовскими сетями описан в источниках [1] и [3]. Для реализации алгоритма необходимо точное описание проводимых вычислений, которое будет представлено далее.

Для расчета ОМД сетевой структуры применяются следующая формула:

$$L(\mathrm{g}, x^n) = \sum_{j=1}^{n} L(j, g, x^n) \tag{2}$$

где $L(\mathrm{g}, x^n)$ ОМД всей, сетевой структуры; $L(j, g, x^n)$ – ОМД отдельно взятой вершины.

ОМД отдельно взятой вершины рассчитывается по следующей формуле:

$$L(j, g, x^n) = H(j, g, x^n) + \frac{k(j, g)}{2} \cdot \ln(\mathrm{n}) \tag{3}$$

где $H(j, g, x^n)$ эмпирическая энтропия j–ой вершины; $k(j, g)$ – значение, зависящее от количества условных вероятностей j–й вершины (количества вершин–родителей); n – количество наблюдений.

$H(j, g, x^n)$ – рассчитывается по формуле:

$$H(j, g, x^n) = \sum_{s \in S(j,g)} \sum_{q \in A^{(j)}} -n[q, s, j, g] \cdot \ln \frac{n[q, s, j, g]}{n[s, j, g]} \tag{4}$$

где $n[s, j, g]$ – количество случаев в обучающем множестве, с конкретным значением вершин родителей s; $n[q, s, j, g]$ – количество случаев в обучающем множестве, с конкретным значением вершин родителей s, и значением q вершины, для которой рассчитывается ОМД.

$k(j, g)$ рассчитывается по формуле:

$$k(j,g) = (\alpha^{(j)} - 1) \cdot \prod_{k \in \phi(j)} \alpha^{(k)} \quad (5)$$

где $\alpha^{(j)}$ – количество возможных значений j–ой вершины; $\alpha^{(k)}$ – количество возможных значений k–ой вершины, где $k \in \phi(j) - k$ принадлежит множеству вершин родителей.

Наиболее трудоемким на данном этапе является вычисление эмпирической энтропии для каждого узла:

$$H(j,g,x^n) = \sum_{s \in S(j,g)} \sum_{q \in A^{(j)}} -n[q,s,j,g] \cdot \ln \frac{n[q,s,j,g]}{n[s,j,g]} \quad (6)$$

Если у вершины имеется несколько родителей, то для нахождения эмпирической энтропии необходимо подсчитать количество вхождений каждой комбинации возможных значений для вершин родителей. Для этого был реализован класс EventValuesWithFrequency, который содержит в себе список значений вершин, и количество вхождений определенного набора значений $-n[s,j,g]$. Далее вычисляется значения $n[q,s,j,g]$, которое является количеством вхождений определенных значений вершины j, для которой рассчитывается энтропия, при конкретных значениях родителей. На следующем этапе происходит вычисление ОМД вершины. Расчитывая таким образом значения ОМД каждой вершины, и просуммировав их, получаем ОМД всей структуры. Данный функционал реализуется методом calculateMDL и несколькими вспомогательными методами.

Выбор наилучшей модели

После того, как рассчитано ОМД для всех моделей, осуществляется выбор модели с наилучшим показателем, то есть, модель с наименьшим числом ОМД. После того как найдена оптимальная структура g^* из G, если между всеми вершинами уже были построены связи, алгоритм заканчивает работу и возвращает модель g^*.

Если же остались вершины между которыми не были построены связи, то из множества значений обоюдной информации Set_MI выбирается следующее максимальное значение $MI(x^{(i\_next)}, x^{(j\_next)})$. С помощью значения $MI(x^{(i\_next)}, x^{(j\_next)})$ и структуры g^* строится множество моделей G вида $\{(g^*; i\_next \to j\_next)$, $(g^*; i\_next \leftarrow j\_next)$, $(g^*; i\_next$ не зависит от $j\_next)\}$, После чего выполняется расчет ОМД. Данный шаг отличается, от первой итерации тем, что получается три новых структуры, так как добавляются связи между одной парой вершин. Первая итерация давала девять новых моделей, так как добавлялись связи между двумя парами вершин. Реализация данной части алгоритма осуществляется с помощью цикла по списку пар вершин типа EventsMutualInformation, который описан в разделе взаимной информации.

Выводы

Описанная выше программная архитектура позволила реализовать улучшения данного алгоритма, которые заключаются во взаимодействии пользователя с сетью во время построения структуры, между итерациями. Пользователь может последовательно

выполнять итерации, наблюдать за порядком добавления связей между вершинами, и высказывать свое экспертное мнение, модифицируя структуру сети. В этом случае, если между вершинами была уже установлена связь, то она заменяется на новую, если же связь еще должна быть построена, то данная пара вершин исключается из списка вершин, для которых необходимо построить связь. Это было достигнуто введением дополнительных методов в класс HeurisiticNetworkBuilder – doHeuristicIteration, который выполняет лишь одну итерацию, давая возможность модифицировать пользователю сеть через модуль интерфейса и взаимодействия. Если говорить о блок схеме, для данного улучшения, то после выбора наилучшей модели, добавляется блок взаимодействия с пользователем, который влияет на построенную модель. На рис. 4 представлена диаграмма классов, реализованных для выполнения эвристического метода, и его улучшения.

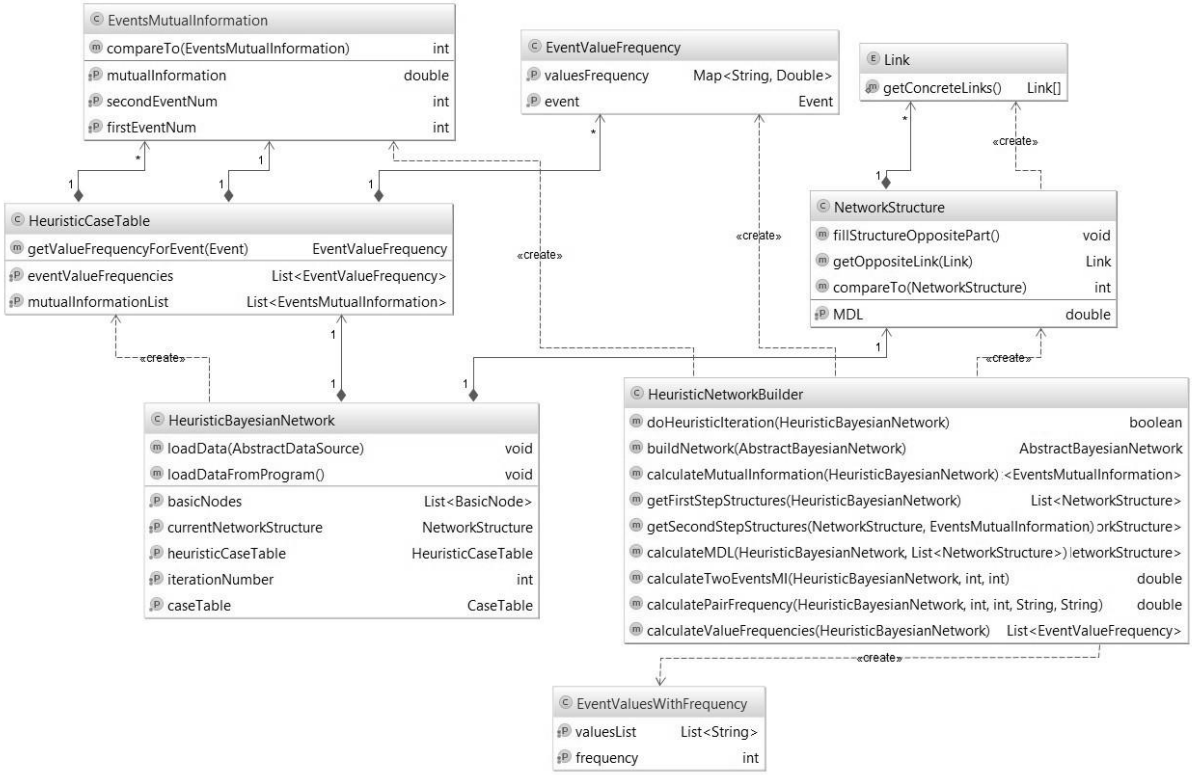


Рис. 4. Диаграмма классов эвристического метода

На данный момент реализованные архитектура и алгоритмы показали себя как эффективное средство, для построения байесовских сетей на мобильных устройствах планшетного типа. Реализованные модули планируется использовать для реализации других алгоритмов построения сети и операций по расчету данных внутри сети. Также их функционал имеет перспективу расширения в сторону реализации полноценной персональной мобильной экспертной системы. Возможность обрабатывать информацию, полученную от различных сенсоров, в комбинации с байесовскими сетями может быть перспективным направлением, для эффективного внедрения экспертных систем в повседневную жизнь человека.

Список литературы

1. Терентьев, А.Н. Эвристический метод построения Байесовских сетей / А.Н. Терентьев, П.И. Бидюк // Мат. машини і системи. – 2006. – № 3. – С. 12 – 23.
2. Cover, T. Elements of Information Theory Second Edition / T.M. Cover, J.A. Thomas // Published by John Wiley & Sons, Inc. – 2006. – 748 p.
3. Grunwald, P. The Minimum Description Length Principle / P.D. Grunwald // Published by The MIT Press. – 2007. – 702 p.

АНАЛІЗ ЕВРИСТИЧНОГО МЕТОДА ПОБУДОВИ БАЄСОВИХ МЕРЕЖ З ТОЧКИ ЗОРУ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ У РАМКАХ РОЗШИРЮВАНОЇ АРХІТЕКТУРИ

Є.Ю. Таран, В.Г. Пенко

Одеський національний університет імені І.І.Мечникова,
вул. Дворянська, 2, Одеса, 65082, Україна; e-mail: e.taran@ukr.net

Ця стаття містить аналіз одного з алгоритмів побудови структури баєсової мережі (евристичний метод на основі даних) з точки зору його програмної реалізації в рамках персональної мобільної експертної системи. Алгоритм був реалізований на платформі Android SDK. У статті пропонується підхід до поліпшення результатів розглянутого алгоритму за рахунок взаємодії з користувачем-експертом. Застосування цього підходу в ряді випадків призводило до поліпшення структури мережі. В результаті дослідження розроблена програмна архітектура, яка реалізує розглянуті алгоритми і володіє можливістю розширення для реалізації інших алгоритмів.

Ключові слова: баєсова мережа, евристичний метод, взаємна інформація, принцип опису мінімальної довжини, архітектура програмної системи.

AN ANALYSIS OF THE HEURISTIC METHOD FOR CONSTRUCTING BAYESIAN NETWORKS IN TERMS OF PROGRAM IMPLEMENTATION WITHIN THE FRAMEWORK OF EXTENSIBLE ARCHITECTURE

Y.Y. Taran, V.G. Penko

Odessa I.I.Mechnikov National University,
str. Dvoryanska, 2, Odesa, 65082, Ukraine; e-mail: e.taran@ukr.net

This article provides an analysis of one of the algorithms for constructing Bayesian network structure (heuristic method based on the data) in terms of program implementation within the framework of the personal mobile expert system. The algorithm has been implemented on the Android SDK platform. The paper proposes an approach to improve the results of the algorithm due to the interaction with the user-expert. The usage of this approach in a number of cases led to improvement of the network structure. The study developed a software architecture that implements algorithms and having considered the possibility of extension for the implementation of the other algorithms.

Keywords: bayesian network, heuristic method, mutual information, the principle of minimum description length, architecture of software system.

УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 6 (2016), No. 2, pp. 193-199

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ МЕТОДА ВЫЯВЛЕНИЯ РЕЗУЛЬТАТОВ КЛОНИРОВАНИЯ В УСЛОВИЯХ ПОСТОБРАБОТКИ ИЗОБРАЖЕНИЯ

С.Н. Григоренко

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: sn_torchuk2012@mail.ru

В работе проведен сравнительный анализ с современными аналогами эффективности разработанного ранее метода выявления результатов клонирования в цифровом изображении в условиях его постобработки. Теоретический базис метода основывается на геометрическом представлении изображения и полученном необходимом условии принадлежности блоков матрицы изображения областям клона и прообраза. В качестве дополнительных возмущающих воздействий рассмотрены наиболее часто используемые для «маскировки» результатов клонирования сжатие изображения с потерями, наложение шума, размытие. В результате установлена высокая эффективность алгоритмической реализации метода независимо от вида и конкретного способа реализации программного средства, используемого при постобработке изображения, силы возмущающего воздействия, относительных размеров областей клона и прообраза, специфики анализируемого изображения. Приведены результаты вычислительных экспериментов.

Ключевые слова: цифровое изображение, клон, прообраз, постобработки изображения, возмущающие воздействия, сжатие с потерями, размытие, наложение шума

Введение

Одним из наиболее широко и часто используемых программных инструментов при неавторизованных изменениях – фальсификациях цифрового изображения (ЦИ) является клонирование, реализованное во всех современных графических редакторах (Adobe Photoshop, Gimp и др.). При клонировании одна область изображения, называемая прообразом, копируется и вставляется в другую область этого же изображения, заменяя собой его оригинальную часть и образуя клон прообраза. Описанная процедура часто используется в случае, когда с ЦИ убирается «нежелательный» объект, изменяется взаимное расположение объектов, дублируется объект (объекты).

На практике ЦИ после выполнения клонирования подвергается дополнительным возмущающим воздействиям – постобработке с целью маскировки результатов клонирования, усложнения процесса его обнаружения, вызванного изменением значений параметров ЦИ в областях клона, прообраза.

Задача выявления такого рода фальсификации не является новой [1-3], однако существующие на сегодняшний день методы не обеспечивают достаточную эффективность ее решения. Даже в условиях отсутствия дополнительных возмущений нулевое значение ошибки первого рода, когда отсутствует пропуск фальсифицированного ЦИ, достигается лишь очень немногими алгоритмами [3]. Большинство из них выявляют области клона/прообраза, когда они составляют 0.85–1% ЦИ и более [3,4], оказываясь несостоятельными в случае малых относительных

размеров области фальсификации. Требует окончательного решения задача выявления результатов клонирования в условиях значительных возмущающих воздействий.

В [5] был предложен, а в [6] усовершенствован новый блоково-ориентированный метод KL выявления результатов клонирования в ЦИ в условиях его постобработки, основанный на геометрическом представлении ЦИ, на основании которого для блоков матрицы изображения было получено формальное необходимое условие их принадлежности областям клона и прообраза [5]. Исходя из теоретических основ метода, его эффективность должна превосходить современные аналоги, не должна зависеть от специфики и силы дополнительных возмущающих воздействий, а также от относительных размеров клона и прообраза [6].

Цель стать и постановка заданий

Целью статьи является проведение анализа эффективности работы алгоритмической реализации метода KL выявления результатов клонирования в условиях дополнительных возмущающих воздействий, в том числе значительных.

При тестировании алгоритмической реализации любого из рассматриваемых в работе методов эффективность оценивалась двумя количественными показателями TPR (true positive rate) и FPR (false positive rate) [3]:

$$TPR = \frac{\text{кол-во фальфицированных ЦИ, определенных как фальсифицированные}}{\text{общее число рассмотренных фальсифицированных ЦИ}},$$

$$FPR = \frac{\text{количество оригинальных ЦИ, определенных как фальсифициованные}}{\text{общее количество рассмотренных оригинальных ЦИ}}.$$

Необходимо отметить, что показатель FPR является показателем ошибок второго рода или «ложных тревог».

Далее для показателя TPR полагается, что фальсифицированное ЦИ определено как фальсифицированное, если в нем обнаружено наличие областей клона и прообраза, причем эти области имеют непустое пересечение с реальными клоном и прообразом. Оригинальное ЦИ определяется как фальсифицированное и учитывается при вычислении показателя FPR, если в нем фиксируется наличие областей клона, прообраза.

Для достижения поставленной цели в работе решаются следующие задачи.

1. Провести сравнительный анализ эффективности KL в условиях отсутствия постобработки ЦИ после клонирования.
2. Определить характер возмущающих воздействий, наиболее часто используемых для «маскировки» результатов клонирования в ЦИ.
3. Провести сравнительный анализ эффективности KL в условиях наиболее часто используемых дополнительных возмущающих воздействий с современными аналогами.

Основная часть

Для сравнительного анализа эффективности метода KL была проведена серия вычислительных экспериментов, в каждом из которых были задействованы 400 цветных (цветовая схема RGB) ЦИ из базы NRCS [7], являющейся традиционной при тестировании алгоритмов обработки и анализа изображений, и 100 ЦИ, полученных непрофессиональными цифровыми камерами, размером 400×400 пикселей. Далее такое множество ЦИ называется экспериментальным множеством (ЭМ).

Единственным ограничением на работу метода KL [6] является принадлежность области, не принадлежащей пересечению клона и прообраза, хотя бы одного $q \times q -$блока, для которого $q \geq 16$. Это говорит о принципиальной возможности эффективной работы метода при выявлении областей клона/прообраза малых относительных размеров. В силу этого везде в работе при проведении вычислительных экспериментов области клона и прообраза составляют $<< 0.85\%$ ЦИ: как правило, от 0.098% до 0.39% ЦИ, хотя использовались и области клона, размер которых был меньше 0.098% изображения.

На первом этапе эксперимента ЦИ подвергались клонированию с последующим сохранением в формате без потерь (Tif). Таким образом, дополнительные возмущающие воздействия отсутствовали.

Анализировалась матрица одной цветовой составляющей ЦИ, которая выбиралась случайным образом. Анализ проводился с использованием $16 \times 16 -$блоков. Показатель TPR в этих условиях дал максимально возможное значение – TPR=100%, значение показателя FPR, полученное при анализе с помощью метода KL оригинальных ЦИ из ЭМ, является сравнимым с лучшими по этому показателю современными аналогами. Результаты сравнительного анализа представлены в табл. 1.

Таблица 1.

Результаты сравнительного анализа эффективности разработанного метода KL и современных аналогов в условиях отсутствия постобработки клонированного ЦИ

Метод	TPR (%)	FPR (%)
Fridrich (2003)[1]	89	84
Lowe (2004)[8]	74	4
Popescu and Farid (2004)[2]	87	86
Pan and Lyu (2010)[9]	83	8.8
Amerini(2011)[3]	100	8
Mishra (2013)[4]	73.6	3.6
Hashmi et al. (2014)[10]	80	10
Diaa et al. (2016)[11]	96	2.9
KL	100	4.8

На втором этапе эксперимента проводился сравнительный анализ алгоритмической реализации разработанного метода KL с современными аналогами в условиях дополнительных возмущающих воздействий (ВВ). Рассмотрим наиболее часто используемые при маскировке результатов клонирования ВВ: сжатие с потерями, наложение шума, размытие ЦИ.

Результаты сравнительного анализа разработанного метода с современными аналогами в условиях сжатия с потерями (сохранения клонированного ЦИ в формате jpeg с различными коэффициентами качества QF) представлены на рис. 1 (для методов, отличных от KL, данные об их эффективности брались из соответствующих статей).

Полученные результаты свидетельствуют о превосходстве по эффективности с точки зрения TPRразработанным методом KL всех рассмотренных современных аналогов. При этом с уменьшением QF эффективность KL падает очень незначительно: при уменьшении QF в 5 раз (с 100 до 20) значение TPRуменьшилось лишь на 7.1% (с 99.2% до 92.1%). Необходимо отметить, что для $QF < 40$ тестирование современных аналогов практически не проводится. Исключение из рассмотренных методов составляет Amerini (2011), для которого проводилось тестирование в условиях сжатия с $QF = 20$. В этих условиях метод KL превосходит Amerini (2011) на 5.6% по значению TPR. Тестирование в условиях сжатия с $QF = 5$ ни одного из современных

аналогов не проводилось вообще, что может говорить об их несостоятельности в данных условиях, в то время как для разработанного метода TPR=69.3% (рис.1). Большинство существующих современных методов выявления результатов клонирования тестируются лишь в условиях $QF \geq 50$ (рис.1). Для $QF = 50$ разработанный KL превосходит Amerini (2011) – лучший из аналогов в этих условиях на 2.6% по показателю TPR. Для наиболее часто используемого при сжатии в формате Jpeg значения коэффициента качества $QF = 75$ алгоритмическая реализация KL превосходит лучший из аналогов Mahmood et al. (2016) по показателю TPR на 4.5%. Максимальное превосходство KL над рассмотренными аналогами наблюдается в условиях $QF = 60$ для Diaa et al. (2016) и составляет 6.7%. При этом области клона для разработанного метода всегда при его тестировании имели малые относительные размеры (меньше 0.85% ЦИ), в отличие от методов-аналогов.

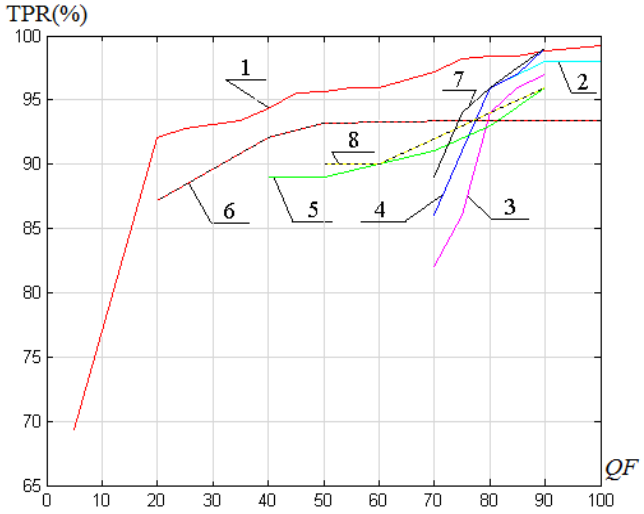


Рис. 1. Зависимость значения TPR от значения коэффициента качества QF, используемого при сжатии ЦИ после клонирования для различных методов: 1 - KL; 2 - Lin et al. (2009) [12]; 3 - Bayram et al. (2009) [13]; 4 - Huang et al. (2011) [14]; 5 - Liu et al. (2011) [15]; 6 – Amerini (2011) [3]; 7 - Mahmood et al. (2016) [16]; 8 - Diaa et al. (2016) [11]

Проведем сравнительный анализ эффективности KL с современными аналогами в условиях наложения на ЦИ после клонирования гауссовского шума. Сила возмущающего воздействия количественно оценивается здесь разностным показателем искажения изображения «сигнал-шум» SNR [3]. Результаты эксперимента, в котором были задействованы ЦИ из ЭМ, приведены в табл. 2. Для методов, отличных от KL, данные об их эффективности брались из соответствующих статей, если информация о тестировании метода в определенных условиях отсутствовала, в табл. 2. ставился прочерк.

Как видно из полученных результатов, предложенный метод превосходит свои аналоги по эффективности с учетом TPR (максимально – на 5.8% для Amerini(2011) в условиях $SNR = 50dB$), при этом являясь состоятельным даже в тех условиях, в которых существовавшие до него методы вообще не работают – при $SNR = 5dB$ TPR=67.8%. Необходим отметить, что значения TPR при уменьшении SNR от 60 до 20 dB практически не меняется, имея высокое значение: $TPR \geq 98.6\%$.

Таблица 2.

Значение *TPR* (%) для различных методов в условиях наложения на ЦИ после клонирования гауссовского шума, приводящего к искажению изображения, определяемого отношением «сигнал-шум» SNR (dB)

Метод / SNR (dB)	Popescu and Farid (2004) [2]	Lin et al. (2009) [12]	Bayram et al. (2009) [13]	Huang et al. (2011) [14]	Ameri ni (2011) [3]	Liu et al. (2011) [15]	Diaa et al. (2016) [11]	Deoli et al. (2016) [17]	Mahmood et al. (2016) [16]	*KL*
60	—	—	—	—	—	—	—	100	—	99.8
50	—	—	—	—	94.1	—	—	—	—	99.6
40	75	—	96	95	93.7	98	—	—	98.5	99.6
35	66	98	96	95	—	98	96	85	97.9	99.2
30	46	—	95	91	92	—	96	—	96.5	98.8
25	31	—	79	82	—	—	96	—	90	98.8
20	26	98	79	71	82.4	97	94	—	80	98.6
15	—	—	—	—	—	96	94	—	—	96.4
10	—	94	—	—	—	—	—	—	—	94.4
5	—	—	—	—	—	—	—	—	—	67.8

Данные по сравнению эффективностей различных методов в условиях Гауссова размытия изображения после клонирования приведены в табл. 3 (маска 5×5). Размытие по Гауссу осуществлялось с использованием маски фильтра нижних частот Гаусса, формируемой при помощи функции *fspecial* (среда Matlab), одним из параметров которой, наряду с размерами маски, является δ, который задает среднеквадратическое отклонение распределения Гаусса, используемое при формировании маски фильтра. Как видно, алгоритм, реализующий метод KL, превосходит современные аналоги по эффективности (с учетом показателя TPR), в том числе и лучший из них Mahmood et al.(2016), причем последний максимально на 4% (в условиях $\delta=2$).

Таблица 3.

Значение *TPR* (%) в условиях размытия по Гауссу ЦИ после клонирования для различных значений параметра гауссова фильтра δ с маской 5×5

Метод / δ	Fridrich (2003) [1]	Huang et al. (2011) [14]	Bayram et al. (2009) [13]	Mahmood et al. (2016) [16]	*KL*
0.5	85	92	89	97	98.2
1	84	91	88	96	97.0
1.5	79	90	87	94	93.0
2	74	85	76	89	92.6
2.5	71	81	76	85	87.2
3	71	80	74	83	85.6

Выводы

Таким образом, серия проведенных вычислительных экспериментов подтвердила на практике высокую эффективность метода KL выявления результатов клонирования как при наличии, так и при отсутствии дополнительных возмущающих воздействий.

Сравнительный анализ эффективности метода выявления результатов клонирования в ЦИ KL, проведенный в условиях сжатия с потерями, наложения гауссовского шума, размытия ЦИ, показал, что для каждого из рассмотренных ВВ алгоритмическая реализация KL превосходит по эффективности современные аналоги, которые не рассчитаны на работу в условиях значительных ВВ (сжатие с $QF < 20$, наложение шума, приводящее к искажению изображения, оцениваемому $SNR < 10dB$), а также областей клона и прообраза малых относительных размеров (<0.85% ЦИ). В условиях сжатия с потерями максимальное превосходство KL достигает 6.7%; в условиях наложения шума 5.8%; в условиях размытия KL превосходит лучший из аналогов максимально на 4% относительно показателя TPR. Значение показателя FPR сравнимо с лучшими из современных аналогов.

При отсутствии постобработки фальсифицированного ЦИ выявление результатов клонирования происходит в 100% ЦИ.

Таким образом, разработанный метод KL позволил повысить эффективность обнаружения клонирования и, как следствие, в целом эффективность выявления нарушения целостности ЦИ, что подтверждено на практике путем представительных вычислительных экспериментов.

Список литературы

1. Fridrich, J. Detection of copy–move forgery in digital images / J. Fridrich, D. Soukal, J. Lukas // Proceedings of Digital Forensic Research Workshop, IEEE Computer Society, Cleveland, OH, USA. – 2003. - Pp. 55–61.
2. Popescu, C. Exposing digital forgeries by detectingduplicated image regions / C.Popescu, H. Farid // Technical Report TR 2004-515, DartmoughCollege. – 2004. – Pp.34-46.
3. Amerini, I. A SIFT-based forensic method for copy move attack detection and transformation recovery / I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, G. Serra // IEEE Transactions on Information Forensics and Security. – 2011. – Vol. 6. – No 3. – Pp. 1099-1110.
4. Mishra P. Region Duplication Forgery Detection Technique Based on SURF and HAC / N. Mishra, S. Sharma, R. Patel // Hindawi Publishing Corporation The Scientific World Journal. – 2013. – 98 p.
5. Кобозева, А.А. Задача обнаружения результатов клонирования в изображении и новый подход к ее решению в условиях дополнительных возмущений / А.А. Кобозева, С.Н. Григоренко // Информационные технологии в управлении, образовании, науке и промышленности: монография/ под ред. В.С. Пономаренко. –Х.: Издатель С. Г.Рожко, 2016. – С. 300-313.
6. Григоренко, С.Н. Усовершенствование метода обнаружения результатов фальсификации в цифровом изображении в условиях атак / А.А.Кобозева, С.Н. Григоренко // Проблемы региональной энергетики. Электронный журнал Академии наук Республики Молдова. – 2016. – №2 (31). – С. 93-103.
7. NRCS Photo Gallery: [Електронний ресурс] // United States Department of Agriculture. Washington, USA. Режим доступа: http://photogallery.nrcs.usda.gov (Дата обращения: 26.07.2012).
8. Lowe, D.G. Distinctive image features from scale-invariant key points / D.G. Lowe // International journal of computer vision. – 2004. – Vol. 60. – No. 2. – Pp. 91 – 110.
9. Pan, X. Region Duplication Detection Using Image Feature Matching / X. Pan, S. Lyu // IEEE Transactions on Information Forensics and Security. – 2010. – Vol. 5. – NO. 4. – Pp. 857 – 867.
10. Farukh, M. Copymove image forgery detection using efficient and robust method combining Un-decimated Wavelet Transform and Scale invariant Feature Transform / M. Farukh, V. Anand, A. Keskar // AASRI conference on circuit and signal processing, Procedia 9. – 2014. – Pp. 84 – 91.
11. Diaa M. Uliyan. Image Region Duplication Forgery Detection Based on Angular Radial Partitioning and Harris Key-Points / M. Diaa, A. Hamid, W. Ainuddin // Symmetry. – 2016. – Vol 8. – Pp. 62 – 72.
12. Lin, H.J. Fast Copy-Move Forgery Detection / H.J. Lin, C.W. Wang // WSEAS Transactions on Signal Processing. – 2009. – Vol.5. – Pp. 188 – 197.

13. Bayram, S. An efficient and robust method for detecting copy-move forgery, in International Coriference on Acoustics / S. Bayram, H. T. Sencar // Speech and Signal Processing, (ICASSP'09). IEEE, 2009. – Pp. 1053 – 1056.
14. Huang, Y. Improved DCT-based detection of copy-move forgery in images / Y. Huang, W. Lu, W. Sun, D. Long // Forensic Science International. – 2011. Pp. 178 – 84
15. Guangjie, L. A passive image authen tication scheme for detecting region- duplication forgery with rotation / L. Guangjie, W. Junwen, L. Shiguo, W. Zhiquan // Journal of Network and Computer Applications. – 2011. –Pp. 1557 – 1565
16. Toqeer M. Copy-Move Forgery Detection Technique for Forensic Analysis in Digital Images / M. Toqeer, N. Tabassam, I. Aun, A. Rehan, S. Mohsin // Mathematical Problems in Engineering. – 2016. – Vol. 2016.
17. Manish D. A Fast and Robust Approach to Detect Copy-Move Forgery in Digital Images / D. Manish // International Journal of Computer Applications. –2016. – Vol. 137 – No.5. – Pp.29 – 33.

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЕФЕКТИВНОСТІ МЕТОДУ ВИЯВЛЕННЯ РЕЗУЛЬТАТІВ КЛОНУВАННЯ В УМОВАХ ПОСТОБРОБКИ ЗОБРАЖЕННЯ

С.М. Григоренко

Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна; e-mail: sn_torchuk2012@mail.ru

У роботі проведений порівняльний аналіз із сучасними аналогами ефективності розробленого раніше методу виявлення результатів клонування в цифровому зображенні в умовах його постобробки. Теоретичний базис методу ґрунтується на геометричному представленні зображення й отриманій необхідній умові належності блоків матриці зображення областям клону й прообразу. У якості додаткових збурних дій розглянуті найбільш часто використовувані для «маскування» результатів клонування: стиск зображення із втратами, накладення шуму, розмиття. У результаті встановлена висока ефективність алгоритмічної реалізації методу незалежно від виду й конкретного способу реалізації програмного засобу, який використовується при постобробці зображення, сили збурної дії, відносних розмірів областей клону й прообразу, специфіки аналізованого зображення. Наведено результати обчислювальних експериментів.

Ключові слова: цифрове зображення, клон, прообраз, постобробка зображення, збурні дії, стиск із втратами, розміття, накладання шуму.

COMPARATIVE ANALYSIS THE EFFICIENCY OF THE METHOD FOR DETECTION THE RESULTS IN THE CLONING IMAGE POSTPROCESSING

S.M. Grygorenko

Odessa national polytechnic university,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: sn_torchuk2012@mail.ru

The comparative analysis of the effectiveness the modern analogs for previously developed method of cloning results in the detection of the digital image in the conditions of post-processing.The theoretical basis of the method is based on the geometric representation of the image and obtain the necessary supplies provided image matrix of blocks and areas clone prototype.As additional disturbances are considered the most frequently used for "masking" image compression cloning results with losses, noise, overlay, blur.In a result, it was set high performance algorithmic method implementation regardless of the type and the particular mode of implementation the software used in the post-processing of the image, the disturbance force, the relative sizes of areas and pre-image clone, the specificity of the analyzed image.There are presented results of computational experiments in this scientific work.

Keywords: digital image, clone, the prototype, image post-processing, disturbing influences, lossy compression, blur, noise.

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 6, номер 2, 2016. Одеса – 99 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 6, номер 2, 2016. Одесса – 99 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 6, No. 2, 2016. Odesa – 99 p.

Засновник: Одеський національний політехнічний університет

Зареєстровано Міністерством юстиції України 04.04.2011р.

Свідоцтво: серія КВ № 17610 - 6460Р

Друкується за рішенням Вченої ради Одеського національного політехнічного університету (протокол №6 від 22.03.2016)

Адреса редакції: Одеський національний політехнічний університет,

проспект Шевченка, 1, Одеса, 65044 Україна

Web: http://www.immm.opu.ua

E-mail: immm.ukraine@gmail.com