ISSN 2078-9181 DOI 10.15622/sp.59

РОССИЙСКАЯ АКАДЕМИЯ НАУК
Отделение нанотехнологий и информационных технологий

САНКТ-ПЕТЕРБУРГСКИЙ
ИНСТИТУТ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ РАН

ТРУДЫ СПИИРАН

proceedings.spiiras.nw.ru

ВЫПУСК 4(59)

Санкт-Петербург
2018

18+

SPIIRAS PROCEEDINGS

Issue № 4(59), 2018

Scientific, educational, and interdisciplinary journal primarily specialized
in computer science, automation, and applied mathematics

Trudy SPIIRAN ♦ Founded in 2002 ♦ Труды СПИИРАН

Founder and Publisher

St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences

Editorial Board's address

14-th line VO, 39, SPIIRAS, St. Petersburg, 199178, Russia,
e-mail: publ@iias.spb.su, web: http://www.proceedings.spiiras.nw.ru/

The journal is indexed in Scopus

ТРУДЫ СПИИРАН

Выпуск № 4(59), 2018

Научный, научно-образовательный, междисциплинарный журнал с базовой специализацией в области информатики, автоматизации и прикладной математики
Журнал основан в 2002 году

Учредитель и издатель

Федеральное государственное бюджетное учреждение науки
Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН)

Адрес редакции

199178, Санкт-Петербург, 14-я линия, д. 39,
e-mail: publ@iias.spb.su, сайт: http://www.proceedings.spiiras.nw.ru/
Журнал индексируется в международной базе данных Scopus
Журнал входит в «Перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертации на соискание ученой степени доктора и кандидата наук»

CONTENTS

СОДЕРЖАНИЕ

УДК 004.056 **DOI** 10.15622/sp.59.1

И.В. Котенко, И.Б. Саенко, А.Г. Кушнеревич

АРХИТЕКТУРА СИСТЕМЫ ПАРАЛЛЕЛЬНОЙ ОБРАБОТКИ БОЛЬШИХ ДАННЫХ ДЛЯ МОНИТОРИНГА БЕЗОПАСНОСТИ СЕТЕЙ ИНТЕРНЕТА ВЕЩЕЙ

Котенко И.В., Саенко И.Б, Кушнеревич А.Г. **Архитектура системы параллельной обработки больших данных для мониторинга безопасности сетей Интернета вещей.**

Аннотация. Сети Интернета вещей в настоящее время находят свое применение во многих областях жизни людей. Краеугольным камнем в вопросе возможности дальнейшего распространения и использования таких сетей является аспект обеспечения их безопасности. Однако особенности сетей данного вида таковы, что использование в них традиционных средств и систем компьютерной защиты затруднено или невозможно. Одной из таких особенностей является необходимость в режиме реального времени и с минимальными вычислительными затратами анализировать очень большие объемы данных, разнородных по своей природе. С учетом особенностей вычислительных мощностей сети Интернета вещей предлагается архитектура системы параллельной обработки больших данных, основанная на использовании технологии обработки потоков данных Complex Event Processing и платформы параллельных вычислений Hadoop. Рассматриваются вопросы, непосредственно связанные с архитектурой системы, а также с реализацией следующих ее основных компонентов: сбора данных, хранения данных, нормализации и анализа данных и визуализации данных. Взаимосвязь между компонентами обеспечивается с помощью распределенной файловой системы Hadoop, которая является основой для построения распределенного хранилища данных. Компонент сбора данных организует распределенный прием данных и их хранение в компоненте хранилища данных. Компонент нормализации и анализа данных преобразует их к единому формату и обрабатывает с помощью правил корреляции. Компонент визуализации данных представляет данные в графическом виде, более удобном для дальнейшего восприятия оператором. Обсуждаются результаты экспериментальной оценки производительности системы, подтверждающие вывод о ее высокой эффективности.

Ключевые слова: Интернет вещей, мониторинг безопасности, Большие Данные, Complex Event Processing, Hadoop.

1. Введение. Сети Интернета вещей (Internet of Things — IoT) позволяют интегрировать в единую информационную инфраструктуру с помощью различных видов коммуникаций (Интернет, мобильные сети, локальные сети и т.д.) разнообразные компьютерные устройства: центральные компьютеры, пользовательские устройства со встроенными контроллерами, датчики информации об окружающей среде, сенсоры и так далее. По этой причине сети IoT в настоящее время находят все более широкое распространения во многих областях: здравоохранение, транспортные системы, умные дома, робототехника и так далее. При этом сети IoT, в отличие от традиционных компьютерных сетей, имеют следующие особенности: очень большое количество источников данных; очень большой входной поток разнородных данных; узлы сети IoT, как правило, имеют ограниченные сетевые, вычислительные и энергети-

ческие ресурсы. При этом основным проблемным вопросом являются вычислительные ограничения. Необходимо обеспечить либо быстрые вычисления непосредственно на узле сети IoT, либо пересылку данных по сети для анализа на более мощных в вычислительном плане узлах. Эти особенности делают проблему безопасности сетей IoT достаточно острой во всех вышеперечисленных областях их применения.

Традиционные методы и средства защиты информации в сетях IoT являются неэффективными, что вызвано малой мощностью вычислительных ресурсов элементов сетей IoT и большим количеством различных типов используемых в них сетей связи. По этой причине особую актуальность для обеспечения безопасности сетей IoT приобретает подход, связанный с созданием и применением в них интеллектуальных систем управления информацией и событиями безопасности (Security Information and Event Management — SIEM) [1-4]. SIEM-системы осуществляют мониторинг безопасности сети, заключающийся в сборе и предварительной обработке данных о событиях безопасности от удаленных устройств, датчиков информации и элементов сетевой инфраструктуры [1]. Многообразие типов источников данных, используемых для мониторинга сетевой безопасности, и высокая интенсивность формируемых ими потоков событий приводит к необходимости разработки решений, относящихся к проблеме обработки Больших данных. Одним из таких решений является разработка и реализация в сети IoT предлагаемой в настоящей статье системы параллельной обработки данных, предназначенной для мониторинга сетевой безопасности. При этом следует отметить, что область применения предлагаемой системы может выходить за рамки мониторинга безопасности сети IoT. За счет настройки правил корреляции событий эта система может достаточно эффективно решать различные задачи, связанные с обработкой Больших данных.

Рассматриваемая в статье система параллельной обработки данных обладает следующими особенностями. Во-первых, она благодаря использованию технологии Complex Event Processing (CEP) реализует в режиме «на лету» основные функции мониторинга, которыми являются нормализация, фильтрация, агрегация и корреляция данных. Во-вторых, кроме указанных выше функций, в этой системе реализована функция визуализации данных с использованием не только стандартных, но и специально разработанных моделей визуализации. В-третьих, эта система функционирует в условиях вычислительных ограничений, свойственных элементам информационной инфраструктуры сетей IoT. В силу наличия таких ограничений, слабые с точки зрения вычислительной способности устройства вынуждены передавать информацию на

верхние уровни сети для последующего анализа. При этом в качестве программно-инструментальной платформы для построения системы мониторинга используется открыто распространяемая программная среда Hadoop, которая в настоящее время является наиболее распространенной и достаточно гибкой платформой, позволяющей создавать системы параллельной обработки [5-7]. Эти особенности определяют теоретическую и практическую значимость настоящей работы.

Таким образом, цель данной статьи заключается в рассмотрении основных архитектурных и системных решений, позволяющих реализовать систему параллельной обработки данных, которая обладает указанными выше особенностями и может быть применима для мониторинга безопасности сетей IoT. Мониторинг безопасности способен выявлять нежелательную и вредоносную активность элементов сети IoT. Эта активность в дальнейшем может стать целью для задач обеспечения безопасности.

2. Состояние исследований. Технология CEP, используемая для разработки предлагаемой системы мониторинга безопасности для сетей IoT, в последнее время находится в фокусе внимания исследований, посвященных обработке Больших данных. Во многих работах проводится анализ и рассматриваются решения, связанные с реализацией технологии CEP в системах, основанных на Hadoop.

Система, которая рассматривается в [8], основана на Hadoop-совместимом программном обеспечении и платформе Java. Эта система имеет три компонента: компонент взаимодействия с пользователем, компонент анализа данных и компонент хранения данных. Взаимодействие между компонентами осуществляется с помощью запросов и управляется контроллерами Java Servlet. Однако эта система ориентирована только на обработку данных в веб-приложениях. Кроме того, отсутствие результатов экспериментальной оценки не позволяют утверждать о возможности ее применения для мониторинга безопасности сетей IoT.

Работа [9] рассматривает систему анализа Больших данных в медицинских информационных инфраструктурах. Выбор Hadoop был обоснован тем, что это средство наиболее популярно для целей обработки больших массивов данных. Система реализована на Java, принадлежит к открытому программному обеспечению под эгидой Apache и использует относительно простую программную модель. Архитектура предложенной системы включает адаптер событий (Event Adaptor), механизм CEP-анализа (CEP Analysis Engine) и генератор отчетов о событиях (Report & Event Generator). Система ориентирована на совместное использование с ERP-системами медицинских институтов. Механизм анализа содержит сборщик событий (Event Collector), ана-

лизатор данных (Data Analyzer) и сервер хранения данных (Storage Server). К сожалению, авторы этой работы не приводят результаты экспериментальной оценки рассматриваемой системы.

В [10] рассматривается CEP-система, предназначенная для обработки больших массивов данных при управлении движением городского пассажирского автотранспорта. Предложенная система объединяет два подхода: CEP и распределенную потоковую обработку (Distributed Stream Processing Systems — DSPS) [11]. CEP поддерживается системой Esper, подход DSPS — системой Storm. Система Hadoop играет роль интегратора, объединяющего эти два подхода. Кроме того, Hadoop обеспечивает анализ исторических данных. Экспериментальная оценка показала высокую масштабируемость рассматриваемой системы. Однако, по нашему мнению, применение ее для мониторинга IoT затруднено из-за больших требований к вычислительным ресурсам. В то же время достигнутые значения производительности этой системы будут служить ориентиром в нашей работе.

Во многих работах исследуются вопросы, связанные с совершенствованием технологии CEP. В работе [12] представлена CEP-система, в которой реализован высокоуровневый язык запросов к событиям (High-Level Event Query Language), близкий к SQL. Для этого языка разработаны алгоритмы оптимизации запросов. Критерием оптимизации является минимум времени работы процессора. В работе [13] представлен язык для типовых запросов в среде CEP, который позволяет более быстро обрабатывать сложные запросы. Однако широкое применение этих систем для мониторинга сетей IoT является затруднительным вследствие необходимости как изучения этих языков конечными пользователями, так и использования дополнительных программных средств, поддерживающих эти языки запросов.

В работе [14] рассматривается платформа, позволяющая интегрировать CEP и методы интеллектуального анализа данных (Data Mining). В качестве примера рассматривается сценарий работы «умного» города. По этой причине данная работа вызывает интерес как пример использования CEP в сетях IoT. Платформа содержит модуль интеграции и предобработки данных, в котором выполняется Data Mining. Однако, по нашему мнению, Data Mining на больших объемах требует значительных вычислительных затрат. Поэтому эти результаты в сетях IoT имеют ограниченное применение.

В работе [15] рассматривается CEP-система, предназначенная для сбора и предобработки данных с RFID. Результаты обработки потоков событий в этой системе хранятся в базе данных MySql. Однако, несмотря на то, что эта система является примером реализации техно-

логии CEP в сети IoT, она не может быть успешно использована для мониторинга безопасности сетей IoT, так как вопросы параллельной обработки больших данных в ней не рассматривались.

В работах [16, 17] предлагаются платформы, позволяющие обрабатывать веб-данные с помощью технологии CEP. В работе [16] веб-данные предварительно переводятся в события легковесной структуры. Работа [17] рассматривает систему, которая позволяет описывать и производить мониторинг сложных событий во времени, близком к реальному. Однако, несмотря на то, что оба предложенных подхода осуществимы, вопросы предварительной обработки событий на основе параллельных вычислений в этих работах не рассматривались.

В работе [18] предлагается подход, названный «активный» CEP, в котором поддерживается точность параллельного выполнения потоков через внедрение активной поддержки правил с помощью механизма CEP. Активные правила помогают поддерживать целостность CEP-транзакций, включая транзакции предобработки событий. Однако распространение этих результатов на параллельную обработку событий в IoT представляется преждевременным.

В работах [19, 20] рассматривается хорошо масштабируемая инфраструктура анализа потоков для CEP, которая для распараллеливания нагрузки осуществляет разбиение запроса на подзапросы и назначает каждому из подзапросов субкластер вычислительных средств. Авторы предложили и исследовали различные стратегии формирования подкластеров. Однако результаты, полученные в этих работах, ориентированы на кластерную вычислительную инфраструктуру с очень большим количеством узлов. По этой причине ее использование в сетях IoT является затруднительным.

Работа [21] предлагает использовать для балансировки нагрузки генетические алгоритмы, в которых учитываются характеристики каналов связи между узлами сети IoT (пропускная способность, входная нагрузка). Однако применение генетических алгоритмов при обработке больших данных может нарушить реальный масштаб времени.

Достаточно близкой к нашей можно считать работу [22], в которой представлена основанная на Hadoop платформа обработки Больших данных в интересах обеспечения общественной безопасности. Платформа содержит сервер приложений и оболочку экспертной системы. Она реализует получение данных с сенсоров, отображение их на интерактивной карте и выполнение определенных действий в соответствии с заданными правилами. Однако результаты экспериментальной оценки производительности этой системы в этой работе отсутствуют.

Интересные результаты по обработке больших данных представлены в работе [23]. Предлагаемая в ней платформа обеспечивает

обработку больших массивов документальных данных на основе парадигмы MapReduce и с использованием системы управления документальными базами данных Mongo. Авторы предложили различные реализованные на этой платформе способы агрегации больших документальных данных. Однако они не привели результаты экспериментальных исследований предлагаемой платформы.

Подводя итоги анализа состояния исследований в области систем параллельной обработки Больших данных и применения CEP для IoT, можно сделать следующие выводы. Во-первых, существуют работы, посвященные реализации CEP в сетях, подобных IoT. Однако в них вопросы параллельной обработки Больших данных не рассматриваются. Во-вторых, существуют CEP-системы, в которых присутствует параллельная обработка больших данных. Однако эти системы не могут быть реализованы в IoT из-за существующих ограничений по пропускной способности каналов связи и производительности вычислительных узлов. Наконец, мониторинг безопасности компьютерных сетей работы является сравнительно новой и недостаточно исследованной областью для систем параллельной обработки Больших данных. Этим подтверждается высокая актуальность нашей работы.

3. Архитектура системы параллельной обработки данных для мониторинга безопасности сетей IoT. В настоящем разделе рассмотрим общую архитектуру системы параллельной обработки данных для мониторинга безопасности сетей IoT и особенности функционирования ее компонентов.

Общая архитектура системы. Система параллельной обработки данных для мониторинга безопасности сетей IoT предназначена для сбора и предварительной обработки больших объемов информации о событиях безопасности, которые поступают в систему от конечных пользовательских устройств («вещей») и элементов сетевой инфраструктуры (маршрутизаторы, антивирусные средства, операционные системы, СУБД, межсетевые экраны и т.д.). Эти события хранятся в соответствующих журналах безопасности.

Источники событий безопасности генерируют большие объемы разнородного трафика, которые можно отнести к категории Больших данных. Поэтому система может конкурировать с традиционными системами сетевой безопасности в случае, если последние не способны справляться с растущими объемами трафика в сети IoT.

Система ориентирована на реализацию в среде Hadoop и включает следующие функциональные компоненты:

– компонент сбора данных, отвечающий за своевременное и достоверное поступление в систему информации о событиях безопасности от источников различных типов;

– компонент хранилища данных, обеспечивающий надежное хранение данных и оперативную обработку запросов;

– компонент нормализации и анализа данных, осуществляющий преобразование собираемых данных к единому формату и выполнение над ними основных операций предварительной обработки;

– компонент визуализации данных, позволяющий в реальном времени проводить визуальный анализ с помощью предварительно разработанных моделей визуализации.

Общая архитектура системы, включающая перечисленные выше компоненты и связи между ними, представлена на рисунке 1. Стрелками указаны направления потоков данных.

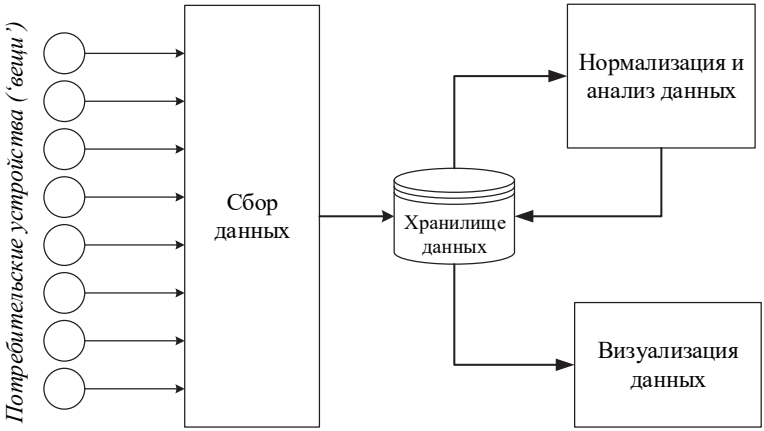


Рис. 1. Архитектура системы

Узлы контролируемой сети IoT отправляют данные для анализа компоненту сбора данных.

Компонент сбора данных организует распределенный прием данных и их хранение в компоненте хранилища данных.

Компонент нормализации и анализа данных получает данные для работы от компонента хранилища данных и в него же передает обратно на сохранение результата своей работы.

Компонент визуализации данных получает от компонента хранилища данных результирующие данные, которые были сформированы компонентом нормализации и анализа данных, и представляет их в виде, удобном для дальнейшего восприятия оператором.

Компонент сбора данных. Этот компонент предназначен для сбора трафика на машинах контролируемой сети IoT и его отправки в компонент хранилища данных.

Узлы (машины), участвующие в работе компонента сбора, по своему функциональному предназначению подразделяются на следующие типы: собирающие, предназначенные для сбора данных; координирующие, предназначенные для управления сбором данных; принимающие, предназначенные для приема собираемых данных. Взаимосвязь между этими типами машин показана на рисунке 2.

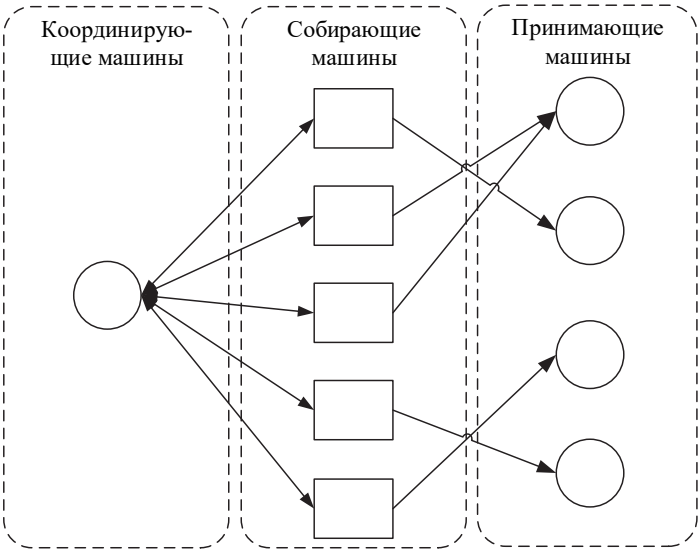


Рис. 2. Взаимосвязь между машинами в компоненте сбора данных

Как правило, координирующая машина присутствует в одном экземпляре и занимается балансировкой потоков трафика, идущего с собирающих машин на принимающие машины.

На собирающие машины контролируемой сети устанавливаются приложения-агенты, выполняющие следующие функции:

– подключение к координирующей машине;

– получение адреса принимающей машины для отправки логов (записей) трафика;

– получение списка принимающих машин для включения их во множество машин, не образующих трафик, который регистрируется при сборе;

– запуск сбора трафика;

– отправка логов трафика на принимающую машину.

Принимающие машины получают логи трафика от собирающих машин и переправляют их в компонент хранилища данных.

Компонент хранилища данных. Этот компонент поддерживает работу распределенного хранилища данных, которое представлено с помощью распределенной файловой системы Hadoop (Hadoop Distributed File System — HDFS) [24]. Файловая система HDFS делит большие файлы на блоки (по умолчанию их размер равен 64 МБ) и сохраняет их на узлах, называемых DataNode. Метаданные, показывающие, каким образом входные данные распределены по узлам DataNodes, хранятся в узле, называемом NameNode. Узел NameNode управляет метаданными в HDFS и администрирует запросы на выдачу данных пользователям. Каждый узел DataNode сохраняет данные, копируя их с компьютера пользователя и распространяя копии блоков между другими узлами DataNode.

DataNode-процессы запущены на каждой принимающей машине. NameNode-процесс запущен только на координирующей машине. Все логи входного трафика загружаются в систему HDFS и доступны после этого для дальнейшей обработки компонентом нормализации и анализа.

Компонент нормализации и анализа данных. Данные, сохраненные компонентом сбора, становятся доступными из системы HDFS для компонента нормализации и анализа.

Нормализация данных заключается в приведении всех входных данных к единому внутреннему формату. В качестве такового формата выбран формат CSV (Comma-Separated Values).

Процесс нормализации данных, реализованный в системе, имеет два режима работы: основной и дополнительный. В основном режиме просматривается содержимое входного файла. Для каждой встретившейся в нем записи формируется отдельная строка в выходном файле с жестко заданным набором атрибутов, определяющим структуру записи. В дополнительном режиме используется фильтр, позволяющий ограничивать выбор только тех записей, которые удовлетворяют описанным в фильтре условиям. Это позволяет снять излишнюю нагрузку, которая может быть вызвана ненужным просмотром данных, не участвующих в анализе.

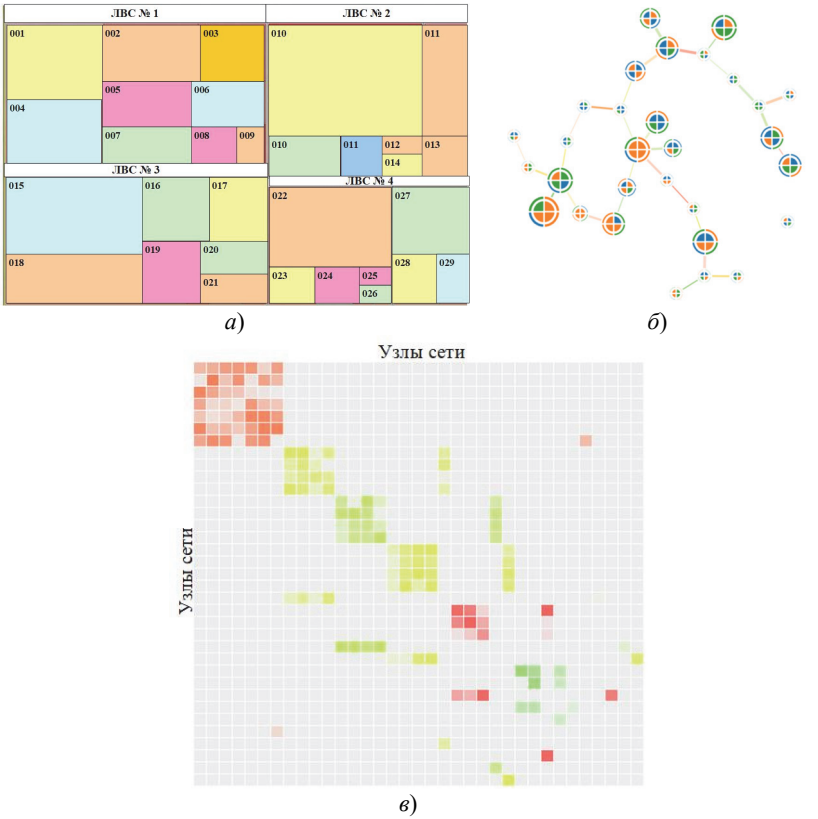
Кроме того, при нормализации с заранее заданной пользователем частотой (ротацией) генерируются выходные CSV-файлы. После этого осуществляется формирование очередных полей, которые записываются в созданные файлы.

Процесс анализа данных заключается в выполнении функций агрегации и корреляции данных. Агрегация представляет собой вычисление мер центральной тенденции (среднего значения, медианы, моды и квантилей). Корреляция призвана выявлять во входном потоке трафика аномальные события негативного характера, используя априори заданные правила. Результаты выполнения функций агрегации и корреляции данных представляются в формате CSV.

Компонент визуализации данных. Этот компонент предназначен для представления пользователю результирующих данных, полученных на этапе анализа в удобном для их визуальной оценки виде. Компонент берет исходные данные из системы HDFS, где они были сохранены после обработки компонентом нормализации и анализа.

Компонент визуализации использует различные стандартные и нестандартные модели визуализации. К стандартным моделям визуализации относятся: гистограммы; круговые диаграммы; линейные графики. Для реализации этих моделей визуализации используются встроенные возможности графических библиотек языка программирования Java.

К нестандартным моделям визуализации (рисунок 3), специально реализованным для мониторинга безопасности сетей IoT, относятся: карты деревьев; графы, дополненные глифами; матрицы.



а) *б*)

в)

Рис. 3. Виды нестандартных моделей визуализации: а) карта деревьев; б) граф с глифами; в) — матрица

Карта деревьев (рисунок 3*а*) отображает элементы сети IoT в виде прямоугольников. Индикаторами различных атрибутов сетевой безопасности являются: цвет, яркость и размер фигуры.

В графе с грифами (рисунок 3*б*) узлы соответствуют элементам сети IoT, а дуги — каналам связи.

Под глифом понимается сектор на круге, закрывающем узел графа. Уровень защищенности элемента характеризуется цветом и размером глифа.

Матрица (рисунок 3*в*) является моделью визуализации, отображающей уровень безопасности телекоммуникаций, соединяющих элементы сети IoT. Столбцы и строки матрицы соответствуют узлам, а ячейки соответствуют линиям связи, соединяющим эти узлы. Цвет и яркость ячейки позволяет кодировать любые две характеристики, например, «важность элемента» и «степень опасности атаки».

4. Реализация системы. С целью оценки производительности разработанной архитектуры был создан вычислительный кластер на базе Hadoop 2.6.4. Аппаратной платформой создания кластера послужила материнская плата Supermicro X9DRL-3F с двумя процессорами Intel Xeon E5-2620 v2 @ 2.1 GHz на борту. На базе гипервизора ESXi 6.0 было создано 7 (6 рабочих и одна главная) виртуальных машин с Ubuntu Server 14.04. Каждой машине было выделено 2 потока с общей тактовой частотой 2 GHz процессора. Также для каждой виртуальной машины было зарезервировано и ограничено 4 GB RAM.

Эти ограничения были вызваны необходимостью соответствия ограничениям типовой сети IoT. Традиционные компьютерные сети могут иметь более мощные вычислительные ресурсы для анализа их трафика. В частности, в традиционных сетях для этих целей можно использовать конфигурацию, в которой одна рабочая/главная машина будет соответствовать Supermicro X9DRL-3F (или аналогичной с одним гнездом под процессор) с процессором Intel Xeon E5-2620 v2 @ 2.1 GHz с 64 GB RAM под управлением Ubuntu Server.

Исходный код Hadoop был собран на одной виртуальной машине и скопирован на остальные машины.

Для моделирования сети IoT были использованы возможности проекта GRANIT, который разрабатывался в Российском прикладном центре компьютерных сетей (http://arccn.ru/media/1385?lang=en). Генерация структуры сети IoT производилась автоматически в соответствии со схемой, исполняемой во встроенном графическом редакторе. Топология сети показана на рисунке 4, где приведен фрагмент панели управления проекта GRANIT.

Первоначальный вариант структуры сети IoT содержал 20 собирающих машин (источников данных) и 10 принимающих машин. Ис-

точники были разбиты на 2 группы: Rack2 и Rack3, на которые было установлено ПО стенда генерации текстовых данных. В группу Rack2 входили машины Virt-slave-2-1, …, Virt-slave-2-10, с ПО, имитирующим кондиционер с функциями регулировки температуры, влажности и тому подобное. В группу Rack3 входили машины Virt-slave-3-1, …, Virt-slave-3-10 с ПО, имитирующим холодильник с функциями регулировки температуры, распознавания содержимого и так далее. Собирающие машины составляли группу Rack1 (машины Virt-slave-1-1, …, Virt-slave-1-10), они получали данные о состоянии устройств в Rack1 и Rack2. Каждая группа была связана с вычислительным кластером.

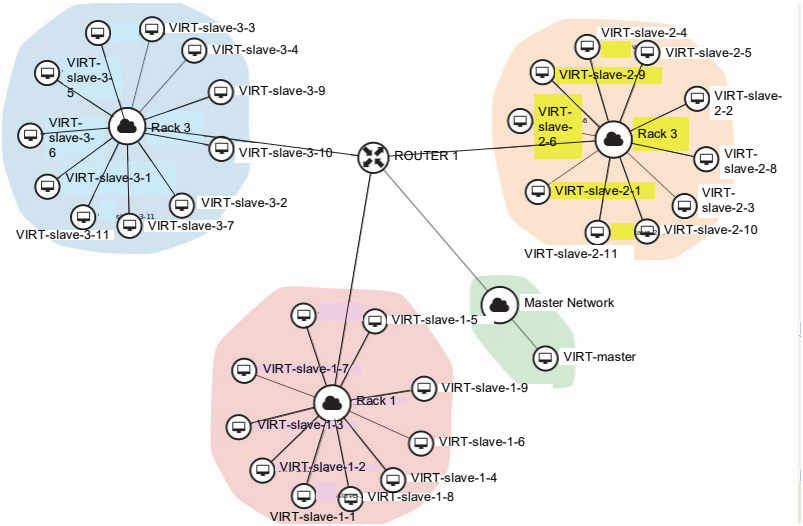


Рис. 4. Контрольная панель топологии сети GRANIT

Управление ресурсами вычислительного кластера осуществлялось с помощью программного средства YARN (Yet Another Resource Negotiator). Компонент YARN входит в состав стандартной конфигурации Hadoop. YARN выделяет ресурсы Hadoop для нужд запускаемых задач и выполняет функцию планировщика задач.

Средство YARN состоит из модуля ResourceManager (RM), который работает на главном узле, и модуля NodeManager (NM), который работает на рабочем узле. Когда на модуль RM поступает запрос на выполнение задачи, он выделяет ресурсы (создает контейнер) у одного из модулей NM и запускает на них процесс ApplicationMaster (AM). Этот процесс определяет, какие ресурсы требуются задаче для ее выполнения, и отправляет запрос модуля RM для выделения контейнеров у моделей NM.

Далее процесс AM получает информацию, на каких модулях NM выделены контейнеры для задачи, и запускает на них процессы выполнения задачи. К тому же процесс AM контролирует штатное исполнение задачи и перезапускает процессы, если они завершились преждевременно.

Модуль NodeManager контролирует состояние конкретных рабочих узлов. Он определяет доступные вычислительные ресурсы и отправляет их модулю RM. Кроме того, он создает и удаляет контейнеры по запросу модуля RM, завершает процессы, которые выходят за рамки ресурсов контейнера, и периодически отправляет тактовые сигналы модулю RM.

Для проведения экспериментов были использованы стандартные настройки YARN и MapReduce, приведенные в таблице 1.

Таблица 1. Настройки YARN и MapReduce

Компонент Hadoop	Параметр	Значение
YARN	yarn.nodemanager.resource.memory-mb	8096
	yarn.scheduler.minimum-allocation-mb	1024
	yarn.scheduler.maximum-allocation-mb	8096
	yarn.scheduler.minimum-allocation-vcores	1
	yarn.scheduler.maximum-allocation-vcores	32
	yarn.nodemanager.vmem-pmem-ratio	2.1
MapReduce	mapreduce.map.memory.mb	1024
	mapreduce.reduce.memory.mb	1024
	mapreduce.map.cpu.vcores	1
	mapreduce.reduce.cpu.vcores	1

Важной задачей реализации системы являлась подготовка исходных данных для моделирования. Входные потоки данных должны были содержать информацию о двух типах событий безопасности:

– о событиях, описывающих сетевой трафик и отражающих легитимную и вредоносную активность;

– о событиях, заключающихся в изменениях программно-аппаратных конфигураций персональных компьютеров, сетевого оборудования и потребительских устройств.

Для этой цели входные данные формировались двумя способами:

– программно-аппаратным стендом генерации тестовых наборов гетерогенных данных;

– на основе внешней базы экспериментальных данных о трафике компьютерной сети.

Программно-аппаратный стенд генерации тестовых наборов гетерогенных данных включал следующие элементы:

– десять персональных компьютеров, из них 8 были реализованы в рамках системы виртуализации;

– три маршрутизатора ASUS RT-N16, по одному для каждой подсети стенда;

– четыре элемента распределенной сети электронных потребительских устройств на базе контроллера Arduino Yun;

– один межсетевой экран, который осуществлял фильтрацию пакетов по заранее настроенным правилам.

В состав программных средств стенда входили следующие программные средства:

– сканер безопасности Nessus Home;

– система анализа трафика Wireshark 1.12.2;

– сетевой сканер NMap 6.47;

– система MetaSploit Framework 4.0;

– система обнаружения вторжений Snort 2.9.7.0.

В качестве внешней базы экспериментальных данных о трафике компьютерной сети использовалась база данных MAVILab [25]. Эта база данных содержит в архивном виде данные о реальном сетевом трафике, циркулирующем между Японией и США и содержащем пакеты различных форматов (tcp, http, ftp и т.д.). Данные из этого источника удовлетворяют требованиям гетерогенности, которые характерны и для сетей IoT. Непосредственно для анализа используются наборы данных, получаемые путем интеграции фонового трафика MAVILab и трафика, сгенерированного тестовым стендом IoT.

Файлы, входящие в состав внешней базы данных, соответствуют сетевому трафику длительностью до 15 минут. Все файлы имеют формат *.pcap.

Использование внешней базы данных позволило включить в состав тестовых данных события, описывающие реальный сетевой трафик, отражающий легитимную и вредоносную активность. Это сделало возможной проверку разработанной системы в условиях, максимально приближенных к условиям реальной эксплуатации системы.

5. Экспериментальные исследования. На текущем этапе создания системы обработки данных для мониторинга безопасности сетей IoT экспериментальной оценке и всестороннему тестированию был подвергнут только компонент нормализации и анализа данных. Цель экспериментов заключалась в определении производительности этого компонента при решении задач распределенного анализа собираемых данных в интересах мониторинга сетевой безопасности. При этом входные потоки представлялись в виде файла большого объема, поступающего на обработку в разработанный компонент. Задержки между событиями безопасности, имеющие место в реальных потоках, не

учитывались, так как при обработке больших объемов данных их влияние не является существенным. Учет таких задержек планируется осуществлять в дальнейших работах.

Анализ входных потоков данных, представляющих собой слияние потоков, генерируемых программно-аппаратным стендом, и потоков, содержащихся во внешней базе данных, проводился на основе заданных правил. В частности, в качестве одного из таких типовых правил использовалось следующее утверждение: «событие безопасности о сканировании портов регистрируется только в том случае, если с одного и того же IP-адреса на другой IP-адрес были высланы пакеты на более чем 10 портов, причем на каждый порт пришлось менее 5 пакетов».

Также в качестве тестовой задачи проводилась агрегация по одному из полей заголовка TCP-пакета, в роли которого выступало поле `src_ip`, определяющее IP-адрес источника.

Всего тестовая программа анализа содержала четыре задачи MapReduce, из которых две отводились на исполнение выше описанного правила и две исполняли функцию агрегации.

Решение задачи анализа по правилу осуществлялось в два этапа. На первом этапе на фазе Map из всего tcp-заголовка в качестве ключа выбирался триплет <`src_ip`, `dst_ip`, `dst_port`>. В качестве значения передавалась единица. Таким образом, на фазе Reduce путем сложения сгруппированных по ключу значений вычислялось количество пакетов, пришедших на конкретный порт конечного IP-адреса с другого IP-адреса. При записи результата ключ оставался без изменения, а в качестве значения передавалось суммарное количество пакетов, поступающее на этот порт. Причем, согласно условию задачи, в выходной файл попадали только те пары «ключ — значение», где сумма пакетов, поступающих на порт, была меньше пяти.

На втором этапе анализа по приведенному выше правилу на фазе Map в качестве ключа выбиралась пара <`src_ip`, `dst_ip`>. В качестве значения отправлялась функция `count`(), определяющая количество пакетов, поступивших на порт (из предыдущего этапа MapReduce). На фазе Reduce количество значений по каждому ключу оказывалось равным количеству портов, на которые передавались пакеты с исходящего IP-адреса на целевой IP-адрес. Согласно условию задачи, если количество портов больше 10, то ключ и количество портов записывались в выходной файл.

Агрегация проводилась по одному из полей tcp-заголовка. Эта задача решалась также в два этапа. На первом этапе, например, для поля `src_ip`, в фазе Map ключом являлось `src_ip`, а значением —

единица. Таким образом, в фазе Reduce путем сложения значений по ключам определялось, сколько вхождений имеет тот или иной `src_ip` в исходных логах. На втором этапе в фазе Map пришедшая пара «ключ — значение» передавалось на Reduce в качестве значения, а сам ключ оставался пустым. В фазе Reduce выполнялся поиск максимального и минимального числа вхождений `src_ip`, а также вычислялось среднее число вхождений.

В ходе экспериментальных исследований проводились многократные замеры времени обработки больших массивов данных, соответствующих входным потокам системы мониторинга сетевой безопасности, в зависимости от объемов этих файлов и количества рабочих машин, входящих в кластер Hadoop. Объемы файлов со входными потоками изменялись в диапазоне от 0,5 до 3 ГБ. Количество машина в вычислительном кластере равнялось 3, 5 или 7 единиц.

Результаты экспериментальной оценки времени обработки файлов входных потоков в зависимости от объема нагрузки и количества узлов в кластере представлены в таблице 2 и на рисунке 5. Учитывалось «чистое» время обработки нагрузки без учета настройки Hadoop. Экспериментальные оценки рассчитывались как средние арифметические значения за 50 прогонов.

Таблица 2. Длительности обработки входной нагрузки (сек)

Объем входной нагрузки, ГБ	Количество узлов в кластере		
	3	*5*	*7*
0,5	76,41	61,85	51,65
1,0	135,98	106,38	102,00
1,5	208,18	161,35	158,93
2,0	322,28	202,32	179,05
2,5	409,81	259,08	210,91
3,0	522,30	357,98	245,12

Так как рассматриваемая система мониторинга сетевой безопасности является разновидностью CEP-систем, то представляет интерес зависимость времени обработки данных не от объема входной нагрузки, а от количества содержащихся в ней событий. Оценка объема данных, содержащихся в файлах формата *.pcap, показывает, что средний объем одной записи в файле формата *.pcap составляет примерно 600…620 байт. Выберем для него значение 612 байт.

Тогда можно перейти от данных, представленных в таблице 2 и на рисунке 5, к зависимости времени обработки данных от количества узлов в кластере и от количества событий, поступивших на обработку (рисунок 6).

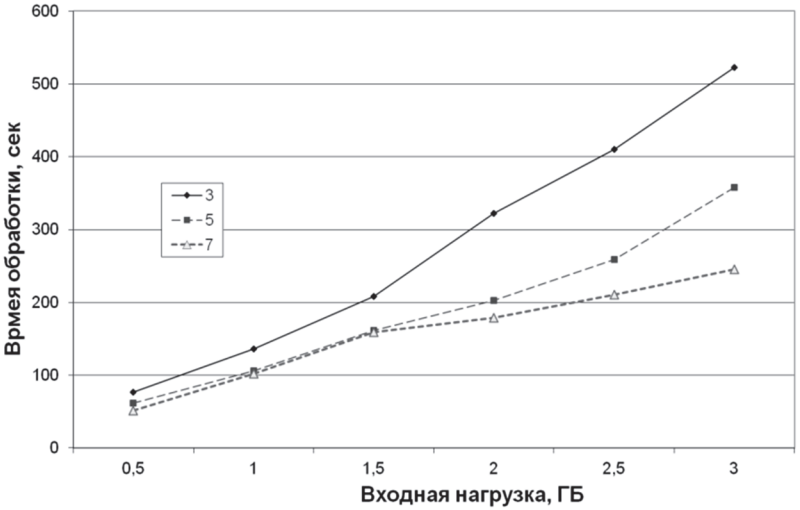


Рис. 5. Зависимость длительности обработки данных от объема входной нагрузки и количества узлов в кластере

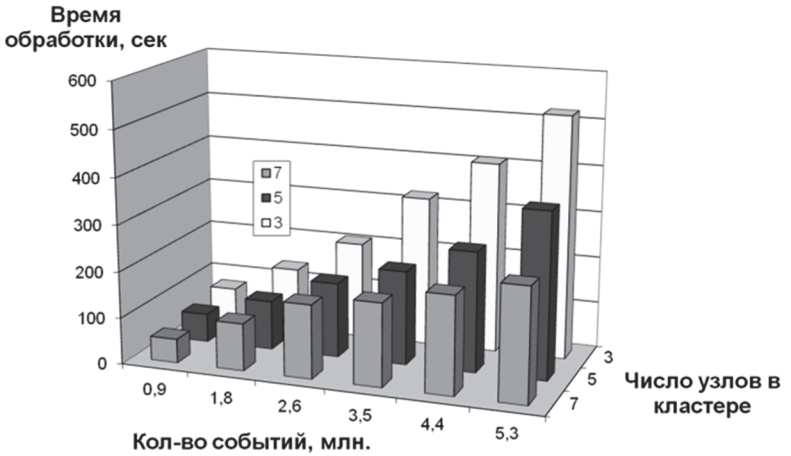


Рис. 6. Зависимость длительности обработки данных от количества обрабатываемых событий и количества узлов в кластере

От зависимости, приведенной на рисунке 6, перейдем к оценке производительности системы мониторинга, которую будем измерять с помощью количества событий, обработанных за единицу времени. Вве-

дем в рассмотрение интегральную и частную производительности системы. Интегральная производительность системы определяется как:

$$ИнтегральнаяПроизводительность = \frac{ЧислоСобытий}{ВремяОбработки}, \quad (1)$$

где *ЧислоСобытий* — общее количество обработанных событий; *ВремяОбработки* — среднее время обработки событий (сек).

Частная производительность системы определяется следующим образом:

$$ЧастнаяПроизводительность = \frac{ЧислоСобытий}{ВремяОбработки * ЧислоУзлов}, \quad (2)$$

где *ЧислоУзлов* — количество узлов в вычислительном кластере.

Результаты расчета интегральной и частной производительности по формулам (1) и (2) приведены на рисунках 7 и 8.

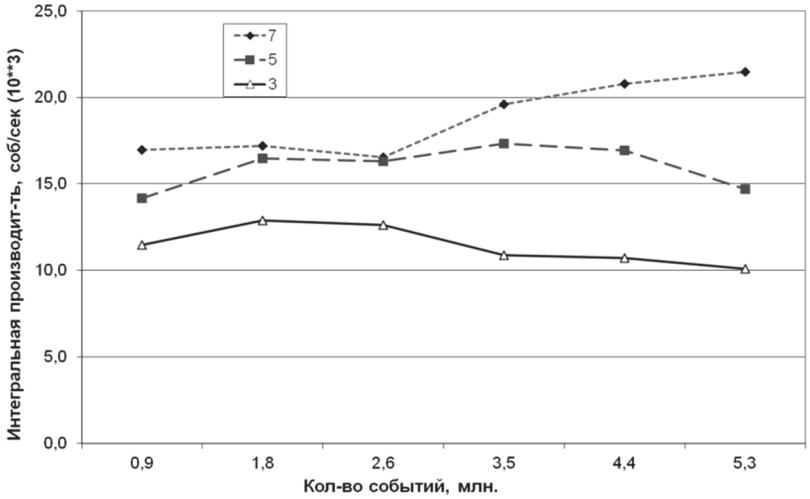


Рис. 7. Зависимость интегральной производительности системы от количества обрабатываемых событий и количества узлов в кластере

Анализ этих данных позволяет сделать следующие выводы. Во-первых, увеличение количества узлов в вычислительном кластере приводит к увеличению интегральной производительности системы. Это видно, если сравнивать между собой графики на рисунке 7 при различных значениях параметра *ЧислоСобытий*.

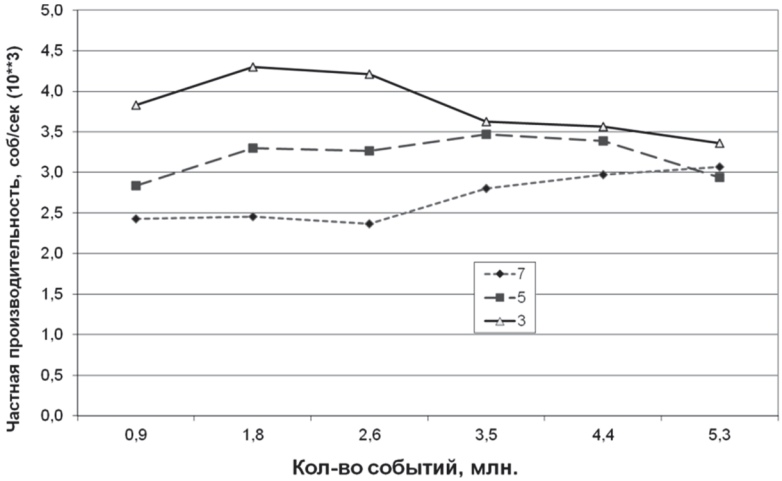


Рис. 8. Зависимость частной производительности системы от количества обрабатываемых событий и количества узлов в кластере

В то же время для частной производительности системы наблюдается другая картина. Частная производительность системы при конфигурации, в которой *ЧислоУзлов* = 3, практически при всех объемах входной нагрузки является максимальной. Правда, при большой и средней нагрузке она начинает падать. В этом случае она практически совпадает с частной производительностью для конфигурации, в которой *ЧислоУзлов* = 5. А при большой нагрузке для всех трех конфигураций частная производительность совпадает.

Кроме того, из рисунка 7 видно, при каких нагрузках и конфигурациях частная производительность достигает своего максимума.

Для условия *ЧислоУзлов* = 3 максимум частной производительности достигается при малой нагрузке, находящейся в диапазоне от 0,9 до 2,6 миллионов событий. В этом случае частная производительность достигает пика, равного $4{,}3*10^3$ событий в секунду. Для конфигурации, в которой *ЧислоУзлов* = 5, максимум частной производительности достигается при средней нагрузке (от 2,6 до 4,4 миллионов событий). Этот максимум равняется $3{,}5*10^3$ событий в секунду. Наконец, для условия *ЧислоУзлов* = 7 максимум частной производительности достигается при большой нагрузке (от 4,4 до 5,6 миллионов событий). Тенденция увеличения частной производительности сохраняется. Можно ожидать, что при дальнейшем увеличении входной нагрузки значение частной производительности будет и дальше увеличиваться.

Такое поведение частной производительности при различной входной нагрузке объясняется следующими причинами. Во-первых,

для конфигурации, в которой *ЧислоУзлов* = 3, каждый узел кластера очень быстро нагружается. Однако при дальнейшем увеличении нагрузки кластерные узлы испытывают перегрузку, что отражается на снижении частной производительности. Насыщение узлов при условии *ЧислоУзлов* = 5 происходит при средней входной нагрузке. Дальнейшее ее увеличение может привести в перегрузке узлов кластера. При условии *ЧислоУзлов* = 7 для рассматриваемых объемов входной нагрузки никакой перегрузки узлов не наблюдается. Узлы постепенно входят в насыщение.

Некоторые расхождения измерений на рисунках 7 и 8 от описанных выше общих тенденций поведения интегральной и частной производительности можно объяснить рядом причин, которые определяются принципами работы Hadoop и, в частности, файловой системы HDFS. В наших экспериментах система HDFS была развернута на одних и тех же жестких дисках. В результате в ряде случаев работу Hadoop могли тормозить блокировки при обращении к узлам DataNode, расположенных на одном и том же жестком диске. Нам следовало бы разнести все узлы DataNode по разным жестким дискам. Однако этот случай мы рассматриваем как будущие исследования.

Завершая анализ полученных экспериментальных результатов, следует отметить, что они не противоречат результатам, полученным в других известных работах [9, 10, 12]. Это позволяет говорить, что производительность разработанной нами системы является не хуже, чем для известных систем, несмотря на наличие вычислительных ограничений, свойственных сетям IoT.

6. Заключение. В настоящей статье предложен новый подход к построению систем мониторинга безопасности сетей IoT, основанный на реализации параллельной потоковой обработки данных о событиях безопасности. Согласно этому подходу, система мониторинга сетевой безопасности реализуется на платформе Hadoop с возможностью использования технологии CEP. Предлагаемая архитектура разрабатываемой системы параллельной обработки данных для мониторинга безопасности сетей IoT включает компоненты, ответственные за сбор, хранение, нормализацию и анализ, а также визуализацию данных. Нормализация, анализ и визуализация данных осуществляются в режиме «на лету». Хранение данных осуществляется в распределенной файловой системе Hadoop, что повышает надежность хранения и оперативность обработки запросов к данным.

Реализация системы для проведения ее экспериментальной оценки была выполнена с учетом вычислительных ограничений, свойственных сетям IoT. Входные потоки моделировались путем использо-

вания специального стенда, генерирующего события безопасности во фрагменте сети IoT, и использования внешней базы данных о трафике в реальной компьютерной сети. Экспериментальная оценка разработанной системы показала, что, несмотря на наличие ограничений в вычислительных ресурсах, система обладает достаточно высокой производительностью, сравнимой, а в некоторых случаях значительно превышающей известные реализации.

Дальнейшие исследования планируется проводить в направлении совершенствования разработанной системы мониторинга сетевой безопасности за счет повышения скорости обращений к блокам данных файловой системы HDFS и более широкого внедрения средств реализации CEP. В частности, планируется реализовать компонент нормализации и анализа данных в среде Spark. Также планируется изучить влияние пропускной способности устройств сети IoT на эффектность работы системы.

Литература

1. *Котенко И.В., Саенко И.Б.* SIEM-системы для управления информацией и событиями безопасности // «Защита информации. Инсайд». 2012. № 5. С. 54–65.
2. *Котенко И.В., Саенко И.Б.* Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН. 2012. № 3(22). С. 84–100.
3. *Котенко И.В.* Интеллектуальные механизмы управления кибербезопасностью // Труды Института системного анализа Российской академии наук. 2009. Т. 41. С. 74–103.
4. *Kotenko I., Chechulin A.* Attack Modeling and Security Evaluation in SIEM Systems // International Transactions on Systems Science and Applications. 2012. vol. 8. pp. 129–147.
5. *De Carvalho O.M., Roloff E., Navaux O.A.* A Survey of the State-of-the-art in Event Processing // Proceedings of the 11th Workshop on Parallel and Distributed Processing (WSPPD). 2013. 16 p.
6. Apache Hadoop 3.0.0-alpha4. URL: http://hadoop.apache.org/docs/current/ (дата обращения: 01.06.2017).
7. Holmes A. Hadoop in Practice // Manning Publications Co. 2012. 536 p.
8. *Scherbakov M. et al.* A Design of Web Application for Coomplex Event Processing Based on Hadoop and Java Servlets // International Journal of Soft Computing. 2015. vol. 10. no. 3. pp. 218–219.
9. *Kim M.-J., Yu Y.-S.* Development of Real-time Big Data Analysis System and a Case Study on the Application of Information in a Medical Institution // International Journal of Software Engineering and Its Applications. 2015. vol. 9. no. 7. pp. 93–102.
10. *Zygouras N. et al.* Insights on a Scalable and Dynamic Traffic Management System // Proceedings of the 18th International Conference on Extending Database Technology (EDBT-2015). 2015. pp. 653–664.
11. *Cherniack M. et al.* Scalable Distributed Stream Processing // Proceedings of the First Biennial Conference on Innovative Data Systems Research (CIDR'03). 2003. vol. 3. pp. 257–268.
12. *Schultz-Møller N.P., Migliavacca M., Pietzuch P.* Distributed Complex Event Processing with Query Rewriting // Proceedings of the Third ACM International Conference on Distributed Event-Based Systems. 2009. Article no. 4. 12 p.

13. *Zhang H., Diao Y., Immerman N.* On Optimization of Expensive Queries in Complex Event Processing // Proceedings of the 2014 ACM SIGMOD International Conference on Management of Data (SIGMOD '14). 2014. pp. 217–228.
14. *Moraru A., Mladenić D.* Complex Event Processing and Data Mining for Smart Cities // Proceedings of the 15th International Multiconference on Information Society (IS-2012). 2012. 4 p. URL: http://ailab.ijs.si/dunja/SiKDD2012/Papers/Moraru_CEP.pdf (дата обращения: 01.06.2017).
15. *Gyllstrom D. et al.* SASE: Complex Event Processing over Streams // 2006. arXiv preprint cs/0612128. 4 p. URL: https://arxiv.org/ftp/cs/papers/0612/0612128.pdf (дата обращения: 01.06.2017).
16. *Liu D., Pedrinaci C., Domingue J.* A framework for feeding Linked Data to Complex Event Processing engines // 1st International Workshop on Consuming Linked Data (COLD 2010) at The 9th International Semantic Web Conference (ISWC 2010). 2010. 12 p. URL: http://oro.open.ac.uk/26057/1/LiuEtAl_COLD2010.pdf (дата обращения: 01.06.2017).
17. *Anicic D., Rudolph S., Fodor P., Stojanovic N.* Stream reasoning and complex event processing in ETALIS // Semantic Web. 2012. vol. 3. no. 4. pp. 397–407.
18. *Wang D., Rundensteiner E.A., Ellison R.T.* Active Complex Event Processing over Event Streams // Proceedings of the VLDB Endowment. 2011. vol. 4. no. 10. pp. 634–645.
19. *Gulisano V., Jimenez-Peris R., Patino-Martinez M., Valduriez P.* StreamCloud: A Large Scale Data Streaming System // Proceedings of the 2010 International Conference on Distributed Computing Systems. 2010. pp. 126–137.
20. *Gulisano V. et al.* StreamCloud: An Elastic and Scalable Data Streaming System // IEEE Transactions on Parallel and Distributed Systems. 2012. vol. 23. no. 12. pp. 2351–2365.
21. *Kotenko I., Saenko I.* An Approach to Aggregation of Security Events in Internet-of-Things Networks Based on Genetic Optimization // Proceedings of the 16th IEEE International Conference on Scalable Computing and Communications (ScalCom 2016). 2016. pp. 657–664.
22. *Толстолес А.А. и др.* Платформа для разработки приложений Интернета вещей на основе модуля анализа больших данных // Информатика и кибернетика (ComCon-2016): Сб. научн. конф. Института компьютерных наук и технологий (ИКНТ). 2016. С. 192–194.
23. *Гончарова М.Н.* Механизм параллельной обработки больших объемов информации в документо-ориентированных системах управления базами данных // Вестник магистратуры. 2014. № 6–1(33). С. 52–56.
24. *Dwivedi K., Dubey S.K.* Analytical review on Hadoop Distributed file system // Proceedings of the 5th International Conference on Confluence the Next Generation Information Technology Summit (confluence). 2014. pp. 174–181.
25. MAVILab URL: http://www.fukuda-lab.org/mawilab/index.html (дата обращения: 01.06.2017).

Котенко Игорь Витальевич — д-р техн. наук, профессор, заведующий лабораторией проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: безопасность компьютерных сетей, в том числе управление политиками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, защита программного обеспечения от взлома и управление цифровыми правами, технологии моделирования и визуализации для противодействия кибер–терроризму. Число научных публикаций — 500.

ivkote@comsec.spb.ru, http://www.comsec.spb.ru; 14-я линия В.О., 39, Санкт-Петербург, 199178; р.т.: +7-(812)328-7181, Факс: +7(812)328–4450.

Саенко Игорь Борисович — д-р техн. наук, профессор, ведущий научный сотрудник лаборатории проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: автоматизированные информационные системы, информационная безопасность, обработка и передача данных по каналам связи, теория моделирования и математическая статистика, теория информации. Число научных публикаций — 350. ibsaen@comsec.spb.ru, http://www.comsec.spb.ru; 14-я линия В.О., 39, Санкт-Петербург, 199178; р.т.: +7(812)328-7181, Факс: +7(812)328-4450.

Кушнеревич Алексей Геннадьевич — младший научный сотрудник лаборатории проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: большие данные, анализ данных. Число научных публикаций — 4. kushnerevich@comsec.spb.ru, http://www.comsec.spb.ru; 14-я линия В.О., 39, Санкт-Петербург, 199178; р.т.: +7(812)328-7181, Факс: +7(812)328-4450.

Поддержка исследований. Работа выполнена при финансовой поддержке РФФИ (проекты 16-29-09482, 18-07-01369 и 18-07-01488), при частичной поддержке бюджетной темы № АААА-А16-116033110102-5, а также при государственной финансовой поддержке ведущих университетов Российской Федерации (субсидия 074-U01).

DOI 10.15622/sp.59.1

I.V. KOTENKO, I.B. SAENKO, A.G. KUSHNEREVICH

ARCHITECTURE OF THE PARALLEL BIG DATA PROCESSING SYSTEM FOR SECURITY MONITORING OF INTERNET OF THINGS NETWORKS

Kotenko I.V., Saenko I.B., Kushnerevich A.G. **Architecture of the Parallel Big Data Processing System for Security Monitoring of Internet of Things Networks.**

Abstract. Internet-of-Things networks are applied in many areas of people life now. A cornerstone in a issue of a possibility of further distribution and use of these networks is the aspect of security support. However, the features of these networks complicate the use of traditional means and systems of computer protection in them. One of such features is the need to analyze very large volumes of data, heterogeneous by the nature, in real time and with the minimum computing expenses. Taking into account the features of computational capabilities of Internet-of-Things networks the architecture of the system for parallel big data processing based on the data processing technology named as Complex Event Processing and the parallel computing platform Hadoop is offered. The issues directly connected to the architecture of the system and with implementation of its principal components are considered. These components are: data collection component, data storage component, data normalization and analysis component, and data visualization component. An interconnection between components is provided by means of the Hadoop Distributed File System that is a basis for creation of the distributed data storage. The data collection component organizes the distributed data acquisition and their storage in the data storage component. The data normalization and analysis component transforms data to a uniform format and processes them by means of correlation rules. The data visualization component presents data in a graphical form more suitable for further perception by the operator. The results of the experimental evaluation of the system performance confirming a conclusion about its high performance are discussed.

Keywords: Internet of things; security monitoring; Big Data; Complex Event Processing; Hadoop.

Kotenko Igor Vitalievich — Ph.D., Dr. Sci., professor, head of computer security problems laboratory, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: computer network security, including security policy management, access control, authentication, network security analysis, intrusion detection, firewalls, deception systems, malware protection, verification of security systems, digital right management, modeling, simulation and visualization technologies for counteraction to cyber terrorism. The number of publications — 500. ivkote@comsec.spb.ru, http://www.comsec.spb.ru; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7-(812)328-7181, Fax: +7(812)328–4450.

Saenko Igor Borisovich — Ph.D., Dr. Sci., professor, leading researcher of computer security problems laboratory, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: automated information systems, information security, processing and transfer of data on data links, theory of modeling and mathematical statistics, information theory. The number of publications — 350. ibsaen@comsec.spb.ru, http://www.comsec.spb.ru; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328-7181, Fax: +7(812)328-4450.

Kushnerevich Alexey Gennadievich — junior researcher computer security problems laboratory, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS). Research interests: Big Data, data analysis. The number of publications — 4. kushnerevich@comsec.spb.ru, http://www.comsec.spb.ru; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328-7181, Fax: +7(812)328-4450.

Acknowledgements. This research was supported by grants of RFBR (projects No. 16-29-09482, 18-07-01369 and 18-07-01488), by the budget (the project No. AAAA-A16-116033110102-5), and by Government of the Russian Federation (grant 074-U01).

References

1. Kotenko I.V., Saenko I.B. SIEM-systems for security information and event management. *Zashhita informacii. Insajd — Zaŝita informacii. Inside*. 2012. vol. 5. pp. 54–65. (In Russ.).
2. Kotenko I.V., Saenko I.B. Developing the system of intelligent services to protect information in cyber warfare. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2012. vol. 3(22). pp. 84–100. (In Russ.).
3. Kotenko I.V. Intelligent mechanisms of cybersecurity management. *Trudy Instituta sistemnogo analiza Rossijskoj akademii nauk – Proceedings of the Institute of System Analysis of the Russian Academy of Sciences*. 2009. vol. 41. pp. 74–103. (In Russ.).
4. Kotenko I., Chechulin A. Attack Modeling and Security Evaluation in SIEM Systems. *International Transactions on Systems Science and Applications*. 2012. vol. 8. pp. 129–147.
5. De Carvalho O.M., Roloff E., Navaux O.A. A Survey of the State-of-the-art in Event Processing. Proceedings of the 11th Workshop on Parallel and Distributed Processing (WSPPD). 2013. 16 p.
6. Apache Hadoop 3.0.0-alpha4. Available at: http://hadoop.apache.org/docs/current/ (accessed: 01.06.2017).
7. Holmes A. Hadoop in Practice. Manning Publications Co. 2012. 536 p.
8. Scherbakov M. et al. A Design of Web Application for Coomplex Event Processing Based on Hadoop and Java Servlets. *International Journal of Soft Computing*. 2015. vol. 10. no. 3. pp. 218–219.
9. Kim M.-J., Yu Y.-S. Development of Real-time Big Data Analysis System and a Case Study on the Application of Information in a Medical Institution. *International Journal of Software Engineering and Its Applications*. 2015. vol. 9. no. 7. pp. 93–102.
10. Zygouras N. et al. Insights on a Scalable and Dynamic Traffic Management System. Proceedings of the 18th International Conference on Extending Database Technology (EDBT-2015). 2015. pp. 653–664.
11. Cherniack M. et al. Scalable Distributed Stream Processing. Proceedings of the First Biennial Conference on Innovative Data Systems Research (CIDR'03). 2003. vol. 3. pp. 257–268.
12. Schultz-Møller N.P., Migliavacca M., Pietzuch P. Distributed Complex Event Processing with Query Rewriting. Proceedings of the Third ACM International Conference on Distributed Event-Based Systems. 2009. Article no. 4. 12 p.
13. Zhang H., Diao Y., Immerman N. On Optimization of Expensive Queries in Complex Event Processing. Proceedings of the 2014 ACM SIGMOD International Conference on Management of Data (SIGMOD '14). 2014. pp. 217–228.
14. Moraru A., Mladenić D. Complex Event Processing and Data Mining for Smart Cities. Proceedings of the 15th International Multiconference on Information Society15th International Multiconference on Information Society (IS-2012). 2012. 4 p. Available at: http://ailab.ijs.si/dunja/SiKDD2012/Papers/Moraru_CEP.pdf (accessed: 01.06.2017).

15. Gyllstrom D. et al. SASE: Complex Event Processing over Streams. 2006. arXiv preprint cs/0612128. 4 p. Available at: https://arxiv.org/ftp/cs/papers/0612/0612128.pdf (accessed: 01.06.2017).
16. Liu D., Pedrinaci C., Domingue J. A framework for feeding Linked Data to Complex Event Processing engines. Proceedings of the 1st International Workshop on Consuming Linked Data (COLD 2010) at The 9th International Semantic Web Conference (ISWC 2010). 2010. 12 p. Available at: http://oro.open.ac.uk/26057/1/LiuEtAl_COLD2010.pdf (accessed: 01.06.2017).
17. Anicic D., Rudolph S., Fodor P., Stojanovic N. Stream reasoning and complex event processing in ETALIS. *Semantic Web*. 2012. vol. 3. no. 4. pp. 397–407.
18. Wang D., Rundensteiner E.A., Ellison R.T. Active Complex Event Processing over Event Streams. Proceedings of the VLDB Endowment. 2011. vol. 4. no. 10. pp. 634–645.
19. Gulisano V., Jimenez-Peris R., Patino-Martinez M., Valduriez P. StreamCloud: A Large Scale Data Streaming System. Proceedings of the 2010 International Conference on Distributed Computing Systems. 2010. pp. 126–137.
20. Gulisano V. et al. StreamCloud: An Elastic and Scalable Data Streaming System. *IEEE Transactions on Parallel and Distributed Systems*. 2012. vol. 23. no. 12. pp. 2351–2365.
21. Kotenko I., Saenko I. An Approach to Aggregation of Security Events in Internet-of-Things Networks Based on Genetic Optimization. Proceedings of the 16th IEEE International Conference on Scalable Computing and Communications (ScalCom 2016). 2016. pp. 657–664.
22. Tolstoles A.A. et al. [Software platform based on Big-Data anasysis module for development Internet-of-Things applications]. *Informatika i kibernetika (ComCon-2016): Sb. nauchn. konf. Instituta komp'juternyh nauk i tehnologij (IKNT)* [Informatics and Cybernetics (ComCon-2016): Proceedings]. 2016. pp. 192–194. (In Russ.).
23. Goncharova M.N. [Mechanism of parallel Big Data analysis in document-oriented DBMSs]. *Vestnik magistratury — Gerald of magistracy*. 2014. vol. 6–1(33). pp. 52–56. (In Russ.).
24. Dwivedi K., Dubey S.K. Analytical review on Hadoop Distributed file system. Proceedings of the 5th International Conference on Confluence the Next Generation Information Technology Summit (confluence). 2014. pp. 174–181.
25. MAVILab Available at: http://www.fukuda-lab.org/mawilab/index.html (accessed: 01.06.2017).

УДК 512.624.5 **DOI** 10.15622/sp.59.2

Д.В. САМОЙЛЕНКО, М.А. ЕРЕМЕЕВ, О.А. ФИНЬКО, С.А. ДИЧЕНКО

ПАРАЛЛЕЛЬНЫЙ ЛИНЕЙНЫЙ ГЕНЕРАТОР МНОГОЗНАЧНЫХ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С КОНТРОЛЕМ ОШИБОК ФУНКЦИОНИРОВАНИЯ

Самойленко Д.В., Еремеев М.А., Финько О.А., Диченко С.А. **Параллельный линейный генератор многозначных псевдослучайных последовательностей с контролем ошибок функционирования.**

Аннотация. Предложен параллельный линейный генератор многозначных псевдослучайных последовательностей, функционирующий в условиях генерации аппаратных ошибок, обусловленных деструктивными воздействиями злоумышленника. Рассмотрены основные виды модификации псевдослучайной последовательности при атаках злоумышленника. Отличительной особенностью рассматриваемого итеративного процесса обеспечения достоверности вычислительных операций является «арифметизация» вычислительных операций путем представления системы порождающих рекуррентных логических формул как системы многозначных функций алгебры логики. Последующая реализация многозначных функций алгебры логики посредством арифметических полиномов позволила распараллелить процесс генерации многозначных псевдослучайных последовательностей и нивелировать существующую сложность (специфику) криптографических преобразований логических типов данных, ограничивающих применение методов избыточного кодирования. В результате предложено решение, позволяющее применить избыточные модулярные коды для контроля безошибочности производимых вычислительных операций узлами генерации псевдослучайной последовательности. Причем в отличие от известных решений предлагаемый метод обеспечивает получение фрагментов псевдослучайной последовательности на основании одной рекурсивной арифметической формулы с параллельным контролем ошибок вычислений. Применение модулярных форм позволило перенести вычисления из арифметики поля рациональных чисел в целочисленную арифметику простого поля.

Среди существующего многообразия кодов, исправляющих ошибки (максимально разнесенных кодов), особое место занимают многозначные коды Рида — Соломона. Применение кодов Рида — Соломона при формировании псевдослучайных последовательностей позволяет формировать кодоподобные структуры, осуществляющие контроль и обеспечение достоверности вычислительных операций. Получены расчетные данные вероятности безотказной работы параллельного линейного генератора многозначных псевдослучайных последовательностей с функцией контроля ошибок по принципу функционирования — скользящее резервирование. Достигнутые результаты могут найти широкое применение при реализации перспективных высокопроизводительных средств криптографической защиты информации.

Ключевые слова: *q*-значные псевдослучайные последовательности, линейные рекуррентные регистры сдвига, модулярная арифметика, модулярные формы многозначных функций алгебры логики, средства криптографической защиты информации.

1. Введение.

Для защищенных информационных систем средства криптографической защиты информации (СКЗИ) являются ключевыми и направленны на обеспечение качественных характеристик целевой функции — информирования [1-3].

Особенность реальных условий функционирования СКЗИ характеризуется наличием ряда независимых деструктивных воздействий (атак) злоумышленника, целью которых является снижение безопасности функционирования узлов СКЗИ. При этом среди существующего многообразия известных атак злоумышленника на СКЗИ [4, 5] особым считается вид атак, основанный на инициализации аппаратных ошибок функционирования СКЗИ и направленный на генерацию массовых сбоев их электронных компонентов. Легко заметить, что среди основных компонентов СКЗИ наиболее чувствительными к атакам, основанным на инициализации аппаратных ошибок функционирования, являются генераторы псевдослучайных последовательностей (ПСП) [5]. На рисунке 1 представлена схема основных видов модификации ПСП.

При этом очевидна прямая зависимость безопасного функционирования СКЗИ от узлов формирования ПСП, качества которых во многом определяют свойства СКЗИ в целом.

В настоящее время для обеспечения безошибочности производимых преобразований узлами формирования ПСП разработано множество методов, наиболее распространенными из которых являются структурные методы обнаружения ошибок: поэлементное резервирование, дублирование, избыточная логика и другие, обеспечивающие достаточную обнаруживающую способность, однако при этом требующие больших аппаратурных затрат [6]. Из области цифровой схемотехники известны решения, обеспечивающие безошибочность производимых преобразований над двоичными ПСП, которые основаны на использовании методов избыточного блочного кодирования. Однако в ряде случаев специфика (сложность) криптографических преобразований логических типов данных ограничивает применение данных методов контроля.

В работах [7, 8] предложены решения, преодолевающие сложность применения кодового контроля узлов формирования двоичной ПСП, основанные на «арифметизации» логического счета и применения аппарата кодов системы остаточных классов, обеспечивающие необходимый уровень достоверности их функционирования. Однако особенность полученных решений ограничивается исключительной применимостью при формировании двоичных ПСП. Вместе с тем дальнейшее развитие и проектирование перспективных СКЗИ многие специалисты связывают с применением многозначных функций алгебры логики (МФАЛ) [9, 10]. Применительно к многозначным ПСП, такие решения обусловлены в первую очередь наличием более широкого спектра уникальных свойств по сравнению с двоичной ПСП [10-12]. Вследствие этого возникает необходимость обобщения полученных решений для обеспечения достоверности функционирования узлов формирования многозначных ПСП.

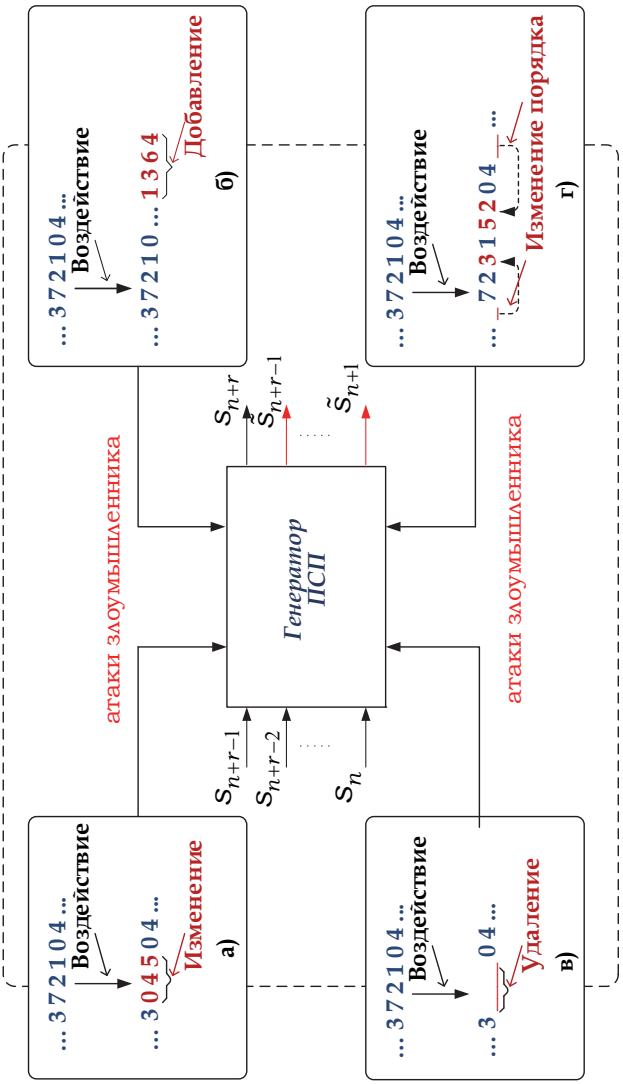


Рис. 1. Схема основных видов модификации ПСП при атаках злоумышленника: а) изменение элементов ПСП; б) добавление новых элементов ПСП; в) удаление элементов ПСП; г) изменение порядка следования элементов ПСП

2. Линейные рекуррентные последовательности над $GF(q)$. Известно, что один из эффективных способов формирования ПСП над $GF(q)$ $(q > 2)$ основан на применении переключательных схем специального вида, называемых линейными рекуррентными регистрами сдвига с обратной связью (ЛРРС) [13-15].

В основе синтеза ЛРРС над $GF(q)$ лежит заданный примитивный неприводимый (характеристический) многочлен:

$$P(z) = z^r + p_{r-1}z^{r-1} + p_{r-2}z^{r-2} + \ldots + p_0,$$

где $p_i \in GF(q)$, r — степень полинома $P(z)$, $r \in N$, $GF(q)$ — поле Галуа из q элементов и построенное в соответствии с ним однородное рекуррентное уравнение:

$$s_{n+r} = -p_{r-1}s_{n+r-1} - p_{r-2}s_{n+r-2} - \ldots - p_1 s_{n+1} - p_0 s_n$$

или:

$$s_{n+r} = p_{r-1}s_{n+r-1} \oplus p_{r-2}s_{n+r-2} \oplus \ldots \oplus p_1 s_{n+1} \oplus p_0 s_n \pmod q, \qquad (1)$$

где $n = 0, 1, 2, \ldots$; $p_j \in GF(q), 0 \le j \le r-1$, $\oplus$ — символ сложения по $(\mathrm{mod}\ q)$.

В общем случае ЛРРС над $GF(q)$ состоит из конструктивных элементов: ячеек D_j $(j = 0, 1, \ldots, r-1)$, сумматоров по $\mathrm{mod}\ q$, усилителей по $\mathrm{mod}\ q$ и имеет начальное заполнение: $s_0, s_1, \ldots, s_{r-1}$. Под «ячейкой» понимается параллельный $\lceil \log_2 q \rceil$-разрядный регистр ($\lceil x \rceil$ — наименьшее целое число равное или превышающее x). После первого такта работы ЛРРС над $GF(q)$ содержит заполнение $s_1, s_2, \ldots, s_r$. В целом q-ЛРРС генерирует бесконечную q-значную последовательность $s_0, s_1, s_2, \ldots, s_{r-1}, \ldots$ с периодом $q^r - 1$ (при ненулевом исходном состоянии), причем каждое ненулевое состояние появляется один раз за период. Сформированный сегмент выходной последовательности длины $q^r - 1$ является ПСП над $GF(q)$.

В терминах линейной алгебры очередной q-значный элемент ПСП s_{n+r} вычисляется произведением [8]:

$$\begin{bmatrix} s_{n+r} \\ s_{n+r-1} \\ \dots \\ s_{n+2} \\ s_{n+1} \end{bmatrix}^{\mathrm{T}} = \begin{bmatrix} s_{n+r-1} \\ s_{n+r-2} \\ \dots \\ s_{n+1} \\ s_n \end{bmatrix}^{\mathrm{T}} \times \begin{bmatrix} p_{r-1} & 1 & 0 & \dots & 0 \\ p_{r-2} & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \ddots & \dots \\ p_1 & 0 & 0 & \dots & 1 \\ p_0 & 0 & 0 & \dots & 0 \end{bmatrix},$$

где T — символ транспонирования.

На рисунке 2 представлена обобщенная граф-схема функционирования ЛРРС над $GF(q)$, генерирующего q-значную ПСП.

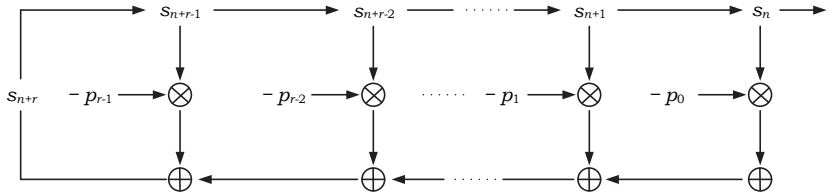


Рис. 2. Граф-схема функционирования ЛРРС над $GF(q)$

3. Многозначные функции алгебры логики. Один из простейших и в тоже время эффективных способов контроля (обнаружения ошибок) в υ-м блоке q-значной ПСП заключается в суммировании элементов υ-го блока ПСП по $\bmod q$ и добавлении в последовательность одного контрольного элемента $\hat{s}_\upsilon$ с тем, чтобы сумма элементов по $\bmod q$ сформированной последовательности соответствовала некоторому эталонному значению ς, например 0. Процедура контроля υ-го блока q-значной ПСП осуществляется в соответствии с выражением:

$$\varsigma_\upsilon^* \equiv \sum_{j=0}^{r-1} s_{\upsilon,j} \oplus \hat{s}_{\upsilon,r} \pmod q, \qquad (2)$$

при этом выполнение условия $\varsigma_\upsilon^* \equiv \varsigma$ свидетельствует об отсутствии обнаруживаемых искажений, в противном случае υ-й блок q-значной ПСП содержит ошибки.

Чтобы обеспечить возможность применения методов кодового контроля к q-значным ПСП, необходимо решить задачу

распараллеливания процесса вычислений q-значной ПСП. При этом в работе [16] в общем виде изложен подход синтеза параллельных генераторов q-значной ПСП на арифметических полиномах, сущность которого заключается в следующем.

Пусть $s_0, s_1, s_2, \ldots, s_{r-1}, \ldots$ — элементы ПСП, удовлетворяющие многозначному рекуррентному уравнению (1). Ввиду того, что произвольный элемент s_n $(n \geq r)$ последовательности $s_0, s_1, s_2, \ldots, s_{r-1}, \ldots$ определяется по предшествующим r элементам, представим элементы участка ПСП длиной r $s_{n+r}, s_{n+r+1}, \ldots, s_{n+2r-1}$ в виде системы рекуррентных уравнений:

$$\begin{cases} s_{n+r} = p_{r-1}s_{n+r-1} \oplus p_{r-2}s_{n+r-2} \oplus \ldots \oplus p_0 s_n \pmod q, \\ s_{n+r+1} = p_{r-1}s_{n+r} \oplus p_{r-2}s_{n+r-1} \oplus \ldots \oplus p_0 s_{n+1} \pmod q, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ s_{n+2r-1} = p_{r-1}s_{n+2r-2} \oplus p_{r-2}s_{n+2r-3} \oplus \ldots \oplus p_0 s_{n+r-1} \pmod q, \end{cases} \quad (3)$$

где $\begin{bmatrix} s_{n+r} & s_{n+r+1} & \ldots & s_{n+2r-1} \end{bmatrix}$ — вектор r-того состояния ПСП (или внутреннее состояние q-ЛРРС на r-м такте работы).

По аналогии с [7, 8] выразим правые части системы (3) через заданные начальные условия:

$$\begin{cases} s_{n+r} = p_{r-1}s_{n+r-1} \oplus p_{r-2}s_{n+r-2} \oplus \ldots \oplus p_0 s_n \pmod q, \\ s_{n+r+1} = p_{r-1}(p_{r-1}s_{n+r-1} \oplus p_{r-2}s_{n+r-2} \oplus \ldots \oplus p_0 s_n) \oplus p_{r-2}s_{n+r-1} \oplus \ldots \\ \qquad \ldots \oplus p_0 s_{n+1} \pmod q, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ s_{n+2r-1} = p_{r-1}(p_{r-1}(p_{r-1}s_{n+r-1} \oplus p_{r-2}s_{n+r-2} \oplus \ldots \oplus p_0 s_n) \oplus p_{r-2}s_{n+r-1} \oplus \ldots \\ \qquad \ldots \oplus p_0 s_{n+1}) \oplus p_{r-2}(p_{r-1}s_{n+r-1} \oplus p_{r-2}s_{n+r-2} \oplus \ldots \oplus p_0 s_n) \oplus \ldots \\ \qquad\qquad \ldots \oplus p_0(p_{r-1}s_{n+r-1} \oplus p_{r-2}s_{n+r-2} \oplus \ldots \oplus p_0 s_n) \pmod q. \end{cases} \quad (4)$$

Упростив выражение (4), запишем полученную систему рекуррентных уравнений как систему r многозначных функций алгебры логики (МФАЛ) от r переменных:

$$\begin{cases} f_1(s_{n+r-1}, \ldots, s_n) = p_{r-1}^{(0)}s_{n+r-1} \oplus p_{r-2}^{(0)} \oplus s_{n+r-2} \oplus \ldots \oplus p_0^{(0)}s_n \pmod q, \\ f_2(s_{n+r-1}, \ldots, s_n) = p_{r-1}^{(1)}s_{n+r-1} \oplus p_{r-2}^{(1)} \oplus s_{n+r-2} \oplus \ldots \oplus p_0^{(1)}s_n \pmod q, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_r(s_{n+r-1}, \ldots, s_n) = p_{r-1}^{(r-1)}s_{n+r-1} \oplus p_{r-2}^{(r-1)} \oplus s_{n+r-2} \oplus \ldots \oplus p_0^{(r-1)}s_n \pmod q. \end{cases} \quad (5)$$

Коэффициенты $p_i^{(j)} \in \{0,1,\ldots,q-1\}$ упрощаются (формируются) после сокращения выражения (5). На рисунке 3 представлена схема параллельных вычислений генератора.

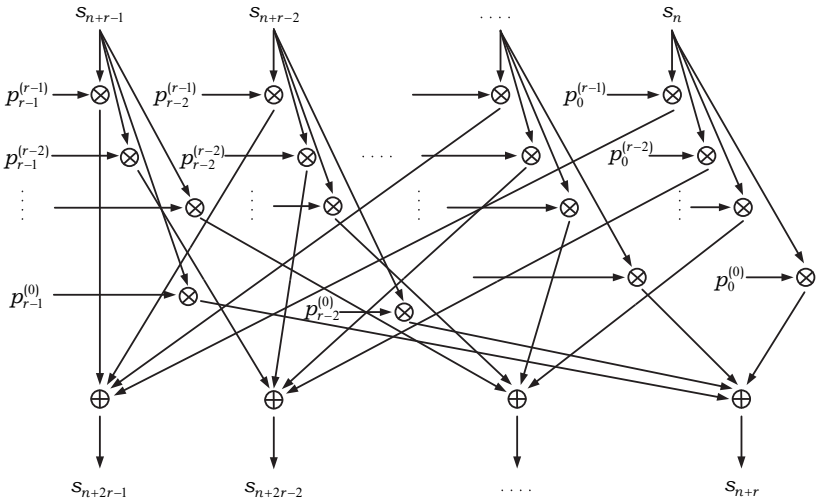


Рис. 3. Граф-схема параллельного q-ЛРРС, функционирующего в соответствии с выражением (5)

Процедура контроля проводимых преобразований (вычислений) для системы (5) МФАЛ может быть обеспечена $(r+1)$ МФАЛ, которая формирует в υ-м блоке q-значной ПСП контрольный элемент.

Тогда система (5) примет вид:

$$\begin{cases} f_1(s_{n+r-1},\ldots,s_n) = p_{r-1}^{(0)} s_{n+r-1} \oplus p_{r-2}^{(0)} \oplus s_{n+r-2} \oplus \ldots \oplus p_0^{(0)} s_n \,(\mathrm{mod}\, q), \\ f_2(s_{n+r-1},\ldots,s_n) = p_{r-1}^{(1)} s_{n+r-1} \oplus p_{r-2}^{(1)} \oplus s_{n+r-2} \oplus \ldots \oplus p_0^{(1)} s_n \,(\mathrm{mod}\, q), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_r(s_{n+r-1},\ldots,s_n) = p_{r-1}^{(r-1)} s_{n+r-1} \oplus p_{r-2}^{(r-1)} \oplus s_{n+r-2} \oplus \ldots \oplus p_0^{(r-1)} s_n \,(\mathrm{mod}\, q), \\ \hat{f}_{r+1}(s_{n+r-1},\ldots,s_n) = b_{r-1} s_{n+r-1} \oplus b_{r-2} \oplus s_{n+r-2} \oplus \ldots \oplus b_0 s_n \,(\mathrm{mod}\, q), \end{cases} \quad (6)$$

где коэффициенты $\sum_{j=0}^{r-1} p_i^{(j)} \oplus b_i \equiv \varsigma \,(\mathrm{mod}\ q)$ $(\mathrm{i} = 0,1,\ldots,r-1)$.

3.1 Полиномиальная арифметика МФАЛ. В соответствии с [17-20] произвольная МФАЛ может быть представлена в виде арифметического полинома, однозначным образом:

$$A(S) = \sum_{i=0}^{q^{r-1}-1} a_i s_n^{i_0} s_{n+1}^{i_1} \dots s_{n+r-1}^{i_{r-1}} \ , \tag{7}$$

где a_i — i-й коэффициент арифметического полинома; $S = s_n, s_{n+1}, \dots, s_{n+r-1}$ — аргументы МФАЛ $s_u \in \{0, 1, \dots, q-1\}$ $(u = n, n+1, \dots, n+r-1)$; $(i_0\ i_1\ \dots\ i_{r-1})_q$ — представление параметра i в q-ичной системе счисления:

$$(i_0\ i_1 \dots i_{r-1}\ )_q = \sum_{u=0}^{r-1} i_u q^{r-u-1} \quad (i_u \in \{0, 1, \dots, q-1\});$$

$$s_u^{i_u} = \begin{cases} 1, & i_u = 0, \\ s_u^{i_u}, & i_u \neq 0. \end{cases}$$

Для МФАЛ известен матричный метод построения арифметического полинома [17, 18]. Прямое и обратное матричное преобразование определяется выражениями:

$$\begin{aligned} \mathbf{A} &= N_q^{-1} \mathbf{K}_{q^{r-1}} \mathbf{S}; \\ \mathbf{S} &= \mathbf{K}_{q^{r-1}}^{-1} \mathbf{A}, \end{aligned} \tag{8}$$

где N_k — нормализирующий множитель; $\mathbf{K}_{q^{r-1}}$ и $\mathbf{K}_{q^{r-1}}^{-1}$ — матрицы прямого и инверсного арифметического преобразования размерности $q^{r-1} \times q^{r-1}$ (базис преобразования); $\mathbf{S}$ — вектор истинности МФАЛ:

$$\mathbf{S} = \left[s^{(0)}\ s^{(1)}\ \dots\ s^{(q^{r-1}-1)} \right]^{\mathrm{T}},$$

где $s^{(i)}$ — числовое значение, принимаемое МФАЛ на i-м наборе переменных; вектор коэффициентов арифметического полинома (7):

$$\mathbf{A} = \left[a_0\ a_1\ \dots\ a_{q^{r-1}-1} \right]^{\mathrm{T}}.$$

Матрицы $\mathbf{K}_{q^{r-1}}$ и $\mathbf{K}^{-1}_{q^{r-1}}$ определяются кронекеровским возведением в степень:

$$\mathbf{K}_{q^{r-1}} = \bigotimes_{j=0}^{r-1} \mathbf{K}_q ;$$

$$\mathbf{K}^{-1}_{q^{r-1}} = \bigotimes_{j=0}^{r-1} \mathbf{K}^{-1}_q ,$$

где $\mathbf{K}_q$ и $\mathbf{K}^{-1}_q$ — базовые матрицы прямого и обратного преобразования (таблица 1 – для q = 2, 3, … , 6).

Для МФАЛ $f(S) = 2s_1 \oplus 2s_2 \pmod 3$ вектор принимаемых значений МФАЛ $(r = 2)$ имеет вид: $\mathbf{S} = [0\,1\,2\,2\,1\,0\,1\,0\,2]$. Соответственно, прямое преобразование (8) может быть выражено:

$$\mathbf{A} = \frac{1}{4}\mathbf{K}_{3^2}\mathbf{S} =$$

$$= \frac{1}{4}\begin{bmatrix} 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -6 & 8 & -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & -4 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ -6 & 0 & 0 & 8 & 0 & 0 & -2 & 0 & 0 \\ 9 & -12 & 3 & -12 & 16 & -4 & 3 & -4 & 1 \\ -3 & 6 & -3 & 4 & -8 & 4 & -1 & 2 & -1 \\ 2 & 0 & 0 & -4 & 0 & 0 & 2 & 0 & 0 \\ -3 & 4 & -1 & 6 & -8 & 2 & -3 & 4 & -1 \\ 1 & -2 & 1 & -2 & 4 & -2 & 1 & -2 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 1 \\ 2 \\ 1 \\ 0 \\ 1 \\ 0 \\ 2 \end{bmatrix} = \frac{1}{4}\begin{bmatrix} 0 \\ 14 \\ -6 \\ 14 \\ -24 \\ 6 \\ -6 \\ 6 \\ 0 \end{bmatrix} \begin{matrix} \\ s_2 \\ s_2^2 \\ s_1 \\ s_1 s_2 \\ s_1 s_2^2 \\ s_1^2 \\ s_1^2 s_2 \\ s_1^2 s_2^2 \end{matrix} .$$

Тогда в соответствии с выражением (7) алгебраическая форма примет вид:

$$A(S) = \frac{1}{4}(14s_2 - 6s_2^2 + 14s_1 - 24s_1 s_2 + 6s_1 s_2^2 - 6s_1^2 + 6s_1^2 s_2) .$$

Например, при $s_1 = 2$, $s_2 = 2$ МФАЛ соответствует значение:

$$A(S) = \frac{1}{4}(14 \times 2 - 6 \times 2^2 + 14 \times 2 - 24 \times 2 \times 2 + 6 \times 2 \times 2^2 - 6 \times 2^2 +$$

$$+6 \times 2^2 \times 2) = \frac{1}{4} \times 8 = 2.$$

Таблица 1. Матрицы прямого и обратного преобразования

q	Матрица прямого преобразования, $\mathbf{K}_q$	Матрица обратного преобразования, $\mathbf{K}_q^{-1}$
2	$\begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$
3	$\begin{bmatrix} 2 & 0 & 0 \\ -3 & 4 & -1 \\ 1 & -2 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 2 & 4 \end{bmatrix}$
4	$\begin{bmatrix} 6 & 0 & 0 & 0 \\ -11 & 18 & -9 & 2 \\ 6 & -15 & 12 & -3 \\ -1 & 3 & -3 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 \\ 1 & 3 & 9 & 27 \end{bmatrix}$
5	$\begin{bmatrix} 24 & 0 & 0 & 0 & 0 \\ -50 & 96 & -72 & 32 & -6 \\ 35 & -104 & 114 & -56 & 11 \\ -10 & 36 & -48 & 28 & -6 \\ 1 & -4 & 6 & -4 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 16 \\ 1 & 3 & 9 & 27 & 81 \\ 1 & 4 & 6 & 64 & 256 \end{bmatrix}$
6	$\begin{bmatrix} 120 & 0 & 0 & 0 & 0 & 0 \\ -274 & 660 & -660 & 400 & -150 & 24 \\ 225 & -770 & 1070 & -780 & 305 & -20 \\ -85 & 355 & -590 & 490 & -205 & 35 \\ 15 & -70 & 130 & -120 & 55 & -10 \\ -1 & 5 & -10 & 10 & -5 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 16 & 32 \\ 1 & 3 & 9 & 27 & 81 & 243 \\ 1 & 4 & 16 & 64 & 255 & 1024 \\ 1 & 5 & 25 & 125 & 625 & 3125 \end{bmatrix}$

Для трехзначной функции алгебры логики, зависящей от двух переменных, в таблице 2 представлены соответствующие модулярные формы арифметических полиномов.

Таблица 2. Арифметические полиномы для $q = 3, r = 2$

№	Функция	Арифметический полином
1	$s_1 \oplus s_2$	$4^{-1}(4s_2 + 4s_1 + 21s_1s_2 - 15s_1s_2^2 - 15s_2s_1^2 + 9s_1^2s_2^2)$
2	$s_1 \oplus 2s_2$	$4^{-1}(14s_2 - 6s_2^2 + 4s_1 - 39s_1s_2 + 21s_1s_2^2 + 15s_2s_1^2 - 9s_1^2s_2^2)$
3	$2s_1 \oplus s_2$	$4^{-1}(4s_2 + 14s_1 - 39s_1s_2 + 15s_1s_2^2 - 6s_1^2 + 21s_2s_1^2 - 9s_1^2s_2^2)$
4	$2s_1 \oplus 2s_2$	$4^{-1}(14s_2 - 6s_2^2 + 14s_1 - 24s_1s_2 + 6s_1s_2^2 - 6s_1^2 + 6s_1^2s_2)$

В таблице 3 в качестве примера представлены рассчитанные арифметические полиномы для 3-значной функции алгебры логики, зависящей от 3 переменных.

Таблица 3. Арифметические полиномы для $q = 3$, $r = 3$

№	Функция	Арифметический полином
1	$s_1 \oplus s_2 \oplus s_3$	$8^{-1}(8s_3 + 8s_2 + 42s_2s_3 - 30s_2s_3^2 - 30s_3s_2^2 + 18s_2^2s_3^2 + 8s_1 + 42s_1s_3 - 30s_1s_3^2 + +42s_1s_2 - 267s_1s_2s_3 + 135s_1s_2s_3^2 - 30s_1s_2^2 + 135s_1s_2^2s_3 - 63s_1s_2^2s_3^2 - 30s_3s_1^2 + +18s_1^2s_3^2 - 30s_1^2s_2 + 135s_1^2s_2s_3 - 63s_1^2s_2s_3^2 + 18s_1^2s_2^2 - 63s_1^2s_3s_2^2 + 27s_1^2s_2^2s_3^2)$
2	$2s_1 \oplus s_2 \oplus s_3$	$8^{-1}(8s_3 + 8s_2 + 42s_2s_3 - 30s_2s_3^2 - 30s_3s_2^2 + 18s_2^2s_3^2 + 28s_1 - 78s_1s_3 + +30s_1s_3^2 - 78s_1s_2 + 78s_1s_2s_3 + 30s_1s_2^2 - 18s_1s_2^2s_3^2 - 12s_1^2 + 42s_3s_1^2 - -18s_1^2s_3^2 + 42s_1^2s_2 - 72s_1^2s_2s_3 + 18s_1^2s_2s_3^2 - 18s_1^2s_2^2 + 18s_1^2s_3s_2^2)$
3	$s_1 \oplus 2s_2 \oplus s_3$	$8^{-1}(8s_3 + 28s_2 - 78s_2s_3 + 30s_2s_3^2 - 12s_2^2 + 42s_3s_2^2 - 18s_2^2s_3^2 + 8s_1 + 42s_1s_3 - -30s_1s_3^2 - 78s_1s_2 + 78s_1s_2s_3 + 42s_1s_2^2 - 72s_1s_2^2s_3 + 18s_1s_2^2s_3^2 - 30s_3s_1^2 + +18s_1^2s_3^2 + 30s_1^2s_2 - 18s_1^2s_2s_3^2 - 18s_1^2s_2^2 + 18s_1^2s_3s_2^2)$
4	$s_1 \oplus s_2 \oplus 2s_3$	$8^{-1}(28s_3 - 12s_3^2 + 8s_2 - 78s_2s_3 + 42s_2s_3^2 + 30s_3s_2^2 - 18s_2^2s_3^2 + 8s_1 - -78s_1s_3 + 42s_1s_3^2 + 42s_1s_2 + 78s_1s_2s_3 - 72s_1s_2s_3^2 - 30s_1s_2^2 + 18s_1s_2^2s_3^2 + 30s_3s_1^2 - 18s_1^2s_3^2 - 30s_1^2s_2 + 18s_1^2s_2s_3^2 + 18s_1^2s_2^2 - 18s_1^2s_3s_2^2)$
5	$2s_1 \oplus 2s_2 \oplus s_3$	$8^{-1}(8s_3 + 28s_2 - 78s_2s_3 + 30s_2s_3^2 - 12s_2^2 + 42s_3s_2^2 - 18s_2^2s_3^2 + 28s_1 - -78s_1s_3 + 30s_1s_3^2 - 48s_1s_2 + 273s_1s_2s_3 - 135s_1s_2s_3^2 + 12s_1s_2^2 - 117s_1s_3s_2^2 + +63s_1s_2^2s_3^2 - 12s_1^2 + 42s_1^2s_3 - 18s_1^2s_3^2 + 12s_1^2s_2 - 117s_1^2s_2s_3 + 63s_1^2s_2s_3^2 + +45s_1^2s_3s_2^2 - 27s_1^2s_2^2s_3^2)$
6	$2s_1 \oplus s_2 \oplus 2s_3$	$8^{-1}(28s_3 - 12s_3^2 + 8s_2 - 78s_2s_3 + 42s_2s_3^2 + 30s_3s_2^2 - 18s_2^2s_3^2 + 28s_1 - -48s_1s_3 + 12s_1s_3^2 - 78s_1s_2 + 273s_1s_2s_3 - 117s_1s_2s_3^2 + 30s_1s_2^2 - -135s_1s_3s_2^2 + 63s_1s_2^2s_3^2 - 12s_1^2 + 12s_1^2s_3 + 42s_1^2s_2 - 117s_1^2s_2s_3 + +45s_1^2s_2s_3^2 - 18s_1^2s_2^2 + 63s_1^2s_3s_2^2 - 27s_1^2s_2^2s_3^2)$
7	$s_1 \oplus 2s_2 \oplus 2s_3$	$8^{-1}(28s_3 - 12s_3^2 + 28s_2 - 48s_2s_3 + 12s_2s_3^2 - 12s_2^2 + 12s_3s_2^2 + 8s_1 - -78s_1s_3 + 42s_1s_3^2 - 78s_1s_2 + 273s_1s_2s_3 - 117s_1s_2s_3^2 + 42s_1s_2^2 - -117s_1s_3s_2^2 + 45s_1s_2^2s_3^2 + 30s_1^2s_3 - 18s_1^2s_3^2 + 30s_1^2s_2 - 135s_1^2s_2s_3 + +63s_1^2s_2s_3^2 - 18s_1^2s_2^2 + 63s_1^2s_3s_2^2 - 27s_1^2s_2^2s_3^2)$
8	$2s_1 \oplus 2s_2 \oplus 2s_3$	$8^{-1}(28s_3 - 12s_3^2 + 28s_2 - 48s_2s_3 + 12s_2s_3^2 - 12s_2^2 + 12s_3s_2^2 + 28s_1 - -48s_1s_3 + 12s_1s_3^2 - 48s_1s_2 - 57s_1s_2s_3 + 63s_1s_2s_3^2 + 12s_1s_2^2 + 63s_1s_3s_2^2 - -45s_1s_2^2s_3^2 - 12s_1^2 + 12s_1^2s_3 + 12s_1^2s_2 - 63s_1^2s_2s_3 - 45s_1^2s_2s_3^2 - 45s_1^2s_3s_2^2 + +27s_1^2s_2^2s_2^2)$

3.2 Арифметический полином для реализации систем МФАЛ. Реализуем систему МФАЛ (6) посредством вычисления некоторого арифметического полинома. Для этого поставим в соответствие системе МФАЛ (6) систему арифметических полиномов вида (7), один из которых выполняет контроль ошибок вычислений.

Тогда получим:

$$\begin{cases} A_1(S) = \sum\limits_{i=0}^{q^{r-1}-1} a_{1,i}\, s_n^{i0} s_{n+1}^{i1} \dots s_{n+r-1}^{ir-1}, \\ A_2(S) = \sum\limits_{i=0}^{q^{r-1}-1} a_{2,i}\, s_n^{i0} s_{n+1}^{i1} \dots s_{n+r-1}^{ir-1}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ A_r(S) = \sum\limits_{i=0}^{q^{r-1}-1} a_{r,i}\, s_n^{i0} s_{n+1}^{i1} \dots s_{n+r-1}^{ir-1}, \\ \hat{A}_{r+1}(S) = \sum\limits_{i=0}^{q^{r-1}-1} a'_{r+1,i}\, s_n^{i0} s_{n+1}^{i1} \dots s_{n+r-1}^{ir-1}. \end{cases} \quad (9)$$

Умножим полиномы системы (9) на соответствующие веса q^{l-1} $(l = 1,2,\dots,r+1)$:

$$\begin{cases} A_1^*(S) = q^0 A_1(S) = \sum\limits_{i=0}^{q^{r-1}-1} a_{1,i}^*\, s_n^{i0} s_{n+1}^{i1} \dots s_{n+r-1}^{ir-1}, \\ A_2^*(S) = q^1 A_2(S) = \sum\limits_{i=0}^{q^{r-1}-1} a_{2,i}^*\, s_n^{i0} s_{n+1}^{i1} \dots s_{n+r-1}^{ir-1}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ A_r^*(S) = q^{r-1} A_r(S) = \sum\limits_{i=0}^{q^{r-1}-1} a_{r,i}^*\, s_n^{i0} s_{n+1}^{i1} \dots s_{n+r-1}^{ir-1}, \\ \hat{A}_{r+1}^*(S) = q^r \hat{A}_{r+1}(S) = \sum\limits_{i=0}^{q^{r-1}-1} \hat{a}_{r+1,i}^*\, s_n^{i0} s_{n+1}^{i1} \dots s_{n+r-1}^{ir-1}, \end{cases}$$

где $a_{l,i}^* = q^{l-1} a_{l,i}$, $a_{r+1,i}^* = q^r a_{r+1,i}$ q^{l-1} $(l = 1,2,\dots,r;\ i = 0,1,\dots,q^{r-1}-1)$.

В результате получим:

$$D(S) = \sum_{i=0}^{q^{r-1}-1} \sum_{l=1}^{r} a^*_{l,\,i}\, s_n^{i0} s_{n+1}^{i1} \dots s_{n+r-1}^{ir-1} + \sum_{i=0}^{q^{r-1}-1} \hat{a}^*_{r+1,i}\, s_n^{i0} s_{n+1}^{i1} \dots s_{n+r-1}^{ir-1}. \qquad (10)$$

Основным недостатком полученного выражения, как правило, считается возможность принятия коэффициентами $a^*_{l,\,i}$, $\hat{a}^*_{r+1,i}$ как положительных, так и отрицательных значений, что требует удваивания числового диапазона по сравнению с использованием неотрицательных коэффициентов. В работе [18] представлены решения представления МФАЛ на основе модулярной формы арифметического полинома, которые осуществляют «перенос» вычислений из поля рациональных чисел $\Re$ в поле $GF(q)$. С использованием модулярных форм МФАЛ [16, 18] выражение (10) примет вид:

$$M(S) = \bigoplus_{i=0}^{q^{r-1}-1} c_i\, s_n^{i0} s_{n+1}^{i1} \dots s_{n+r-1}^{ir-1} \pmod{q^r}, \qquad (11)$$

где $c_i = \bigoplus_{l=1}^{r} a^*_{l,\,i} \oplus \hat{a}^*_{r+1,i}$ $(i = 0,1,\dots,q^{r-1}-1)$.

Вычислим значения искомых МФАЛ. Для этого результат вычисления $M(S)$ представим в q-ичной системе счисления и применим оператор маскирования $\Xi^t\{M(S)\}$:

$$\Xi^t\{(s_j^{(1)},\dots,\boxed{s_{j+i}^{(t)}},\dots,s_{j+n}^{(n)})_q\} = \left\lfloor \frac{M(S)}{q^t} \right\rfloor \pmod{q},$$

где t — искомый q-ичный разряд представления $M(S)$. На рисунке 4 представлена схема параллельного генератора с контролем ошибок вычислений, соответствующая выражению (11).

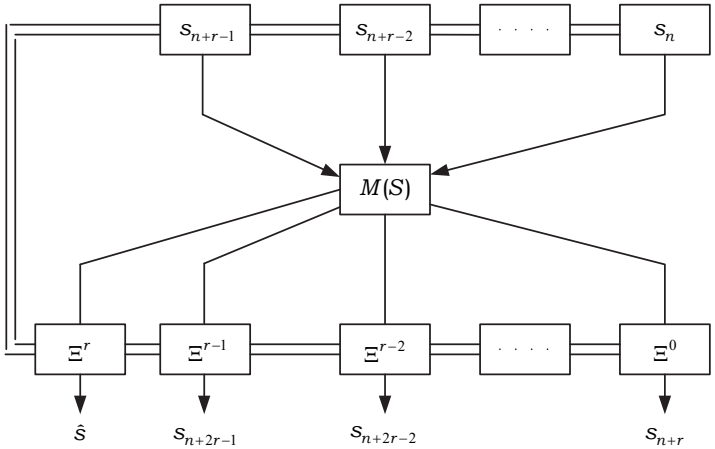


Рис. 4. Схема параллельного q-ЛРРС с контролем ошибок вычислений, функционирующего в соответствии с выражением (11)

Рассмотрим построение 3-ЛРРС, генерирующего 3-значную ПСП, задаваемую характеристическим уравнением: $s_{k+3} = s_{k+2} \oplus 2s_k \pmod 3$ и начальным заполнением: $s_0 = 0, \quad s_1 = 0, \quad s_2 = 2.$

Соответствующий характеристический многочлен имеет вид: $P(z) = z^3 + 2z^2 + 1$.

Тогда система характеристических уравнений для участка ПСП длиной три элемента примет вид:

$$\begin{cases} s_3 = s_2 \oplus 2s_0 \pmod 3, \\ s_4 = s_3 \oplus 2s_1 \pmod 3, \\ s_5 = s_4 \oplus 2s_2 \pmod 3. \end{cases}$$

Далее запишем систему характеристических уравнений как систему с правыми частями равенств, выраженными через заданные начальные условия, с вычисленным уравнением, формирующим контрольный элемент:

$$\begin{cases} f_3(s_2, s_1, s_0) = s_2 \oplus \quad \oplus 2s_0 \pmod 3, \\ f_4(s_2, s_1, s_0) = s_2 \oplus 2s_1 \oplus \quad \oplus 2s_0 \pmod 3, \\ f_5(s_2, s_1, s_0) = \quad 2s_1 \oplus \quad \oplus 2s_0 \pmod 3, \\ \hat{f}(s_2, s_1, s_0) = s_2 \oplus 2s_1 \oplus \quad 0 \pmod 3. \end{cases}$$

В соответствии с (7) получим систему арифметических полиномов следующего вида:

$$\begin{cases} A_3(S) = \frac{1}{4}(4s_2 + 14s_0 - 39s_0s_2 + 15s_0s_2^2 - 6s_0^2 + 21s_2s_0^2 - 9s_0^2s_2^2), \\ A_4(S) = \frac{1}{8}(8s_2 + 28s_1 - 78s_1s_2 + 30s_1s_2^2 - 12s_1^2 + 42s_2s_1^2 - 18s_1^2s_2^2 + 28s_0 - \\ \quad - 78s_0s_2 + 30s_0s_2^2 - 48s_0s_1 + 273s_0s_1s_2 - 135s_0s_1s_2^2 + 12s_0s_1^2 - \\ \quad - 117s_0s_2s_1^2 + 63s_0s_1^2s_2^2 - 12s_0^2 + 42s_0^2s_2 - 18s_0^2s_2^2 + 12s_0^2s_1 - \\ \quad - 117s_0^2s_1s_2 + 63s_0^2s_1s_2^2 + 45s_0^2s_2s_1^2 - 27s_0^2s_1^2s_2^2), \\ A_5(S) = \frac{1}{4}(14s_1 - 6s_1^2 + 14s_0 - 24s_0s_1 + 6s_0s_1^2 - 6s_0^2 + 6s_0^2s_1), \\ \hat{A}(S) = \frac{1}{4}(4s_2 + 14s_1 - 39s_1s_2 + 15s_1s_2^2 - 6s_1^2 + 21s_2s_1^2 - 9s_1^2s_2^2). \end{cases}$$

Далее систему арифметических выражений реализуем в виде арифметического полинома:

$$\begin{aligned} D(S) &= \frac{1}{4}(4s_2 + 14s_0 - 39s_0s_2 + 15s_0s_2^2 - 6s_0^2 + 21s_2s_0^2 - 9s_0^2s_2^2) + \\ &+ 3^1(\frac{1}{8}(8s_2 + 28s_1 - 78s_1s_2 + 30s_1s_2^2 - 12s_1^2 + 42s_2s_1^2 - 18s_1^2s_2^2 + 28s_0 - \\ &- 78s_0s_2 + 30s_0s_2^2 - 48s_0s_1 + 273s_0s_1s_2 - 135s_0s_1s_2^2 + 12s_0s_1^2 - 117s_0s_2s_1^2 + \\ &+ 63s_0s_1^2s_2^2 - 12s_0^2 + 42s_0^2s_2 - 18s_0^2s_2^2 + 12s_0^2s_1 - 117s_0^2s_1s_2 + 63s_0^2s_1s_2^2 + \\ &+ 45s_0^2s_2s_1^2 - 27s_0^2s_1^2s_2^2)) + 3^2(\frac{1}{4}(14s_1 - 6s_1^2 + 14s_0 - 24s_0s_1 + 6s_0s_1^2 - 6s_0^2 + \\ &+ 6s_0^2s_1)) + 3^3(\frac{1}{4}(4s_2 + 14s_1 - 39s_1s_2 + 15s_1s_2^2 - 6s_1^2 + 21s_2s_1^2 - 9s_1^2s_2^2)). \end{aligned}$$

Модулярная полиномиальная форма примет вид:

$$\begin{aligned} M(S) &= 5s_0 + 21s_0^2 + 15s_1 + 9s_0s_1 + 18s_0^2s_1 + 63s_1^2 + 18s_0s_1^2 + 31s_2 + 42s_0s_2 + \\ &+ 21s_0^2s_2 + 72s_1s_2 + 72s_0s_1s_2 + 27s_0^2s_1s_2 + 36s_1^2s_2 + 27s_0s_1^2s_2 + \\ &+ 27s_0^2s_1^2s_2 + 15s_0s_2^2 + 72s_0^2s_2^2 + 72s_1s_2^2 + 54s_0^2s_1s_2^2 + \\ &+ 54s_1^2s_2^2 + 54s_0s_1^2s_2^2 \pmod{81}. \end{aligned}$$

В соответствии с заданным начальным заполнением можно получить следующие фрагменты 3-значной ПСП с 1 контрольной цифрой:

$$\textit{шаг } 1\begin{cases} s_3^{(1)} = \Xi^0\{62\} = \Xi^0\{(2,\ 0,\ 2,\ \boxed{2})_3\} = 2, \\ s_4^{(2)} = \Xi^1\{62\} = \Xi^1\{(2,\ 0,\ \boxed{2},\ 2)_3\} = 2, \\ s_5^{(3)} = \Xi^2\{62\} = \Xi^2\{(2,\ \boxed{0},\ 2,\ 2)_3\} = 0, \\ \hat{s} = \Xi^3\{62\} = \Xi^3\{(\boxed{2},\ 0,\ 2,\ 2)_3\} = 2; \end{cases}$$

$$\textit{шаг } 2\begin{cases} s_6^{(1)} = \Xi^0\{52\} = \Xi^0\{(1,\ 2,\ 2,\ \boxed{1})_3\} = 1, \\ s_7^{(2)} = \Xi^1\{52\} = \Xi^1\{(1,\ 2,\ \boxed{2},\ 1)_3\} = 2, \\ s_8^{(3)} = \Xi^2\{52\} = \Xi^2\{(1,\ \boxed{2},\ 2,\ 1)_3\} = 2, \\ \hat{s} = \Xi^3\{52\} = \Xi^3\{(\boxed{1},\ 2,\ 2,\ 1)_3\} = 1; \end{cases}$$

$$\textit{шаг } 3\begin{cases} s_9^{(1)} = \Xi^0\{7\} = \Xi^0\{(0,\ 0,\ 2,\ \boxed{1})_3\} = 1, \\ s_{10}^{(2)} = \Xi^1\{7\} = \Xi^1\{(0,\ 0,\ \boxed{2},\ 1)_3\} = 2, \\ s_{11}^{(3)} = \Xi^2\{7\} = \Xi^2\{(0,\ \boxed{0},\ 2,\ 1)_3\} = 0, \\ \hat{s} = \Xi^3\{7\} = \Xi^3\{(\boxed{0},\ 0,\ 2,\ 1)_3\} = 0; \end{cases}$$

$$\textit{шаг } 4\begin{cases} s_{12}^{(1)} = \Xi^0\{29\} = \Xi^0\{(1,\ 0,\ 0,\ \boxed{2})_3\} = 2, \\ s_{13}^{(2)} = \Xi^1\{29\} = \Xi^1\{(1,\ 0,\ \boxed{0},\ 2)_3\} = 0, \\ s_{14}^{(3)} = \Xi^2\{29\} = \Xi^2\{(1,\ \boxed{0},\ 0,\ 2)_3\} = 0, \\ \hat{s} = \Xi^3\{29\} = \Xi^3\{(\boxed{1},\ 0,\ 0,\ 2)_3\} = 1; \end{cases}$$

$$\textit{шаг } 5\begin{cases} s_{15}^{(1)} = \Xi^0\{13\} = \Xi^0\{(0,\ 1,\ 1,\ \boxed{1})_3\} = 1, \\ s_{16}^{(2)} = \Xi^1\{13\} = \Xi^1\{(0,\ 1,\ \boxed{1},\ 1)_3\} = 1, \\ s_{17}^{(3)} = \Xi^2\{13\} = \Xi^2\{(0,\ \boxed{1},\ 1,\ 1)_3\} = 1, \\ \hat{s} = \Xi^3\{13\} = \Xi^3\{(\boxed{0},\ 1,\ 1,\ 1)_3\} = 0; \end{cases}$$

$$\textit{шаг } 6\begin{cases} s_{18}^{(1)} = \Xi^0\{15\} = \Xi^0\{(0,\ 1,\ 2,\ \boxed{0})_3\} = 0, \\ s_{19}^{(2)} = \Xi^1\{15\} = \Xi^1\{(0,\ 1,\ \boxed{2},\ 0)_3\} = 2, \\ s_{20}^{(3)} = \Xi^2\{15\} = \Xi^2\{(0,\ \boxed{1},\ 2,\ 0)_3\} = 1, \\ \hat{s} = \Xi^3\{15\} = \Xi^3\{(\boxed{0},\ 1,\ 2,\ 0)_3\} = 0; \end{cases}$$

$$\textit{шаг } 7 \begin{cases} s_{21}^{(1)} = \Xi^0\{70\} = \Xi^0\{(2,\,1,\,2,\,\boxed{1})_3\} = 1, \\ s_{22}^{(2)} = \Xi^1\{70\} = \Xi^1\{(2,\,1,\,\boxed{2},\,1)_3\} = 2, \\ s_{23}^{(3)} = \Xi^2\{70\} = \Xi^2\{(2,\,\boxed{1},\,2,\,1)_3\} = 1, \\ \hat{s} = \Xi^3\{70\} = \Xi^3\{(\boxed{2},\,1,\,2,\,1)_3\} = 2; \end{cases}$$

$$\textit{шаг } 8 \begin{cases} s_{24}^{(1)} = \Xi^0\{57\} = \Xi^0\{(2,\,0,\,1,\,\boxed{0})_3\} = 0, \\ s_{25}^{(2)} = \Xi^1\{57\} = \Xi^1\{(2,\,0,\,\boxed{1},\,0)_3\} = 1, \\ s_{26}^{(3)} = \Xi^2\{57\} = \Xi^2\{(2,\,\boxed{0},\,1,\,0)_3\} = 0, \\ \hat{s} = \Xi^3\{57\} = \Xi^3\{(\boxed{2},\,0,\,1,\,0)_3\} = 2; \end{cases}$$

.....

Рассмотрим 3-й блок 3-значной ПСП $[1,2,0,0]$, который не содержит ошибок. В соответствии с выражением (2) вычислим эталонное значение ς_3^*:

$$\varsigma_3^* = |1+2+0+0|_3 = |3|_3 = 0\,.$$

Пусть в 8-м блоке 3 ПСП произошла ошибка $\{+2\}$ во втором разряде $[0,\tilde{0},0,2]$. Тогда $\varsigma_8^* = |0+\tilde{0}+0+2|_3 = |2|_3 = 2$.

Полученное эталонное значение $\varsigma_8^* = 2$ не соответствует заданному значению, следовательно, 8-й блок 3 ПСП содержит ошибку.

Положениями [17] вычислительные затраты процесса представления МФАЛ с помощью арифметических полиномов по критерию вычислительной сложности количества операций сложения и умножения при синтезе полиномов и вычислении их значений предполагают: количество операций сложения $(q^{r-1}-1)q^{r-1}$; количество операций умножения — $(q^{r-1})^2$.

4. Контроль ошибок функционирования *q*-ЛРРС многозначными кодами Рида — Соломона. Известно, что среди существующего многообразия «мощных» помехоустойчивых кодов (циклических эквидистантных, Рида — Малера, Боуза — Чоудхури — Хоквингема (БЧХ)) наибольшее распространение

получили коды Рида — Соломона (недвоичные коды БЧХ) [21]. Во-первых, потому что имеют максимально допустимое минимальное кодовое расстояние $d_{\min}$, и следовательно, обладают наибольшей корректирующей способностью, а во-вторых, могут быть систематическими. Как правило, коды Рида — Соломона (РС) задаются с помощью порождающих многочленов $g(z)$, обозначаются как $(m, r, d_{\min})$, где m — длина кодовой комбинации, r — количество информационных символов. При этом несистематический вид кода РС образуется путем произведения порождающего $g(z)$ и информационного многочленов $b(z)$. Систематический — путем сдвига информационного многочлена $b(z)$ на k разрядов, его деление на порождающий многочлен $g(z)$ и добавление полученного остатка $h(z)$ к сдвинутому информационному многочлену $b(z)$. Вместе с тем не менее интересным является решение синтеза кодов РС, основанное на классических преобразованиях в линейных пространствах — матрицах Вандермонда.

4.1 Систематический код РС, основанный на матрицах Вандермонда. Матрица Вандермонда $\mathbf{B}$, состоящая из r строк и m столбцов, определяется последовательностью $[b_0, b_1, \ldots, b_{m-1}]$ элементов, при этом каждый b_i удовлетворяет условию $b_i \in GF(q)$, то есть:

$$\mathbf{B} = \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ b_0 & b_1 & b_2 & \ldots & b_{m-1} \\ b_0^2 & b_1^2 & b_2^2 & \ldots & b_{m-1}^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_0^{r-1} & b_1^{r-1} & b_2^{r-1} & \ldots & b_{m-1}^{r-1} \end{bmatrix}. \qquad (12)$$

Хорошо известно, что для матриц $\mathbf{B}$ над $GF(q)$ характерной структурной особенностью является наличие внутренних вырожденных квадратных подматриц [21, 22], которые препятствуют без дополнительных преобразований их использованию для синтеза систематических кодов РС.

В [21, 22] предложены решения, позволяющие строить порождающие (генераторные) матрицы $\mathbf{G}$ систематической формы на

основе матриц $\mathbf{B}$ для последующего синтеза кодов РС. На первом шаге порождающая матрица $\mathbf{G}$ представляется в виде двух матриц: первой $\mathbf{B}_{r\times r}$, образованной первыми r столбцами второй матрицы $\mathbf{B}_{r\times m}$, определенной ранее. На втором шаге первая матрица $\mathbf{B}_{r\times r}$ инвертируется и умножается на матрицу $\mathbf{B}_{r\times m}$. При этом произведение матриц $\mathbf{B}_{r\times r}^{-1}$ и $\mathbf{B}_{r\times m}$ образует результирующую матрицу $\mathbf{G}$, состоящую в итоге из двух блоков: единичной матрицы $\mathbf{E}_r$ порядка r и следующей за ней матрицы размера $r\times(m-r)$. В общем виде процедуре построения порождающей матрице $\mathbf{G}$ систематической формы соответствует совокупность выражений:

$$\mathbf{G}=\mathbf{B}_{r\times r}^{-1}\times\mathbf{B}_{r\times m}=\left[\mathbf{E}_r\,|\,\mathbf{B}_{r\times r}^{-1}\times\mathbf{B}_{r\times m}\right]=\left[\mathbf{E}_r\,|\,\mathbf{V}_{r\times(m-r)}\right]. \qquad (13)$$

4.2 Кодирование и декодирование ПСП кодами РС. Теперь представим систему характеристических уравнений (4) в виде матричного уравнения:

$$\begin{bmatrix} s_{n+r} \\ s_{n+r+1} \\ \vdots \\ s_{n+2r-1} \end{bmatrix}^{\mathrm{T}} = \begin{bmatrix} p_{r-1}^{(0)} & p_{r-2}^{(0)} & \cdots & p_0^{(0)} \\ p_{r-1}^{(1)} & p_{r-2}^{(1)} & \cdots & p_0^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ p_{r-1}^{(r-1)} & p_{r-2}^{(r-1)} & \cdots & p_0^{(r-1)} \end{bmatrix} \times \begin{bmatrix} s_{n+r-1} \\ s_{n+r-2} \\ \vdots \\ s_n \end{bmatrix}^{\mathrm{T}},$$

где $\mathbf{P}_r=\left[p_r^{(r)}\right]$ — матрица порядка r.

Далее, заменив в порождающей матрице $\mathbf{G}$ единичную матрицу $\mathbf{E}_r$ на матрицу $\mathbf{P}_r^{\mathrm{T}}$, получим:

$$\mathbf{G}''=\left[\mathbf{P}_r^{\mathrm{T}}\,|\,\mathbf{V}_{r\times(m-r)}\right], \qquad (14)$$

то есть итоговое выражение, позволяющее формировать фрагменты q-значной ПСП длины r с контролем вычислительных операций, которые отождествляются как кодоподобные комбинации кода РС.

Основываясь на классических положениях теории помехоустойчивого кодирования, вполне очевидно, что на полученные кодоподобные q-значные ПСП длины m с r информационными

элементами и $(m-r)$ контрольными элементами соответственно, также распространяются корректирующие свойства кода РС, характеризующиеся числом гарантированно обнаруживаемых

$$\chi_{\text{обн}} \le d_{\min} - 1,$$

и гарантированно исправляемых ошибок

$$\chi_{\text{исп}} \le \left\lfloor \frac{(d_{\min} - 1)}{2} \right\rfloor,$$

в метрике Хэмминга, где $d_{\min} = m - r + 1$, $\lfloor \bullet \rfloor$ — процедура округления до ближайшего меньшего целого числа.

При этом получение υ-го фрагмента q-значной ПСП длины r с контрольными $(m-r)$ цифрами (кодоподобный блок кода РС)

$$\mathbf{S}_\upsilon = \left[s_{\upsilon,\, r-1}\ s_{\upsilon,\, r-2}\ \cdots\ s_{\upsilon,1}\ s_{\upsilon,0}\ \hat{s}_{\upsilon,\, m-r-1}\ \hat{s}_{\upsilon,\, m-r-2}\ \cdots\ \hat{s}_{\upsilon,1}\ \hat{s}_{\upsilon,0} \right]^{\mathrm{T}}$$

находится как скалярное произведение:

$$\mathbf{S}_\upsilon = \mathbf{S}_{\upsilon-1}\mathbf{G}'', \tag{15}$$

где

$$\mathbf{S}_{\upsilon-1} = \left[s_{\upsilon-1,\, r-1}\, s_{\upsilon-1,\, r-2} \cdots s_{\upsilon-1,1}\ s_{\upsilon-1,0}\ \hat{s}_{\upsilon-1,\, m-r-1}\ \hat{s}_{\upsilon-1,\, m-r-2} \cdots \hat{s}_{\upsilon-1,1}\, \hat{s}_{\upsilon-1,0} \right]^{\mathrm{T}}.$$

Известно, что процедура декодирования значительно сложнее процедуры кодирования, вследствие чего проверочной матрице $\mathbf{H}$ необходимо задать специальную форму, при которой последующая процедура декодирования упрощается. Для этого выполним следующие преобразования:

$$\mathbf{H} = (\mathbf{P}_r^{\mathrm{T}})^{-1} \times \mathbf{G}'' = \left[-\mathbf{A}_{r\times(m-r)} \,|\, \mathbf{E}_r \right] = \left[-\mathbf{A}^{\mathrm{T}}_{(m-r)\times r} \,|\, \mathbf{E}_{m-r} \right]. \tag{16}$$

Скалярное произведение υ-го фрагмента q-значной ПСП (кодоподобного блока кода РС) $\mathbf{S}_\upsilon$ на проверочную матрицу $\mathbf{H}$ позволяет получить вектор-синдром $\boldsymbol{\alpha}_\upsilon = \left[\alpha_{\upsilon,\, m-r-1}, \alpha_{\upsilon,\, m-r-2}, \ldots, \alpha_{\upsilon,0} \right]$,

$$\boldsymbol{\alpha}_\upsilon = \mathbf{S}_\upsilon \mathbf{H}^{\mathrm{T}}. \tag{17}$$

Очевидно, что при отсутствии искажений синдром $\boldsymbol{\alpha}_{\upsilon}$ принимает нулевое значение:

$$\boldsymbol{\alpha}_{\upsilon} = 0.$$

Рассмотрим синтез 11-ЛРРС, генерирующего 11-значную ПСП (код РС), задаваемую характеристическим уравнением: $s_{k+7} = 7s_{k+6} \oplus 9s_{k+4} \oplus 9s_{k+1} \oplus 6s_k \pmod{11}$ и начальным заполнением: $s_0 = 1, \quad s_1 = 0, \quad s_2 = 3, \quad s_3 = 0, \quad s_4 = 0, \quad s_5 = 1, \quad s_6 = 7.$

Соответствующий характеристический многочлен имеет вид:

$$P(z) = z^7 + 4z^6 + 2z^4 + 2z + 5.$$

Тогда система характеристических уравнений для участка ПСП длиной семь элементов примет вид:

$$\begin{cases} s_7 = 7s_6 \oplus 9s_4 \oplus 9s_1 \oplus 6s_0 \pmod{11}, \\ s_8 = 7s_7 \oplus 9s_5 \oplus 9s_2 \oplus 6s_1 \pmod{11}, \\ s_9 = 7s_8 \oplus 9s_6 \oplus 9s_3 \oplus 6s_2 \pmod{11}, \\ s_{10} = 7s_9 \oplus 9s_7 \oplus 9s_4 \oplus 6s_3 \pmod{11}, \\ s_{11} = 7s_{10} \oplus 9s_8 \oplus 9s_5 \oplus 6s_4 \pmod{11}, \\ s_{12} = 7s_{11} \oplus 9s_9 \oplus 9s_6 \oplus 6s_5 \pmod{11}, \\ s_{13} = 7s_{12} \oplus 9s_{10} \oplus 9s_7 \oplus 6s_6 \pmod{11}. \end{cases}$$

Далее запишем систему характеристических уравнений как систему с правыми частями равенств, выраженными через заданные начальные условия:

$$\begin{cases} s_7 = 7s_6 \oplus 9s_4 \oplus 9s_1 \oplus 6s_0 \pmod{11}, \\ s_8 = 5s_6 \oplus 9s_5 \oplus 8s_4 \oplus 9s_2 \oplus 3s_1 \oplus 9s_0 \pmod{11}, \\ s_9 = 8s_5 \oplus s_4 \oplus 9s_3 \oplus 3s_2 \oplus 10s_1 \oplus 8s_0 \pmod{11}, \\ s_{10} = 8s_6 \oplus s_5 \oplus 9s_4 \oplus 3s_3 \oplus 10s_2 \oplus 8s_1 \pmod{11}, \\ s_{11} = 2s_6 \oplus 9s_5 \oplus 9s_4 \oplus 10s_3 \oplus 8s_2 \oplus 6s_1 \oplus 4s_0 \pmod{11}, \\ s_{12} = s_6 \oplus 9s_5 \oplus 6s_4 \oplus 8s_3 \oplus 6s_2 \oplus s_0 \pmod{11}, \\ s_{13} = 5s_6 \oplus 6s_5 \oplus 6s_4 \oplus 6s_3 \oplus 10s_2 \oplus 6s_0 \pmod{11}. \end{cases} \quad (18)$$

Построим матрицу $\mathbf{B}$, соответствующую выражению (12):

$$\mathbf{B} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 0 & 1 & 4 & 9 & 5 & 3 & 3 & 5 & 9 & 4 & 1 \\ 0 & 1 & 8 & 5 & 9 & 4 & 7 & 2 & 6 & 3 & 10 \\ 0 & 1 & 5 & 4 & 3 & 9 & 9 & 3 & 4 & 5 & 1 \\ 0 & 1 & 10 & 1 & 1 & 1 & 10 & 10 & 10 & 1 & 10 \\ 0 & 1 & 9 & 3 & 4 & 5 & 5 & 4 & 3 & 9 & 1 \end{bmatrix},$$

на основании которой, в соответствии с выражением (13), сформируем порождающую матрицу $\mathbf{G}$ (для кода РС) систематической формы:

$$\mathbf{G} = \left[\begin{array}{ccccccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 7 & 6 & 7 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 4 & 7 & 9 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 10 & 8 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 9 & 7 & 7 & 9 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 8 & 10 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 9 & 7 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 7 & 6 & 7 & 1 \end{array}\right]. \quad (19)$$

Представим систему характеристических уравнений (18) в виде матричного уравнения, из которого извлечем матрицу $\mathbf{P}_7$:

$$\mathbf{P}_7 = \begin{bmatrix} 7 & 0 & 9 & 0 & 0 & 9 & 6 \\ 5 & 9 & 8 & 0 & 9 & 3 & 9 \\ 0 & 8 & 1 & 9 & 3 & 10 & 8 \\ 8 & 1 & 9 & 3 & 10 & 8 & 0 \\ 2 & 9 & 9 & 10 & 8 & 6 & 4 \\ 1 & 9 & 6 & 8 & 6 & 0 & 1 \\ 5 & 6 & 6 & 6 & 0 & 10 & 6 \end{bmatrix}.$$

Далее в выражении (19) единичную матрицу $\mathbf{E}_7$ заменим на матрицу $\mathbf{P}_7^{\mathrm{T}}$, в результате получим:

$$\mathbf{G}'' = \left[\begin{array}{ccccccc|cccc} 7 & 5 & 0 & 8 & 2 & 1 & 5 & 1 & 7 & 6 & 7 \\ 0 & 9 & 8 & 1 & 9 & 9 & 6 & 4 & 7 & 9 & 1 \\ 9 & 8 & 1 & 9 & 9 & 6 & 6 & 10 & 8 & 1 & 2 \\ 0 & 0 & 9 & 3 & 10 & 8 & 6 & 9 & 7 & 7 & 9 \\ 0 & 9 & 3 & 10 & 8 & 6 & 0 & 2 & 1 & 8 & 10 \\ 9 & 3 & 10 & 8 & 6 & 0 & 10 & 1 & 9 & 7 & 4 \\ 6 & 9 & 8 & 0 & 4 & 1 & 6 & 7 & 6 & 7 & 1 \end{array}\right].$$

Наконец, фрагменты 11-значной ПСП, формируемые в соответствии с выражением (15) и отождествляемые как систематический код РС с $d_{\min}$=5, имеют вид:

$$\textit{шаг}\ 1\begin{cases} s_{6,7}^{(1)} = 0, \\ s_{5,8}^{(1)} = 3, \\ s_{4,9}^{(1)} = 3, \\ s_{3,10}^{(1)} = 10, \\ s_{2,11}^{(1)} = 7, \\ s_{1,12}^{(1)} = 2, \\ s_{0,13}^{(1)} = 3, \\ \hat{s}_3^{(1)} = 2, \\ \hat{s}_2^{(1)} = 10, \\ \hat{s}_1^{(1)} = 5, \\ \hat{s}_0^{(1)} = 4; \end{cases} \quad \textit{шаг}\ 2\begin{cases} s_{6,14}^{(2)} = 1, \\ s_{5,15}^{(2)} = 4, \\ s_{4,16}^{(2)} = 9, \\ s_{3,17}^{(2)} = 8, \\ s_{2,18}^{(2)} = 9, \\ s_{1,19}^{(2)} = 7, \\ s_{0,20}^{(2)} = 5, \\ \hat{s}_3^{(2)} = 4, \\ \hat{s}_2^{(2)} = 4, \\ \hat{s}_1^{(2)} = 4, \\ \hat{s}_0^{(2)} = 4; \end{cases} \quad \textit{шаг}\ 3\begin{cases} s_{6,21}^{(3)} = 4, \\ s_{5,22}^{(3)} = 9, \\ s_{4,23}^{(3)} = 3, \\ s_{3,24}^{(3)} = 10, \\ s_{2,25}^{(3)} = 4, \\ s_{1,26}^{(3)} = 10, \\ s_{0,27}^{(3)} = 6, \\ \hat{s}_3^{(3)} = 4, \\ \hat{s}_2^{(3)} = 10, \\ \hat{s}_1^{(3)} = 1, \\ \hat{s}_0^{(3)} = 8; \end{cases} \quad \textit{шаг}\ 4\begin{cases} s_{6,28}^{(4)} = 7, \\ s_{5,29}^{(4)} = 0, \\ s_{4,30}^{(4)} = 8, \\ s_{3,31}^{(4)} = 6, \\ s_{2,32}^{(4)} = 2, \\ s_{1,33}^{(4)} = 2, \\ s_{0,34}^{(4)} = 2, \\ \hat{s}_3^{(4)} = 10, \\ \hat{s}_2^{(4)} = 3, \\ \hat{s}_1^{(4)} = 7, \\ \hat{s}_0^{(4)} = 0; \end{cases} \ \ldots,$$

при этом $\chi_{\text{обн}} \le 4$, а $\chi_{\text{исп}} \le 2$.

Далее проверочная матрица **H** систематического кода РС вычисляется по формуле (16) и представляется в следующей форме:

$$\mathbf{H} = \left[\begin{array}{ccccccc|cccc} 6 & 5 & 3 & 3 & 4 & 10 & 10 & 1 & 0 & 0 & 0 \\ 1 & 7 & 8 & 10 & 0 & 9 & 1 & 0 & 1 & 0 & 0 \\ 9 & 2 & 0 & 9 & 2 & 0 & 2 & 0 & 0 & 1 & 0 \\ 10 & 4 & 1 & 9 & 1 & 3 & 7 & 0 & 0 & 0 & 1 \end{array}\right].$$

Рассмотрим 3-й блок 11-значной ПСП $[4, 9, 3, 10, 4, 10, 6, 4, 10, 1, 8]$, не содержащий ошибок. В соответствии с выражением (17) получим вектор-синдром $\boldsymbol{\alpha}_3$:

$$\begin{bmatrix}0\\0\\0\\0\end{bmatrix} = \begin{bmatrix}4\\9\\3\\10\\4\\10\\\underline{6}\\\underline{4}\\10\\1\\8\end{bmatrix} \times \left[\begin{array}{cccc}6&1&9&10\\5&7&2&4\\3&8&0&1\\5&10&9&9\\4&0&2&1\\10&9&0&3\\\underline{10}&\underline{1}&\underline{2}&\underline{7}\\\hline 1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{array}\right].$$

Как видно, все четыре компоненты полученного вектора-синдрома равны 0, следовательно, 3-й блок 11-значной ПСП не содержит искажений.

Внесем ошибку. Например, на символы $s_{3,31}^{(4)}$, $s_{0,34}^{(4)}$ воздействует искажение $\{+2\}$, то есть примем за 4-й блок 11-значной ПСП следующее значение $\left[7, 0, 8, \tilde{8}, 2, 2, \tilde{4}, 10, 3, 7, 0\right]$. Найдем вектор-синдром $\boldsymbol{\alpha}_4$:

$$\begin{bmatrix}8\\0\\0\\10\end{bmatrix} = \begin{bmatrix}7\\0\\8\\\underline{8}\\2\\2\\\underline{4}\\\underline{10}\\3\\7\\0\end{bmatrix} \times \left[\begin{array}{cccc}6&1&9&10\\5&7&2&4\\3&8&0&1\\5&10&9&9\\4&0&2&1\\10&9&0&3\\\underline{10}&\underline{1}&\underline{2}&\underline{7}\\\hline 1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{array}\right].$$

Полученный вектор-синдром $\boldsymbol{\alpha}_4$ не является нулевым, следовательно, 4-й блок 11-значной ПСП содержит ошибки. При этом

процедура исправления обнаруженных искажений может быть реализована с помощью известных правил [6].

5. Отказоустойчивость функционирования *q*-ЛРРС. Разработанный в настоящей работе подход является, по сути, инструментом решения задачи обеспечения безопасного (надежного) функционирования дискретных устройств. При этом результативность рассматриваемого решения может быть охарактеризована свойством отказоустойчивости. Тогда в качестве показателя отказоустойчивости определим вероятность безотказной работы в течение времени t (показатель $P(t)$). Тогда вероятности безотказной работы $P_{\text{Sl}}(t)$ параллельного многозначного генератора ПСП с функцией контроля ошибок по принципу функционирования — скользящее резервирование соответствует выражение:

$$P_{\text{Sl}}(t) = \sum_{i=0}^{m} \frac{((g-m)\lambda g^{-1}t)^i}{i\,!}\, e^{-(g-m)\lambda g^{-1}t},$$

где g — общее число элементов схемы, m — число резервных элементов схемы, λ — интенсивность отказов, $e = 2,71828$ — число Эйлера.

Оценивание произведем, например, при продолжительности эксплуатации 56450 часов и интенсивности отказов – $\lambda = 0,00001$ *час*$^{-1}$. В качестве исходных данных рассмотрим параллельные многозначные генераторы ПСП следующих структур: $g = \{5, 9, 11\}$, $m = 2 - const$. Результаты оценивания приведены в таблице 4.

Таблица 4. Расчетные данные вероятности безотказной работы

Суммарная продолжительность эксплуатации t, час	$P_{\text{Sl1}}(t)$ $g = 5,\ m = 2$	$P_{\text{Sl2}}(t)$ $g = 9,\ m = 2$	$P_{\text{Sl3}}(t)$ $g = 13,\ m = 2$
2400	0.999999	0.999999	0.999999
6050	0.999992	0.999983	0.999978
13250	0.999921	0.999831	0.999784
20450	0.999719	0.999404	0.999241
27650	0.999328	0.998588	0.998207
34850	0.998696	0.997288	0.996569
42050	0.997782	0.995428	0.994237
49250	0.996549	0.992952	0.991146
56450	0.994966	0.989814	0.98725

Графическое представление полученных результатов представлено на рисунке 5.

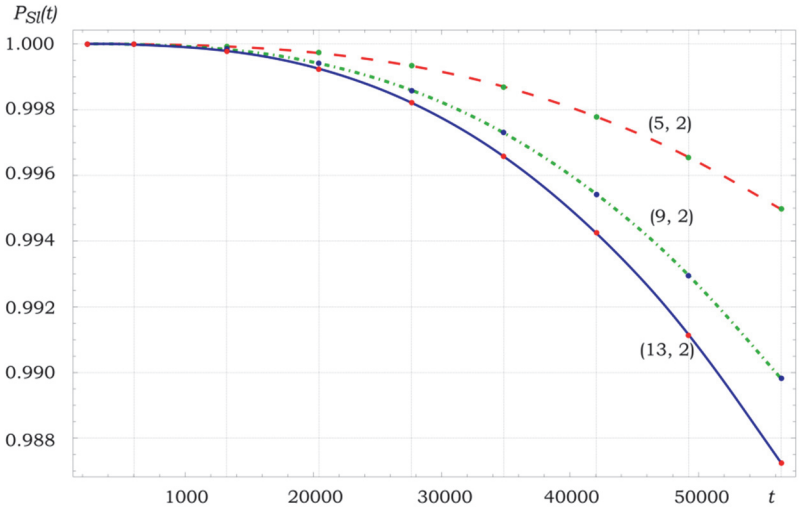


Рис. 5. Зависимость вероятности безотказной работы генератора ПСП от числа информационных элементов g при фиксированном числе контрольных $m - const$

6. Заключение. Представлен параллельный линейный генератор многозначных псевдослучайных последовательностей с контролем ошибок функционирования. Отличительная особенность предлагаемого решения заключается в итеративной процедуре арифметического представления МФАЛ и применения арифметического модулярного кода. Совокупность указанных решений обеспечивает параллельную реализацию фрагментов ПСП с контролем ошибок вычислений в рамках одной рекурсивной арифметической формулы. При этом в реальном масштабе времени обеспечивается функциональный контроль оборудования, что является принципиальным для СКЗИ. Также предложены решения контроля ошибок функционирования многозначных генераторов ПСП, основанные на многозначных помехоустойчивых кодах Рида — Соломона, позволяющие существенно повысить уровень отказоустойчивости без увеличения аппаратной избыточности. И несмотря на то, что в работе рассмотрены классические q-ЛРРС, полученные решения могут лежать в основе синтеза более сложных q-ЛРРС, предназначенных для перспективных высокопроизводительных средств криптографической защиты информации.

Очевидно, что в рамках этой работы не уделяется внимания важной области — оценивания и проверки качества ПСП с контрольными (избыточными) элементами. Однако существующее многообразие различных критериев (тесты автокорреляции, профиля сложности линейной, серий, частот цепочек и т.д.) требует отдельного рассмотрения как направление дальнейших исследований.

Литература

1 *Козлитин О.А.* Использование 2-линейного регистра сдвига для выработки псевдослучайных последовательностей // Математические вопросы криптографии. 2014. № 1. С. 39–72.

2 *Hwang T., Gope P.* Robust stream-cipher mode of authenticated encryption for secure communication in wireless sensor network // Security and communication networks. 2016. pp. 667–679.

3 *Chen D. et al.* Multi-message Authentication over Noisy Channel with Secure Channel Codes // 2017. arXiv preprint arXiv:1708.02888. 15 p. URL: https://arxiv.org/pdf/1708.02888.pdf (дата обращения: 14.05.2018).

4 *Zou M.H., Ma K, Wu K.J.* Scan-based attack on stream ciphers: A case study on eSTREAM finalists // Computer science and technology. 2014. vol. 29. pp. 646–655.

5 *Yang B., Wu K., Karri R.* Scan Based Side Channel Attack on Data Encryption Standart. IACR Cryptology ePrint Archive. 2004. vol. 2004. 6 p. URL: http://eprint.iacr.org/2004/083.pdf (дата обращения: 14.05.2018).

6 *Хетагуров Я.А., Пруднев Ю.П.* Повышение надежности цифровых устройств методами избыточного кодирования // М.: Энергия. 1974. 270 с.

7 *Диченко С.А., Финько О.А.* Безопасные генераторы псевдослучайных линейных последовательностей на арифметических полиномах для защищенных систем связи // Нелинейный мир. 2013. № 9. С. 632−647.

8 *Finko O.A., Dichenko S.A.* Secure Pseudo-Random Linear Binary Sequences Generators Based on Arithmetic Polynoms: Soft Computing in Computer and Information Science // Soft computing in computer and information science. 2015. vol. 342. pp. 279−290.

9 *Tao S., Dubrova E.* MVL-PUFs: multiple-valued logic physical unclonable functions // International Journal of Circuit Theory and Applications. 2017. vol. 2. no. 45. pp. 292−304.

10 *Соколов А.В., Жданов О.Н., Айвазян О.А.* Методы синтеза алгебраической нормальной формы функций многозначной логики // Системный анализ и прикладная информатика. 2016. № 1. С. 69–76.

11 *Abd-EI-Barr M., Al-Noori A.* Logic Design and Comparison of Arithmetic Structures for AES Cryptographic Systems // International Conference on Security and Management (SAM'2015). 2015. pp. 185–191.

12 *Abd-EI-Barr M., Al-Noori A.* Arithmetic structures for AES cryptographic systems // 2nd International Conference on Electronics and Communication Systems (ICECS). 2015. pp. 1364–1370.

13 *Gardner D., Sălăgean A., Phan R.C.W.* Efficient Generation of Elementary Sequences: Cryptography and Coding // IMA International Conference on Cryptography and Coding. 2013. LNCS 8308. pp. 16–27.

14 *Kim S-Y., Cho K-R., Lee J-H.* Design of *q*-Parallel LFSR-Based Syndrome Generator // IEICE Transaction on Electronics. 2015. pp. 594–596.

15 *Мельников С.Ю.* Статистические свойства неавтономных обобщенных двоичных регистров сдвига // Доклады Томского государственного университета систем управления и радиоэлектроники. 2017. № 1. С.93−95.

16 *Finko O.A., Samoylenko D.V.* Parallel generator of *q*-valued pseudorandom sequences based on arithmetic polynomials // Przeglad Elektrotechniczny. 2015. vol. 91. no. 3. pp. 24–28.

17 *Антоненко В.М., Иванов А.А., Шмерко В.П.* Линейные арифметические формы *k*-значных логических функций и их реализация на систолических массивах // Автоматика и телемеханика. 1995. № 3. С. 139–155.

18 *Финько О.А.* Модулярные формы систем *k*-значных функций алгебры логики // Автоматика и телемеханика. 2005. № 7. С. 66–86.

19 *Дзюжаньски П., Малюгин В.Д., Шмерко В.П., Янушкевич С.Н.* Линейные модели схем на многозначных элементах // Автоматика и телемеханика. 2002. № 6. С. 99–119.

20 *Мамонтов А.И.* О связи функциональных систем полиномов и арифметических полиномов, представляющих системы булевых функций // Вестник Московского энергетического института. 2017. № 6. С. 161–165.

21 *Mattoussi F., Roca V., Sayadi B.* Complexity Comparison of the Use of Vandermonde versus Hankel Matrices to Build Systematic MDS Reed-Solomon Codes // 2012 IEEE 13th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC). 2012. pp. 344–348. URL: https://arxiv.org/pdf/1708.02888.pdf (дата обращения: 14.05.2018).

22 *Mattoussi F., Khalighi A.M, Bourennane S.* Improving the performance of underwater wireless optical communication links by channel coding // Applied Optics. 2018. vol. 57. no. 9. pp. 2115–2120.

Самойленко Дмитрий Владимирович — к-т техн. наук, докторант кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского (ВКА им. А.Ф. Можайского). Область научных интересов: безопасность информации, системы криптокодовой защиты информации, модулярная арифметика многомерных числовых систем. Число научных публикаций — 20. 19sam@mail.ru; ул. Ждановская, 13, Санкт-Петербург, 197198; р.т.: +7-812-237-19-60.

Еремеев Михаил Алексеевич — д-р техн. наук, профессор, профессор кафедры прикладных информационных технологий института комплексной безопасности и специального приборостроения, МИРЭА – Российский технологический университет, (РТУ МИРЭА). Область научных интересов: информационная безопасность, криптография, моделирование конфликтующих систем, автоматизированные системы сбора и обработки информации. Число научных публикаций — 200. mae1@rambler.ru; Проспект Вернадского, 78, Москва, 119454; р.т.: +7-812-237-19-60.

Финько Олег Анатольевич — д-р техн. наук, профессор, профессор специальной кафедры, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко, академический советник, Российская академия ракетных и артиллерийских наук (отделение технических средств и технологий разведки, навигации, связи и управления). Область научных интересов: параллельные вычисления в системе остаточных классов, числовая реализация систем функций алгебры логики, функциональное диагностирование цифровых устройств избыточными кодами, контроль целостности информации в системах электронного документооборота и других информационных системах, аспекты инженерной реализации криптографических примитивов, системы счисления. Число научных публикаций — 150. ofinko@yandex.ru, http://www.mathnet.ru/rus/person40004; ул. Красина, 4, Краснодар, 350065; р.т.: +79882411171.

Диченко Сергей Александрович — к-т техн. наук, преподаватель, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко. Область научных интересов: инженерные аспекты криптографии: компьютерная алгебра, логические вычисления в криптографии, контроль ошибок криптографических преобразований. Число научных публикаций — 30. dichenko.sa@yandex.ru; ул. Красина, 4, Краснодар, 350065; р.т.: 7-861-268-35-09.

DOI 10.15622/sp.59.2

D.V. SAMOYLENKO, M.A. EREMEEV, O.A. FINKO, S.A. DICHENKO

PARALLEL LINEAR GENERATOR OF MULTIVALUED PSEUDORANDOM SEQUENCES WITH OPERATION ERRORS CONTROL

Samoylenko D.V., Eremeev M.A., Finko O.A., Dichenko S.A. **Parallel Linear Generator of Multivalued Pseudorandom Sequences with Operation Errors Control.**

Abstract. A parallel linear generator of multi-valued pseudorandom sequences, which operates under conditions of generating hardware errors caused by destructive adversary actions is proposed. The main types of modification of the pseudorandom sequence in case of adversary attack are considered. A distinctive feature of the iterative process of ensuring the reliability of computational operations is the "arithmetic" of computational operations by representing a system of generating recurring logical formulas as a system of many-valued logic algebra functions. The subsequent realization of multivalued logic algebra functions by means of arithmetic polynomials allowed us to parallelize the process of generating multivalued pseudorandom sequences and level out the existing complexity (specificity) of cryptographic transformations of logical data types which limit the use of redundant coding methods. As a result, a solution that allows to apply redundant modular codes to control the accuracy of the computational operations performed by the nodes of pseudorandom sequence generation is proposed. Moreover, unlike the known solutions, the proposed method provides obtaining fragments of a pseudorandom sequence on the basis of one recursive arithmetic formula with parallel calculation errors control. The use of modular forms made it possible to transfer computations from the rational numbers field arithmetic to integer arithmetic of a simple field.

Among the existing variety of codes correcting errors (maximally spaced codes), a special place is occupied by multivalued Reed-Solomon codes. Reed-Solomon codes usage in the formation of pseudorandom sequences allows the formation of code-like structures that monitor and ensure the reliability of computational operations. The calculated probability of failure-free operation of the parallel linear generator of multivalued pseudorandom sequences with an error control function based on the principle of functioning — sliding redundancy is obtained. The achieved results can find wide application at realization of perspective high-efficiency cryptographic information protection facility.

Keywords: *q*-valued pseudorandom sequences, linear recurrent shift registers, modular arithmetic, modular forms of multivalued, logic algebra functions, cryptographic information protection facility.

Samoylenko Dmitry Vladimirovich — Ph.D., doctoral student of system for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: information security, crypto-coded information security systems, and modular arithmetic of multidimensional numerical systems. The number of publications — 20. 19sam@mail.ru; 13, Zhdanovskaya str., St.-Petersburg, 197198, Russia; office phone: +7-812-237-19-60.

Eremeev Mikhail Alekseevich — Ph.D., Dr. Sci., professor, professor of applied information technology the department of institute a comprehensive safety and special instrumentation, MIREA – Russian Technological University. Research interests: information security, cryptography, modeling of the conflicting systems. The number of publications — 200. mae1@rambler.ru; 78, pr. Vernadskogo, Moscow, 119454, Russia; office phone: +7-812-237-19-60.

Finko Oleg Anatolievich — Ph.D., Dr. Sci., professor, professor of the special department, The Krasnodar higher military college of a name of general Shtemenko S.M., academic adviser, Russian Academy of Rocket and Artillery Sciences. Research interests: parallel computations in the residual class system, numerical implementation of the systems of logic algebra functions, functional diagnostics of digital devices with redundant codes, information integrity control in electronic document management systems and other information systems, aspects of the engineering implementation of cryptographic primitives, the number system. The number of publications — 150. ofinko@yandex.ru, http://www.mathnet.ru/eng/person40004; 4, Krasina str., Krasnodar, 350065, Russia; office phone: +79882411171.

Dichenko Sergey Aleksandrovich — Ph.D., lecturer, The Krasnodar higher military college of a name of general Shtemenko S.M.. Research interests: engineering aspects of cryptography: computer algebra, logical calculations in cryptography, error control of cryptographic transformations. The number of publications — 30. dichenko.sa@yandex.ru; 4, Krasina str., Krasnodar, 350065, Russia; office phone: 7-861-268-35-09.

References

1. Kozlitin O.A. [Constructing pseudorandom sequences by means of 2-linear shift register]. *Matematicheskie Voprosy Kriptografii − Mathematical Aspects of Cryptography*. 2014. vol. 9. pp. 632–647. (In Russ.).
2. Hwang T., Gope P. Robust stream-cipher mode of authenticated encryption for secure communication in wireless sensor network. *Security and communication networks*. 2016. pp. 667–679.
3. Chen D. et al. Multi-message Authentication over Noisy Channel with Secure Channel Codes. 2017. arXiv preprint arXiv:1708.02888. 15 p. Available at: https://arxiv.org/pdf/1708.02888.pdf (accessed: 14.05.2018).
4. Zou M.H., Ma K, Wu K.J. Scan-based attack on stream ciphers: A case study on eSTREAM finalists. Computer science and technology. 2014. vol. 29. pp. 646–655.
5. Yang B., Wu K., Karri R. Scan Based Side Channel Attack on Data Encryption Standart. IACR Cryptology ePrint Archive. 2004. vol. 2004. 6 p. Available at: http://eprint.iacr.org/2004/083.pdf (accessed: 14.05.2018).
6. Hetagurov Ya.A., Prudnev Yu.P. *Povyshenie nadezhnosti cifrovyh ustrojstv metodami izbytochnogo kodirovanija* [Increasing the reliability of digital devices by redundant coding methods]. M.: Jenergija. 1974. 270 p. (In Russ.).
7. Dichenko S.A., Finko O.A. [Safe generators of pseudo-random linear sequences on arithmetic polynomials for secure communication systems]. *Nelineinyi mir – Nonlinear World.* 2013. vol. 9. pp. 632−647. (In Russ.).
8. Finko O.A., Dichenko S.A. Secure Pseudo-Random Linear Binary Sequences Generators Based on Arithmetic Polynoms: Soft Computing in Computer and Information Science. Soft computing in computer and information science. 2015. vol. 342. pp. 279−290.
9. Tao S., Dubrova E. MVL-PUFs: multiple-valued logic physical unclonable functions. *International Journal of Circuit Theory and Applications*. 2017. vol. 2 no. 45. pp. 292−304.
10. Sokolov A.V., Zhdanov O.N., Ayvazian O.A. [Synthesis methods of algebraic normal form of many-valued logic functions]. *Sistemnyj analiz i prikladnaja informatika – System analysis and applied information science.* 2016. vol. 1. pp. 69−76. (In Russ.).
11. Abd-EI-Barr M., Al-Noori A. Logic Design and Comparison of Arithmetic Structures for AES Cryptographic Systems. International Conference on Security and Management (SAM'2015). 2015. pp. 185−191.
12. Abd-EI-Barr M., Al-Noori A. Arithmetic structures for AES cryptographic systems. 2nd International Conference on Electronics and Communication Systems (ICECS). 2015. pp. 1364−1370.

13. Gardner D., Sălăgean A., Phan R.C.W. Efficient Generation of Elementary Sequences: Cryptography and Coding. IMA International Conference on Cryptography and Coding. 2013. LNCS 8308. pp. 16−27.
14. Kim S-Y., Cho K-R., Lee J-H. Design of *q*-Parallel LFSR-Based Syndrome Generator. *IEICE Transaction on Electronics*. 2015. pp. 594−596.
15. Melnikov S.Yu. [Statistical properties of generalized binary shift registers]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioehlektroniki – Proceedings of Tomsk State University of Control Systems and Radioelectronics.* 2017. vol. 1. pp. 93–95. (In Russ.).
16. Finko O.A., Samoylenko D.V. Parallel generator of *q*-valued pseudorandom sequences based on arithmetic polynomials. *Przeglad Elektrotechniczny*. 2015. vol. 91. no. 3. pp. 24−28.
17. Antonenko V.M., Ivanov A.A., Shmerko V.P. [Linear arithmetic forms of *k*-valued logic functions and their implementation on systolic arrays]. *Avtomatika i telemehanika – Automation and Remote Control*. 1995. vol. 3. pp. 139–155. (In Russ.).
18. Finko O.A. [Modular forms of systems of *k*-valued functions of the algebra of logic]. *Avtomatika i telemehanika – Automation and Remote Control*. 2005. vol. 7. pp. 66–86. (In Russ.).
19. Dziurzanskii P., Malyugin V.D., Shmerko V.P., Yanushkevich S.N. [Linear Models of Circuits Based on the Multivalued Components]. *Avtomatika i telemehanika – Automation and Remote Control.* 2002. vol. 6. pp. 99–119. (In Russ.).
20. Mamontov A.I. [On the Connection between the Functional Systems of Polynomials and Arithmetic Polynomials Representing Systems of Boolean Functions]. *Vestnik Moskovskogo ehnergeticheskogo instituta – Vestnik Moscow Power Engineering Institute.* 2017. vol. 6. pp. 161–165. (In Russ.).
21. Mattoussi F., Roca V., Sayadi B. Complexity Comparison of the Use of Vandermonde versus Hankel Matrices to Build Systematic MDS Reed-Solomon Codes. 2012 IEEE 13th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC). 2012. pp. 344–348. Available at: https://arxiv.org/pdf/1708.02888.pdf (accessed: 14.05.2018).
22. Mattoussi F., Khalighi A.M, Bourennane S. Improving the performance of underwater wireless optical communication links by channel coding. *Applied Optics*. 2018. vol. 57. no. 9. pp. 2115–2120.

УДК 681.518.5:004.052.32 **DOI** 10.15622/sp.59.3

Д.В. Ефанов

СИНТЕЗ САМОПРОВЕРЯЕМЫХ КОМБИНАЦИОННЫХ УСТРОЙСТВ НА ОСНОВЕ КОДОВ С ЭФФЕКТИВНЫМ ОБНАРУЖЕНИЕМ СИММЕТРИЧНЫХ ОШИБОК

Ефанов Д.В. **Синтез самопроверяемых комбинационных устройств на основе кодов с эффективным обнаружением симметричных ошибок.**

Аннотация. При создании надежных и безопасных компонентов систем автоматического управления часто используются методы помехоустойчивого кодирования — как при передаче данных между узлами системы, так и на уровне архитектуры аппаратных и программных средств. Широко применяется избыточное кодирование при организации контроля комбинационных логических устройств. При этом используются коды, ориентированные именно на обнаружение, а не исправление ошибок. Такие особенности кодов позволяют реализовывать контролепригодные системы автоматики с приемлемой избыточностью, не превышающей избыточности при использовании дублирования. В статье освещается метод синтеза самопроверяемых комбинационных устройств, позволяющий учитывать при решении задачи построения технических средств диагностирования особенности архитектуры исходных устройств, а также свойства обнаружения ошибок избыточными кодами. Даются базовые сведения из теории синтеза контролепригодных дискретных систем на основе избыточных кодов с суммированием. Определены ключевые этапы анализа топологий объектов диагностирования с выделением специальных групп выходов — групп структурно и функционально симметрично независимых выходов устройств. Приводятся формулы, позволяющие установить наличие или отсутствие симметричной зависимости выходов объекта диагностирования. Дается пример, иллюстрирующий процесс вычислений. Сформулированы основные этапы анализа применения избыточных кодов при выявлении ошибок на функционально симметрично зависимых выходах. Дан алгоритм синтеза самопроверяемых логических устройств с учетом особенностей структуры объекта диагностирования и свойств избыточных кодов.

Ключевые слова: логические устройства автоматики, контролепригодная структура, техническая диагностика, диагностирование, контроль технического состояния, равномерный блочный код, код Бергера, коды с суммированием, обнаружение ошибок.

1. Введение. Важная задача разработки и конструирования современных аппаратно-программных систем автоматического управления и контроля — обеспечение высокого уровня надежности и безопасности функционирования их компонентов. Эта задача решается за счет разнообразных методов как на аппаратном, так и на программном уровнях системы: широко используются методы структурного, временного и информационного резервирования и технического диагностирования [1-7]. Для контроля корректности выполняемых вычислительных процедур по реализации ответственных технологических алгоритмов применяются методы сигнатурного анализа и сканирования, используются структуры устройств, обладающие свойством самопроверяемости, а также проводится тестирование блоков и компонентов в свободное от выполнения ими своих функций время [8, 9].

Еще на этапе разработки и синтеза компонентов систем управления в структуры будущих устройств закладываются такие технические решения, которые позволяют обеспечить наиболее рациональную реализацию процедур технического диагностирования [10, 11]. Это обеспечивает реализацию контролепригодных систем автоматического управления. При этом часто учитываются и другие требования по реализации компонентов, ориентированные на снижение избыточности аппаратных средств, повышение их быстродействия, снижение энергопотребления и в конечном итоге снижение капиталовложений на их разработку и затрат на последующую эксплуатацию [12-15].

Вопросам синтеза контролепригодных дискретных систем посвящено множество публикаций отечественных и зарубежных ученых [16-21]. Среди методов синтеза подобных систем особое место занимает применение равномерных блочных кодов, в которых глубоко проработаны вопросы использования равновесных кодов и кодов с суммированием [22-27]. Зачастую снижая требования к классам идентифицируемых неисправностей (и, например, ограничиваясь некоторой общепринятой моделью неисправностей), можно синтезировать устройства с простыми и контролепригодными структурами, а избыточность конечных блоков становится меньшей, чем при использовании традиционного подхода дублирования [16, 28].

Данная работа посвящена развитию методов применения избыточного кодирования при построении контролепригодных дискретных систем и освещает новый подход, который учитывает как особенности топологии исходного комбинационного логического устройства, так и свойства выбираемого для организации технического диагностирования избыточного кода.

2. Постановка задачи. Рассматриваемый класс логических устройств — это класс устройств, не обладающих памятью (комбинационные логические схемы). Такие устройства могут быть формально описаны различными способами. Если речь идет о разрабатываемом устройстве с известной элементной базой, например простейшие логические элементы, реализующие элементарные функции алгебры логики, то описание содержит: набор входов и выходов устройства; состав логических элементов; конфигурацию логических связей между входами и выходами устройства, а также между входами и выходами логических элементов. Такой подход в описании используется во всех современных средствах логического проектирования — как с изображением структурной схемы, так и с описанием на уровне языка логического проектирования [29].

Для организации контроля технического состояния комбинационных логических устройств используются схемы контроля, которые реализуются исходя из требований покрытия максимального количества физических дефектов (согласно выбранной или заданной модели неисправностей), а также с установленными ограничениями на структурную избыточность получаемой системы, ее энергопотребление, быстродействие и так далее.

В данной работе ставится следующая задача: развить известные алгоритмы синтеза комбинационных логических устройств на основе избыточных кодов с обнаружением монотонных ошибок с целью более полного учета свойств кодов по обнаружению других классов ошибок для снижения структурной избыточности синтезируемой контролепригодной системы.

3. Особенности обнаружения ошибок кодами с суммированием. Использование избыточных равномерных кодов, ориентированных на обнаружение ошибок, а не на их исправление, при построении систем автоматики с обнаружением неисправностей связано с диагностическими способностями первых. Те свойства, которые присущи избыточным кодам и используются при организации сетей передачи данных, применяются и для решения задач технической диагностики [30-32]. Известно [33, 34], что равновесные коды, а также классические коды с суммированием (коды Бергера) обладают возможностью обнаружения любых однонаправленных искажений (монотонных ошибок) в разрядах кодовых слов. Эта особенность данных кодов применяется при условии использования асимметричных каналов передачи данных (в таких каналах возможны только монотонные проявления помех). С другой стороны, при построении надежных систем автоматического управления использование свойства обнаружения любых монотонных ошибок равновесными кодами и кодами Бергера позволяет осуществлять контроль технического состояния их компонентов именно по свойству монотонного проявления любых ошибок в структуре на их выходах. Это свойство широко используется как при решении задач тестового, так и рабочего диагностирования [32, 35-39]. Кроме того, при синтезе устройств автоматики еще на этапе кодирования состояний абстрактного автомата часто применяется кодирование этих состояний кодом с обнаружением монотонных ошибок, что исключает наличие состязаний при работе устройства, а также облегчает процедуры технического диагностирования [40]. Свойство монотонного проявления неисправностей учитывается и в современных системах автоматизированного проектирования логических устройств автоматики и вычислительной техники.

С точки зрения использования равномерных блочных кодов при решении задач синтеза контролепригодных устройств автоматики и организации их диагностического обеспечения, ошибки в кодовых словах (или же в информационных векторах кодовых слов) классифицируются на монотонные и немонотонные ошибки (рисунок 1). В классе монотонных ошибок выделяются одиночные ошибки, которые обнаруживаются любыми помехоустойчивыми кодами. Немонотонные ошибки принято разделять на класс симметричных и класс асимметричных ошибок [41]. При возникновении немонотонной ошибки четной кратностью и равном количестве искажений нулевых и единичных разрядов ошибку относят к симметричному типу. Остальные немонотонные ошибки, связанные с искажениями неравного количества нулевых и единичных разрядов, являются асимметричными.

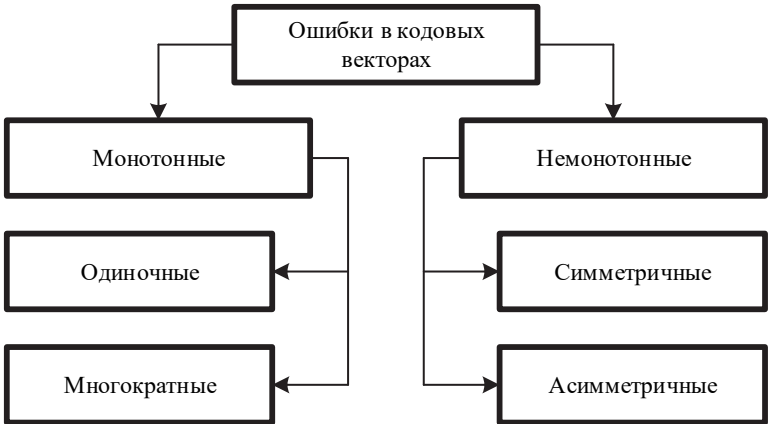


Рис. 1. Классификация ошибок в кодовых словах (или информационных векторах кодовых слов)

В [41] показано, что с увеличением количества разрядов в кодовых словах или информационных векторах кодовых слов доля монотонных ошибок от общего количества возможных ошибок стремительно уменьшается (в том числе и одиночных), тогда как доля асимметричных ошибок от общего их количества, наоборот, существенно возрастает. Симметричные же ошибки могут иметь только четную кратность, и их доля от общего количества ошибок является существенной. К примеру, при количестве разрядов, равным 10, распределение ошибок между одиночными, монотонными, симметричными и асимметричными ошибками следующее: 0,978%, 10,101%, 17,539%, 71,383%. Аналогичная закономерность наблюдается и при увеличении кратности монотонных, симметричных и асимметричных ошибок.

Остановимся на рассмотрении широкого класса кодов с суммированием [42]. Введем их обозначение — (m,k)-коды, где m и k — количество информационных и контрольных разрядов (длины информационных и контрольных векторов). Классические коды Бергера (S(m,k)-коды), которые строятся путем подсчета числа нулевых или единичных разрядов в информационных векторах и записи полученного числа в двоичном виде в разряды контрольного вектора, обладают свойством идентификации любых монотонных и асимметричных ошибок. Класс таких кодов обозначим как $UAED$(m,k)-коды (unidirectional and asymmetrical error-detection codes). Однако ценой этого свойства является невозможность обнаружения любых симметричных ошибок, число которых сравнительно велико (к примеру, это 50% двукратных и 37,5% четырехкратных ошибок в информационных векторах [43]). Избыточность S(m,k)-кодов определяется величиной $k = \lceil \log_2 (m+1) \rceil$, где запись $\lceil ... \rceil$ обозначает целое сверху от вычисляемого значения. По своим характеристикам m и k и свойству обнаружения любых монотонных и асимметричных ошибок коды Бергера являются оптимальными кодами, обнаруживающими максимум обозначенных видов ошибок.

Существует большое количество кодов с суммированием, ориентированных на сохранение свойства обнаружения любых монотонных ошибок или любых монотонных ошибок до определенной кратности d_0 — так называемых, UED(m,k) или d_0-UED(m,k) кодов [25]. Такие коды строятся путем различных модификаций классических кодов. Некоторые из них реализуемы только для частных случаев значений длин информационных векторов. Например, известны модификации кодов, связанные с использованием операции конкатенации контрольных векторов иных различных («базовых») кодов при образовании новых кодов с заданными свойствами. Известны также и коды, которые возможно строить для любых значений длин информационных векторов. Наверное, самыми известными из таких кодов являются коды Боуза — Лина (коды с суммированием единичных информационных разрядов в кольце вычетов по модулю M=4 или M=8 (SM(m,k)-коды)). Эти коды относятся к 4-UED(m,k) и 8-UED(m,k) кодам соответственно.

При использовании свойства обнаружения любых монотонных ошибок в процессе решения задач технической диагностики и синтеза контролепригодных систем автоматики никак не учитываются возможности кодов по обнаружению симметричных и асимметричных ошибок. S(m,k) и SM(m,k) коды не обнаруживают 100% симметричных ошибок. Однако известны модификации данных кодов, которые обладают уменьшенной долей необнаруживаемых симметричных ошибок в информационных векторах. При этом имеется некоторая доля моно-

тонных и асимметричных ошибок. Такие модифицированные коды с суммированием строятся за счет различных правил, включающих в себя взвешивание разрядов или переходов между разрядами, занимающими соседние позиции в информационных векторах, вычисление поправочных коэффициентов в виде сверток по модулю два, выделение подмножеств разрядов информационных векторов и отдельный их контроль и прочее [42, 44, 45]. Используя свойства кодов с суммированием, а также особенности топологии устройств автоматики, можно синтезировать системы автоматики с уменьшенной по сравнению с дублированием избыточностью [16, 30, 37]. Возможности обнаружения (m,k)-кодом некоторой доли симметричных ошибок при обнаружении любых монотонных ошибок (либо любых монотонных ошибок до определенной кратности) могут быть использованы для сокращения структурной избыточности при преобразованиях схем объектов диагностирования (рисунок 2).

Рассмотрим особенности использования свойств кодов по обнаружению монотонных и симметричных ошибок при синтезе устройств с контролепригодными структурами.

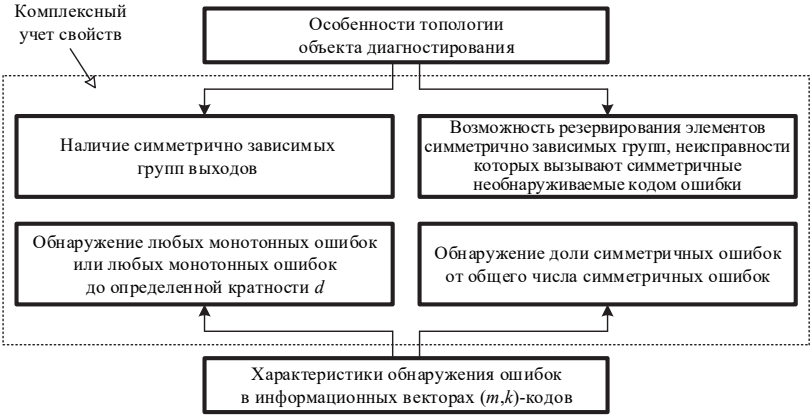


Рис. 2. Характеристики объекта диагностирования и (m,k)-кода

4. Структурно симметричная зависимость выходов. Обозначим как p_0 и p_1 — число путей, ведущих от выхода логического элемента G_q к выходам логического устройства через четное и через нечетное число инверсий соответственно (такие пути обозначим n_0-пути и n_1-пути). Тогда максимальная возможная кратность ошибки определяется суммой:

$$d_{\max} = p_0 + p_1. \quad (1)$$

Вид вызываемой внутренней неисправностью логического элемента ошибки на выходах логического устройства определяется соотношениями между числами p_0 и p_1. Ошибка на выходах будет монотонной в том случае, если все n_0-пути или же все n_1-пути от конкретного логического элемента не будут существенными из-за компенсаций сигналов ошибок в схеме устройства (под компенсацией понимается событие поглощения ошибки корректным сигналом с исправного входа логического элемента). В противном случае, если на каком-либо входном наборе будут активизированы хотя бы один существенный n_0-путь и хотя бы один существенный n_1-путь, ведущие к разным выходам, это приведет к возникновению немонотонной ошибки (симметричной или асимметричной).

Анализируя топологию логического устройства, можно установить «предварительные» условия, которые будут указывать на невозможность возникновения монотонных ошибок определенной кратности.

Пусть $p_0^{\max}$ и $p_1^{\max}$ — это максимальное число n_0-путей и n_1-путей, ведущих от всех логических элементов структуры логического устройства к его выходам. Тогда справедливы следующие положения.

Утверждение 1. Монотонная ошибка на выходах логического устройства будет иметь кратность:

$$d_\upsilon \le \max\left(p_0^{\max}; p_1^{\max}\right). \tag{2}$$

Утверждение 2. Симметричная ошибка на выходах логического устройства будет иметь кратность:

$$d_\sigma \le 2n_{0/1}^{\max}, \tag{3}$$

где $n_{0/1}^{\max}$ — максимальное число случаев $p_0 = p_1$ для одного логического элемента.

Утверждение 3. Асимметричная ошибка на выходах логического устройства будет иметь кратность:

$$d_\alpha \le \begin{cases} \max\left(p_0 + p_1\right), & \text{при} \quad p_0, p_1 \ne 0; \\ \max\left(p_0 + p_1\right) - 1, & \text{при} \quad p_0 = p_1. \end{cases} \tag{4}$$

Для примера поиска чисел d_υ, d_σ и d_α рассмотрим комбинационное логическое устройство, приведенное на рисунке 3. Данное устройство имеет двухуровневую схему, снабжено четырьмя входами и шестью выходами. Описание структуры логического устройства дано в

таблице 1, где перечислены все логические элементы второго ранга и указаны характеристики путей, ведущих от каждого элемента к элементам первого ранга, выходы которых являются непосредственно и выходами самого устройства.

Таблица 1. Характеристики заданного комбинационного логического устройства

Логический элемент	p_0	p_1	n_0-пути	n_1-пути
G_1	2	2	G_8, G_9	G_6, G_7
G_2	3	0	G_6, G_{10}, G_{11}	–
G_3	1	1	G_7	G_{10}
G_4	2	1	G_{10}, G_{11}	G_8
G_5	1	0	G_9	–

Неисправности элемента G_5 могут вызывать только одиночные ошибки, так как от данного пути идет всего один n_0-путь. Неисправности элемента G_3 могут вызывать либо одиночные ошибки, либо двукратные симметричные ошибки, так как для данного элемента имеется по одному n_0-пути и n_1-пути, ведущих к элементам G_7 и G_{10}. Ошибка на выходе элемента G_4 может трансформироваться либо в одиночную ошибку, либо в двукратную симметричную или монотонную ошибку, либо в трехкратную асимметричную ошибку. Это следует из соотношений между числом n_0-путей и n_1-путей. Ошибка на выходе G_1 может вызывать на выходах устройства те же варианты ошибок, плюс еще один — четырехкратную симметричную ошибку. И, наконец, неисправность элемента G_2 может повлечь за собой только одиночную или же двух- или трехкратную монотонную ошибку. Анализ показывает, что для приведенного на рисунке 2 логического устройства, согласно формулам (2)-(4):

$$d_\upsilon = 3 \le \max\left(p_0^{\max}; p_1^{\max}\right) = \max(3;2);$$

$$d_\sigma = 4 \le 2n_{0/1}^{\max} = 2 \cdot 2;$$

$$d_\alpha = 3 \le \max\left(p_0 + p_1\right) - 1 = \max(2+2) - 1, \text{ так как } p_0 = p_1 = 2.$$

Наличие информации о числах d_υ, d_σ и d_α для конкретного логического устройства дает возможность подбора кода с суммированием для организации контроля. Поскольку при малом количестве разрядов в контрольных векторах всегда будут присутствовать симметричные необнаруживаемые ошибки [46], то и число d_σ для большого числа кодов будет равным d_σ=2 либо d_σ=4.

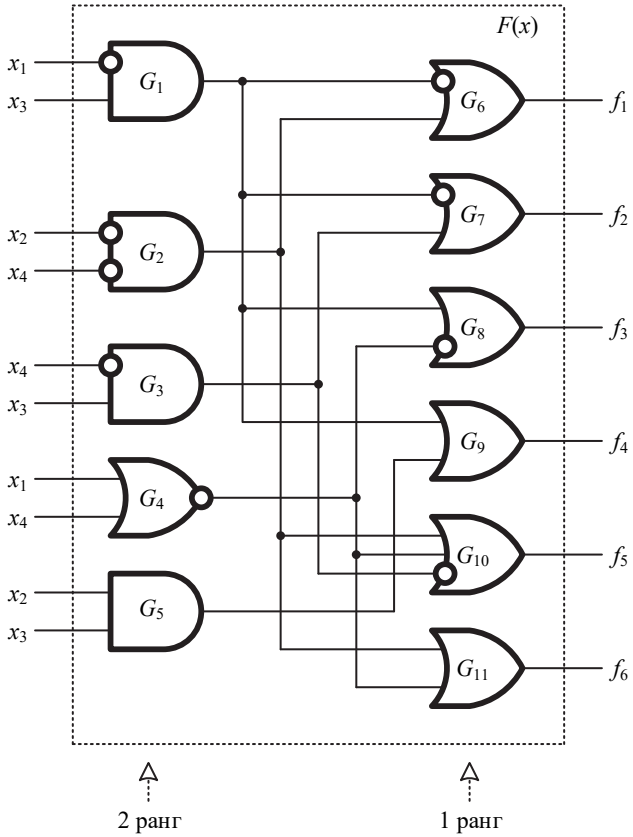


Рис. 3. Комбинационное логическое устройство

Выберем для контроля приведенного логического устройства двухмодульный код *TM*(6,4), описанный в [47]. Данным кодом идентифицируются любые монотонные и асимметричные ошибки, однако в классе необнаруживаемых имеется 336 симметричных ошибок (192 двукратных и 144 четырехкратных). Как показано в [48], генератор *TM*(6,4)-кода практически вдвое проще генератора классического кода Бергера, *S*(6,3)-кода, обладающего свойством идентификации любых монотонных и асимметричных ошибок. При этом *S*(6,3)-кодом не обнаруживается 860 симметричных ошибок (480 двукратных, 360 четырехкратных и 20 шестикратных).

Исходя из представленных характеристик *TM*(6,4)-кода и установленных особенностей топологии комбинационного логического устройства можно сделать вывод о необходимости защиты от симмет-

ричных двукратных и четырехкратных ошибок, что реализуется путем резервирования элементов по методике, описанной в [36, 37].

Определение 1. Назовем группу выходов структурно симметрично зависимой группой выходов (ССЗ-группой), если анализ топологии показал наличие случаев $p_0 = p_1$ хотя бы для одного логического элемента в структуре логического устройства.

Из таблицы 1 следует, что три логических элемента G_1, G_3 и G_4 связаны путями с выходами таким образом, что образуют следующие ССЗ-группы: $\{f_1; f_2; f_3; f_4\}$, $\{f_2; f_5\}$, $\{f_3; f_5; f_6\}$.

5. Функционально симметричная зависимость выходов. Структурная симметричная зависимость выходов еще не означает реальной функциональной зависимости, поскольку визуальный анализ схемы говорит только о потенциальной возможности возникновения симметричной ошибки. Такой анализ никак не затрагивает функциональных особенностей логических элементов структуры логического устройства.

Определение 2. Назовем группу выходов функционально симметрично зависимой группой выходов (ФСЗ-группой), если хотя бы на одном входном наборе при неисправности какого-либо элемента, связанного путями с данными выходами, формируется симметричная ошибка.

Поиск ФСЗ-групп позволяет учесть и особенности структуры логического устройства и исключить случаи избыточного резервирования элементов при преобразовании схемы устройства в схему с контролепригодной топологией.

Теорема 1. Неисправность логического элемента G_q внутренней структуры логического устройства будет вызывать на выходах f_{i_1} и f_{i_2} симметричную ошибку в том случае, если выполнено условие:

$$\psi^{2,\sigma} = \frac{\partial f_{i_1}}{\partial y_q}\frac{\partial f_{i_2}}{\partial y_q}\left(f_{i_1} \oplus f_{i_2}\right) \neq 0, \qquad (5)$$

где y_q – функция, реализуемая на выходе логического элемента G_q.

Доказательство. В формуле (5) сомножитель $\frac{\partial f_{i_1}}{\partial y_q}\frac{\partial f_{i_2}}{\partial y_q}$ определяет условия одновременного искажения выходов f_{i_1} и f_{i_2} (те входные наборы, которые вызывают двукратное искажение), а сомножитель $\left(f_{i_1} \oplus f_{i_2}\right)$ позволяет установить вид ошибки. Если значения функций на каких-либо входных наборах были равны, то

двукратная ошибка на этих же входных наборах будет монотонной, в противном случае — симметричной. Таким образом, выражение (5) определяет те входные наборы, на которых возникает симметричная ошибка на выходах f_{i_1} и f_{i_2}. Это и зафиксировано в условии теоремы 1.

Формула (5) используется для поиска монотонно независимых групп выходов [16, 36, 37].

Теорема 2. Неисправность логического элемента G_q внутренней структуры логического устройства будет вызывать симметричную ошибку на четном количестве выходов f_{i_1}, f_{i_2}, …, f_{i_d} в том случае, если выполнено условие:

$$\psi^{d,\sigma} = F^d F^\sigma \neq 0, \tag{6}$$

где $F^d = \frac{\partial f_{i_1}}{\partial y_q}\frac{\partial f_{i_2}}{\partial y_q}\cdot\ldots\cdot\frac{\partial f_{i_d}}{\partial y_q}$, $F^\sigma = \bigvee\limits_{f_{i_1} f_{i_2} \cdot\ldots\cdot f_{i_d} \in R} f_{i_1} f_{i_2} \cdot\ldots\cdot f_{i_d}$, где F^d — функция, определяющая искажение кратностью *d*; F^σ — функция, позволяющая выявить, является ли ошибка кратностью d симметричной или нет; $f_{i_1} f_{i_2} \cdot\ldots\cdot f_{i_d}$ — конъюнкция значений выходных функций длиной d; R — множество кодовых векторов с весом $\frac{d}{2}$ и длиной d (их общее число определяется величиной $C_d^{d/2}$).

Доказательство. Функция F^d определяет входные наборы, на которых искажаются все рассматриваемые выходы, а функция F^σ — те входные наборы, на которых половина значений выходов в группе равна нулю, а половина — единице (при четном значении *d* ошибка будет симметричной, если хотя бы одна из конъюнкций равновесного кода «$\frac{d}{2}$ из *d*» не будет равна нулю). Таким образом, формула (6) позволяет определить те входные наборы, при которых происходит четное симметричное искажение рассматриваемой группы выходов.

Условие (6) необходимо проверять для всех значений четной кратности тех выходов, которые структурно допускают возможность возникновение симметричных ошибок.

Определим для рассматриваемой схемы, на каких входных наборах возникают симметричные ошибки.

Неисправности элемента G_3 могут давать только двукратные симметричные ошибки:

$$f_2 = \overline{\overline{x_1}x_3} \vee \overline{x_4}x_3 = \overline{\overline{x_1}x_3} \vee y_3,$$

$$f_5 = \overline{\overline{x_2}x_4} \vee \overline{x_1}\overline{x_4} \vee \overline{x_4}x_3 = \overline{\overline{x_2}x_4} \vee \overline{x_1}\overline{x_4} \vee \overline{y_3},$$

$$\frac{\partial f_2}{\partial y_3} = \left(\overline{\overline{x_1}x_3} \vee (y_3 = 0)\right) \oplus \left(\overline{\overline{x_1}x_3} \vee (y_3 = 1)\right) = \overline{\overline{x_1}x_3} \oplus 1 = \overline{x_1}x_3,$$

$$\frac{\partial f_5}{\partial y_3} = \left(\overline{\overline{x_2}x_4} \vee \overline{x_1}\overline{x_4} \vee \overline{(y_3 = 0)}\right) \oplus \left(\overline{\overline{x_2}x_4} \vee \overline{x_1}\overline{x_4} \vee \overline{(y_3 = 1)}\right) =$$

$$= 1 \oplus \left(\overline{\overline{x_2}x_4} \vee \overline{x_1}\overline{x_4}\right) = \overline{\overline{\overline{x_2}x_4} \vee \overline{x_1}\overline{x_4}} = \overline{\overline{x_2}x_4} \cdot x_1 x_4 =$$

$$= (x_2 \vee x_4)x_1 x_4 = x_1 x_4,$$

$$\left(\overline{x_1}x_3\right)(x_1 x_4)\left(\left(\overline{\overline{x_1}x_3} \vee \overline{x_4}x_3\right) \oplus \overline{\overline{x_2}x_4} \vee \overline{x_1}\overline{x_4} \vee \overline{x_4}x_3\right) = 0.$$

Таким образом, неисправности выхода G_3 не вызывают симметричных ошибок.

Неисправности элемента G_4 также могут давать только двукратные симметричные ошибки, причем, как следует из таблицы 1, либо в паре выходов $\{f_3; f_5\}$, либо $\{f_3; f_6\}$:

$$f_3 = \overline{x_1}x_3 \vee x_1 \vee x_4 = \overline{x_1}x_3 \vee x_1 \vee \overline{y_4},$$

$$f_5 = \overline{\overline{x_2}x_4} \vee \overline{x_1}\overline{x_4} \vee \overline{x_4}x_3 = \overline{\overline{x_2}x_4} \vee y_4 \vee \overline{x_4}x_3,$$

$$f_6 = \overline{\overline{x_2}x_4} \vee \overline{x_1}\overline{x_4} = \overline{\overline{x_2}x_4} \vee y_4,$$

$$\frac{\partial f_3}{\partial y_4} = \left(\overline{x_1}x_3 \vee x_1 \vee \overline{(y_4 = 0)}\right) \oplus \left(\overline{x_1}x_3 \vee x_1 \vee \overline{(y_4 = 1)}\right) =$$

$$= 1 \oplus \left(\overline{x_1}x_3 \vee x_1\right) = \overline{\overline{x_1}x_3 \vee x_1} = \overline{x_1}\left(x_1 \vee \overline{x_3}\right) = \overline{x_1}\overline{x_3},$$

$$\frac{\partial f_5}{\partial y_4} = \left(\overline{\overline{x_2}x_4} \vee (y_4 = 0) \vee \overline{x_4}x_3\right) \oplus \left(\overline{\overline{x_2}x_4} \vee (y_4 = 1) \vee \overline{x_4}x_3\right) =$$

$$= \left(\overline{\overline{x_2}x_4} \vee \overline{x_4}x_3\right) \oplus 1 = \overline{\overline{\overline{x_2}x_4} \vee \overline{x_4}x_3} =$$

$$= \left(x_4 \vee \overline{x_3}\right)(x_2 \vee x_4) = x_4 \vee x_2\overline{x_3},$$

$$\frac{\partial f_6}{\partial y_4} = \left(\overline{\overline{x_2}x_4} \vee (y_4 = 0)\right) \oplus \left(\overline{\overline{x_2}x_4} \vee (y_4 = 1)\right) = \overline{\overline{\overline{x_2}x_4}} = x_2 \vee x_4,$$

$$\frac{\partial f_3}{\partial y_4}\frac{\partial f_5}{\partial y_4}(f_3 \oplus f_5) = \left(\overline{\overline{x_1}\,\overline{x_3}}\right)\left(x_4 \vee x_2\overline{x_3}\right)\times$$

$$\times\left(\left(\overline{x_1}x_3 \vee x_1 \vee x_4\right) \oplus \left(\overline{\overline{x_2}\,\overline{x_4}} \vee \overline{x_1\overline{x_4}} \vee \overline{x_4}x_3\right)\right) =$$

$$= \left(\overline{\overline{x_1}\,\overline{x_3}}x_4 \vee \overline{x_1}x_2\overline{x_3}\right)\left(\overline{\overline{x_1}x_3 \vee x_1 \vee x_4}\left(\overline{\overline{x_2}\,\overline{x_4}} \vee \overline{x_1\overline{x_4}} \vee \overline{x_4}x_3\right) \vee \right.$$

$$\left. \vee \left(\overline{x_1}x_3 \vee x_1 \vee x_4\right)\overline{\overline{\overline{x_2}\,\overline{x_4}} \vee \overline{x_1\overline{x_4}} \vee \overline{x_4}x_3}\right) =$$

$$= \left(\overline{\overline{x_1}\,\overline{x_3}}x_4 \vee \overline{x_1}x_2\overline{x_3}\right)\left(\left(x_1 \vee \overline{x_3}\right)\overline{x_1\overline{x_4}}\left(\overline{\overline{x_2}\,\overline{x_4}} \vee \overline{x_1\overline{x_4}} \vee \overline{x_4}x_3\right) \vee \right.$$

$$\left. \vee \left(\overline{x_1}x_3 \vee x_1 \vee x_4\right)\left(x_2 \vee x_4\right)x_1x_4\left(\overline{x_3} \vee x_4\right)\right) =$$

$$= \left(\overline{x_1\overline{x_3}}x_4 \vee \overline{x_1}x_2\overline{x_3}\right)\left(\overline{x_1x_2x_3\overline{x_4}} \vee x_1x_4\right) = 0.$$

$$\frac{\partial f_3}{\partial y_4}\frac{\partial f_6}{\partial y_4}(f_3 \oplus f_6) = \left(\overline{\overline{x_1}\,\overline{x_3}}\right)\left(x_2 \vee x_4\right)\times$$

$$\times\left(\left(\overline{x_1}x_3 \vee x_1 \vee x_4\right) \oplus \left(\overline{\overline{x_2}\,\overline{x_4}} \vee \overline{x_1\overline{x_4}}\right)\right) =$$

$$= \left(\overline{x_1}x_2\overline{x_3} \vee \overline{\overline{x_1}\,\overline{x_3}}x_4\right)\left(\overline{\overline{x_1}x_3 \vee x_1 \vee x_4}\left(\overline{\overline{x_2}\,\overline{x_4}} \vee \overline{x_1\overline{x_4}}\right) \vee \right.$$

$$\left. \vee \left(\overline{x_1}x_3 \vee x_1 \vee x_4\right)\overline{\overline{\overline{x_2}\,\overline{x_4}} \vee \overline{x_1\overline{x_4}}}\right) =$$

$$= \left(\overline{x_1}x_2\overline{x_3} \vee \overline{\overline{x_1}\,\overline{x_3}}x_4\right)\left(\left(x_1 \vee \overline{x_3}\right)\overline{x_1\overline{x_4}}\left(\overline{x_1} \vee \overline{x_4}\right) \vee \right.$$

$$\left. \vee \left(\overline{x_1}x_3 \vee x_1 \vee x_4\right)\left(x_2 \vee x_4\right)x_1x_4\right) =$$

$$= \left(\overline{x_1}x_2\overline{x_3} \vee \overline{\overline{x_1}\,\overline{x_3}}x_4\right)\left(\overline{x_1\overline{x_3}\,\overline{x_4}} \vee x_1x_4\right) = \overline{x_1}x_2\overline{x_3}\,\overline{x_4} \neq 0.$$

Неисправности выхода элемента G_4 (ошибка типа константа 0) вызывают симметричную ошибку в паре выходов $\{f_3; f_6\}$ при подаче на входы устройства двоичного набора <0100>.

Анализ топологии логического устройства показывает, что неисправности элемента G_1 могут давать двукратные и четырехкратные симметричные ошибки. Двукратные симметричные ошибки могут возникать на выходах пар $\{f_1; f_3\}$, $\{f_1; f_4\}$, $\{f_2; f_3\}$ и $\{f_2; f_4\}$. Четырехкратные ошибки возникают во всей группе выходов $\{f_1; f_2; f_3; f_4\}$.

$$f_1 = \overline{\overline{x_1}x_3} \vee \overline{x_2}\,\overline{x_4} = \overline{y_1} \vee \overline{x_2}\,\overline{x_4},$$

$$f_2 = \overline{\overline{x_1}x_3} \vee \overline{x_4}x_3 = \overline{y_1} \vee \overline{x_4}x_3,$$

$$f_3 = \overline{x_1} x_3 \vee x_1 \vee x_4 = y_1 \vee x_1 \vee x_4,$$

$$f_4 = \overline{x_1} x_3 \vee x_2 x_3 = y_1 \vee x_2 x_3,$$

$$\frac{\partial f_1}{\partial y_1} = \left(\overline{(y_1 = 0)} \vee \overline{x_2}\,\overline{x_4}\right) \oplus \left(\overline{(y_1 = 1)} \vee \overline{x_2}\,\overline{x_4}\right) = \overline{\overline{x_2}\,\overline{x_4}} = x_2 \vee x_4,$$

$$\frac{\partial f_2}{\partial y_1} = \left(\overline{(y_1 = 0)} \vee \overline{x_4} x_3\right) \oplus \left(\overline{(y_1 = 1)} \vee \overline{x_4} x_3\right) = \overline{x_3} \vee x_4,$$

$$\frac{\partial f_3}{\partial y_1} = \left((y_1 = 0) \vee x_1 \vee x_4\right) \oplus \left((y_1 = 1) \vee x_1 \vee x_4\right) = \overline{x_1 x_4},$$

$$\frac{\partial f_4}{\partial y_1} = \left((y_1 = 0) \vee x_2 x_3\right) \oplus \left((y_1 = 1) \vee x_2 x_3\right) = \overline{x_2} \vee \overline{x_3},$$

$$\frac{\partial f_1}{\partial y_1}\frac{\partial f_3}{\partial y_1}(f_1 \oplus f_3) = (x_2 \vee x_4)\left(\overline{x_1}\,\overline{x_4}\right)\left(\left(\overline{\overline{x_1} x_3 \vee \overline{x_2}\,\overline{x_4}}\right) \oplus \left(\overline{x_1} x_3 \vee x_1 \vee x_4\right)\right) =$$

$$= \overline{x_1} x_2 \overline{x_4}\left(\overline{\overline{\overline{x_1} x_3 \vee \overline{x_2}\,\overline{x_4}}}\left(\overline{x_1} x_3 \vee x_1 \vee x_4\right) \vee \left(\overline{\overline{x_1} x_3 \vee \overline{x_2}\,\overline{x_4}}\right)\overline{\overline{x_1} x_3 \vee x_1 \vee x_4}\right) =$$

$$= \overline{x_1} x_2 \overline{x_4}\left(\overline{x_1} x_3 (x_2 \vee x_4)\left(\overline{x_1} x_3 \vee x_1 \vee x_4\right) \vee \left(\overline{\overline{x_1} x_3 \vee \overline{x_2}\,\overline{x_4}}\right)\left(x_1 \vee \overline{x_3}\right)\overline{x_1}\,\overline{x_4}\right) =$$

$$= \overline{x_1} x_2 \overline{x_4}\left(\overline{x_1} x_2 x_3 \vee \overline{x_1} x_3 x_4 \vee \overline{x_1} x_3 \overline{x_4}\right) = \overline{x_1} x_2 x_3 \overline{x_4} \vee \overline{x_1} x_2 \overline{x_3}\,\overline{x_4} \neq 0,$$

$$\frac{\partial f_1}{\partial y_1}\frac{\partial f_4}{\partial y_1}(f_1 \oplus f_4) = (x_2 \vee x_4)\left(\overline{x_2} \vee \overline{x_3}\right)\left(\left(\overline{\overline{x_1} x_3 \vee \overline{x_2}\,\overline{x_4}}\right) \oplus \left(\overline{x_1} x_3 \vee x_2 x_3\right)\right) =$$

$$= \left(\overline{x_2} x_4 \vee x_2 \overline{x_3} \vee \overline{x_3} x_4\right)\left(\overline{\overline{\overline{x_1} x_3 \vee \overline{x_2}\,\overline{x_4}}}\left(\overline{x_1} x_3 \vee x_2 x_3\right) \vee \right.$$

$$\left. \vee \left(\overline{\overline{x_1} x_3 \vee \overline{x_2}\,\overline{x_4}}\right)\overline{\overline{x_1} x_3 \vee x_2 x_3}\right) = \left(\overline{x_2} x_4 \vee x_2 \overline{x_3} \vee \overline{x_3} x_4\right) \times$$

$$\times\left(\overline{x_1} x_3 (x_2 \vee x_4)\left(\overline{x_1} x_3 \vee x_2 x_3\right) \vee \left(\overline{\overline{x_1} x_3 \vee \overline{x_2}\,\overline{x_4}}\right)\left(x_1 \vee \overline{x_3}\right)\left(\overline{x_2} \vee \overline{x_3}\right)\right) =$$

$$= \left(\overline{x_2} x_4 \vee x_2 \overline{x_3} \vee \overline{x_3} x_4\right)\left(\overline{x_1} x_2 x_3 \vee x_1 \overline{x_2} \vee \overline{x_3}\right) = x_1 \overline{x_2} x_4 \vee x_2 \overline{x_3} \vee \overline{x_3} x_4 \neq 0,$$

$$\frac{\partial f_2}{\partial y_1}\frac{\partial f_3}{\partial y_1}(f_2 \oplus f_3) = \left(\overline{x_3} \vee x_4\right)\left(\overline{x_1}\,\overline{x_4}\right)\left(\left(\overline{\overline{x_1} x_3 \vee \overline{x_4} x_3}\right) \oplus \left(\overline{x_1} x_3 \vee x_1 \vee x_4\right)\right) =$$

$$= \overline{x_1}\,\overline{x_3}\,\overline{x_4}\left(\overline{\overline{\overline{x_1} x_3 \vee \overline{x_4} x_3}}\left(\overline{x_1} x_3 \vee x_1 \vee x_4\right) \vee \left(\overline{\overline{x_1} x_3 \vee \overline{x_4} x_3}\right)\overline{\overline{x_1} x_3 \vee x_1 \vee x_4}\right) =$$

$$= \overline{x_1}\,\overline{x_3}\,\overline{x_4}\left(\overline{x_1} x_3 \left(\overline{x_3} \vee x_4\right)\left(\overline{x_1} x_3 \vee x_1 \vee x_4\right) \vee \left(x_1 \vee \overline{x_3} \vee \overline{x_4} x_3\right)\left(x_1 \vee \overline{x_3}\right)\right) = \overline{x_1}\,\overline{x_3}\,\overline{x_4} \neq 0,$$

$$\frac{\partial f_2}{\partial y_1}\frac{\partial f_4}{\partial y_1}(f_2 \oplus f_4) = \left(\overline{x_3} \vee x_4\right)\left(\overline{x_2} \vee \overline{x_3}\right)\left(\left(\overline{\overline{x_1}x_3 \vee \overline{x_4}x_3}\right) \oplus \left(\overline{x_1}x_3 \vee x_2x_3\right)\right) =$$

$$= \left(\overline{x_3} \vee \overline{x_2}x_4\right)\left(\overline{\overline{\overline{x_1}x_3 \vee \overline{x_4}x_3}\left(\overline{x_1}x_3 \vee x_2x_3\right) \vee \left(\overline{\overline{x_1}x_3 \vee \overline{x_4}x_3}\right)\overline{x_1x_3 \vee x_2x_3}}\right) =$$

$$= \left(\overline{x_3} \vee \overline{x_2}x_4\right)\left(\overline{x_1}x_3x_4 \vee x_1\overline{x_2} \vee \overline{x_3}\right) = \overline{x_1}\,\overline{x_2}x_3x_4 \vee x_1\overline{x_2}x_4 \vee \overline{x_3} \neq 0.$$

Из приведенных выкладок следует, что все четыре выхода образуют попарно группы ФСЗ-выходов.

Обратимся к анализу группы из четырех выходов.

$$\frac{\partial f_1}{\partial y_1}\frac{\partial f_2}{\partial y_1}\frac{\partial f_3}{\partial y_1}\frac{\partial f_4}{\partial y_1} = \left(x_2 \vee x_4\right)\left(\overline{x_3} \vee x_4\right)\left(\overline{x_1x_4}\right)\left(\overline{x_2} \vee \overline{x_3}\right) =$$

$$= \left(x_2\overline{x_3} \vee x_4\right)\left(\overline{x_1x_2x_4} \vee \overline{x_1x_3x_4}\right) = \overline{x_1}\,\overline{x_2}\,\overline{x_3}\,\overline{x_4}.$$

Так как существует только один вариант возникновения четырехкратной симметричной ошибки в группе рассматриваемых выходов (см. рисунок 3), необходимо проверить только условие $F^{\sigma} = \overline{f_1 f_2} f_3 f_4 \vee f_1 f_2 \overline{f_3 f_4} \neq 0$:

$$\overline{f_1 f_2} f_3 f_4 = \left(\overline{\overline{\overline{x_1}x_3 \vee \overline{x_2}x_4}}\right)\left(\overline{\overline{\overline{x_1}x_3 \vee \overline{x_4}x_3}}\right)\left(\overline{x_1}x_3 \vee x_1 \vee x_4\right)\left(\overline{x_1}x_3 \vee x_2x_3\right) =$$

$$= \left(\overline{x_1}x_3\left(x_2 \vee x_4\right)\right)\left(\overline{x_1}x_3\left(\overline{x_3} \vee x_4\right)\right)\left(\overline{x_1}x_3 \vee x_1x_2x_3 \vee x_2x_3x_4\right) =$$

$$= \left(\overline{x_1}x_2x_3 \vee \overline{x_1}x_3x_4\right)\left(\overline{x_1}x_3x_4\right)\left(\overline{x_1}x_3 \vee x_1x_2x_3 \vee x_2x_3x_4\right) = \overline{x_1}x_3x_4.$$

$$f_1 f_2 \overline{f_3 f_4} = \left(\overline{\overline{x_1}x_3 \vee \overline{x_2}x_4}\right)\left(\overline{\overline{x_1}x_3 \vee \overline{x_4}x_3}\right)\left(\overline{\overline{x_1}x_3 \vee x_1 \vee x_4}\right)\left(\overline{\overline{x_1}x_3 \vee x_2x_3}\right) =$$

$$= \left(x_1 \vee \overline{x_3} \vee \overline{x_2}x_3\overline{x_4}\right)\left(x_1 \vee \overline{x_3}\right)\overline{x_1}\,\overline{x_4}\left(x_1 \vee \overline{x_3}\right)\left(\overline{x_2} \vee \overline{x_3}\right) =$$

$$= \overline{x_1}\,\overline{x_4}\left(x_1\overline{x_2} \vee \overline{x_3}\right) = \overline{x_1}\,\overline{x_3}\,\overline{x_4}.$$

Проверим условие (6):

$$\psi^{d=4,\sigma=4} = F^{d=4}F^{\sigma=4} =$$

$$= \left(\overline{x_1}x_2\,\overline{x_3}\,\overline{x_4}\right)\left(\overline{x_1}\,\overline{x_3}\,\overline{x_4} \vee \overline{x_1}x_3x_4\right) = \overline{x_1}x_2\,\overline{x_3}\,\overline{x_4} \neq 0,$$

откуда следует, что симметричная ошибка на рассматриваемых выходах возникает при условии поступления на входы набора <0100> и формировании на выходе элемента G_1 сигнала типа константа 1.

6. Учет свойств кодов с суммированием при преобразовании структур. Если для контроля логического устройства выбирается классический код Бергера ($S(m,k)$-код), то анализ возникающих ошибок не потребуется, поскольку любая симметричная ошибка ими обнаружена не будет [43]. В этом случае используют следующий алгоритм преобразования структур логических устройств в контролепригодные структуры [36, 37].

Алгоритм 1. Реконфигурация элементов и связей в схеме объекта диагностирования:

1. Определяется множество W таких элементов, которые допускают возникновение симметричных искажений на выходах (так называемых *немонотонных элементов*).

2. Для каждого элемента из множества W проводится анализ путей в схеме логического устройства, ведущих к выходам схемы: если на пути к выходу от немонотонного логического элемента встречается какой-либо логический элемент, то он также включается во множество W.

3. Каждый элемент $G_i \in W$ заменяется двумя своими копиями G_i^0 и G_i^1.

4. В полученной структуре реконфигурируются соединения входов и выходов элементов по следующим правилам:

– если в исходной схеме логического устройства выход элемента G_i соединен со входом элемента G_j и соединение содержит четное число инверсий (при этом учитываются инверсии выхода элемента G_i и входа элемента G_j), то в преобразованной схеме соединяются элементы G_i и G_j с одинаковыми верхними индексами, в противном случае — с разными верхними индексами;

– если элемент G_i не был дублирован (не входил во множество W), то его выход соединяется с обеими копиями элемента G_j;

– если выходной элемент G_i на своем выходе имеет инверсию, то соответствующий выход схемы соединяется с элементом G_i^1, в противном случае — с G_i^0;

– все несвязанные с выходами схемы элементы удаляются.

Приведенный алгоритм для изображенной на рисунке 1 схемы дает результат преобразования, представленного на рисунке 4. Два логических элемента внутренней структуры логического устройства потребовалось резервировать.

При использовании двухмодульного кода для контроля заданного логического устройства целесообразно проанализировать те входные наборы, на которых вызываются симметричные ошибки и классифицировать их на обнаруживаемые и не обнаруживаемые кодом. Это

позволит установить необходимость резервирования каких-либо элементов. Другими словами, множество немонотонных элементов можно уменьшить за счет установления свойства схемы, связанного с тем, что на определенных входных наборах симметричная ошибка может оказаться обнаруженной двухмодульным кодом.

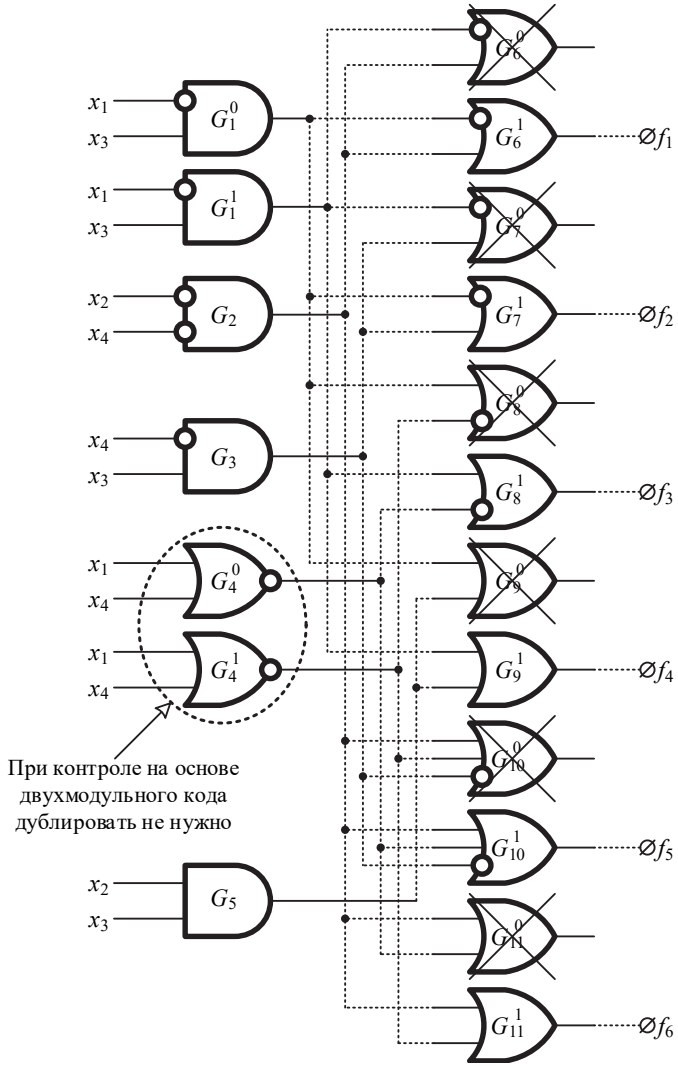


Рис. 4. Комбинационное логическое устройство с контролепригодной по коду Бергера структурой

Определение 3. Назовем группу выходов функционально симметрично независимой группой выходов при контроле кодом с суммированием (СН-группой), если ошибка, вызываемая неисправностью каждого логического элемента, связанного путями с этими выходами, идентифицируется заданным кодом с суммированием.

Для того чтобы установить, является ли группа выходов СН-группой, необходимо проанализировать «поведение» логического устройства при возникновении неисправностей при подаче на входы тех комбинаций, которые создают условия формирования симметричных ошибок на выходах устройства. Решим эту задачу, внеся данные в таблицу 2.

Из таблицы 2 следует, что группы выходов $\{f_3; f_6\}$, $\{f_1; f_4\}$, $\{f_2; f_4\}$ являются СН-группами, а группы выходов $\{f_1; f_3\}$, $\{f_2; f_3\}$ и $\{f_1; f_2; f_3; f_4\}$ таковыми не являются. Отметим, что группа из четырех выходов СН-группой не является в силу того, что в нее полностью входят группы $\{f_1; f_3\}$ и $\{f_2; f_3\}$. Таким образом, при контроле схемы на основе двухмодульного кода элемент G_4 дублировать не требуется.

Отметим также, что для контроля схемы можно использовать и любой другой код, имеющий уменьшенное число симметричных необнаруживаемых ошибок. Например, к такому коду относится описанный в [49] модифицированный $RS(6,3)$-код, для которого поправочный коэффициент вычислен по формуле $\alpha = f_3 \oplus f_4$. В классе необнаруживаемых у такого кода присутствует 224 двукратных симметричных ошибки, 56 четырехкратных монотонных и 168 симметричных ошибок и 20 шестикратных симметричных и 12 асимметричных ошибок. За счет дополнительной проверки $\alpha = f_3 \oplus f_4$ будет обеспечено обнаружение любых симметричных ошибок в парах $\{f_3; f_6\}$, $\{f_1; f_4\}$, $\{f_2; f_4\}$, $\{f_1; f_3\}$, $\{f_2; f_3\}$. Однако четырехкратная симметричная ошибка обнаружена не будет. Это потребует дублирования элемента G_1, неисправности которого вызывают данную ошибку на входном наборе <0100>.

Кроме приведенных кодов для контроля рассматриваемого логического устройства подходит взвешенный $WS(6,4)$-код с последовательностью весовых коэффициентов $[w_6 \div w_1]=[112211]$ [50]. Данный код обнаруживает любые монотонные ошибки и не обнаруживает 224 двукратные симметричные, 120 четырехкратных симметричных, 12 шестикратных симметричных и 2 асимметричные ошибки. Взвешивание разрядов f_3 и f_4 обеспечит обнаружение симметричных ошибок во всех группах ФСЗ-выходов за счет разделения взвешиваемых выходов при контроле. В таблице 3 приводятся параметры об-

наружения монотонных и симметричных ошибок основными $UED(m,k)$ и d_v-$UED(m,k)$ кодами.

Таблица 2. Поиск СН-групп выходов

Элементы	Вид неисправности	Группа выходов	Комбинации	Формируемое кодовое слово без неисправности		Формируемое кодовое слово с неисправностью		Тип ошибки
				Информационный вектор	Контрольный вектор	Информационный вектор	Контрольный вектор	
G_4	Кон. 0	$\{f_3; f_6\}$	0100	110011	1010	111000	1100	Обн.
G_1	Кон. 1	$\{f_1; f_3\}$	0100	110011	1010	011011	1010	Необн.
	Кон. 0		0110	001100	0101	100100	0101	Необн.
G_1	Кон. 1	$\{f_1; f_4\}$	0001	111010	1101	011110	1010	Обн.
	Кон. 1		0100	110011	1010	010111	0111	Обн.
	Кон. 1		0101	111010	1101	011110	1010	Обн.
	Кон. 1		1001	111010	1101	011110	1010	Обн.
	Кон. 1		1011	111010	1101	011110	1010	Обн.
	Кон. 1		1100	111010	1101	011110	1010	Обн.
	Кон. 1		1101	111010	1101	011110	1010	Обн.
G_1	Кон. 1	$\{f_2; f_3\}$	0000	110011	1010	101011	1010	Необн.
	Кон. 1		0100	110011	1010	101011	1010	Необн.
G_1	Кон. 1	$\{f_2; f_4\}$	0000	110011	1010	100111	0111	Обн.
	Кон. 1		0001	111010	1101	101110	1010	Обн.
	Кон. 0		0011	001110	0110	011010	1001	Обн.
	Кон. 1		0100	110011	1010	100111	0111	Обн.
	Кон. 1		0101	111010	1101	101110	1010	Обн.
	Кон. 1		1000	111010	1101	101110	1010	Обн.
	Кон. 1		1001	111010	1101	101110	1010	Обн.
	Кон. 1		1011	111010	1101	101110	1010	Обн.
	Кон. 1		1100	111010	1101	101110	1010	Обн.
	Кон. 1		1101	111010	1101	101110	1010	Обн.
G_1	Кон. 1	$\{f_1; f_2; f_3; f_4\}$	0100	110011	1010	001111	0111	Обн.

Таблица 3. Параметры основных $UED(m,k)$ и d_0-$UED(m,k)$ кодов при m=8÷15

Код	M	k	Параметры обнаружения монотонных ошибок	Доля необнаруживаемых симметричных ошибок от общего числа симметричных ошибок кратностью d			
				2	4	6	8
$S(m,k)$	2^{k*}	$k*$	$UED(m,k)$-код $\forall m$	100%	100%	100%	100%
$S8(m,k)$	8	3	8-$UED(m,k)$-код $\forall m$	100%	100%	100%	100%
$S4(m,k)$	4	2	4-$UED(m,k)$-код $\forall m$	100%	100%	100%	100%
$RS(m,k)$	2^{k*-1}	$k*$	M-$UED(m,k)$-код $\forall m$	42,875% – 46,667%	20,769% – 54,286%	42,857% – 49,65%	50,272% – 100%
$RS4(m,k)$	4	3	4-$UED(m,k)$-код $\forall m$	42,857% – 46,667%	50,769% – 54,286%	42,857% – 49,65%	50,272% – 100%
$TM(m,k)$	4	4	$UED(m,k)$-код при m=6, 4-$UED(m,k)$-код $\forall m$	42,875% – 46,667%	36,508% – 37,143%	25,714% – 30,07%	27,646% – 30,159%
$WS(m,k,w)$	2^{k*}	$k*$	$UED(m,k)$-код $\forall m$	42,857% – 46,667%	50,769% –54,286%	42,857% – 49,65%	50,272% – 100%

Примечание. $k* = \lceil \log_2(m+1) \rceil$.

7. Алгоритм синтеза самопроверяемого комбинационного устройства. Аккумулируя приведенные выше сведения, приведем алгоритм синтеза системы встроенного контроля для логических устройств с учетом особенностей их топологии и свойств кодов с суммированием.

Алгоритм 2. Синтез самопроверяемого комбинационного устройства:

1. На основании анализа топологии логического устройства определяются ССЗ-группы выходов.

2. Путем функционального анализа ССЗ-групп выходов выделяются ФСЗ-группы выходов.

3. Выбирается код с суммированием, свойства которого позволяют решать задачу обнаружения максимального числа симметричных

ошибок с минимальным резервированием элементов в структуре логического устройства при минимальной избыточности кода.

4. Выполняется процедура преобразования структуры исходного логического устройства в устройство с контролепригодной по выбранному коду структурой с учетом уменьшения множества W немонотонных элементов (см. алгоритм 1).

Оценим сложность алгоритма 2.

Сам алгоритм включает в себя четыре подчиненных алгоритма. Первый подалгоритм подразумевает анализ связей внутренних логических элементов исходного логического устройства с его выходами. Сложность данного подалгоритма напрямую связана с числом внутренних логических элементов без элементов первого каскада (N_G) и числом выходов самого устройства (m). Количество операций первого подалгоритма определяется произведением mN_G. После выполнения операций первого подалгоритма в качестве выходных данных будет перечень ССЗ-групп выходов и логических элементов, наличие связей с которыми обуславливает такую зависимость. Максимальное количество вызывающих структурно симметричную зависимость определяется величиной N_G (все логические элементы), а количество выходов в каждой ССЗ-группе будет находиться в диапазоне от 2 до m.

Дальнейший функциональный анализ во втором подалгоритме будет связан с проверкой условия (6), где требуется вычислять булевы производные функций выходов схемы по функциям, реализуемым на выходах рассматриваемых логических элементов. Для каждого логического элемента потребуется выполнить максимум $\sum_{d=2}^{d_{\max}} C_m^d$ (d — четное) процедур вычисления. Общее количество операций — максимум $N_G \sum_{d=2}^{d_{\max}} C_m^d$.

Третий подалгоритм осуществляет процедуру выбора кода с учетом обнаружения симметричных ошибок на выходах. Требуется сформировать список входных комбинаций, на которых вызываются симметричные ошибки выходов устройства, а затем осуществить поиск кода с учетом наилучших характеристик обнаружения симметричных ошибок (аналог таблицы 2). Максимальное количество строк такого списка определяется числом входных комбинаций, на которых вызывается симметричная ошибка для каждого логического элемента, формирующего ФСЗ-группу выходов. Число входных комбинаций может быть различным для всех логических элементов. Максимум процедур перебора для

каждого логического элемента — 2^t (t — число входов устройства). Таким образом, для каждого кода $2^t N_G$ операций вычислений.

Четвертый подалгоритм связан с выполнением процедур поиска немонотонных элементов и их резервированием по алгоритму 1. Здесь основная процедура — для каждого логического элемента проверка путей, ведущих к выходам и соединение выходов. Максимальное число проверок mN_G.

Сложность конечного алгоритма определяется функцией нескольких переменных:

$$g = 2mN_G + N_G \sum_{d=2}^{d_{\max}} C_m^d + 2^t N_G, \qquad (7)$$

где t — число входов устройства; m — число выходов устройства; N_G — число логических элементов.

Асимптотическая оценка трудоемкости алгоритма определяется по выражению:

$$Q = O\left(2mN_G + N_G \sum_{d=2}^{d_{\max}} C_m^d + 2^t N_G\right).$$

От числа логических элементов в структуре логического устройства сложность реализации алгоритма зависит линейно; от числа входов логического устройства зависимость является степенной (экспоненциальной) и от количества выходов устройства — факториальной. Другим словами, алгоритм наиболее эффективен для комбинационных устройств с небольшим (до 20-30) числом входов и выходов. При большем их числе потребуется декомпозиция устройства и отдельный контроль подсхем.

Вопрос выбора кода для контроля логического устройства может решаться двумя путями: последовательным перебором кодов из имеющегося множества, либо обоснованным анализом возможностей контроля в разных разрядах контрольного вектора значений рабочих функций объекта диагностирования в ФСЗ-группах.

8. Заключение. Сформулированные в представленной статье условия поиска структурно и функционально зависимых выходов позволяют на практике устанавливать множество тех логических элементов структур комбинационных логических устройств, неисправности которых будут вызывать симметричные ошибки на выхо-

дах самого объекта диагностирования. При этом установлена наиболее удобная последовательность анализа топологии объекта диагностирования (сокращается число вычислительных процедур), заключающаяся в том, что сначала находятся структурно симметрично зависимые группы выходов, а затем среди найденных групп с использованием приведенных в статье условий находятся группы функционально зависимых выходов. Финальным этапом (что и является принципиально новым по отношению к известным исследованиям), непосредственно определяющим множество резервируемых элементов, следует проверка для групп функционально зависимых выходов и конкретных элементов, вызывающих симметричные ошибки на выходах устройства, обнаруживается или нет конкретная ошибка на конкретном входном наборе выбранным (m,k)-кодом. За счет особенностей обнаружения ошибок в информационных векторах кодов удается уменьшить число резервируемых элементов по отношению к тому, как это сделано для классических кодов Бергера в известном алгоритме [36, 37].

Представленный подход к синтезу самопропроверяемых комбинационных устройств универсален и не ориентирован на конкретную элементную базу, он затрагивает только функциональное описание логических устройств и может быть легко адаптирован на использование любой элементной базы.

Литература

1. *Сапожников В.В., Сапожников Вл.В., Христов Х.А., Гавзов Д.В.* Методы построения безопасных микроэлектронных систем железнодорожной автоматики / под ред. Вл.В. Сапожникова // М.: Транспорт. 1995. 272 с.
2. *Ubar R., Raik J., Vierhaus H.-T.* Design and Test Technology for Dependable Systems-on-Chip (Premier Reference Source) // New York: IGI Global. 2011. 578 p.
3. *Drozd A. et al.* The use of natural resources for increasing a checkability of the digital components in safety-critical systems // Proceedings of 11th IEEE East-West Design & Test Symposium (EWDTS`2013). 2013. pp. 1–6.
4. *Kharchenko V., Kondratenko Yu., Kacprzyk J.* Green IT Engineering: Concepts, Models, Complex Systems Architectures // Springer Book series "Studies in Systems, Decision and Control". 2017. vol. 74. 305 p.
5. *Sklyar V., Kharchenko V., Bardis N.G.* Assurance case for green IT applications: proof of compliance with power consumption claims // Proceedings of 4th International Conference on Mathematics and Computers in Sciences and in Industry (MCSI). 2017. pp. 124–127.
6. *Аксёнова Г.П.* Локализация кратных неисправностей при групповом контроле в дискретном устройстве // Автоматика и телемеханика. 2017. № 12. С. 118–130.
7. *Drozd O., Nikul V., Antoniuk V., Drozd M.* Hidden faults in FPGA-built digital components of safety-related systems // Proceedings of 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET). 2018 pp. 805–809.

8. *Shah T., Matrosova A., Singh V.* Test pattern generation to detect multiple faults in ROBDD based combinational circuits // Proceedings of IEEE 23rd International Symposium on On-Line Testing and Robust System Design (IOLTS). 2017. pp. 211–2012.
9. *Mosin S.* Automated simulation of faults in analog circuits based on parallel paradigm // Proceedings of 15th IEEE East-West Design & Test Symposium (EWDTS`2017). 2017. pp. 73–78.
10. *Аксёнова Г.П.* Матричный способ локализации неисправностей в ПЛИС // Автоматика и телемеханика. 2013. № 9. С. 119–124.
11. *Dautov R., Mosin S.* A Technique to aggregate classes of analog fault diagnostic data based on association rule mining // Proceedings of 19th International Symposium on Quality Electronic Design (ISQED). 2018. pp. 238–243.
12. *Бибило П.Н. и др.* Автоматизация логического синтеза КМОП схем с пониженным энергопотреблением // Программная инженерия. 2013. № 8. С. 35–41.
13. *Черемисинова Л.Д.* Логический синтез комбинационных КМОП схем с учетом рассеивания мощности // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. 2014. № 3. С. 89–98.
14. *Поттосин Ю.В.* Энергосберегающее противогоночное кодирование состояний асинхронного автомата // Прикладная дискретная математика. Приложение. 2015. № 8. С. 120–123.
15. *Степченков Ю.А., Каменских А.Н., Тюрин С.Ф., Рождественский Ю.В.* Модели отказоустойчивых самосинхронных схем // Системы и средства информатики. 2016. Том 26. № 4. С. 19–30.
16. *Согомонян Е.С., Слабаков Е.В.* Самопроверяемые устройства и отказоустойчивые системы // М.: Радио и связь. 1989. 208 с.
17. *Nicolaidis M., Zorian Y.* On-Line Testing for VLSI – A Compendium of Approaches // Journal of Electronic Testing: Theory and Applications. 1998. vol. 12. pp. 7–20.
18. *Матросова А.Ю., Останин С.А., Паршина Н.А.* К синтезу контролепригодных комбинационных устройств // Автоматика и телемеханика. 1999. № 2. С. 129–137.
19. *Nicolaidis M.* On-Line Testing for VLSI: State of the Art and Trends // Integration, the VLSI Journal. 1998. vol. 26. Issue 1-2. pp. 197–209.
20. *Matrosova A.Yu., Levin I., Ostanin S.A.* Self-Checking Synchronous FSM Network Design with Low Overhead // VLSI Design. 2000. vol. 11. Issue 1. pp. 47–58.
21. *Mitra S., McCluskey E.J.* Which concurrent error detection scheme to choose? // Proceedings of International Test Conference. 2000. pp. 985–994.
22. *Kubalík P., Kubátová H.* Parity Codes Used for On-Line Testing in FPGA // Acta Polytechnika. 2005. vol. 45. no. 6. pp. 53–59.
23. *Butorina N.* Self-testing checker design for incomplete m-out-of-n codes // Proceedings of 12th IEEE East-West Design & Test Symposium (EWDTS`2014). 2014. pp. 258–261.
24. *Сапожников В.В., Сапожников Вл.В.* Самопроверяемые дискретные устройства // СПб: Энергоатомиздат. 1992. 224 с.
25. *Piestrak S.J.* Design of Self-Testing Checkers for Unidirectional Error Detecting Codes // Wrocław: Oficyna Wydawnicza Politechniki Wrocławskiej. 1995. 111 p.
26. *Das D., Touba N.A.* Synthesis of Circuits with Low-Cost Concurrent Error Detection Based on Bose-Lin Codes // Journal of Electronic Testing: Theory and Applications. 1999. vol. 15. Issue 1-2. pp. 145–155.
27. *Fujiwara E.* Code Design for Dependable Systems: Theory and Practical Applications // New Jersey: John Wiley & Sons. 2006. 720 p.
28. *Borecký J., Kohlík M., Kubátová H.* Parity Driven Reconfigurable Duplex System // Microprocessors and Microsystems. 2017. vol. 52. pp. 251–260.

29. *Бибило П.Н., Романов В.И.* Логическое проектирование дискретных устройств с использованием продукционно-фреймовой модели представления знаний // Минск: Беларус. навука. 2011. 279 с.
30. *Sogomonyan E.S., Gössel M.* Design of Self-Testing and On-Line Fault Detection Combinational Circuits with Weakly Independent Outputs // Journal of Electronic Testing: Theory and Applications. 1993. vol. 4. Issue 4. pp. 267–281.
31. *Гессель М., Морозов А.А., Сапожников В.В., Сапожников Вл.В.* Исследование комбинационных самопроверяемых устройств с независимыми и монотонно независимыми выходами // Автоматика и телемеханика. 1997. № 2. С. 180–193.
32. *Göessel M., Ocheretny V., Sogomonyan E., Marienfeld D.* New Methods of Concurrent Checking: Edition 1 // Springer Netherlands. 2008. 184 p.
33. *Berger J.M.* A Note on Error Detecting Codes for Asymmetric Channels // Information and Control. 1961. vol. 4. Issue 1. pp. 68–73.
34. *Freiman C.V.* Optimal Error Detection Codes for Completely Asymmetric Binary Channels // Information and Control. 1962. vol. 5. Issue 1. pp. 64–71.
35. *Busaba F.Y., Lala P.K.* Self-Checking Combinational Circuit Design for Single and Unidirectional Multibit Errors // Journal of Electronic Testing: Theory and Applications, 1994. vol. 5. Issue 1. pp. 19–28.
36. *Saposhnikov V.V., Morosov A., Saposhnikov Vl.V., Göessel M.* A New Design Method for Self-Checking Unidirectional Combinational Circuits // Journal of Electronic Testing: Theory and Applications. 1998. vol. 12. Issue 1-2. pp. 41–53.
37. *Morosow A., Sapozhnikov V.V., Sapozhnikov Vl.V., Goessel M.* Self-Checking Combinational Circuits with Unidirectionally Independent Outputs // VLSI Design. 1998. vol. 5. Issue 4. pp. 333–345.
38. *Матросова А.Ю., Останин С.А., Сингх В.* Обнаружение несущественных путей логических схем на основе совместного анализа И-ИЛИ деревьев и SSBDD-графов // Автоматика и телемеханика. 2013. № 7. С. 126–142.
39. *Ostanin S.* Self-checking synchronous FSM network design for path delay faults // Proceedings of 15th IEEE East-West Design & Test Symposium (EWDTS`2017). 2017. pp. 696–699.
40. *Matrosova A., Andreeva V., Tomkov V.* Fully delay and multiple stuck-at faults testable FSM design // Proceedings of 13th IEEE East-West Design & Test Symposium (EWDTS`2015). 2015. pp. 212–215.
41. *Сапожников В.В., Сапожников Вл.В., Ефанов Д.В.* Классификация ошибок в информационных векторах систематических кодов // Известия вузов. Приборостроение. 2015. Том 58. № 5. С. 333–343.
42. *Efanov D., Sapozhnikov V., Sapozhnikov Vl.* Generalized algorithm of building summation codes for the tasks of technical diagnostics of discrete systems // Proceedings of 15th IEEE East-West Design & Test Symposium (EWDTS`2017). 2017. pp. 365–371.
43. *Ефанов Д.В., Сапожников В.В., Сапожников Вл.В.* Условия обнаружения неисправности логического элемента в комбинационном устройстве при функциональном контроле на основе кода Бергера // Автоматика и телемеханика. 2017. № 5. С. 152–165.
44. *Das D., Touba N.A.* Weight-based codes and their application to concurrent error detection of multilevel circuits // Proceedings of 17th IEEE Test Symposium. 1999. pp. 370–376.
45. *Das D., Touba N.A., Seuring M., Goessel M.* Low cost concurrent error detection based on modulo weight-based codes // Proceedings of IEEE 6th International On-Line Testing Workshop (IOLTW). 2000. pp. 171–176.

46. *Сапожников В.В., Сапожников Вл.В., Ефанов Д.В.* Коды с суммированием, обнаруживающие любые симметричные ошибки // Электронное моделирование. 2017. Том 39. № 3. С. 47–60.
47. *Efanov D.V., Sapozhnikov V.V., Sapozhnikov Vl.V.* Two-Modulus Codes with Summation of One-Data Bits for Technical Diagnostics of Discrete Systems // Automatic Control and Computer Sciences. 2018. vol. 52. Issue 1. pp. 1–12.
48. *Efanov D., Sapozhnikov V., Sapozhnikov Vl.* Generic two-modulus sum codes for technical diagnostics of discrete systems problems // Proceedings of 14th IEEE East-West Design & Test Symposium (EWDTS`2016). 2016. pp. 256–260.
49. *Блюдов А.А., Ефанов Д.В., Сапожников В.В., Сапожников Вл.В.* О кодах с суммированием единичных разрядов в системах функционального контроля // Автоматика и телемеханика. 2014. № 8. С. 131–145.
50. *Сапожников В.В., Сапожников Вл.В., Ефанов Д.В.* Взвешенные коды с суммированием для организации контроля логических устройств // Электронное моделирование. 2014. Том 36. № 1. С. 59–80.

Ефанов Дмитрий Викторович — д-р техн. наук, доцент, профессор кафедры автоматики, телемеханики и связи на железнодорожном транспорте, Российский университет транспорта (МИИТ), руководитель направления систем мониторинга и диагностики, ООО «ЛокоТех-Сигнал». Область научных интересов: дискретная математика, надежность и техническая диагностика дискретных систем. Число научных публикаций — 300. TrES-4b@yandex.ru; ул. Образцова, 9, Москва, 127994; р.т.: +7(911)709-2164.

DOI 10.15622/sp.59.3

D.V. EFANOV

THE SYNTHESIS OF SELF-CHECKING COMBINATIONAL DEVICES ON THE BASIS OF CODES WITH THE EFFECTIVE SYMMETRICAL ERROR DETECTION

Efanov D.V. **The Synthesis of Self-Checking Combinational Devices on the Basis of Codes with the Effective Symmetrical Error Detection.**

Abstract. The methods of fault-tolerant coding are often used in the designing of reliable and safety components of automatic control systems: both in the data transmission between system nodes, and at the level of hardware and software architecture.

The redundant coding is widely used in the management of combinational logic devices control. In this case, codes, which are oriented to the error detection rather than correction of this, are in use. Such features of codes make it possible to implement the checkable automation systems with acceptable redundancy, which does not exceed the redundancy in the situation of duplication using.

The paper highlights the method of the synthesis of self-checking combinational devices, which makes it possible to take into account the features of the source devices architecture, as well as the properties of error detection by redundant codes in solving the problem of the synthesis of technical means for diagnosis. The paper gives the basic information on the theory of the checkable digital systems synthesis on the basis of redundant codes with summation.

The basic stages of the analysis of the diagnosis objects topologies are determined with the selection of groups of outputs — groups of structurally and functionally symmetrically independent devices outputs. The formulas are given to determine the presence or the absence of a symmetrical dependence of the diagnosis object outputs. The example illustrating the calculation process is given. The main stages of the analysis of the redundant codes application in the error detection on the functionally symmetric dependent outputs are formulated. The algorithm of the synthesis of the self-checking combinational devices with taking into account the object of diagnosis structure features and the redundant codes properties is proposed.

Keywords: logic devices in automation, checkable structure, technical diagnostics, diagnosis, technical condition monitoring, uniform block code, Berger code, sum codes, error detection.

Efanov Dmitry Viktorovich — Ph.D., Dr. Sci., associate professor, professor of automation, remote control and communication on railway transport department, Russian University of Transport, head of monitoring and diagnostic systems direction, «LocoTech-Signal» LCC. Research interests: discrete mathematics, reliability and technical diagnostics of discrete devices. The number of publications — 300. TrES-4b@yandex.ru; 9, Obraztsova str., Moscow, 127994, Russia; office phone: +7(911)709-2164.

References

1. Sapozhnikov V.V., Sapozhnikov Vl.V., Hristov H.A., Gavzov D.V. *Metody postroeniya bezopasnyh mikroehlektronnyh sistem zheleznodorozhnoj avtomatiki. Pod red. Vl.V. Sapozhnikova* [Methods for constructing safe microelectronic systems for railway automation. Edited by Vl.V. Sapozhnikov]. M.: Transport. 1995. 272 p. (In Russ.).
2. Ubar R., Raik J., Vierhaus H.-T. Design and Test Technology for Dependable Systems-on-Chip (Premier Reference Source). New York: IGI Global. 2011. 578 p.
3. Drozd A., Kharchenko V., Antoshchuk S., Drozd J., Lobachev M., Sulima J. The use of natural resources for increasing a checkability of the digital components in safety-

critical systems. Proceedings of 11th IEEE East-West Design & Test Symposium (EWDTS`2013). 2013. pp. 1–6.
4. Kharchenko V., Kondratenko Yu., Kacprzyk J. Green IT Engineering: Concepts, Models, Complex Systems Architectures. Springer Book series "Studies in Systems, Decision and Control". 2017. vol. 74. 305 p.
5. Sklyar V., Kharchenko V., Bardis N.G. Assurance case for green IT applications: proof of compliance with power consumption claims. Proceedings of 4th International Conference on Mathematics and Computers in Sciences and in Industry (MCSI). 2017. pp. 124–127.
6. Aksyonova G.P. [Localization of multiple faults with group control on a discrete device]. *Avtomatika i telemekhanika – Automation and remote control*. 2017. vol. 12. pp. 118–130. (In Russ.).
7. Drozd O., Nikul V., Antoniuk V., Drozd M. Hidden faults in FPGA-built digital components of safety-related systems. Proceedings of 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET). 2018 pp. 805–809.
8. Shah T., Matrosova A., Singh V. Test pattern generation to detect multiple faults in ROBDD based combinational circuits. Proceedings of IEEE 23rd International Symposium on On-Line Testing and Robust System Design (IOLTS). 2017. pp. 211–2012.
9. Mosin S. Automated simulation of faults in analog circuits based on parallel paradigm. Proceedings of 15th IEEE East-West Design & Test Symposium (EWDTS`2017). 2017. pp. 73–78.
10. Aksyonova G.P. [A matrix method for PLD failure localization]. *Avtomatika i telemekhanika – Automation and remote control*. 2013. vol. 9. pp. 119–124. (In Russ.).
11. Dautov R., Mosin S. A Technique to aggregate classes of analog fault diagnostic data based on association rule mining. Proceedings of 19th International Symposium on Quality Electronic Design (ISQED). 2018. pp. 238–243.
12. Bibilo P.N. et al. [Low-power logical synthesis of CMOS circuits automation]. *Programmnaja inzhenerija – Software Engineering*. 2013. vol. 8. pp. 35–41. (In Russ.).
13. Cheremisinova L.D. [Lower-power logic synthesis of combinational CMOS circuits]. *Vestnik Tomskogo gosudarstvennogo universiteta. Upravlenie, vychislitel'naya tekhnika i informatika – Tomsk state university journal of control and computer science*. 2014. vol. 3. pp. 89–98. (In Russ.).
14. Pottosin Yu.V. [Low power race-free state assignment of an asynchronous automaton]. *Prikladnaya diskretnaya matematika. Prilozhenie – Applied Discrete Mathematics. Supplement*. 2015. vol. 8. pp. 120–123. (In Russ.).
15. Stepchenkov Yu.A., Kamenskih A.N., Tyurin S.F., Rozhdestvenskij Yu.V. [Models of fault-tolerant self-timed circuits]. *Sistemy i sredstva informatiki – Systems and means of informatics.* 2016. Issue 26. vol. 4. pp. 19–30. (In Russ.).
16. Sogomonyan E.S., Slabakov E.V. *Samoproveryaemyie ustroystva i otkazoustoychivyie sistemy* [Self-Checking and Fail-Safety Systems]. M.: Radio and Communication. 1989. 207 p. (In Russ.).
17. Nicolaidis M., Zorian Y. On-Line Testing for VLSI – A Compendium of Approaches. *Journal of Electronic Testing: Theory and Applications*. 1998. vol. 12. pp. 7–20.
18. Matrosova A.Yu., Ostanin S.A., Parshina N.A. [Synthesizing testable combinational circuits]. *Avtomatika i telemekhanika – Automation and remote control.* 1999. vol. 2. pp. 129–137. (In Russ.).
19. Nicolaidis M. On-Line Testing for VLSI: State of the Art and Trends. *Integration, the VLSI Journal*. 1998. vol. 26. Issues 1-2. pp. 197–209.

20. Matrosova A.Yu., Levin I., Ostanin S.A. Self-Checking Synchronous FSM Network Design with Low Overhead. *VLSI Design*. 2000. vol. 11. Issue 1. pp. 47–58.
21. Mitra S., McCluskey E.J. Which concurrent error detection scheme to choose? Proceedings of International Test Conference. 2000. pp. 985–994.
22. Kubalík P., Kubátová H. Parity Codes Used for On-Line Testing in FPGA. *Acta Polytechnika*. 2005. vol. 45. no. 6. pp. 53–59.
23. Butorina N. Self-testing checker design for incomplete m-out-of-n codes. Proceedings of 12th IEEE East-West Design & Test Symposium (EWDTS`2014). 2014. pp. 258–261.
24. Sapozhnikov V.V., Sapozhnikov Vl.V. *Samoproveryaemye diskretnye ustrojstva* [Self-checking discrete devices]. St. Petersburg: Energoatomizdat. 1992. 224 p. (In Russ.).
25. Piestrak S.J. Design of self-testing checkers for unidirectional error detecting codes. Wrocław: Oficyna Wydawnicza Politechniki Wrocławskiej, 1995. 111 p.
26. Das D., Touba N.A. Synthesis of Circuits with Low-Cost Concurrent Error Detection Based on Bose-Lin Codes. *Journal of Electronic Testing: Theory and Applications*. 1999. vol. 15. Issue 1-2. pp. 145–155.
27. Fujiwara E. Code Design for Dependable Systems: Theory and Practical Applications. New Jersey: John Wiley & Sons. 2006. 720 p.
28. Borecký J., Kohlík M., Kubátová H. Parity Driven Reconfigurable Duplex System. *Microprocessors and Microsystems*. 2017. vol. 52. pp. 251–260.
29. Bibilo P.N., Romanov V.I. *Logicheskoe proektirovanie diskretnyh ustrojstv s ispol'zovaniem produkcionno-frejmovoj modeli predstavleniya znanij* [Logical design of discrete devices using the product-frame model of knowledge representation]. Minsk: Belarus. navuka. 2011. 279 p. (In Russ.).
30. Sogomonyan E.S., Gössel M. Design of Self-Testing and On-Line Fault Detection Combinational Circuits with Weakly Independent Outputs. *Journal of Electronic Testing: Theory and Applications*. 1993. vol. 4. Issue 4. pp. 267–281.
31. Gessel' M., Morozov A.A., Sapozhnikov V.V., Sapozhnikov Vl.V. [Investigation of combination self-testing devices having independent and monotone independent outputs]. *Avtomatika i telemekhanika – Automation and remote control*. 1997. vol. 2. pp. 180-193. (In Russ.).
32. Göessel M., Ocheretny V., Sogomonyan E., Marienfeld D. New Methods of Concurrent Checking: Edition 1. Springer Netherlands. 2008. 184 p.
33. Berger J.M. A Note on Error Detecting Codes for Asymmetric Channels. *Information and Control*. 1961. vol. 4. Issue 1. pp. 68–73.
34. Freiman C.V. Optimal Error Detection Codes for Completely Asymmetric Binary Channels. *Information and Control*. 1962. vol. 5. Issue 1. pp. 64–71.
35. Busaba F.Y., Lala P.K. Self-Checking Combinational Circuit Design for Single and Unidirectional Multibit Errors. *Journal of Electronic Testing: Theory and Applications*. 1994. vol. 5. Issue 1. pp. 19–28.
36. Saposhnikov V.V., Morosov A., Saposhnikov Vl.V., Göessel M. A New Design Method for Self-Checking Unidirectional Combinational Circuits. *Journal of Electronic Testing: Theory and Applications*. 1998. vol. 12. Issue 1-2. pp. 41–53.
37. Morosow A., Sapozhnikov V.V., Sapozhnikov Vl.V., Goessel M. Self-Checking Combinational Circuits with Unidirectionally Independent Outputs. *VLSI Design*. 1998. vol. 5. Issue 4. pp. 333–345.
38. Matrosova A.Yu., Ostanin S.A., Singh V. [Detection of false paths in logical circuits by joint analysis of the AND/OR trees and SSBDD-graphs]. *Avtomatika i telemekhanika – Automation and remote control*. 2013. vol. 7. pp. 126–142. (In Russ.).

39. Ostanin S. Self-checking synchronous FSM network design for path delay faults. Proceedings of 15th IEEE East-West Design & Test Symposium (EWDTS`2017). 2017. pp. 696–699.
40. Matrosova A., Andreeva V., Tomkov V. Fully delay and multiple stuck-at faults testable FSM design. Proceedings of 13th IEEE East-West Design & Test Symposium (EWDTS`2015). 2015. pp. 212–215.
41. Sapozhnikov V.V., Sapozhnikov Vl.V., Efanov D.V. [Errors classification in information vectors of systematic codes]. *Izvestiya vysshih uchebnyh zavedenij. Priborostroenie – Journal of Instrument Engineering.* 2015. Issue 58. vol. 5. pp. 333–343. (In Russ.).
42. Efanov D., Sapozhnikov V., Sapozhnikov Vl. Generalized algorithm of building summation codes for the tasks of technical diagnostics of discrete systems. Proceedings of 15th IEEE East-West Design & Test Symposium (EWDTS`2017). 2017. pp. 365–371.
43. Efanov D.V., Sapozhnikov V.V., Sapozhnikov Vl.V. [Conditions for Detecting a Logical Element Fault in a Combination Device under Concurrent Checking Based on Berger`s Code]. *Avtomatika i telemekhanika – Automation and remote control*. 2017. vol. 5. pp. 152–165. (In Russ.).
44. Das D., Touba N.A. Weight-based codes and their application to concurrent error detection of multilevel circuits. Proceedings of 17th IEEE Test Symposium. 1999. pp. 370–376.
45. Das D., Touba N.A., Seuring M., Goessel M. Low cost concurrent error detection based on modulo weight-based codes. Proceedings of IEEE 6th International On-Line Testing Workshop (IOLTW). 2000. pp. 171–176.
46. Sapozhnikov V.V., Sapozhnikov Vl.V., Efanov D.V. [On the class of codes with summation with all symmetric errors detection]. *Elektronnoje Modelirovanije – Electronic modeling.* 2017. Issue 39. vol. 3. pp. 47–60. (In Russ.).
47. Efanov D.V., Sapozhnikov V.V., Sapozhnikov Vl.V. Two-Modulus Codes with Summation of One-Data Bits for Technical Diagnostics of Discrete Systems. *Automatic Control and Computer Sciences*. 2018. vol. 52. Issue 1. pp. 1–12.
48. Efanov D., Sapozhnikov V., Sapozhnikov Vl. Generic two-modulus sum codes for technical diagnostics of discrete systems problems. Proceedings of 14th IEEE East-West Design & Test Symposium (EWDTS`2016). 2016. pp. 256–260.
49. Blyudov A.A., Efanov D.V., Sapozhnikov V.V., Sapozhnikov Vl.V. [On Codes with Summation of Unit Bits in Concurrent Error Detection Systems]. *Avtomatika i telemekhanika – Automation and remote control*. 2014. vol. 8. pp. 131–145. (In Russ.).
50. Sapozhnikov V.V., Sapozhnikov Vl.V., Efanov D.V. [Weight-based sum codes for logical devices checking organization]. *Elektronnoje Modelirovanije – Electronic modeling*. 2014. Issue 36. vol. 1. pp. 59–80. (In Russ.).

УДК 004.728.3 **DOI** 10.15622/sp.59.4

М.А. Перегудов, А.С. Стешковой, А.А. Бойко

ВЕРОЯТНОСТНАЯ МОДЕЛЬ ПРОЦЕДУРЫ СЛУЧАЙНОГО МНОЖЕСТВЕННОГО ДОСТУПА К СРЕДЕ ТИПА CSMA/CA

Перегудов М.А., Стешковой А.С., Бойко А.А. **Вероятностная модель процедуры случайного множественного доступа к среде типа CSMA/CA.**

Аннотация. Сегодня вопрос обеспечения безопасности функционирования сетей цифровой радиосвязи в условиях деструктивных воздействий со стороны злоумышленника имеет особое значение. Для предотвращения деструктивных воздействий на физическом уровне OSI применяются методы помехозащиты, а на сетевом и высших уровнях — шифрование. Практика показывает, что наиболее опасные уязвимости для деструктивных воздействий сосредоточены на канальном уровне сетей цифровой радиосвязи в процедурах, отвечающих за случайный множественный доступ абонентов к среде.

И только для процедуры случайного множественного доступа к среде сетей цифровой радиосвязи типа S-ALOHA разработаны математические модели, позволяющие оценивать эффективность ее функционирования в условиях потенциально возможных деструктивных воздействий. Даная процедура применяется в сетях цифровой радиосвязи стандартов GSM, TETRA, DMR, LTE. Однако в Wi-Fi и Bluetooth сетях, используемых в настоящее время в каждом доме, применяется процедура случайного множественного доступа к среде типа CSMA/CA. В работе представлена математическая модель процедуры случайного множественного доступа к среде сетей цифровой радиосвязи типа CSMA/CA. Модель учитывает потенциально возможные деструктивные воздействия со стороны злоумышленника путем уточнения аналитических выражений для вероятностных и временных характеристик в известных моделях, а также за счет использования нового показателя — вероятности занятости канала связи. В Wi-Fi и Bluetooth сетях в случае занятости канала связи по причине коллизии или успешной передачи таймер отсрочки передачи каждого абонентского терминала останавливается. В известных моделях данная особенность сетей цифровой радиосвязи со случайным множественным доступом к среде типа CSMA/CA не учитывается, а в настоящей работе учитывается с использованием вероятности занятости канала связи. Установлено, что при потенциально возможных деструктивных воздействиях эффективность существующих алгоритмов реализации случайного множественного доступа к среде типа CSMA/CA стремится к нулю. Результаты работы применимы в области разработки алгоритмов автоматического восстановления работоспособности сетей цифровой радиосвязи на канальном уровне OSI.

Ключевые слова: сеть цифровой радиосвязи, деструктивное воздействие, процедура случайного множественного доступа к среде, CSMA/CA, цепь Маркова, эффективность функционирования.

1. Введение. Особое значение имеет проблема обеспечения безопасности функционирования сетей цифровой радиосвязи (СЦР) в условиях деструктивных воздействий (ДВ) со стороны злоумышленника. Целью данных воздействий является нарушение конфиденциальности, целостности и доступности информации легитимных устройств СЦР. Для предотвращения данных воздействий на физическом уровне СЦР применяются методы

помехозащиты, а на сетевом и высших уровнях — шифрование. Практика показывает, что наиболее опасные уязвимости для ДВ сосредоточены на канальном уровне СЦР в процедурах, отвечающих за случайный множественный доступ абонентов к среде (СМДС). В качестве деструктивных воздействий со стороны злоумышленника могут выступать создание коллизий в канале передачи данных и ложные соединения от имени абонентских терминалов (АТ) сети. Оценке защищенности СЦР на канальном уровне в условиях ДВ посвящен ряд работ [1-5]. Однако среди этих работ только в работах [1, 2] рассмотрены потенциально возможные ДВ на уровне процедуры СМДС. В них анализируется процедура СМДС типа S-ALOHA, которая используется, например, в стандартах GSM, TETRA, DMR, LTE. Не менее важен вопрос оценки эффективности функционирования сетей цифровой радиосвязи в условиях деструктивных воздействий на уровне процедуры СМДС с контролем несущей и предотвращением коллизий (CSMA/CA), с применением которой функционируют, например, сети радиосвязи стандартов IEEE 802.11 (Wi-Fi), IEEE 802.15.1 (Bluetooth), IEEE 802.15.4 (ZigBee).

В процедуре CSMA/CA известна уязвимость, связанная с возможностью непреднамеренного захвата всего радиоресурса сети одним АТ [6]. Данная уязвимость устранена применением алгоритмов, разграничивающих АТ доступ к радиоресурсу [7-9]. Однако данные алгоритмы не учитывают возможность захвата злоумышленником радиоресурса сети с использованием одновременно нескольких абонентских терминалов, адреса канального уровня которых могут входить или не входить в список легитимных адресов сети. Эта уязвимость вызвана тем, что на уровне процедуры СМДС типа CSMA/CA в СЦР управляющая (служебная) информация не шифруется [10]. Кроме того, актуальной является классическая уязвимость сетей радиосвязи, связанная с постановкой злоумышленником с некоторой вероятностью преднамеренных помех в радиоканале. Практическое противоречие в рассматриваемой предметной области связано с потребностью в обеспечении работоспособности сетей цифровой радиосвязи с процедурой СМДС типа CSMA/CA и отсутствием сведений об опасности деструктивных воздействий в таких сетях, комплексно использующих вышеуказанные уязвимости. Данное обстоятельство порождает научное противоречие, связанное с наличием очевидной потребности и фактическим отсутствием математических моделей процедуры СМДС типа CSMA/CA, способных предоставить возможность оценки того, насколько эффективно может функцио-

нировать сеть в условиях комплекса ДВ, направленных на имитацию работы входящих и не входящих в атакуемую сеть устройств и на формирование преднамеренных помех в радиоканале. Цель данной работы — устранение указанного противоречия путем разработки математической модели для оценки эффективности СМДС типа CSMA/CA в условиях потенциально возможных ДВ.

2. Анализ существующих работ. В настоящее время известен ряд моделей процедуры СМДС типа CSMA/CA [11-23]. Базовой моделью этой процедуры является модель Bianchi [11]. В работах [12, 13] исследован вопрос оценки количества конечных попыток передач информационного пакета для успешного установления соединения, в работе [14] учитываются неидеальные условия канала, в [15] изучена стабильность, пропускная способность и задержки распространения при работе в однородных буферизованных сетях IEEE 802.11. Также был проведен анализ пропускной способности беспроводных сетей CSMA/CA, в которых участники информационного обмена имеют конечную предлагаемую нагрузку [16]. Были предложены алгоритмы оптимизации процедуры CSMA/CA в части минимизации времени ожидания и коллизии [17]. В работах [18-23] рассмотрены проблемы оптимизации процедуры CSMA/CA в части функционирования большого количества абонентов и различных режимов работы сетей цифровой радиосвязи. Однако существующие модели не оценивают влияния потенциально возможных деструктивных воздействий со стороны злоумышленника. Таким образом, разработка математической модели, позволяющей оценивать эффективность СМДС типа CSMA/CA в условиях ДВ, является актуальной задачей.

3. Описательная модель процедуры СМДС типа CSMA/CA. Метод случайного множественного доступа к среде типа CSMA/CA базируется на контроле канала связи на предмет наличия сторонних передач и выборе случайного значения отсрочки передачи. Данная процедура предусматривает два основных алгоритма реализации СМДС типа CSMA/CA: основной (без предварительного резервирования радиоканала) и дополнительный (с предварительным резервированием радиоканала).

Учитывая результаты известных работ [11-13] и потенциально возможные ДВ со стороны злоумышленника, описательную модель процедуры СМДС типа CSMA/CA можно представить в виде функциональной схемы (рисунок 1). Основными элементами сети являются: средство коммутации и управления (СКУ), абонентские терминалы и злоумышленник.

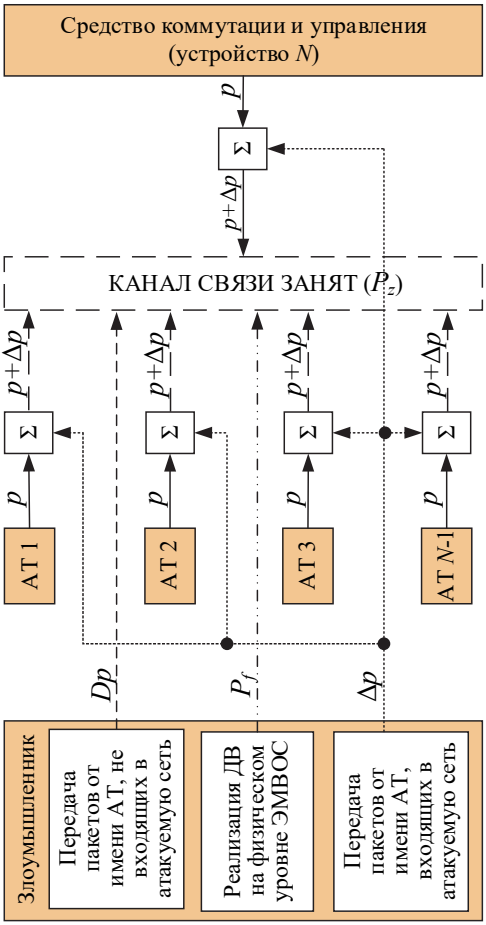


Рис. 1. Функциональная схема процедуры СМДС типа CSMA/CA с учетом ДВ со стороны злоумышленника

Между (N-1) абонентскими терминалами и СКУ происходит конкурирующий доступ к каналу связи. Абонентские терминалы и СКУ на уровне СМДС типа CSMA/CA функционируют по одинаковым алгоритмам. В связи с этим далее по тексту под устройством сети цифровой радиосвязи с процедурой случайного множественного доступа к среде типа CSMA/CA будем понимать либо АТ, либо СКУ. Следовательно, общее количество равноправных устройств в сети соответствует N.

Каждое устройство такой СЦР осуществляет передачу информационного пакета (пакета данных или пакета с запросом на установление сеанса связи) в случайный момент времени с вероятностью p. Передача считается успешной, если в любой дискретный временной интервал (тайм-слот) осуществляет передачу только одно устройство. В противном случае в канале связи происходит коллизия (столкновение пакетов).

К потенциально возможным ДВ со стороны злоумышленника в интересах захвата радиоресурса и создания преднамеренных коллизий относятся следующие воздействия:

– передача злоумышленником информационных пакетов от имени N устройств (АТ), входящих в атакуемую сеть, с вероятностью Δp;

– имитация злоумышленником информационного обмена с вероятностью D_p от имени K устройств (АТ), не входящих в атакуемую сеть;

– формирование радиопомехи на физическом уровне эталонной модели взаимодействия открытых систем с вероятностью P_f.

4. Математическая модель процедуры СМДС типа CSMA/CA. На основании изложенной описательной модели для оценки эффективности СМДС типа CSMA/CA с учетом потенциально возможных деструктивных воздействий со стороны злоумышленника воспользуемся представленной в работе [11] двумерной цепью Маркова с дискретным отсчетом времени, граф состояний которой показан на рисунке 2.

Система состояний цепи Маркова представляет собой установившийся режим работы сети. Цепь показывает, что в результате коллизий информационный пакет может быть повторно передан (m+1) раз. Каждому этапу повторной передачи соответствует случайное значение отсрочки передачи в диапазоне (0, W_i-1), где (W_i) максимальное значение счетчика отсрочки передачи при каждой повторной попытке передачи. P_{cl1} — вероятность возникновения коллизии переданного кадра для каждого АТ.

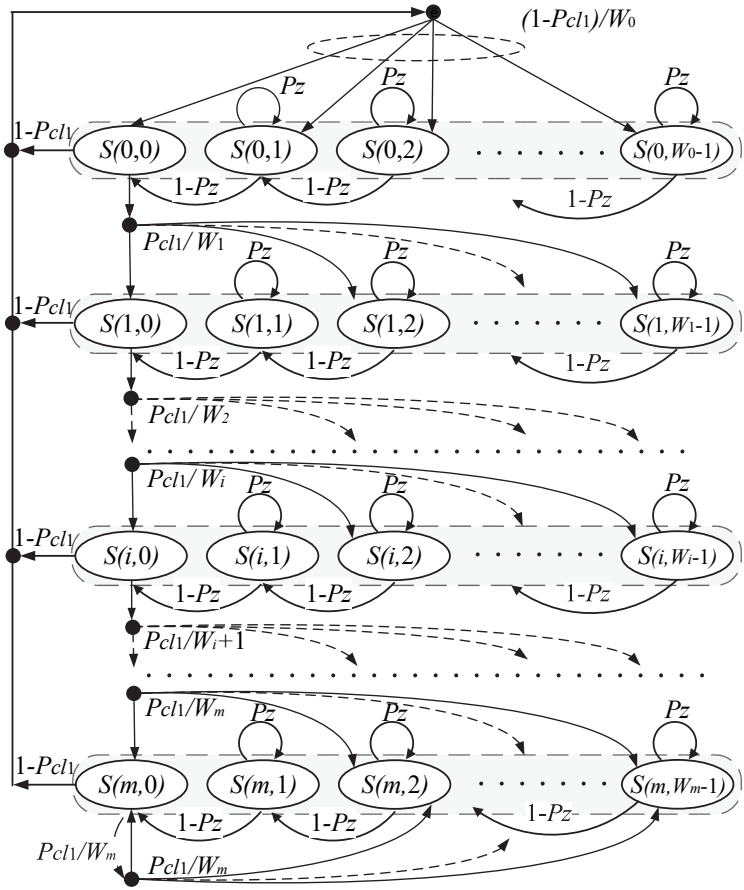


Рис. 2. Граф состояний Марковской цепи процедуры СМДС типа CSMA/CA

В части учета ДВ, направленного на захват радиоресурса, в отличие от работ [11-13] предлагается уточнить аналитическое описание существующих переходов представленной цепи Маркова в части вероятности коллизии для каждого АТ и ввести новые переходы, учитывающие вероятность занятости канала. При этом уточненная вероятность коллизии для каждого АТ P_{cl1} определяется вероятностью передачи информационного пакета легитимным устройством СЦР p и количеством устройств в сети N и имеет следующий вид:

$$P_{cl1} = 1-(1-(p+\Delta p))^{N-1}\prod_{p=0}^{K}(1-D_p)(1-P_f), \quad (1)$$

а вероятность занятости канала связи P_z определяется выражением:

$$P_z = 1-(1-(p+\Delta p))^N \prod_{p=0}^{K}(1-D_p)(1-P_f). \quad (2)$$

В данных выражениях Δp представляет вероятность передачи злоумышленником информационных пакетов от имени N легитимных устройств (АТ), входящих в атакуемую сеть, D_p — вероятность передачи злоумышленником информационных пакетов от имени K устройств (АТ), не входящих в атакуемую сеть, P_f — вероятность формирования злоумышленником радиопомех на физическом уровне эталонной модели взаимодействия открытых систем. При этом злоумышленник, получив из радиоэфира служебные адреса всех устройств в сети, способен сымитировать информационный обмен полностью всех устройств в сети на основе общепринятых правил доступа к каналу связи, указав в передаваемых кадрах MAC-адреса легитимных устройств, тем самым повысив общую вероятность передачи легитимных АТ с p на $(p + \Delta p)$.

Вероятности перехода в рассматриваемой цепи с учетом вероятностей коллизии для каждого АТ и занятости канала предлагается рассчитывать следующим образом.

1. После каждой успешной передачи информационного пакета значение отсрочки передачи случайным образом выбирается в диапазоне (0, W_0-1) с равной вероятностью. При этом, вероятность перехода из состояния $S(i,0)$, где $i \in (0, m)$ — повторные попытки передачи, в состояние $S(0,k)$ где $k \in (0, W_0\text{-}1)$ — начальный диапазон счетчика отсрочки, задается следующим образом:

$$P\{0,k \mid i,0\} = \frac{1-P_{cl1}}{W_0}, \quad (3)$$

где P_{cl1} — вероятность создания коллизии в момент времени t для каждого устройства в сети в условиях ДВ со стороны злоумышленника, W_0 — максимальное значение начального диапазона счетчика отсрочки, устанавливаемое конкретным стандартом связи.

2. Счетчик отсрочки передачи останавливает обратный отсчет при занятости канала связи. При этом вероятность того, что состояние цепи $S(i,k)$ не изменится (цепь останется в том же самом состоянии), соответствует вероятности занятости канала связи:

$$P\{i,k|i,k\}=P_z. \quad (4)$$

3. Счетчик отсрочки передачи продолжает отсчет при освобождении канала связи. Вероятность перехода цепи из состояния *S(i,k+1)* на одно состояние влево (в состояние *S(i,k),* где $k \in (0, W_i+1)$) для каждого этапа повторной попытки передачи i, где $i \in (0, m)$ соответствует вероятности свободного канала связи:

$$P\{i,k|i,k+1\}=1-P_z. \tag{5}$$

4. Если в момент времени t одновременно начали передачу n устройств (произошла коллизия), то каждое устройство, вступившее в коллизию, увеличивает значение повторной попытки передачи i и интервал значений счетчика отсрочки. В данном случае, вероятность перехода из состояния *S(i-1,0)* на один этап повторной попытки передачи вниз (в состояние *S(i,k)*, где $i \in (0, m)$, $k \in (0, W_i+1)$) соответствует:

$$P\{i,k \mid i-1,0\} = \frac{P_{cl1}}{W_i+1}. \tag{6}$$

5. При достижении максимальных значений повторных попыток передач m и счетчика отсрочки передачи k, где $k \in (0, W_m+1)$, устройство останавливается на достигнутых значениях. В этом случае, вероятность перехода цепи из состояния *S(m,0)* в любое из состояний *S(m,k)*, где $k \in (0, W_m+1)$, обуславливается вероятностью коллизии для каждого АТ P_{cl1}:

$$P\{m,k \mid m,0\} = \frac{P_{cl1}}{W_m}. \tag{7}$$

Таким образом, при каждой передаче информационного пакета сеть может изменить свое состояние на один шаг: из состояния *S(i,k)* в состояние *S(0,k)* (где $k \in (0, W_0)$) — при успешной передаче или в состояние *S(i+1,k)* (где $k \in (0, W_i+1)$) — в случае коллизии.

Представляя вероятности перехода из состояния *S(i,0)* в состояние *S(i+1,0)*, не учитывая выбор значения отсрочки передачи (*k,* где $k \in (0,W_i-1)$), методом индукции выразим вероятность перехода цепи $P_{i,0}$ в состояние *S(i,0)*:

$$\left.\begin{aligned} P_{1,0} &= P_{0,0}P_{cl1} \\ P_{2,0} &= P_{1,0}P_{cl1} = P_{0,0}P_{cl1}P_{cl1} \\ P_{3,0} &= P_{2,0}P_{cl1} = P_{0,0}P_{cl1}P_{cl1}P_{cl1} \end{aligned}\right\} \Rightarrow P_{i,0} = P_{0,0}P_{cl1}{}^{i}, 0 < i < m. \tag{8}$$

Вероятность $P_{m,0}$ перехода цепи в состояние *S(m,0)* с учетом максимального количества повторных попыток передач m представляется в следующем виде:

$$P_{m,0} = \frac{P_{0,0} P_{cl1}{}^{m}}{1 - P_{cl1}}. \quad (9)$$

Вероятность $P_{i,k}$ перехода цепи в состояние *S(i,k)* обуславливается следующими совместными событиями: вероятностью достижения значения повторных попыток передач i, где $i \in (0, m)$ и вероятностью выбора случайного таймера отсрочки k, где $k \in (0, W_i\text{-}1)$, и имеет следующий вид:

$$P_{i,k} = \frac{W_i - k}{W_i} \frac{P_{i,0}}{1 - P_z}, 0 \le i \le m,\ 0 < k < W_i - 1. \quad (10)$$

Значения $\sum_{i=0}^{m} P_{i,0}$ и $\sum_{k=0}^{W_i-1} P_{0,k}$ образуют полную группу событий для всех состояний i=0,1,…,m:

$$\sum_{i=0}^{m} P_{i,0} \sum_{k=0}^{W_i-1} P_{0,k} = 1. \quad (11)$$

Подставляя выражения (8)-(10) в выражение (11), получим следующее уравнение:

$$\frac{1}{1 - P_z} \sum_{i=0}^{m} P_{i,0} \sum_{k=0}^{W_i-1} P_{0,k} = \frac{P_{0,0}}{2(1 - P_z)} \times \left(\sum_{i=0}^{m-1} (2P_{cl1})^{i} W_0 + \frac{(2P_{cl1})^{m} W_0 + 1}{1 - P_{cl1}} \right) = 1. \quad (12)$$

Начальное значение диапазона случайной отсрочки передачи W_0 и максимальное количество повторных попыток передач m являются постоянными и устанавливаются в зависимости от параметров сети. Из уравнения (12) получаем функцию зависимости вероятности состояния *S(0,0)* от вероятностей возникновения коллизии для каждого АТ в сети P_{cl1} и занятости канала связи P_z:

$$S_{0,0} = \frac{2(1 - P_z)(1 - P_{cl1})}{W_0 (1 - P_{cl1}) \sum_{i=0}^{m-1} (2P_{cl1})^{i} + (2P_{cl1})^{m} W_0 + 1}. \quad (13)$$

Каждое устройство осуществляет передачу, когда счетчик случайной отсрочки достигает нуля, то есть $p = \sum_{i=0}^{m} P_{i,0}$. Вероятность передачи устройством СЦР в случайный момент времени t определяется как функция зависимости от параметров m, W_0, P_{cl1} и P_z:

$$p = \sum_{i=0}^{m} P_{i,0} = \frac{P_{0,0}}{1-P_{cl1}} = \frac{2\left(1-P_z\right)}{W_0\left(1-P_{cl1}\right)\sum_{i=0}^{m-1}\left(2P_{cl1}\right)^i + \left(2P_{cl1}\right)^m W_0 + 1}. \quad (14)$$

Для определения вероятности передачи АТ необходимо решить систему уравнений, отражающую особенности СМДС типа CSMA/CA в условиях ДВ:

$$\begin{cases} p = \dfrac{2\left(1-P_z\right)}{W_0\left(1-P_{cl1}\right)\sum_{i=0}^{m-1}\left(2P_{cl1}\right)^i + \left(2P_{cl1}\right)^m W_0 + 1}; \\ P_{cl1} = 1-(1-(p+\Delta p))^{N-1}\prod_{p=0}^{K}(1-D_p)(1-P_f); \\ P_z = 1-(1-(p+\Delta p))^{N}\prod_{p=0}^{K}(1-D_p)(1-P_f). \end{cases} \quad (15)$$

Данная система представляет собой систему из 3 нелинейных уравнений и 3 неизвестных, которую можно решить численно.

С учетом изложенного, для оценки эффективности СМДС типа CSMA/CA и разработки алгоритмов автоматического восстановления работоспособности сети цифровой радиосвязи предлагается использовать систему показателей, представленную на рисунке 3.

Вероятность того, что канал в случайный момент времени t является свободным, предлагается определять следующими совместными событиями: отсутствием передачи N легитимных устройств СЦР, а также отсутствием воздействия со стороны злоумышленника.

$$P_{fr} = (1-(p+\Delta p))^{N}\prod_{p=0}^{K}(1-D_p)(1-P_f). \quad (16)$$

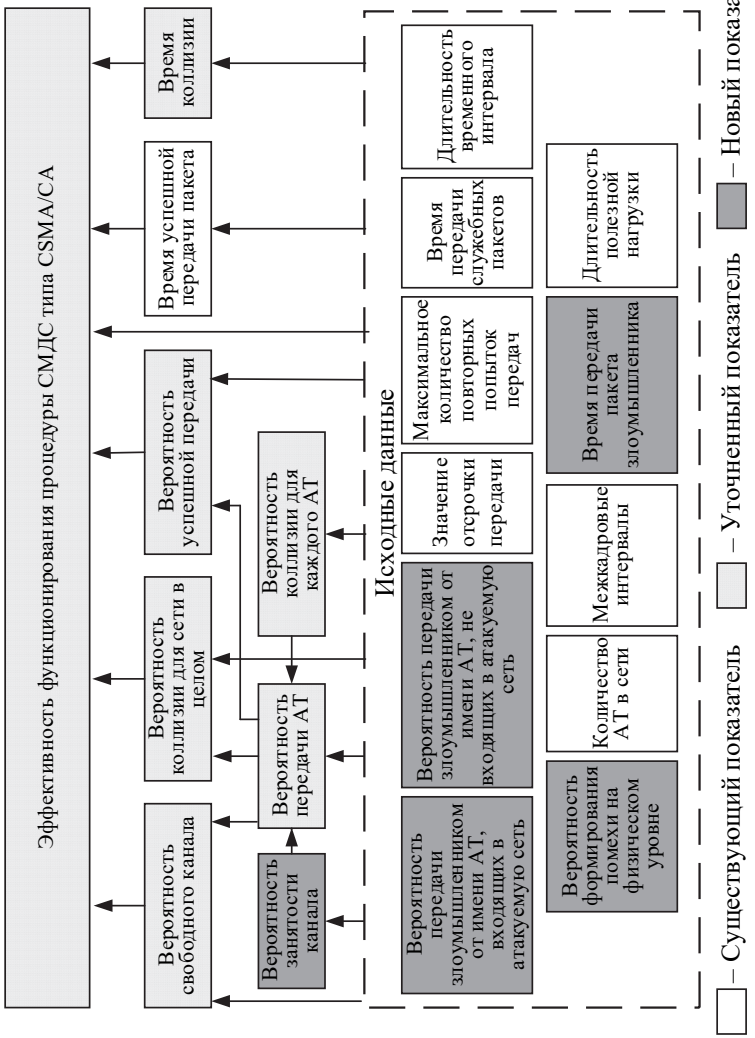


Рис. 3. Система показателей оценки эффективности СМДС типа CSMA/CA

Вероятность успешной передачи информационного пакета легитимным устройством обуславливается тем, что в конкретный момент времени t передает только одно из N устройств и отсутствует воздействие со стороны злоумышленника.

$$P_{sc} = Np(1-(p+\Delta p))^{N-1}\prod_{p=0}^{K}(1-D_p)(1-P_f). \quad (17)$$

Успешная передача, коллизия и свободный канал образуют полную группу событий. Поэтому вероятность коллизии для сети в целом определяется следующим выражением:

$$P_{cl} = 1-P_{fr}-P_{sc} = 1-\prod_{p=0}^{K}(1-D_p)(1-P_f)\times \\ \times\left[(1-(p+\Delta p))^{N} - Np(1-(p+\Delta p))^{N-1}\right]. \quad (18)$$

Для различных стандартов связи, использующих процедуру СМДС типа CSMA/CA, отличительными особенностями являются временные характеристики, определяемые различными алгоритмами реализации случайного множественного доступа к среде. Для стандарта Wi-Fi существует два алгоритма реализации СМДС типа CSMA/CA — основной и дополнительный [10].

Основной алгоритм реализации СМДС типа CSMA/CA заключается в следующем:

1. Устройство, инициирующее передачу кадра данных *DATA*, ожидает временной интервал *DIFS*, в течение которого канал связи должен быть свободен.

2. По окончании интервала *DIFS* осуществляется передача кадра *DATA*.

3. Приемное устройство в ответ на корректно принятый кадр данных *DATA* передает кадр *ACK* спустя интервал *SIFS* вне зависимости от занятости канала связи.

Дополнительный алгоритм реализации СМДС типа CSMA/CA отличается предварительным резервированием канала связи перед передачей кадров данных *DATA* и заключается в следующем:

1. Передающее устройство отправляет кадр запроса на передачу *RTS*.

2. Если запрос *RTS* успешно принят, и устройство, которому адресован запрос, готово к приему данных, то приемное устройство отправляет кадр разрешения на передачу *CTS* спустя интервал *SIFS.* Далее повторяется механизм основного алгоритма реализации СМДС типа CSMA/CA.

С учетом алгоритмов реализации СМДС типа CSMA/CA в сетях цифровой радиосвязи стандарта Wi-Fi и деструктивных воздействий со стороны злоумышленника время успешной передачи и время коллизии основного и дополнительного алгоритмов реализации СМДС имеет следующий вид:

$$\begin{cases} T_{sc}^{bas} = T_D + SIFS + \sigma + ACK + DIFS + \sigma; \\ \begin{cases} T_{cl}^{bas} = T_D + DIFS + \sigma, (\Delta p = 0) \cap (Dp_P = 0); \\ T_{cl}^{bas} = E[P_z] + DIFS + \sigma, \\ ((\Delta p > 0) \cup (Dp_P > 0)) \cap E[P_z] > T_D; \end{cases} \\ \begin{cases} T_{sc}^{rts} = RTS + SIFS + \sigma + CTS + SIFS + \sigma + \\ + T_D + SIFS + \sigma + ACK + DIFS + \sigma; \end{cases} \\ \begin{cases} T_{cl}^{rts} = RTS + DIFS + \sigma, (\Delta p = 0) \cap (Dp_P = 0); \\ T_{cl}^{rts} = E[P_z] + DIFS + \sigma, \\ ((\Delta p > 0) \cup (Dp_P > 0)) \cap E[P_z] > RTS, \end{cases} \end{cases} \quad (19)$$

где T_{sc}^{bas} — время успешной передачи основного алгоритма реализации СМДС, T_{cl}^{bas} — время коллизии основного алгоритма, T_{sc}^{rts} — время успешной передачи дополнительного алгоритма, T_{cl}^{rts} — время коллизии дополнительного алгоритма, T_D — время передачи полезной нагрузки, *SIFS* — межкадровый интервал, σ — задержка распространения сигнала, *ACK* — временя передачи пакета подтверждения, *DIFS* — увеличенный межкадровый интервал, *RTS* — время передачи кадра запроса, *CTS* — время передачи кадра ответа на запрос, $E[P_z]$ — время передачи пакета злоумышленника.

Из аналитического выражения (19) видно, что в стандарте Wi-Fi в условиях деструктивных воздействий со стороны злоумышленника время коллизии дополнительного алгоритма реализации СМДС

типа CSMA/CA T_{cl}^{rts} эквивалентно времени коллизии основного алгоритма T_{cl}^{bas} .

С учетом вышесказанного под эффективностью СМДС типа CSMA/CA понимается доля от суммарных временных затрат, требуемая на передачу полезной нагрузки, с учетом вероятностей успешной передачи, коллизии и свободного канала. В соответствии с [11], эффективность СМДС типа CSMA/CA определяется отношением произведения вероятности успешной передачи пакетов P_{sc} на длительность полезной нагрузки T_D к сумме произведений вероятности успешной передачи P_{sc} на время успешной передачи пакета T_{sc}, вероятности возникновения коллизии P_{cl} на время коллизии T_{cl} и вероятности свободного канала P_{fr} на длительность одного временного интервала (слота) τ.

$$\Omega = \frac{T_D P_{sc}}{P_{sc} T_{sc} + P_{cl} T_{cl} + P_{fr} \tau}. \tag{20}$$

В основном и дополнительном алгоритмах реализации СМДС типа CSMA/CA стандарта Wi-Fi длительность полезной нагрузки определяется по формуле:

$$T_D = \frac{Ep}{Rate}, \tag{21}$$

где *Ep* — среднее значение размера полезной нагрузки легитимных АТ в битах, *Rate* — скорость передачи информации, измеряемое в бит/с.

Среднее значение размера полезной нагрузки определяется статистически в зависимости от применяемого стандарта связи. Скорость передачи информации также зависит от конкретной реализации стандарта.

5. Методика оценки эффективности СМДС типа CSMA/CA. Методика оценки эффективности случайного множественного доступа к среде типа CSMA/CA учитывает полную группу событий в канале связи, а также исходных данных, включая параметры потенциально возможных деструктивных воздействий, и заключается в выполнении следующих действий.

Шаг 1. Задаются параметры сети цифровой радиосвязи. К основным параметрам относятся: количество устройств в сети, максимальное количество повторных попыток передач, начальное значение интервала отсрочки передачи, временные интервалы используемого стандарта связи.

Шаг 2. Определяются значения вероятности передачи пакетов p и вероятности коллизии P_{cl1} для каждого устройства СЦР в соответствии с системой уравнений (15).

Шаг 3. Определяются вероятностные характеристики сети: вероятность свободного канала $P_{fr,}$ вероятность успешной передачи пакетов P_{sc} и вероятность возникновения коллизии для сети в целом P_{cl} по формулам (16), (17), (18) соответственно.

Шаг 4. Определяются по межкадровым интервалам и времени передачи пакетов временные характеристики сети в зависимости от применяемого стандарта связи и его алгоритма реализации СМДС типа CSMA/CA. Для стандарта Wi-Fi используется выражение (19).

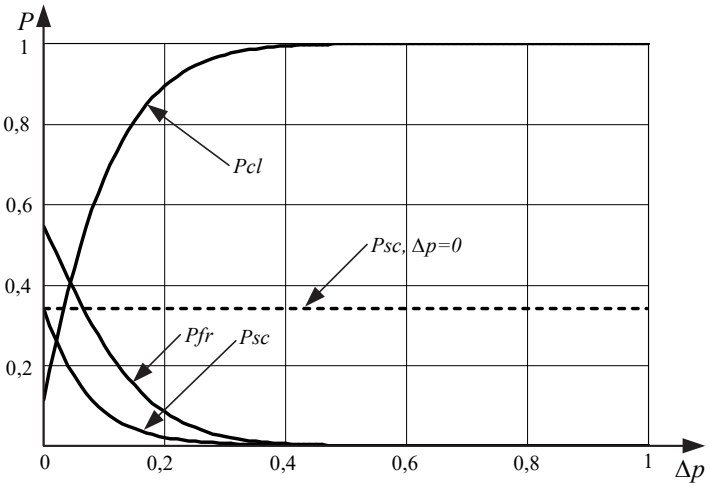
Шаг 5. Оценивается эффективность СМДС типа CSMA/CA по формуле (20).

6. Результаты численного эксперимента. В качестве частного применения процедуры случайного множественного доступа к среде типа CSMA/CA рассмотрим стандарт цифровой радиосвязи IEEE 802.11 (Wi-Fi) [10].

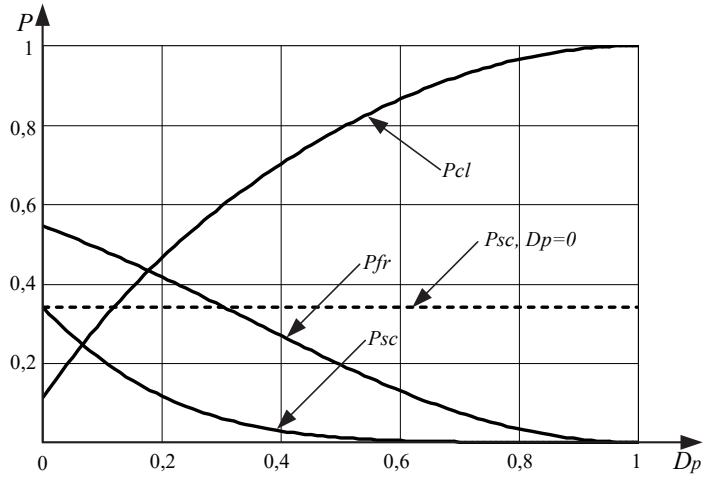
Зависимости вероятностей P_{sc}, P_{cl} и P_{fr} от параметров ДВ определяются настройками сети: m, W_0 и количеством устройств $N,$ и не зависят от используемого алгоритма реализации СМДС типа CSMA/CA.

На рисунке 4 представлены результаты моделирования вероятностей возникновения коллизии P_{cl}, свободного канала P_{fr} и успешной передачи P_{sc} от параметров ДВ, а именно: от вероятности передачи информационных пакетов от имени N абонентских терминалов, входящих в атакуемую сеть Δp и от вероятности имитации информационного обмена от имен K=3 устройств, не входящих в атакуемую сеть D_p. В качестве параметров сети выступают следующие значения: m=3, W_0=16, N=10.

На рисунке 4 изображено возрастание вероятности возникновения коллизии P_{cl} и уменьшение вероятности успешной передачи пакетов $P_{sc.}$ Это вызвано тем, что злоумышленник осуществляет передачу информационных пакетов, игнорируя общие правили доступа к каналу связи.



а)



б)

Рис. 4. Зависимости вероятностных характеристик сети от ДВ с параметрами: а) Δp; б) D_p

Деструктивное воздействие, направленное на передачу пакетов от имени всех устройств, входящих в атакуемую сеть, с вероятностью Δp оказывает более существенное влияние на вероятностные характеристики процедуры СМДС типа CSMA/CA. Это вызвано преднамеренным увеличением вероятностей передачи всех легитимных устройств СЦР.

Зависимости эффективности СМДС типа CSMA/CA для основного и дополнительного алгоритмов от количества устройств в сети N в условиях ДВ, направленных на имитацию АТ, входящих и не входящих в атакуемую сеть, с параметрами $\Delta p = 0{,}15$ и $D_p = 0{,}7$, $K = 3$ представлены на рисунке 5.

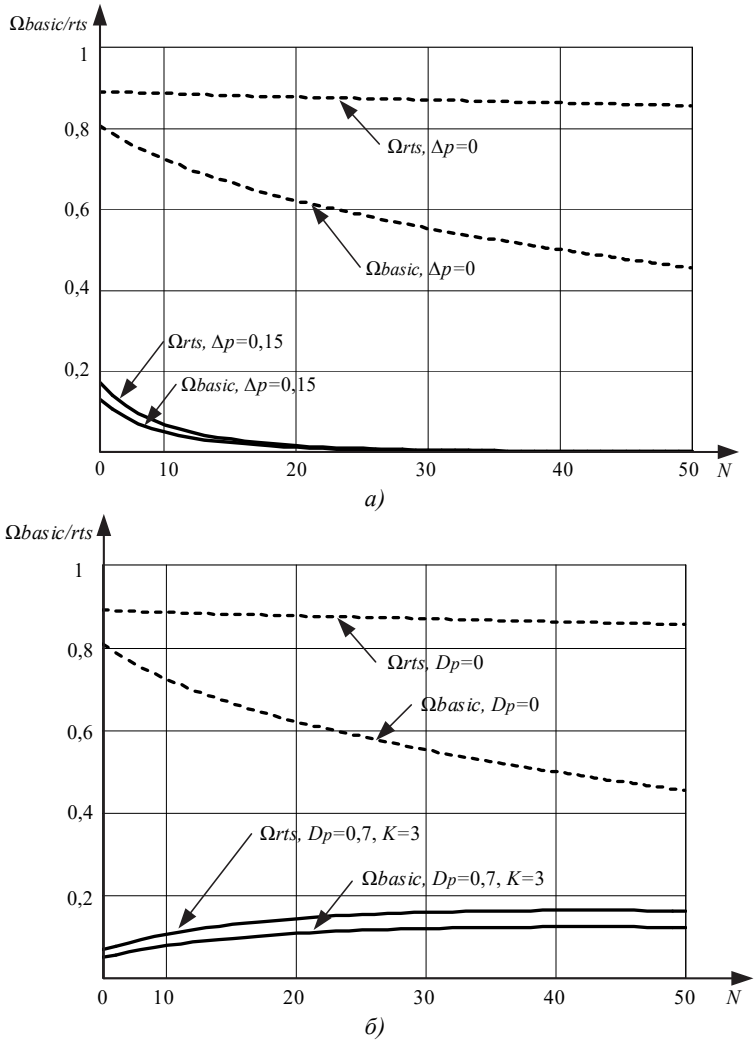


Рис. 5. Результаты оценки эффективности СМДС типа CSMA/CA в условиях ДВ для: *а*) Δp=0,15; *б*) D_p=0,7 и K=3

Анализ представленных на рисунке 5 зависимостей позволяет сделать вывод о том, что в условиях деструктивного воздействия со стороны злоумышленника эффективность СМДС типа CSMA/CA для дополнительного алгоритма эквивалентна эффективности основного алгоритма. При ДВ с параметром Δp=0,15 эффективность основного алгоритма снижается в 30 раз, эффективность дополнительного алгоритма снижается в 45 раз, а при ДВ с параметром D_p=0,7 эффективность основного алгоритма снижается в 5,5 раз, эффективность дополнительного алгоритма снижается в 6,2 раза. Как следствие, применение известных алгоритмов, ограничивающих устройствам доступ к радиоресурсу в условиях различных ДВ, является малоэффективным. Поэтому, возникает потребность в разработке дополнительных механизмов защиты процедуры СМДС типа CSMA/CA.

Достоверность представленных результатов была подтверждена экспериментальными исследованиями. В основу данных исследований были положены существующие аппаратные части беспроводных модулей стандарта 802.11 a/b/g/n/ac (USB Adapter Alfa AWUS036ACH) с измененной программной частью. Данная реализация позволила осуществить формирование и передачу информационных кадров с изменяемыми параметрами (интенсивностью, длительностью, MAC-адресами). Полученные экспериментальные результаты полностью подтверждают адекватность представленной математической модели.

7. Заключение. Таким образом, предложена математическая модель процедуры случайного множественного доступа к среде типа CSMA/CA, основанная на применении Марковских процессов и методов теории вероятностей, позволяющая проводить оценку эффективности случайного множественного доступа к среде в условиях потенциально возможных деструктивных воздействий со стороны злоумышленника. Результаты моделирования могут быть применимы при разработке дополнительных методов защиты процедуры случайного множественного доступа к среде типа CSMA/CA для существующих и перспективных средств цифровой радиосвязи.

Литература

1. *Перегудов М. А., Бойко А.А.* Оценка защищенности сети пакетной радиосвязи от имитации абонентских терминалов на уровне процедуры случайного множественного доступа к среде типа S-ALOHA // Информационные технологии. 2015. № 7. С. 527–534.

2. *Перегудов М. А., Бойко А.А.* Модель процедуры случайного множественного доступа к среде типа S-ALOHA // Информационно-управляющие системы. 2014. № 6. С. 75–81.
3. *Перегудов М. А., Бойко А.А.* Модель процедуры зарезервированного доступа к среде сети пакетной радиосвязи // Телекоммуникации. 2015. № 6. С. 7–15.
4. *Перегудов М. А., Бойко А.А.* Модель процедуры управления питанием сети пакетной радиосвязи // Телекоммуникации. 2015. № 9. С. 13–18.
5. *Kleinrock, L., Lam S.S.* On Stability of Packet Switching in a Random Multi-Access Broadcast Channel // Seventh Hawaii International Conference on System Sciences. 1974. pp. 73–77.
6. *Bianchi G.* IEEE 802.11–Saturation Throughput Analysis // IEEE Communications Letters. 1998. vol. 2 no. 12. pp. 318–320.
7. *Wang C., Li B., Li L.* A New Collision Resolution Mechanism to Enhance the Performance of IEEE 802.11 DCF // IEEE Transactions on Vehicular Technology. 2004. vol. 53. no. 4. pp. 1235–1246.
8. *Aad I., Ni Q., Barakat C., Turletti T.* Enhancing IEEE 802.11 MAC in Congested Environments // Computer communications. 2005. vol. 28. no. 14. pp. 1605–1617.
9. *Choi J., Yoo J., Kim C.* A Distributed Fair Scheduling Scheme with a new Analysis Model in IEEE 802.11 wireless LANs // IEEE Transactions on Vehicular Technology. 2008. vol. 57. no. 5. pp. 3083–3093.
10. IEEE Standard for Information Technology—Telecommunications and information exchange between systems Local and metropolitan area networks–Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications // IEEE 802.11. 2012.
11. *Bianchi G.* Performance Analysis of the IEEE 802.11 Distributed Coordination Function // IEEE Journal on Selected Areas in Communication. 2000. vol. 18. no. 3. pp. 535–547.
12. *Wu H. et al.* Performance of reliable transport protocol over IEEE 802.11 wireless LAN: analysisand enhancement // Proceedings of Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. 2002. vol. 2. pp 599–607.
13. *Choi J., Yoo J., Kim C.* A novel performance analysis model for an IEEE 802.11 wireless LAN // IEEE Communications Letters. 2006. vol. 10. no. 5. pp. 335–337.
14. *Chen H.* Revisit of the Markov model of IEEE 802.11 DCF for an error-prone channel // IEEE Communications Letters. 2011. vol. 15. no. 12. pp. 1278–1280.
15. *Dai L., Sun X.* A unified analysis of IEEE 802.11 DCF networks: Stability, throughput and delay // IEEE Transactions on Mobile Computing. 2013. vol. 12. no. 8. pp. 1558–1572.
16. *Kai C., Zhang S.* Throughput analysis of CSMA wireless networks with finite offered-load // 2013 IEEE International Conference on Communications (ICC). 2013. pp. 6101–6106.
17. *Hosseinabadi G., Vaidya N.* Token-DCF: An opportunistic mac protocol for wireless networks. COMSNETS. 2013. pp. 1–9.
18. *Laufer R., Kleinrock L.* The Capacity of Wireless CSMA/CA Networks // IEEE/ACM Transactions on Networking. 2016. vol. 24. pp. 1518–1532.
19. *Оруджева М.Я.* Модели беспроводных локальных сетей с методом коллективного доступа CSMA/CA // Телекоммуникации. 2010. № 6. С. 15–18.
20. *Ушаков Ю.А., Полежаев П.Н., Коннов А.Л., Бахарева Н.Ф.* Вопросы оптимизации механизма CSMA/CA в беспроводных сетей высокой плотности // Системы управления и информационные технологии. 2014. Том 57. № 3.2. С. 286–291.

21. *Doost-Mohammady R., Naderi M., Kaushik R.* Performance Analysis of CSMA/CA based Medium Access in Full Duplex Wireless Communications // IEEE Transactions on Mobile Computing. 2015. vol. 15. no. 6. pp. 1457–1470.
22. *Yang Y., Chen B., Srinivasan K., Shroff N.* Characterizing the achievable throughput in wireless networks with two active RF chains // IEEE Conference on Computer Communications (INFOCOM). 2014. pp. 262–270.
23. *Макаренко С. И., Татарков М. А.* Моделирование обслуживания нестационарного информационного потока системной связи со случайным множественным доступом // Информационно-управляющие системы. 2012. № 1. С. 44–50.

Перегудов Максим Анатольевич — к-т техн. наук, начальник лаборатории НИИИ (РЭБ), Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина». Область научных интересов: методы и системы защиты информации. Число научных публикаций — 14. maxaperegudov@mail.ru; ул. Ст. Большевиков, 54А, Воронеж, 394064; р.т.: +7(473)236-5228, Факс: 7(473)244-7860.

Стешковой Анатолий Сергеевич — младший научный сотрудник, Военный учебно-научный центр Военно-воздушных сил "Военно-воздушная академия имени Н.Е. Жуковского и Ю.А. Гагарина". Область научных интересов: методы и системы защиты информации. Число научных публикаций — 6. 9515431635@mail.ru; ул. Ст. Большевиков, 54А, Воронеж, 394064; р.т.: +7(473)236-5228, Факс: +7(473)244-7860.

Бойко Алексей Александрович — к-т техн. наук, доцент, начальник отдела, Военный учебно-научный центр Военно-воздушных сил "Военно-воздушная академия имени Н.Е. Жуковского и Ю.А. Гагарина". Область научных интересов: методы и системы защиты информации, методы оценки качества сложных систем. Число научных публикаций — 120. algeminy@mail.ru; ул. Ст. Большевиков, 54А, Воронеж, 394064; р.т.: +7(473)236-5228, Факс: +7(473)244-7860.

DOI 10.15622/sp.59.4

M.A. PEREGUDOV, A.S. STESHKOVOY, A.A. BOYKO

PROBABILISTIC RANDOM MULTIPLE ACCESS PROCEDURE MODEL TO THE CSMA/CA TYPE MEDIUM

Peregudov M.A., Steshkovoy A.S., Boyko A.A. **Probabilistic Random Multiple Access Procedure Model to the CSMA/CA Type Medium.**

Abstract. Nowadays the issue of digital radio network security during destructive impacts by intruder is particularly important. For destructive impacts on physical OSI level prevention noise protection methods are applied and encryption is applied on network and higher levels. In fact most dangerous vulnerabilities from destructive impacts are focused on digital radio network channel level in procedures random multiply access procedure to the digital radio network medium. Only for procedure of random multiply access to digital radio network of S-ALOHA type math models have been developed which allow to estimate it functionality efficiency in conditions of potentially destructive impacts. This procedure applies for GSM, TETRA, DMR, LTE digital radio networks. But for Wi-Fi and Bluetooth networks, which are used currently in every house, random multiply access procedure for CSMA/CA is used. The paper presents a math model of the procedure for random multiple access to the digital radio networks of CSMA/CA type. The model take into consideration potential destructive intruder impact by analytic expression adjusting for probabilistic and time characteristic in well-known model and because of usage new indicator — network channel occupancy probability. In Wi-Fi and Bluetooth networks in case of channel occupancy due reason collisions and successfully transfer delay timer for each abonent terminal is stopped. In well-known models this feature of digital networks with random multiply access to CSMA/CA is not considered. It established that existing CSMA/CA random multiply access algorithm functioning efficiency tends to zero because of possible destructive impacts. Work results can be used in the digital radio network OSI channel level automatic recovering efficiency area of algorithm development.

Keywords: digital radio network, destructive impact, random multiple access procedure, CSMA/CA, Markov chain, efficiency.

Peregudov Maksim Anatol'evich — Ph.D., head of research laboratory, Military education-science center of Military aviation forces “Military aviation academy named for prof. N.E. Zhukovsky and Yu.A. Gagarin”. Research interests: methods and systems of information protection. The number of publications — 14. maxaperegudov@mail.ru; 54A, Old Bolsheviks str., Voronezh, 394064, Russia; office phone: +7(473)236-5228, Fax: 7(473)244-7860.

Steshkovoy Anatoliy Sergeevich — junior researcher, Military education-science center of Military aviation forces “Military aviation academy named for prof. N.E. Zhukovsky and Yu.A. Gagarin”. Research interests: methods and systems information security. The number of publications — 6. 9515431635@mail.ru; 54A, Old Bolsheviks str., Voronezh, 394064, Russia; office phone: +7(473)236-5228, Fax: +7(473)244-7860.

Boyko Aleksey Aleksandrovich — Ph.D., associate professor, head of department, Military education-science center of Military aviation forces “Military aviation academy named for prof. N.E. Zhukovsky and Yu.A. Gagarin”. Research interests: methods and systems of infor-

mation protection, methods of assessing the quality of complex systems. The number of publications — 120. algeminy@mail.ru; 54A, Old Bolsheviks str., Voronezh, 394064, Russia; office phone: +7(473)236-5228, Fax: +7(473)244-7860.

References

1. Peregudov M.A., Boyko A.A. [Evaluation security of packet radio network from simulation of subscriber terminals at level of random multiple access procedure to environment of S-ALOHA type]. *Informacionnye tehnologii – Information Technology*. 2015. vol. 7. pp. 527–534. (In Russ.).
2. Peregudov M.A., Boyko A.A. [Model of the procedure of random multiple access to the medium of S-ALOHA type]. *Informacionno-upravljajushhie sistemy – Information-control systems.* 2014. vol. 6. pp. 75–81. (In Russ.).
3. Peregudov M.A., Boyko A.A. [Model of the procedure of reserved access to the packet radio network environment]. *Telekommunikacii – Telecommunications.* 2015. vol. 6. pp. 7–15. (In Russ.).
4. Peregudov M. A., Boyko A.A. [Model of the Power Management Procedure of the Packet Radio Network]. *Telekommunikacii – Telecommunications*. 2015. vol. 9. pp. 13–18. (In Russ.).
5. Kleinrock L., Lam S., On Stability of Packet Switching in a Random Multi-Access Broadcast Channel. Seventh Hawaii International Conference on System Sciences. 1974. pp. 73–77.
6. Bianchi G. IEEE 802.11–Saturation Throughput Analysis. *IEEE Communications Letters*. 1998. vol. 2. no. 12. pp. 318–320.
7. Wang C., Li B., Li L. A New Collision Resolution Mechanism to Enhance the Performance of IEEE 802.11 DCF. *IEEE Transactions on Vehicular Technology.* 2004. vol. 53. no. 4. pp. 1235–1246.
8. Aad I., Ni Q., Barakat C., Turletti T. Enhancing IEEE 802.11 MAC in Congested Environments. *Computer communications*. 2005. vol. 28. no. 14. pp. 1605–1617.
9. Choi J., Yoo J., Kim C. A Distributed Fair Scheduling Scheme with a new Analysis Model in IEEE 802.11 wireless LANs. *IEEE Transactions on Vehicular Technology*. 2008. vol. 57. no. 5. pp. 3083–3093.
10. IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks–Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE 802.11. 2012.
11. Bianchi G. Performance Analysis of the IEEE 802.11 Distributed Coordination Function. *IEEE Journal on Selected Areas in Communication*. 2000. vol. 18. no. 3. pp. 535–547.
12. Wu H., Peng Y., Long K., Cheng S., Ma J. Performance of Reliable Transport Protocol over IEEE 802.11 Wireless LAN: Analysisand Enhancement. Proceedings of Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. 2002. vol. 2. pp. 599–607.
13. Choi J., Yoo J., Kim C. A Novel Performance Analysis Model for an IEEE 802.11 Wireless LAN. *IEEE Communications Letters*. 2006. vol. 10. no. 5. pp. 335–337.
14. Chen H. Revisit of the Markov Model of IEEE 802.11 DCF for an Error-Prone Channel. *IEEE Communications Letters*. 2011. vol. 15. no. 12. pp. 1278–1280.
15. Dai L., Sun X. A unified analysis of IEEE 802.11 DCF networks: Stability, throughput and delay. *IEEE Transactions on Mobile Computing*. 2013. vol. 12. no. 8. pp. 1558–1572.

16. Kai C., Zhang S. Throughput analysis of CSMA wireless networks with finite offered-load. 2013 IEEE International Conference on Communications (ICC). 2013. pp. 6101–6106.
17. Hosseinabadi G., Vaidya N. Token-DCF: An opportunistic mac protocol for wireless networks. COMSNETS. 2013. pp. 1–9.
18. Laufer R., Kleinrock L. The Capacity of Wireless CSMA/CA Networks. *IEEE/ACM Transactions on Networking*. 2016. vol. 24. pp. 1518–1532.
19. Orudzheva M.Ya. [Models of wireless LANs with the method of collective access CSMA/CA]. *Telekommunikacii – Telecommunications.* 2010. vol. 6. pp. 15–18. (In Russ.).
20. Ushakov Yu.A., Polezhaev P.N., Konnov A.L., Bahareva N.F. [Optimization of the CSMA/CA Mechanism in High-Density Wireless *Networks]. Sistemy upravlenija i informacionnye tehnologii – Control systems and information technologies.* 2014. vol. 3.2. pp. 286–291. (In Russ.).
21. Doost-Mohammady R., Naderi M., Kaushik R. Performance Analysis of CSMA/CA based Medium Access in Full Duplex Wireless Communications. *IEEE Transactions on Mobile Computing.* 2015. vol. 15. no. 6. pp. 1457–1470.
22. Yang Y., Chen B., Srinivasan K., Shroff N. Characterizing the achievable throughput in wireless networks with two active RF chains. IEEE Conference on Computer Communications (INFOCOM). 2014. pp. 262–270.
23. Makarenko S.I., Tatarkov M.A. [Modeling the maintenance of a non-stationary information stream of system communication with random multiple access]. *Informacionno-upravljajushhie sistemy – Information-control systems.* 2012. vol. 1. pp. 44–50. (In Russ.).

DOI 10.15622/sp.59.5

A.A. TEILANS, A.V. ROMANOVS, Yu. A. MERKURYEV, P.P. DOROGOVS, A.YA. KLEINS, S.A. POTRYASAEV

ASSESSMENT OF CYBER PHYSICAL SYSTEM RISKS WITH DOMAIN SPECIFIC MODELLING AND SIMULATION

Teilans A.A., Romanovs A.V., Merkuryev Yu.A., Dorogovs P.P., Kleins A.Ya., Potryasaev S.A. **Assessment of Cyber Physical System Risks with Domain Specific Modelling and Simulation.**

Abstract. Nowadays, the systems developed to integrate real physical processes and virtual computational processes — the cyber-physical systems (CPS), are used in multiple areas of industry and critical national infrastructure, such as manufacturing, medicine, traffic management and security, automotive engineering, industrial process control, energy saving, ecological management, industrial robots, technical infrastructure management, distributed robotic systems, protection target systems, nanotechnology and biological systems technology. With wide use, the level of IT and cyberrisks increases drastically and successful attacks against the CPS will lead to unmanageable and unimaginable consequence. Thus, the need in well-designed risk assessment system of CPS is clear and such system can provide an overall view of CPS security status and support efficient allocations of safeguard resources. The nature of CPS differs from IT mainly with the requirement for real-time operations, thus, traditional risk assessment method for IT system can be adopted in CPS. Design of a unified modelling language based domain specific language described in this paper achieves synergy from in IT industry widely used UML modelling technique and the domain specific risk management extensions. As a novelty for UML modelling, especially for simulation purposes, the presented DSL is enriched by a set of stochastic attributes of modelled activities. Such stochastic attributes are usable for further implementation of discrete-event system simulators.

Keywords: Cyber Physical System, IT, Risks, Risk Assessment, Domain Specific Language, Modelling, UML, CORAS, Disaster Tolerance Cyber Physical System, Structure Dynamic Control System.

1. Introduction. New competitive approach to the physical and virtual world integration with cyber-physical systems is one of the European Union research priorities. Cyber-physical systems (CPS) will change the way people interface with systems, the same way as the Internet has transformed the way people interface with information.

Concept of cyber-physical systems, their history and main components and characteristics are considered in this paper. Main accent is directed to the great influence of effective risk management on profit abilities in modern business systems, especially highly automated ones with complex use of Information Technology. IT risk consists not only of breakdowns in computer software or hardware, or lack of expertise of the IT staff. IT risk also may relate to risk of loss resulting from theft of company's data or client information. IT risk also may be the risk of loss that originates from computer software malfunction, such as a manufacturer's software license expiration or glitches, and the ways it affects corporate activities [1, 2]. A risk assessment initiative for IT systems

generally helps management understand areas in which significant losses may arise. IT risk assessment is carried out by identifying and evaluating assets, vulnerabilities and threats of using information technologies in business. An asset is anything that has value to the company — hardware, software, people, infrastructure, data, suppliers and partners, etc [3].

Taking into consideration the extreme complexity of IT risk assessment, we conclude that there is necessity to apply international frameworks of IT governance and risk management, such as Enterprise Risk Management Framework by Committee of Sponsoring Organizations of the Treadway Commission, Control Objectives for Information and related Technology, Code of Practice for Information Security Management, Information Technology Infrastructure Library, etc [4, 5].

Within our research, an IT risk management domain specific language is developed [6]. Nowadays, in the IT industry, majority of system specifications and procedure descriptions are made using the Unified Modelling Language (UML). UML is a graphical language and it consists from diagrams which are united in a model. The description of a system can be made from just a few diagrams in case of simple system or from hundreds of diagrams in case of a complex system. These diagrams are designed by system architects and system analysts.They are used in whole life cycle of a system. These models are frequently the main documentation for the system that is used for its operation and maintenance. That is why the authors have chosen UML as the base for designing the IT risk analysis DSL. UML uses general system organization terms such as Use Case, Activity, Action, State, Event etc. However, risk analysis professionals work with terms such as Threat, Vulnerability, Asset, Incident, Risk, Treatment etc. Therefore, to create an IT risk analysis tool, it was necessary to extend UML modelling approach with elements used by risk analysts. In fact there was an attempt to develop our own Risk analysis Domain specific modelling language, suitable for system developers and maintenance personnel and for risk analysts as well. Design of modelling tools necessary for risk analysts was based on CORAS language which is well known in professional community [7]. The CORAS language is a graphical modelling language for communication, documentation and analysis of security threat and risk scenarios in security risk analyses. This paper explains how the authors use CORAS Threat and Treatment diagrams, connecting them with UML Uses Case and Activity diagrams [8]. The result of this work provides means to unify both risk analysis model and IT system model.

2. Concept of a cyber-physical system. Cyber-physical systems are developed to integrate real physical processes and virtual computational processes. Many objects used in modern daily life are cyber-physical systems. Concept of CPS is complicated, it can be illustrated with a concept map (see Figure 1), developed in Berkley University [9, 10].

The definition of Cyber-physical system from Cyber-Physical Systems Week (www.cpsweek.org): "Cyber-physical systems (CPS) are complex engineering systems that rely on the integration of physical, computation, and communication processes to function."

Cyber-physical systems have not appeared from nowhere, they have a long history of development, which continues. This paper is an introduction to cyber-physical systems, their history and overview of the main components and characteristics.

Always growing need for different purpose information management systems leads to optimization of computing tools design techniques. Most of the world's currently used information management systems are embedded systems and networks. They are closely related to the control or management objects.

From certain common computing systems' classifications best suited to the modern situation is classification proposed by David Patterson and John Hennesy [11]. Their classification was guided by the use of the system. They divided computing system into 3 categories: desktop computers, servers and embedded systems. Embedded systems by the area of use are separated into:

- Automatic control systems;
- Measuring systems and systems that read information from sensors;
- Real-time "question – answer" type information systems;
- Digital data transmission systems;
- Complex real-time systems;
- Moving objects management systems;
- A general purpose computer system subsystems;
- Multimedia systems.

The concept of embedded systems appeared in the early 50's and it is in rapid development even today. It is interesting to view the evolution of embedded systems:

- Information management systems, 60's;
- Embedded computing systems, 70's;
- Embedded distributed systems, 90's;
- Cyber-physical systems, from 2006.

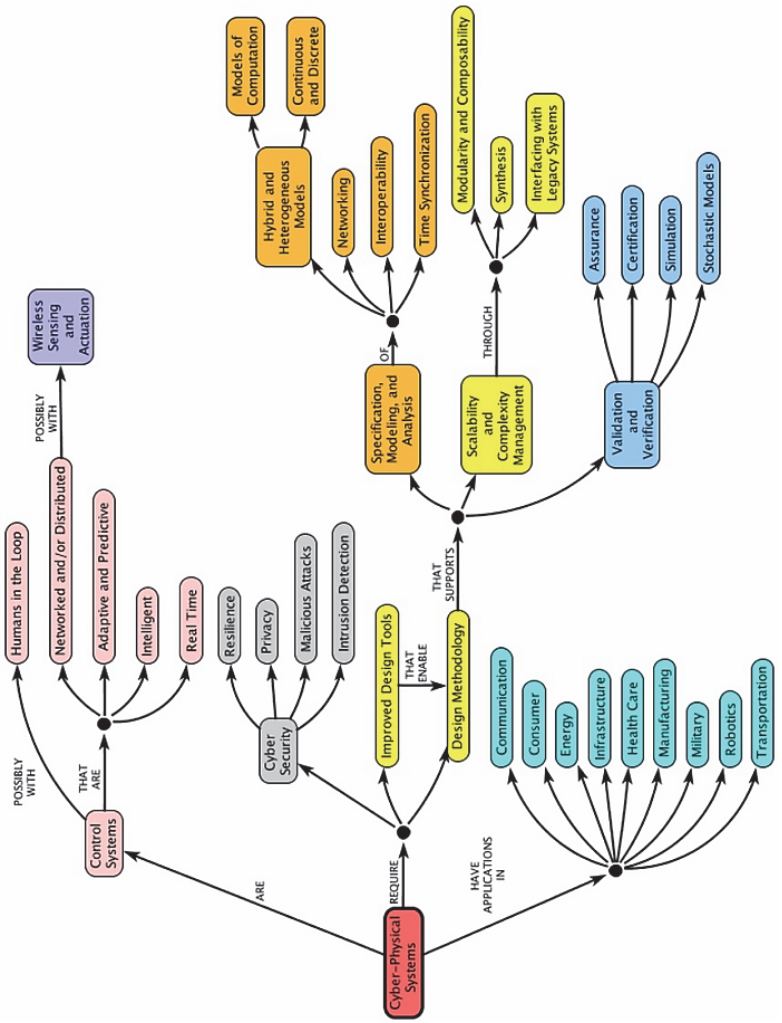


Fig. 1. A concept map of Cyber-physical systems

Information management system is a computing system designed for management purposes, but it is the most alienated from the control object. Integrated micro-scheme and microprocessors development led to information management system bringing directly to the management object. World had entered the era of embedded systems. System elements are gradually becoming cheaper and their integration increases, as well as the security level and the opportunity to combine them in controlled networks.

Downturn in embedded systems' elements prices and increasing connection with physical management objects led to appearance of cyber-physical systems.

Cyber-physical systems are specialized computing systems that interact with control or management objects. Cyber-physical systems integrate computing, communication, data storage with real world's objects and physical processes. All above said processes must occur in real-time, in safe, secure and efficient manner. Cyber-physical systems must be scalable, cost-effective and adaptive. Cyber-physical systems are in use in various areas such as smart medical technologies, environmental monitoring and traffic management.

Wireless sensor networks can become an important part of cyber-physical systems, because of high sensitivity capability it is one of the main driving factors of cyber-physical systems application distribution. The rapid development of WSN, medical sensors and cloud computing systems makes cyber-physical systems impressive candidates for use in inpatient and outpatient health care improvement [12]. Cloud computing maturity is a direct result of few technologies such as distributed computing, internet technology, system management and hardware development [13].

Cyber-physical systems integrate computing and physical processes. Compared with embedded systems much more physical components are involved in CPS. In embedded systems, the key focus is on the computing element, but in cyber-physical systems, it is on the link between computational and physical elements. Cyber-physical system parts exchange information with each other that is why the third component - communication is added there. For this reason, cyber-physical system is denoted by the symbol C3 (Computation, Communication and Control). Links improvement between computational and physical elements, extends cyber-physical systems usage possibilities.

Cyber-physical systems are used in multiple areas such as medicine, traffic management and security, automotive engineering, industrial and process control, energy saving, ecological monitoring and management, avionics and space equipment, industrial robots, technical infrastructure management, distributed robotic systems, protection target systems,

nanotechnology and biological systems technology. In all cases increased use of CPS are closely tied with cyber and IT risks, that need to be managed well.

3. Common IT risk management problems. It is possible to indicate a set of IT risks management problems which are typical for Latvian business [4]. They are:

– customer service malfunction due to interruptions of continuous access to IT services;

– unsatisfied demand for qualified IT personnel;

– delayed modernization of information systems software and hardware;

– insufficient IT qualification of information system users;

– inadequate level of existing IT services quality monitoring;

– inadequate level of cooperation between IT specialists and other employees;

– inadequate assessment of financial losses resulting from failures or interruptions within information systems;

– absence of IT system development strategic plan, based on a general development plan of company;

– inadequately low IT security level;

– absence of strategy of IT system restoration after potential failures and interruptions.

Taking into consideration the extreme complexity of IT risk management within the framework of operational risk management system, it could be concluded that it is necessary to apply international standards and frameworks of IT governance, such as Information Technology Infrastructure Library, Control Objectives for Information and related Technology, Code of Practice for Information Security Management.

The proposed technique for IT risk assessment and management could be successfully used as a start point for development of the IT risks assessment support systems prototype, based on an IT risk management domain specification language with a metamodel that defines an abstract UML based language for graphical approach to identify, explain and document security threats and risk scenarios. The next chapter describes the Domain Specific Language (DSL) for IT risk analysis modelling and simulation. The presented tool will provide both IT process modelling and documentation as well as connection of these processes with identified risks.

4. DSL for IT risk analysis. A Domain specific language (DSL) is language for programming, specification or modelling suitable for particular problem domain specialists to solve their specific technical tasks [14, 15]. This chapter describes domain specific language for IT risk analysis designed by the authors. This language has organically emerged from

unifying several methods and graphical languages which are used by developers and maintenance specialists from information systems domain, and also analysts responsible for risk analysis and risk mitigation activities for IT systems. The designed DSL (see Fig. 2) is based on approach to Unified Modelling Language (UML), CORAS method and Misuse Case Alignment Method [7, 8, 16, 17].

Currently, using UML is one of the most commonly used approaches in IT system modelling. The authors' experience acquired while working in IT and UML belongs to the group of graphical modelling languages. Initially UML was built for information systems modelling to facilitate the development and maintenance processes. Nowadays the usage of UML is broadened. This language is used for building business models, which exceed the initial task of modelling of information systems. Industry shows that UML modelling is used to some extent in all medium and large scale projects.

UML belongs to the group of graphical modelling languages. Initially UML was built for information systems modelling to facilitate the development and maintenance processes. Nowadays the usage of UML is broadened. This language is used for building business models, which exceed the initial task of modelling of information systems.

As regards system modelling, UML modelling is widely used at systems development or enhancement phases. UML modelling describes the structure and behaviour of the system. This language consists of graphical notations called diagrams and builds up an abstract model of a system. The UML standard is maintained by OMG (Object Management Group). In the beginning, UML was built for specification visualization and documentation of IT systems development. Nowadays usages of UML are not only limited to tasks of software engineering. UML is also used for business process modelling and for the development of systems which are not pure information systems.

Modelling with UML promotes model-driven technologies, such as Model Driven Development (MDD), Model Driven Engineering (MDE) and Model Driven Architecture (MDA). Supplementing graphical notations with terms such as class, component, generalization, aggregation and behaviour, helps save system designer's time for system architectural tasks and design.

A UML model consists of a set of diagrams. A diagram is a partial representation of the model. A system model could be divided into two parts. The first part is a functional model, which reflects functionality of a system from the system user's point of view. This kind of model is constructed using Use Case diagrams. The second part is the dynamical model that reflects internal behaviour of the system. A model of that kind is constructed using Activity, State, Sequence and Collaboration diagrams.

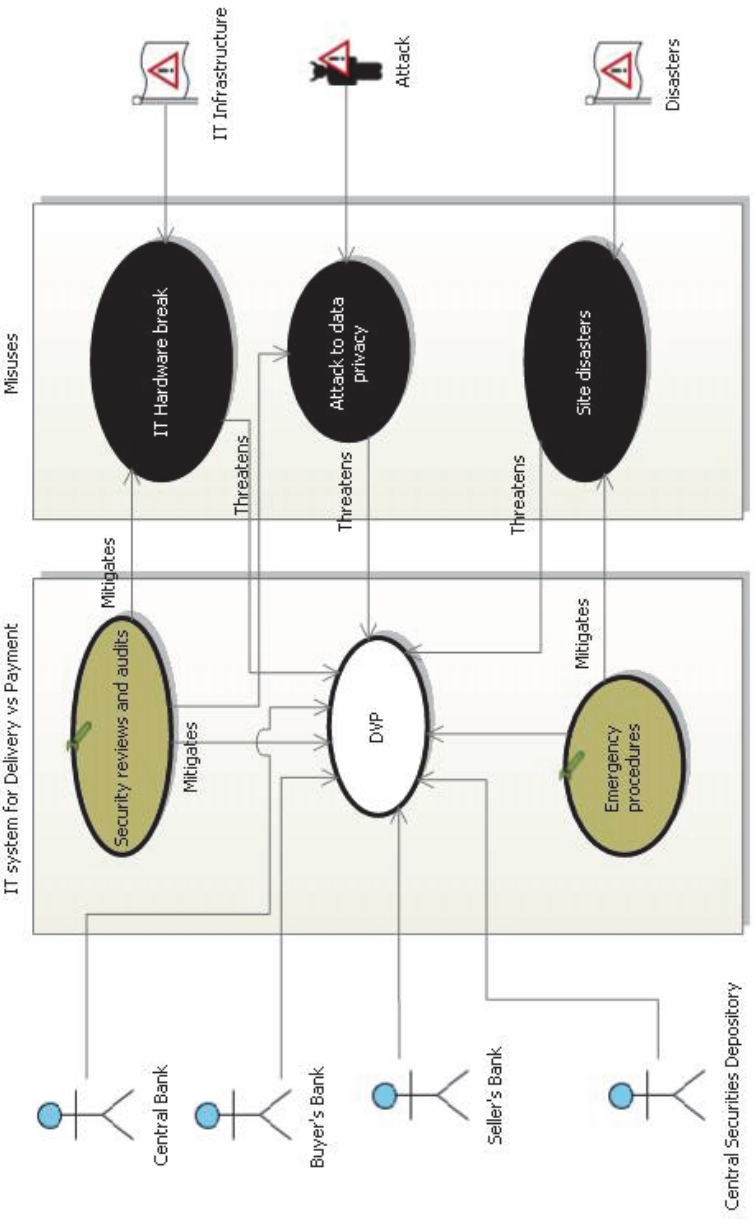


Fig. 2. DVP IT System Use cases

A system model to be created with UML language should not necessarily contain all diagrams. For example, when creating Information System vision model or requirement specification, it is enough for the system analyst to create Use Case and Activity diagrams. Use Case diagram answers a question – what a system does. Activity diagrams describe scenarios of every Use Case, i.e., Business processes. Therefore we prefer this work use only Use Case and Activity diagrams.

As mentioned above, IT industry use of UML is mostly directed to specification and documentation of a system [14].

The authors as representatives of simulationist community would like to improve this situation and to add more dynamic to this static construction. Obviously simulation of the model can give to developer's possibilities to evaluate and forecast behaviour of a target system. The authors already addressed this issue in [8]. During development of the presented DSL for IT risk analysis, which is based on UML, one of the objectives was possibility of simulation of a model. Activity Diagram elements are complemented with stochastic attributes for simulation purposes (Table 1).

Table 1. Stohastic attributes of Activity diagram

UML element	Stohastic attribute
Task	Duration
Branch	Decision probabilities
Timer	Start Delay
	Number of Events in group
	Delay between groups
	Number of Groups

One more approach for the developed DSL is application of Misuse Case in a UML Use Case model. Misuse cases improve UML diagrams with a better support to analyse problems of IT risk management. The *Use Case* diagram is extended with graphically black *Use case*, called *Misuse Case* and black *Actor* called *Misuser*. *Misusers* are related with *Misuse Case*. *Misuse cases* are related to *Use Cases* with relation <threatens>. During risk analysis stage *Use Case* diagrams are extended with additional *Use Cases* for risk mitigation, which are connected with system *Use Case* with relation <include> and with *Misuse Case* with relation <mitigate> (see Figure 2).

Considering that the task to be solved by the authors was to provide a government institution responsible for IT risk evaluation with

tools necessary for such tasks, the third technology used in this work is security risk modelling, analysis and documentation language CORAS. The initial CORAS approach was developed within the CORAS project funded by the European Commission that ran from 2001 until 2003. CORAS is both a language and a methodology for its application, described in the book [7]. Although initially CORAS was designed for security risk analysis, its syntax and semantics allows applying this language to complete IT risk analysis scope. In the developed prototype only one CORAS language diagram – the Treatment diagram – Is used. Treatment diagram is CORAS method all-inclusive diagram, in which all main risk analysis entities – *Threat*, *Vulnerability*, *Risk*, *Asset*, *Threat Scenario*, *Unwanted Incident* and *Treatment Scenario* are included. In turn, by methodology developed by the authors, *Unwanted Incident* is common entity, which connects risk analysis Treatment diagram with UML Activity diagram used in IT system Activity diagram model (see Figure 3).

Additionally, we did similar enhancements to CORAS Treatment diagram as we did with UML activity diagram. For simulation purposes, Treatment diagram is complemented with stochastic attributes (Table 2).

Table 2. Stohastic attributes of Treatment diagram

Diagramm element	Stohastic attribute
Relation between Risk and Asset	Impact
Unwanted incident	Used as connector between risk and system models. Transfer events from treatment scenario to system model. Event raises a disability of selected activity of a system model
	Duration of disability
TreatmentScenario	Start Delay
	Number of Threat events in group
	Delay between groups
	Number of Groups

Using the DSL described in the paper, a corresponding Activity diagram describing IT system functionality should be designed for each system Use case, a corresponding risk mitigation Activity diagram for each risk mitigation Use case should be designed, and Treatment diagram should be designed for each Misuse Case (see Figure 3).

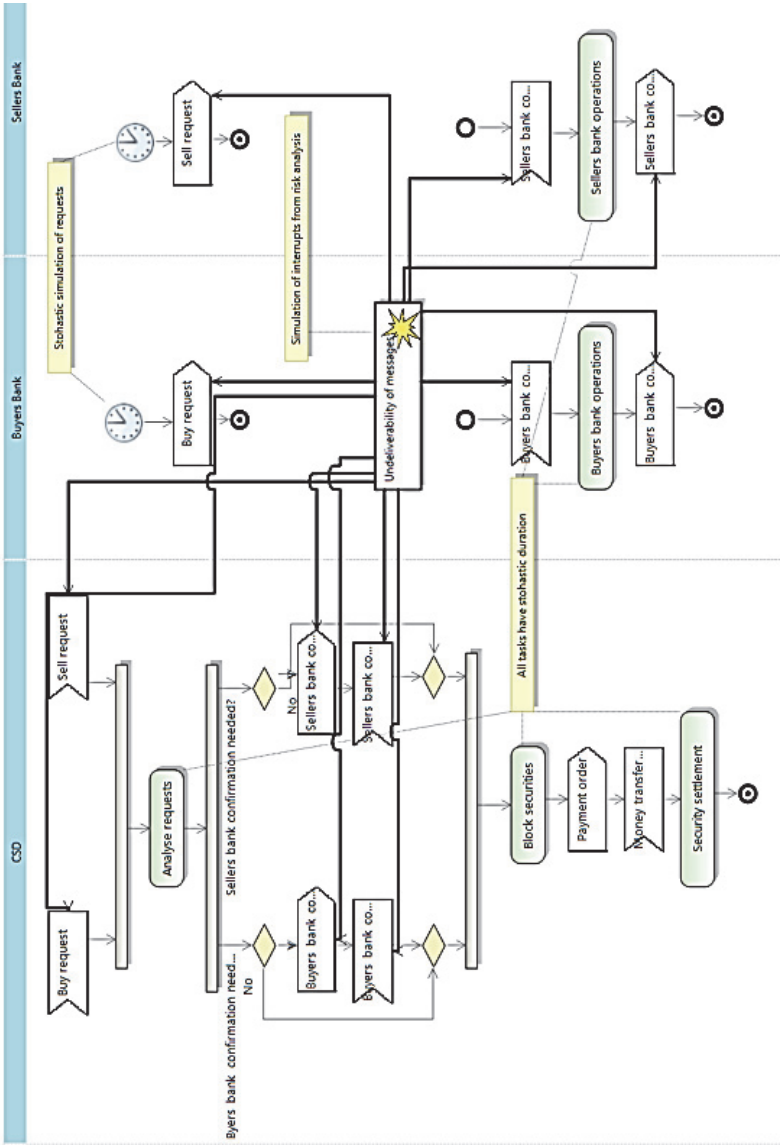


Fig.3. DVP Activity diagram

Simulation will allow to perform simulation experiments on two models simultaneously – the risk analysis model (see Figure 4) and IT system model (see Figure 3) and gather more adequate risk estimation results.

For such IT risk analysis approach, a tool prototype which is based on Microsoft Visualization and Modelling SDK (VMSDK) is developed while designing DSL. This implemented modelling tool is functioning inside Microsoft Visual Studio Shell. It could be distributed either with Microsoft Visual Studio Shell, or as Microsoft Visual Studio Add-In (see Figure 5). Additionally this approach ensures ability of simulation program code generation, compilation and execution for any Microsoft .NET Framework supported language. Specially designed templates ar used for code generation purposes, and they consist of code snippets for simulation of diagram elements. The authors currently are working on this solution.

Another approach is code generation from DSL diagrams for some general purpose simulation package (for example ARENA).

5. Reducing managerial risks by the use of disaster-tolerant CPS. Currently, there is a widespread of opportunities, provided by the Internet of Things and the Industrial Internet of Things both in terms of created systems of technologies and services, provided by these systems [18, 19]. In these conditions, ensuring the continuity of business-processes (BP) and improving disaster tolerance of relevant business-systems (BS) are one of the most important strategic directions of any organization (company) development. At the same time ubiquitous implementation of cyber physical systems as basic components and subsystems in existing and perspective information systems (IS), that make up the main core of large and commercial crucial infrastructure, leads to the need of giving them such an important system-cybernetic property as disaster tolerance [20]. Further, under the disaster tolerance of CPS should be understood the ability distributed computer complex, consisting of several CPS, to store critically important data and structure, and also continue to perform their functions after a massive (perhaps, purposeful) destruction of their components as a result of various cataclysms not only natural character, but also human-inspired [20–22]. This definition is accurately corresponds to the English term "Disaster Tolerance" (DT), but generally the term "Disaster Recovery" (DR) (literally "recovery after catastrophe") can also be translate as "Disaster Tolerance". The difference between DR and DT is that DR focuses on the security of data (with strictly controlled losses, if they unavoidable), and the means for continuing full-fledged work are in many cases assumed external to the actual disaster-tolerant part of the complex. Thus, the disaster tolerance of CPS supposes first of all ensuring the safety of data, and the possibility to recover the data after a major local or global cataclysm, and at the same time an appropriate level of reliability (traditional, "local", fault-tolerant) of all or critical subsystems is provided by the same means [20-22].

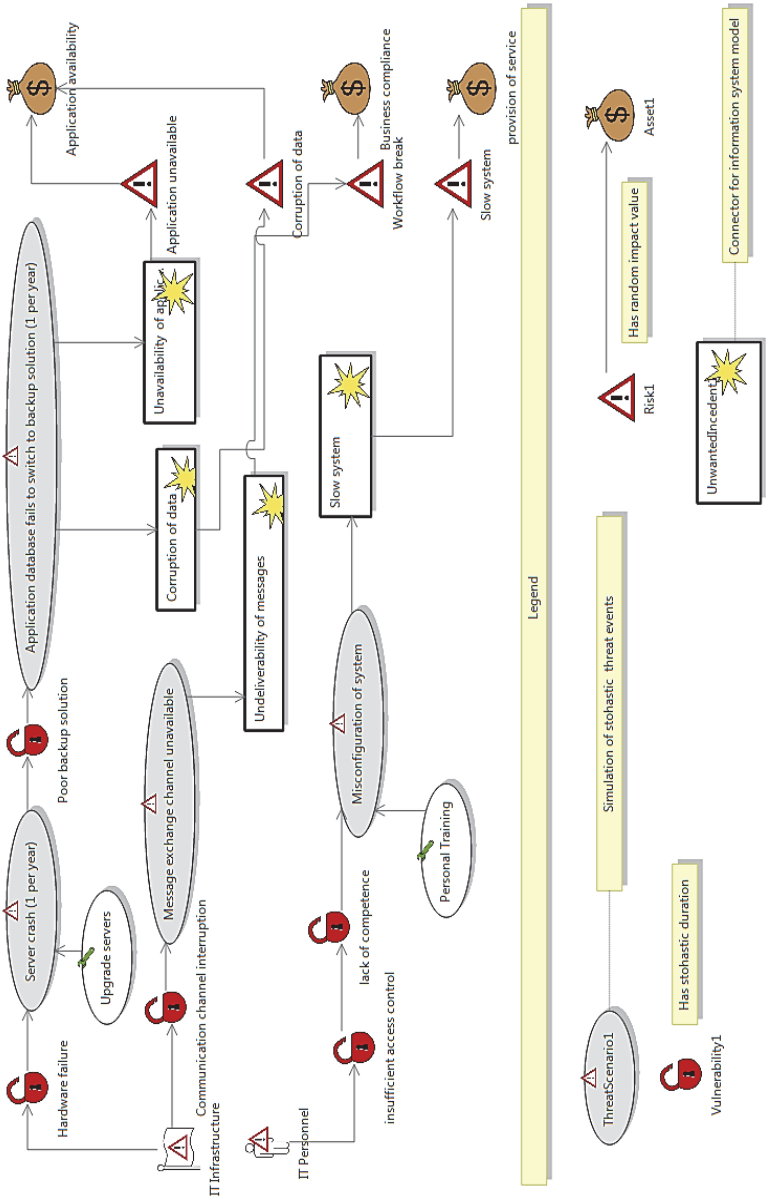


Fig. 4. Treatment diagram for IT Hardware break

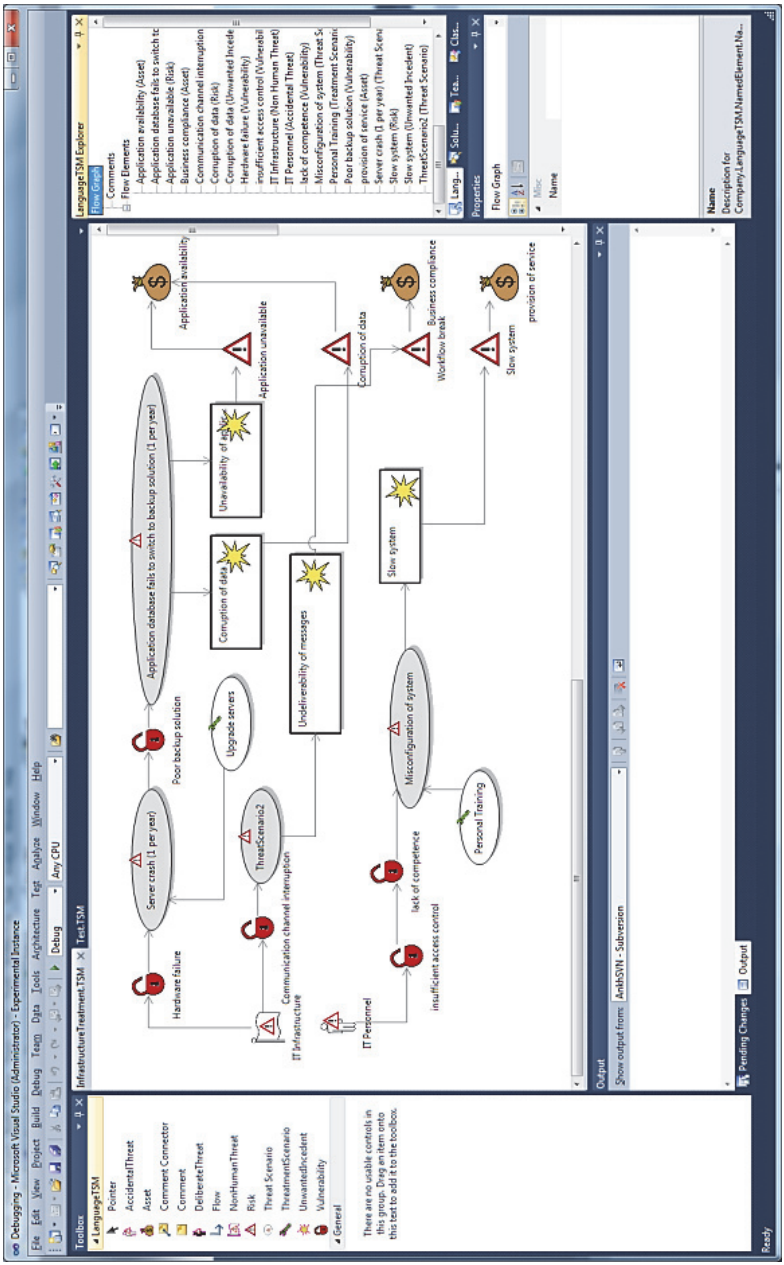


Fig. 5. IT risk analysis tool

As subsystems of modern corporate IS (CIS), which include the CFS, are distributed, in case of mass failures on one site, the main performance can be removed to another site. The listed features of disaster-tolerant CPS lead to the need for principally new approaches to solving bothproblems of creation and development of this class CPS, and the problem of assessing the managerial risks associated with their application, that is considered at this paper.

Studies have shown, that in order to neutralize threats and minimize losses caused by abnormal, emergency, extreme and catastrophic situations, leading to an avalanche-like increase in degradation processes and destruction of CPS, management of the relevant organizational structures, (business-systems (BS)) must be prepared in advance for the solution of at least the following five groups of interrelated problems [23]:

– identification of potential threats to possible emergencies due to socio-economic crises, natural and technogenic disasters, development of model options solutions for their prevention, localization and stabilization;

– development of proposals and draft decisions aimed at increasing sustainability objects of the BS infrastructure to the action of destabilizing and destructive factors possible emergencies;

– identify trends and early detection of potential threats, estimate and predicting the possibility of emergencies;

– prompt formation and justification of decisions on management of all types of CPS and BS resources as a whole in order to minimize the negative consequences of destructive and destabilizing factors in the conditions of the emerged emergency situation;

– assessment of the negative consequences of an emergency situation and the development of draft decisions, aimed at their elimination with minimal costs.

Preliminary analysis of problems and tasks that need to be solved at various stages of CPS life cycle and the existing theoretical methods and approaches to their solution shows that within the framework of the earlier developed theories and methodologies for managing complex systems, these issues, as a separate subject of research, from a single system-wide point vision was practically not considered. In this case, the subject area covering them has a number of significant features, radically different from the subject of research existing theories of managing complex systems. Among them you can specify, in particular following features [21, 23]:

– extreme and catastrophic situations, as a rule, are difficult to predict and arise suddenly (temporary uncertainty in the provision of readiness for management);

– the scale of the negative consequences associated with them is also difficult to predict; they can quickly increase over time and have various long-term negative consequences for heterogeneous, including territorially distributed objects (uncertainty boundaries and content of the subject area);

– information about such situations, as a rule, is contradictory and bad predictable in its composition and volume character and enters the management system with different time delays (uncertainty in the identification of current situations);

– decision making in such situations is carried out in conditions of a strict limit time, risks and various limitations in the options for selecting and implementing managers effects, etc.

Accounting for these and a number of other specific features of management processes of complex systems in emergency and catastrophic situations requires the development of fundamentally new, special principles and methods of monitoring, analysis and forecasting situations, developing options for management decisions, procedures for their selection and implementation.

Thus, for example, analysis shows that the principles and methods of traditional diagnostic systems are conceptually failures, faults, defects and oriented to diagnose the standard mode. This does not take into account a number of important properties of the dynamics of the functioning of complex objects in abnormal and critical conditions situations. In particular, the specificity of their probabilistic properties is not taken into account, the possibility sudden appearance of dynamic chaos in the form of disordered processes in deterministic systems, the "fine" structure of the dynamics of the mechanisms of aging and destruction materials and structures, as well as a number of other practically important properties of the dynamics of non-standard and critical situations. Many conceptual problems related to management of the structural dynamics of complex systems with their various degradations, assessments and forecasting of risks of occurrence of supernumerary and critical situations, and also risks selection and implementation of relevant management decisions, etc. [21, 23, 24].

In these conditions, it is necessary to investigate and solve the problems of ensuring the disaster tolerance of CPS within the framework of the interdisciplinary approach, interpreting them as tasks of structural dynamics control (SDC) of these systems. The tasks of SDC of CPS in its content belong to the class of problems of structural and functional synthesis of CPS shape and formation appropriate programs to manage their development (modernization). The main difficulty and singularity of

the class problems solution under consideration consists in the following. Determination of optimal programs and laws of main elements and subsystems of CPC management (planning) in a dynamically changing environment can only be carried out after the list of functions and algorithms of information processing and management becomes known, which should be implemented in the specified elements and subsystems. In its turn, the distribution of functions and algorithms for CPS elements and subsystems depends on the structure and parameters of the laws governing the management of these elements and subsystems. The difficulty of resolution this contradictory situation is aggravated by the fact that under the influence of various causes (objective, subjective, external and internal) over time, CPS composition and structure at various stages of its life cycle differs. By now the class of structural-functional synthesis tasks and management of CPS development has been investigated not deep enough. New scientific and practical results have been obtained in the following directions of research [21–24]: the synthesis of CPS technical structure under certain laws of functioning of the main CPS elements and subsystems (1st direction); synthesis of CPS functional structure, or, in another way, the synthesis of management programs of the CPS main elements and subsystems under the well-known CPS technical structure (2nd direction); of synthesis programs for the creation and development of new generations of CPS without taking into account the stage of joint functioning of the existing CPS and the implemented CPS. A number of iterative procedures for obtaining a joint solution of problems, the research of which is carried out within the framework of the 1 and the 2 directions. In general, all existing models and methods of CPS structural-functional synthesis appearance and the formation of programs for their development (modernization) are used in stages of external and internal design of CPS shape, i.e. when the time factor is not essential. However, in practice, when non-standard, critical and emergency situations in CPS, characterized by inaccurate and contradictory information, time becomes one of the most important parameters by means of which the effectiveness of activities, related to the maintenance and restoration of business processes.

Existing foreign and domestic business continuity planning tools (Business Continuity Planning) allow: using universal database architectures to simplify procedures for risk analysis and development plans for recovery and business continuity; simplify the processes of supporting current business continuity plans; synchronize and maintain up-to-date information using the interfaces of other applications; to adjust the management of the company taking into account business continuity plans.

At the same time, they do not provide for the comprehensive automation of the processes of managing the structural dynamics of CPS in order to improve their security, are poorly adapted to situations in which it is possible to create unrealistic abnormal situations.

Thus, at the present time it becomes very important to develop methodical and methodological foundations for the integrated automation of adaptive planning and scheduling of the modernization and operation of disaster-tolerant CPS based on the development of concepts, principles, models, methods and algorithms for analyzing and managing the structural dynamics of CPS in real conditions of incompleteness, uncertainty, inaccuracy and inconsistency of information about the emerging situation and in the presence of an unavoidable threshold time limitation on the cycle of the formation and implementation of solutions to prevent possible critical, emergency and extreme situations.

An important role in management theory development of complex organizational and organizational and technical systems in crisis situations should be given to issues of creation of appropriate model-algorithmic support for problem solving, planning and management of these systems under dynamically changing conditions.Resulting from what has been said so far, a conceptual scenarios of creation and functioning of CPS, possible approaches to organization and carrying out of complex modeling and multicriteria options estimation for the functioning of CPS under different conditions of the situation, as well as relevant risks of the choice of management decisions related to the application of both CPS and whole BS, in which they are included. In particular, the following list was proposed main CPS performance indicators: CPS availability indicators (total IS downtime for any reason, indicators that assess risks occurrence and development of accidents and disasters), indicators that assess the consequences of accidents and catastrophes for specific business processes (duration, scale and extent of damage), indicators that estimate the total time and completeness of the operations performed restoration of CPS working capacity, indicators evaluating, capital and operational costs to ensure the required level of catastrophic stability, costs of other types of resources, indicators assessing the degree of criticality of operations performed in CIS, the importance of resources and information used to provide the required level of disaster tolerance.

By now, a polimodel process description of creation and operation of disaster-tolerant CPS has been developed, providing work of the virtual enterprise (VE) in conditions of RFID technologies implementation. Part of this complex includes: deterministic and

stochastic static and dynamic models of CPS program management at various stages of their life cycle, allowing to describe both business processes performed within the framework of the VE, and processes of CPS modernization and functioning. Coordination of all listed models is based on the concepts and approaches developed by the proactive management theory of structural dynamics of complex technical objects (including CPS). Conducted preliminary analysis of the implementation of the concept of system modeling in the tasks of proactive CPS planning and scheduling shows the following advantages of joint use of the proposed static and logical-dynamic models of CPS proactive management:

– static models of CPS functioning allowed to take into account those factors (information losses, bandwidth limitations), which with dynamic modeling lead to the corresponding phase constraints;

– on the basis of static models, initial data are generated, dynamic model would not be possible (in this case, in fact, the aggregated variant of the technology of receiving, storing and processing data is determined);

– static models allowed, in the first approximation, to take into account the distribution and structural dynamics of the considered CPS, allowed to quantify the overall planned amount of data received, transmitted, processed or lost.

At the same time, a detailed description of the processes of information distribution and processing the operation of the VE with reference to specific time points in a static model is quite difficult. To do this, it was suggested to use a dynamic model of CPS functioning. In this case, the proposed dynamic description of the processes allows:

– to form and optimize such quality indicators of a manageable systemic dynamics (MSD) of CPS, which are difficult to describe in a static model (for example, estimating the uniformity (unevenness) of the use of CPS resources on the entire interval management and at each current time);

– to study the processes of CPS MSD involve an extremely rich mathematical apparatus of the theory of optimal control, allowing to solve a wide range of actual tasks of analysis and synthesis of management programs of CPS and its main subsystems.

In the Table 3 in its left part are the fundamental scientific results that have been obtained to date in modern management theory of complex technical objects. In the right part of this figure are those new scientific and applied results that were obtained within the framework of the developed theory of CPS proactive management, based on these fundamental scientific results.

Table 3. Results of a qualitative analysis of proactive management processes of disaster tolerant CPS

№	Contents and ways of implementing results	
	The main results of qualitative analysis of the management of complex technical objects (CTO)	Ways of results implementation
1	Analysis of the solutions existence in control problems of CTO	Checking the adequacy of the description of cyber physical systems (CPS) proactive management
2	Conditions for controllability and attainability in control problems of CTO	Verification of the feasibility of CPS control technology. Identifying the main factors (constraints) affecting the indicators of the target and information technology capabilities of CPS
3	The uniqueness condition for optimal programmed controls in the tasks of planning the operation of CTO	Assessment of the possibility of obtaining optimal plans for CPS use
4	Necessary and sufficient conditions for optimality in control problems of CTO	Preliminary analysis of the structure of optimal program management, obtaining basic relationships for constructing scheduling algorithms of CPS application
5	Stability and sensitivity conditions in control problems	Estimation of stability (sensitivity) of CPS proactive management to disturbing effects, to a change in the composition and structure of the initial data, calculation of management risk indicators

6. Conclusions. The current situation within business indicates the necessity for more complicated and more effective IT risk management system development. In the presented paper the given approach allows to perform IT risk analysis which is based on the unified IT system model specification. In this way the one window approach is realised for both system developers and maintainers and for those responsible for the security policy of a system. The presented DSL and modelling based tool are in design stage. Further work will be performed to improve the Domain specific language. The second group of further activities will be devoted to implementation of an appropriate simulation engine, including generation of experimental frames from available business data and maschine learning approaches for model parameter finetuning. Model repository and tools for storing and processing simulation results will be developed for domain specific decision support.

This approach will be approved on state-wide IT systems and Industry 4.0 solutions.

References

1. Biro M., Mashkoor A., Sametinger J., Seker R. Software Safety and Security Risk Mitigation in Cyber-physical Systems. *IEEE Software*. 2018. vol. 35. no. 1. pp. 24–29.
2. Hu F. Cyber-Physical Systems: Integrated Computing and Engineering Design. New York: CRC Press. 2018. 398 p.
3. Romanovs A. Security in the Era of Industry 4.0. 2017 Open Conference of Electrical, Electronic and Information Sciences (eStream). 2017. 1 p.
4. Klimov R., Reznik A., Solovjova I., Slihte J. The Development of the IT Risk Management Concept. *Computer Science*. 2008. vol. 5. pp. 131–139.
5. Romanovs A., Merkuryev Y., Klimov R., Solovjova I.A Technique for Operational IT Risk Management in Latvian Monetary and Financial Institutions. Proc. of 8th WSEAS International Conference on Applied Computer Science «Recent Advances on Applied Computer Science». 2008. pp. 230–235.
6. Teilans A. et al. Domain Specific Simulation Language for IT Risk Assessment. Proceedings 25th European Conference on Modelling and Simulation (ECMS2011). 2011. pp. 342–347.
7. Lund M.S., Solhaug B., Stølen K. Model-Driven Risk Analysis: The CORAS Approach. Springer. 2010. 460 p.
8. Kleins A., Merkuryev Y., Teilans A., Filonik M. A meta-model based approach to UML modelling and simulation. Proceedings of the 7th International Conference on System Science and Simulation in Engineering. 2008. 6 p.
9. Skorobogatjko A., Romānovs A., Kuņicina N. State of the Art in the Healthcare Cyber-physical Systems. *Information Technology and Management Science*. 2014. vol. 17. pp.126–131.
10. Cyber-Physical Systems. Available at: https://ptolemy.berkeley.edu/projects/cps/ (accessed: 11.02.2018).
11. Patterson D.A., Hennessy J.L. Computer Organization and Design: The Hardware/Software Interface: 5th ed. Morgan Kaufmann. 2013. 800 p.
12. Milenkovic A., Otto C., Jovanov E. Wireless sensor networks for personal health monitoring: issues and an implementation. *Computer Communications*. 2006. vol. 29. no. 13-14. pp. 2521–2533.
13. Buyya R., Broberg J., Goscinski A. Cloud Computing: Principles and Paradigms. John Wiley & Sons 2010. 637 p.
14. Achim D., Brucker J.D. Metamodel-based UML notations for domain-specific languages. Proceeding of 4th International Workshop on Language Engineering (ATEM 2007). 2007. 15 p.
15. Lenz G., Wienands C., Greenfield J., Kozaczynski W. Practical software factories in. NET. New York: Apress. 2006. 214 p.
16. Sindre G., Opdahl A.L. Eliciting Security Requirements by Misuse Cases. *Requirements engineering*. 2005. vol. 10. no. 1. pp. 34–44.
17. Matulevicius R., Mayer N., Heymans P. Alignment of misuse cases with security risk management. Third International Conference on Availability, Reliability and Security (ARES 08). 2008. pp. 1397–1404.
18. Kupriyanovskij V.P., Namiot D.E., Sinyagov S.A. [Cyber-physical systems as the basis of the digital economy]. *International Journal of Open Information Technologies*. 2016. vol. 4. no. 2. pp. 18–24. (In Russ.).
19. Wolf W. Cyber-physical systems. *Computer*. 2009. vol. 3. pp. 88–89.
20. Belenkov V.G., Budzko V.I., Sinicyn I.N. *Katastrofoustojchivost' korporativnyh informacionnyh sistem* [Catastrophic stability of corporate information systems]. Part 1. M.: IPI RAN. 2002. (In Russ.).
21. Belov P.G. *Sistemnyj analiz i modelirovanie opasnyh processov v tekhnosfere: Uchebnoe posobie dlya stud. vyssh. ucheb. zaedenij* [System analysis and modeling of dangerous processes in the technosphere: Textbook for students of higher educational institutions]. M.: Izdatel'skij centr «Akademiya». 2003. 512 p. (In Russ.).

22. Budzko V.I., Belenkov V.G., Kejer P.A. [Problems of Creation of Disaster-Tolerant Automated Systems of Banking Settlements]. *Sistemy i sredstva informatiki — Systems and Means of Informatics*. 2002. vol. 12. pp. 48–57. (In Russ.).
23. Yusupov R.M. et al. [New scientific direction in creating technologies for situational management in emergency situations]. *Trudy Mezhdunarodnaoj Nauchnaoj SHkoly «Modelirovanie i Analiz Bezopasnosti i Riska v Slozhnyh Sistemah (MA BR-2007)»* [Proceedings of the International Scientific School "Modeling and Analysis of Security and Risk in Complex Systems (MA BR-2007)"]. 2007. pp. 94–99. (In Russ.).
24. Ohtilev M.Ju., Sokolov B.V., Jusupov R.M. *Intellektual'nye tehnologii monitoringa i upravlenija strukturnoj dinamikoj slozhnyh tehnicheskih ob'ektov* [Intellectual technologies of monitoring and management of complex technical objects structural dynamics] M.: Nauka. 2006. 410 p. (In Russ.).

Teilans Artis Andreevich — Ph.D., Dr. Sci., professor, head of information and communications technologyresearch centre, Rezekne Academy of Technologies. Research interests: software engineering, discrete event computer simulation, design of domain specific languages. The number of publications — 25. artis.teilans@rta.lv; 115, Atbrivosanas aleja, LV-5001, Latvia; office phone: +37126529669.

Romanovs Andrejs Vasil'evich — Ph.D., Dr. Sci., associate professor, deputy head of the modelling and simulation department of Institute of information technology, Riga Technical University. Research interests: modeling and design of management and industrial information systems, cybersecurity, IT governance and IT risk management, information systems for health care, e-commerce, integrated information technologies in business of logistics, as well as education in these areas.. The number of publications — 79. andrejs.romanovs@rtu.lv; 1, Kalku street, LV-1658, Riga, Latvia; office phone: +37167089514, Fax: +37167089513.

Merkuryev Yuri Anatolievich — Dr. Habil., professor, Academician of the Latvian Academy of Sciences, head of the modelling and simulation department of Institute of information technology, Riga Technical University. Research interests: modelling and simulation of complex systems, methodology of discrete-event simulation, supply chain simulation and management. The number of publications — 357. jurijs.merkurjevs@rtu.lv, http://www.itl.rtu.lv/mik/ymerk.html; 1, Kalku street, LV-1658, Riga, Latvia; office phone: +37129454253, Fax: +37167089513.

Dorogovs Pjotrs Petrovich — chief of information centre, Ministry of Interior of Republic of Latvia. Research interests: architecture modeling of integrated information systems, governance of IT, cybersecurity. The number of publications — 20. Pjotrs.dorogovs@inbox.lv; 1, Kalku str., LV-1658, Riga, Latvia; office phone: +37167089514.

Kleins Arnis Yanovich — software developer, Computer Hardware Design Ltd. Research interests: software engineering, discrete event computer simulation, design and development of domain specific languages. The number of publications — 12. arnis12321@gmail.com; 17, Draudzibas iela, LV-5001, Ogre, Latvia; office phone: +37129491955.

Potryasaev Semen Alekseevich — Ph.D., senior researcher of laboratory for information technologies in systems analysis and modeling, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS). Research interests: system analysis and operations research, theory of managing the structural dynamics of complex organizational and technical systems. The number of publications — 90. spotryasaev@gmail.com, http://litsam.ru; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328-0103, Fax: +7(812)328-4450.

Acknowledgements. The research described in Section 5 supported by the state research #0073–2018–0003 (# of state registr. AAAA-A16-116030250074–1).

УДК 004 **DOI** 10.15622/sp.59.5

А.А. Тейланс, А.В. Романов, Ю.А. Меркурьев, П. Дорогов,
А.Я. Клейнс, С.А. Потрясаев

ОЦЕНКА РИСКОВ КИБЕРФИЗИЧЕСКИХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ МОДЕЛИРОВАНИЯ ДОМЕНОВ И ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ

Тейланс А.А., Романов А.В., Меркурьев Ю.А., Дорогов П.П., Клейнс А.Я., Потрясаев С.А.
Оценка рисков киберфизических систем с использованием моделирования доменов и имитационного моделирования.

Аннотация. В настоящее время системы, разрабатываемые для интеграции реальных физических процессов и виртуальных вычислительных процессов — киберфизических систем (КФС), используются во многих областях промышленности и национальной инфраструктуры, таких как производство, медицина, управление транспортом и безопасность, автомобилестроение, управление промышленными процессами, энергосбережение, экологический менеджмент, промышленные роботы, управление технической инфраструктурой, распределенные роботизированные системы, целевые системы защиты, технологии нанотехнологий и биологических систем. При широком использовании подобных систем уровень ИТ-рисков и киберрисков резко возрастает, в результате чего атаки против КФС могут привести к неуправляемым и непредсказуемым последствиям. Таким образом, существует необходимость в хорошо продуманной системе оценки рисков КФС, что обеспечит общее представление о состоянии безопасности КФС, а также эффективное распределение защищаемых ресурсов. Характер КФС отличается от ИТ-систем главным образом потребностью в операциях реального времени, поэтому традиционный метод оценки рисков для ИТ-систем может быть адаптирован для условий работы КФС. Разработка языка моделирования доменов (“domain specific language”, DSL), основанного на унифицированном языке моделирования UML и описанного в данной статье, обеспечивает синергизм широко используемой в ИТ-индустрии методики с используемыми в конкретных областях подходами к управлению рисками. В отличие от традиционного использования UML для целей имитационного моделирования, описанный в статье язык моделирования DSL обогащен набором стохастических атрибутов моделируемых процессов. Подобные стохастические атрибуты можно использовать для дальнейшей реализации дискретно-событийных симуляторов.

Ключевые слова: киберфизические системы, информационные технологии, риски, оценка рисков, язык моделирования доменов, моделирование, UML, CORAS, катастрофоустойчивые киберфизические системы, структурная динамика.

Тейланс Артис Андреевич — д-р техн. наук, профессор, руководитель научно-исследовательского центра информационных и коммуникационных технологий, Резекненская технологическая академия. Область научных интересов: программная инженерия, имитационное моделирование дискретно-событийных систем, разработка доменно-специфичных языков программирования. Число научных публикаций — 25. artis.teilans@rta.lv; аллея Освобождения, 115, LV-4601, Резекне, Латвия; р.т.: +37126529669.

Романов Андрей Васильевич — д-р техн. наук, доцент, заместитель заведующего кафедрой имитационного моделирования института информационных технологий, Рижский технический университет. Область научных интересов: моделирование и проектирование управленческих и индустриальных информационных систем,

кибербезопасность, управление ИТ и рисками, информационные системы для здравоохранения, электронная коммерция, интегрированные ИТ в логистике и цепях поставок, а также образование в этих областях. Число научных публикаций — 79. andrejs.romanovs@rtu.lv; ул. Калкю, 1, LV-1658, Рига, Латвия; р.т.: +37167089514, Факс: +37167089513.

Меркурьев Юрий Анатольевич — Dr. Habil., профессор, академик Латвийской академии наук, заведующий кафедрой имитационного моделирования института информационных технологий, Рижский технический университет. Область научных интересов: имитационное моделирование сложных систем, методология дискретно-событийного имитационного моделирования, моделирование логистических систем и цепей поставок и управление ими. Число научных публикаций — 357. jurijs.merkurjevs@rtu.lv, http://www.itl.rtu.lv/mik/ymerk.html; ул. Калкю, 1, LV-1658, Рига, Латвия; р.т.: +37129454253, Факс: +37167089513.

Дорогов Пётр Петрович — начальник информационного центра, Министерство внутренних дел Республики Латвия. Область научных интересов: моделирование архитектур интегрированных информационных систем, управление ИТ, кибербезопасность. Число научных публикаций — 20. Pjotrs.dorogovs@inbox.lv; ул. Калкю, 1, LV-1658, Рига, Латвия; р.т.: +37167089514.

Клейнс Арнис Янович — разработчик программного обеспечения, Computer Hardware Design Ltd. Область научных интересов: программная инженерия, имитационное моделирование дискретно-событийных систем, разработка доменно-специфичных языков программирования. Число научных публикаций — 12. arnis12321@gmail.com; ул. Драудзибас, 17, LV-5001, Огре, Латвия; р.т.: +37129491955.

Потрясаев Семен Алексеевич — к-т техн. наук, старший научный сотрудник лаборатории информационных технологий в системном анализе и моделировании, Федеральное государственное бюджетное учреждение науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: системный анализ и исследование операций, теория управления структурной динамикой сложных организационно-технических систем. Число научных публикаций — 90. spotryasaev@gmail.com, http://litsam.ru; 14-я линия В.О., 39, Санкт-Петербург, 199178; р.т.: +7(812)328-0103, Факс: +7(812)328-4450.

Поддержка исследований. Результаты исследований, представленные в разделе 5, осуществлялись при финансовой поддержки госбюджетной темы №0073–2018–0003 (№ гос. регистр. АААА-А16-116030250074–1).

Литература

1. *Biro M., Mashkoor A., Sametinger J., Seker R.* Software Safety and Security Risk Mitigation in Cyber-physical Systems // IEEE Software. 2018. vol. 35. no. 1. pp. 24–29.
2. *Hu F.* Cyber-Physical Systems: Integrated Computing and Engineering Design // New York: CRC Press. 2018. 398 p.
3. *Romanovs A.* Security in the Era of Industry 4.0 // 2017 Open Conference of Electrical, Electronic and Information Sciences (eStream). 2017. 1 p.
4. *Klimov R., Reznik A., Solovjova I., Slihte J.* The Development of the IT Risk Management Concept // Computer Science. 2008. vol. 5. pp. 131–139.
5. *Romanovs A., Merkuryev Y., Klimov R., Solovjova I.A* Technique for Operational IT Risk Management in Latvian Monetary and Financial Institutions // Proc. of 8th WSEAS International Conference on Applied Computer Science «Recent Advances on Applied Computer Science». 2008. pp. 230–235.

6. *Teilans A. et al.* Domain Specific Simulation Language for IT Risk Assessment // Proceedings 25th European Conference on Modelling and Simulation (ECMS2011). 2011. pp. 342–347.
7. *Lund M.S., Solhaug B., Stølen K.* Model-Driven Risk Analysis: The CORAS Approach // Springer. 2010. 460 p.
8. *Kleins A., Merkuryev Y., Teilans A., Filonik M.* A meta-model based approach to UML modelling and simulation // Proceedings of the 7th International Conference on System Science and Simulation in Engineering. 2008. 6 p.
9. *Skorobogatjko A., Romānovs A., Kuņicina N.* State of the Art in the Healthcare Cyber-physical Systems // Information Technology and Management Science. 2014. vol. 17. pp. 126–131.
10. Cyber-Physical Systems. URL: https://ptolemy.berkeley.edu/projects/cps/ (дата обращения: 11.02.2018).
11. *Patterson D.A., Hennessy J.L.* Computer Organization and Design: The Hardware/Software Interface: 5th ed. // Morgan Kaufmann. 2013. 800 p.
12. *Milenkovic A., Otto C., Jovanov E.* Wireless sensor networks for personal health monitoring: issues and an implementation // Computer Communications. 2006. vol. 29. no. 13-14. pp. 2521–2533.
13. *Buyya R., Broberg J., Goscinski A.* Cloud Computing: Principles and Paradigms // John Wiley & Sons. 2010. 637 p.
14. *Achim D., Brucker J.D.* Metamodel-based UML notations for domain-specific languages // Proceeding of 4th International Workshop on Language Engineering (ATEM 2007). 2007. 15 p.
15. *Lenz G., Wienands C., Greenfield J., Kozaczynski W.* Practical software factories in. NET // New York: Apress. 2006. 214 p.
16. *Sindre G., Opdahl A.L.* Eliciting Security Requirements by Misuse Cases // Requirements engineering. 2005. vol. 10. no. 1. pp. 34–44.
17. *Matulevicius R., Mayer N., Heymans P.* Alignment of misuse cases with security risk management // Third International Conference on Availability, Reliability and Security (ARES 08). 2008. pp. 1397–1404.
18. *Куприяновский В.П., Намиот Д.Е., Синягов С.А.* Кибер-физические системы как основа цифровой экономики // International Journal of Open Information Technologies. 2016. vol. 4. no. 2. pp. 18–24.
19. *Wolf W.* Cyber-physical systems // Computer. 2009. vol. 3. pp. 88–89.
20. *Беленков В.Г., Будзко В.И., Синицын И.Н.* Катастрофоустойчивость корпоративных информационных систем. Часть 1 // М.: ИПИ РАН. 2002.
21. *Белов П.Г.* Системный анализ и моделирование опасных процессов в техносфере: учебное пособие для студ. высш. учеб. заведений // М.: Издательский центр «Академия». 2003. 512 с.
22. *Будзко В.И., Беленков В.Г., Кейер П.А.* Проблемы создания катастрофоустойчивых автоматизированных систем банковских расчетов // Системы и средства информатики. 2002. Вып. 12. С. 48–57.
23. *Юсупов Р.М. и др.* Новое научное направление в создании технологий ситуационного управления в чрезвычайных ситуациях // Труды Международной Научной Школы «Моделирование и Анализ Безопасности и Риска в Сложных Системах (МА БР-2007)». 2007. С. 94–99.
24. *Охтилев М.Ю., Соколов Б.В., Юсупов Р.М.* Интеллектуальные технологии мониторинга и управления структурной динамикой сложных технических объектов // М.: Наука. 2006. 410 с.

УДК 681.883 **DOI** 10.15622/sp.59.6

А.С. Миронов, Е.С. Фомина

МЕТОДЫ ОБРАБОТКИ СИГНАЛОВ В ГИДРОЛОКАЦИОННЫХ СИСТЕМАХ ПРИ РЕШЕНИИ ЗАДАЧИ ЗОНДИРОВАНИЯ ДОННОЙ ПОВЕРХНОСТИ

Миронов А.С., Фомина Е.С. **Методы обработки сигналов в гидролокационных системах при решении задачи зондирования донной поверхности.**

Аннотация. В статье рассматриваются вопросы обработки гидроакустических данных, регистрируемых с помощью гидроакустических исследовательских комплексов. Особое внимание уделено обзорным и интерферометрическим гидролокаторам. Проведен анализ существующих решений по теме исследования, отмечены основные результаты, достигнутые российскими коллективами разработчиков-исследователей. В соответствии с нормативной документацией определены минимально допустимые погрешности измерений при формировании карт донной поверхности для различных хозяйственных отраслей.

В качестве одной из важных проблем, влияющих на эффективность проведения обзорных работ с помощью гидролокационных комплексов авторами определяется проблема сжатия первичных данных, которая, как правило, приводит к потере информации без возможности ее восстановления. Указанные недостатки применяемых в комплексах методов сжатия-восстановления первичной информации и обработки гидроакустических данных снижают общую эффективность применения комплексов как при использовании обзорного гидролокатора, так и при использовании интерферометрического гидролокатора бокового обзора. Следует отметить, что указанная авторами проблема характерна исключительно при использовании в качестве зондирующих импульсов простых тональных сигналов. В рамках численного эксперимента показано, что использование в качестве зондирующих импульсов сигналов с линейно-частотной модуляцией позволяет достаточно эффективно применять комплекс в режиме обзорного гидролокатора.

Приведены результаты численного эксперимента для оценки пространственного положения объекта на дне по гидролокационным изображениям с применением информации о разнице фаз принимаемых сигналов при использовании интерферометрического гидролокатора. На основании результатов эксперимента определены требования для качества регистрации отраженных сигналов различного типа в интерферометрических гидролокаторах бокового обзора.

Авторами предложен способ разрешения отраженных (с частичным перекрытием и наложением) гидроакустических тональных сигналов, основанный на методе деления спектров. Для повышения эффективности при обработке сигналов с линейно-частотной модуляцией авторами предлагается улучшать точность определения момента обнаружения сигнала за счет корректировки по фазе, рассчитанной через наклон скорости изменения частоты модулированного сигнала.

Ключевые слова: интерферометрический гидролокатор, гидролокатор бокового обзора, гидроакустика, тональный сигнал, ЛЧМ, обработка сигналов.

1. Введение. Для проведения исследований при экологическом мониторинге, подводном строительстве и картировании водоемов основными средствами получения информации являются гидроакустические комплексы. В состав комплексов могут входить

гидролокаторы бокового обзора (ГБО), многолучевые эхолоты, профилографы, системы позиционирования и сенсоры движения. Такие комплексы могут использоваться автономно на подводных (АНПА) и надводных необитаемых аппаратах либо в составе исследовательского судна.

Разработкой подобных комплексов занимаются крупнейшие лаборатории по всему миру. На сегодняшний день в России разработка и испытание таких комплексов ведется в ряде организаций, в том числе в лабораториях на базе НИИП им. В.В. Тихомирова, Института радиотехники и радиоэлектроники им. В.А. Котельникова РАН, ЦНИИ «Океанприбор» и Института проблем морских технологий ДВО РАН.

НИИП имени В.В. Тихомирова занимается разработкой интерферометрических гидролокаторов бокового обзора (ИГБО), а также проведением натурных испытаний. В статье [1] представлены результаты получения и обработки данных с ИГБО Неман-500, проведенных на полигоне института. В работе [2] сотрудниками НИИП им. В.В. Тихомирова произведено теоретическое обоснование выбора параметров съемки ИГБО, рассмотрена геометрия распространения акустических волн с учетом особенностей их распространения в водной среде. Таким образом, погрешность измерения высоты объекта на дне может быть вычислена следующим образом:

$$\sigma_Z^2 = \sigma_{Z\varphi}^2 + \sigma_{ZH}^2 + \sigma_R^2, \quad (1)$$

где $\sigma_{Z\varphi}^2$, σ_{ZH}^2, σ_R^2 — дисперсии оценки ординаты элемента разрешения на дне водоема из-за погрешностей интерферометрической разности фаз, измерения глубины и расстояния до элемента разрешения. Данные вычисления не оценивают зависимость точности определения относительного положения объекта на дне от точности обнаружения прихода отраженного сигнала на приемник.

В соавторстве с сотрудниками Института радиотехники и радиоэлектроники им. В.А. Котельникова сотрудниками НИИП им. В.В. Тихомирова было опубликовано несколько результатов [3-4] использования интерферометрического гидролокатора производства ЦНИИ «Океанприбор» и многолучевого эхолота, а также собственной разработки Института радиотехники и радиоэлектроники им. В.А. Котельникова — многофункционального гидролокационного комплекса «Кедр». По результатам исследований сделан вывод о содержании осадков на дне водоема и типе грунта, произведена компенсация качки судна-носителя ИГБО. В работе [5] проводится

сравнение батиметрических данных, полученных при зондировании одного участка многолучевым эхолотом (МЛЭ) и ИГБО. Согласно представленным в статье результатам, на средних глубинах около 110 метров (район в Балтийском море) с расчлененными формами рельефа, разброс в измерениях МЛЭ и ИГБО на некоторых участках составляет 2 метра, что около 2% от глубины водоема. Для донной поверхности со сложносочлененным рельефом отличие в определении глубины этими устройствами на некоторых участках достигает 2,5 метров при глубине водоема от 75 до 160 метров, также приведены данные для измерений на полигоне, в условиях которого на глубинах до 40 метров ошибка достигает менее 1%. Однако авторами не приводится методика определения глубин водоема, что не позволяет произвести оценку достоверности получаемых данных.

Институт Проблем морских технологий ДВО РАН занимается разработкой систем управления и навигации подводными аппаратами и их системами, а также разработкой автономных и буксируемых аппаратов для выполнения комплексной гидролокационной съемки. За последние годы в Институте было разработано несколько роботизированных комплексов («Галтель», «Марк», «Клавесин» и др). Также одним из направлений работы сотрудников Института является обнаружение объектов на дне по информации с ГБО-снимков, что является непростой задачей, решение которой зависит от структуры дна, формы объекта, его расположения и звукоотражающих свойств поверхности. Для уточнения данной информации сотрудники Института предлагают проводить дообследования средствами телевизионной системы, модернизацию ГБО дополнительными приемниками и использование его в качестве ИГБО [6].

Еще одним направлением работы ИПМТ ДВО РАН является разработка методов обработки гидроакустических сигналов для целей улучшения качества отображения обстановки на дне. В работах [7-8] рассматриваются задачи улучшения качества гидролокационных изображений путем восстановления принимаемого гидроакустического сигнала. Известно, что гидроакустический канал достаточно специфичный вследствие нестационарности, рефракции и других физических эффектов, проявляющихся в виде многолучевости и интерференции. Это приводит к сильным искажениям передаваемой информации или даже к полной ее потере. Авторами предлагается для улучшения качества регистрируемого сигнала использовать интерполяционные методы и методы двойной фильтрации, однако вопрос достоверности получаемых с ИГБО данных и ее зависимость от ошибки регистрации сигнала в гидроакустическом канале освещен слабо.

Всеми научными коллективами, проводящими исследования в данной области, выделяется перспективность использования обзорных и интерферометрических гидролокаторов для определения пространственного положения объектов на дне водоема. Однако проблема повышения точности реконструируемой модели дна по информации с ИГБО освящена недостаточно, в отдельных работах предоставляется сравнение получаемых карт дна с аналогичными, полученными в результате зондирования донной поверхности МЛЭ. Также в исследованиях не затронут вопрос прямой зависимости качества обследования дна от погрешности детектирования отраженного сигнала. Известно, что при выполнении мониторинга объектов инфраструктуры, имеющих подводные переходы, а также портовых сооружений, необходимая точность замеров составляет 10 сантиметров, что чаше всего менее 1% от глубины водоема. Недостаточность информации в приведенных выше статьях приводит к невозможности реализации готового устройства, удовлетворяющего выдвигаемым требованиям точности реконструкции донной поверхности [10-12]. Согласно этим источникам, необходима следующая точность определения пространственного положения объектов для различных хозяйственных отраслей:

1) Для нефтегазовой отрасли (проверка состояний подводных переходов нефтепроводов), исходя из нормы проседания трубопровода, — 0,1 метра по глубине.

2) Для строительства мостов, исходя из нормы точности установки опорных закладных деталей — 0,1 метра в поперечном направлении и 0,25-0,5 метра в продольном направлении конструкции, кривизна — не более 0,15 метра на каждые 2 метра.

3) Для эксплуатации портовых сооружений и причалов, промеры выполняются с точностью 0,1 метра для глубин до 10 метров, свыше — 0,2 метра. При детальном обследовании навигационных опасностей — до 0,05 метра по глубине и дальности.

Таким образом, необходимое разрешение гидроакустической съемки должно быть не хуже 0,1 метра по глубине и дальности, что говорит о том, что проблема повышения точности построения реконструкции дна интерферометрическим ГБО для нужд инженерно-строительной и инфраструктурных сфер стоит достаточно остро.

2. Сжатие гидроакустических сигналов. Следует отметить, что в некоторых гидроакустических средствах применяют алгоритмы сжатия и восстановления сигнала. Рассмотрим алгоритм сжатия, применяемый в ИГБО «Гидра» со следующими характеристиками:

рабочие частоты – 100-700 кГц (ГБО), 620-790 (эхолот); дальность — до 300 метров на каждый борт, суммарная полоса обзора — 550 метров; диапазон глубин – до 70 метров (ГБО), до 120 метров (эхолот). Для тональных сигналов в комплексе предусмотрен способ сжатия и предоставления пользователю сырой информации для последующей обработки, основанный на предположении, что каждый период простого сигнала может быть восстановлен по двум значениям мгновенной амплитуды, условно названными Re и Im, и фазе между ними. Ниже описан процесс восстановления зондирующего отраженного импульса.

Введены следующие обозначения: f_0 — частота оцифровки — частота следования значений $\mathrm{Re}-\mathrm{Re}$ и $\mathrm{Im}-\mathrm{Im}$; $f_н$ — несущая частота зондирующего импульса; f_d — частота дискретизации, период которой определяет величину отставания значения мгновенной амплитуды Im от Re. На рисунке 1 наглядно представлен процесс сжатия и восстановления сигнала в комплексе, где t_0 и t_d — период частоты оцифровки и частоты дискретизации соответственно, а $t_н$ — период несущей частоты. В зависимости от параметров обследуемой акватории, в комплексе предусмотрен выбор из нескольких конфигураций параметров зондирующего импульса. В дальнейшем при моделировании в работе рассматривается случай, когда частота сигнала $f_н$ выше f_0 в 1,15 раза, а $f_d / f_н = 4$.

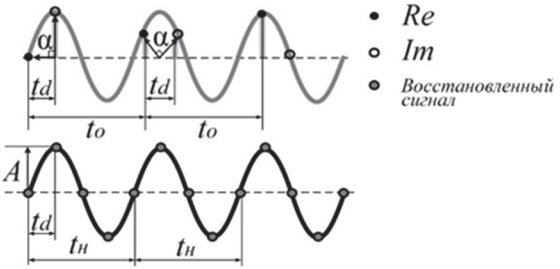


Рис. 1. Сжатие регистрируемого тонального сигнала в комплексе «Гидра

Амплитуда A для рассматриваемого периода рассчитывается по формуле, основанной на теореме косинусов:

$$A = \sqrt{\mathrm{Re}^2 + \mathrm{Im}^2 - 2\,\mathrm{Re}\,\mathrm{Im}\cos\alpha}\,, \qquad (2)$$

где α — фазовое смещение между значениями мгновенной амплитуды Re и Im.

Учитывая принцип однозначности соответствия значений величин мгновенных амплитуд фазам тонального сигнала, можно достроить недостающие точки периода несущей с заданной частотой дискретизации f_d .

Метод восстановления, описанный выше, не применим для сигналов с линейно-частотной модуляцией (ЛЧМ), и восстановить сигнал таким образом не представляется возможным. Поэтому в ГБО «Гидра» для сжатия и восстановления ЛЧМ-сигналов реализован следующий способ: дискретизация сигнала и обнаружение сигнала корреляционным методом. В комплексе предусмотрена дискретизация только с частотами $f_d \le f_н$.

3. Оценка вычисления пространственного положения объекта на дне. Существующие методы, позволяющие определить пространственное положение точки поверхности, используя данные ГБО-снимков, основываются на определении длины акустической тени [13-15]. На рисунке 2 показан данный метод, где H — глубина водоема в точке излучения гидроакустического сигнала, γ — угол визирования, L_1 и L_2 — расстояние до точек, соответствующих началу и концу акустической тени, d — длина акустической тени, h — высота объекта, отбрасывающего рассматриваемую тень.

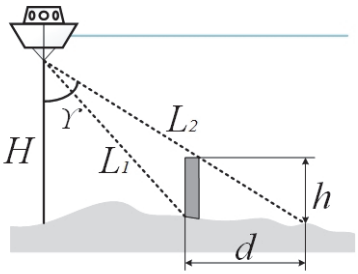


Рис. 2. Формирование гидролокационного изображения и определение высоты объекта на дне

Определение высоты объекта на дне акватории сводится к умножению величины тени d на тангенс угла визирования γ :

$$h = d \tan \gamma . \qquad (3)$$

Высота объекта может быть определена некорректно вследствие искажения проекции объекта, неточной прорисовкой акустической тени из-за флуктуаций амплитуды, неточностью

определения длины этой тени, а также потенциально низкой контрастностью объекта, что приводит к недостоверному восстановлению высоты объекта [16-17].

К общим недостаткам определения пространственного положения объекта на дне по длине тени относится то, что данный способ вычисления дает удовлетворительные результаты только для искусственных объектов простых форм, так как тень является акустической проекцией объекта, и в поперечном сечении определить форму объекта сложной формы затруднительно. Необходимо так же учитывать, что акустические тени на гидролокационном изображении не всегда достоверно отражают обстановку на дне, в частности при наличии более высоких частей, например обломков мачт затонувших кораблей, которые не бросают обнаруживаемую тень [18-19].

Наибольшую погрешность в определение длины тени на дне вносит ошибка обнаружения отраженного сигнала. Погрешность определения длины тени по регистрируемому на приемнике ГБО сигналу составляется из суммы погрешностей определения начала и конца фиксирования отсутствия отраженного сигнала, определенная в результате высота h приобретает следующую ошибку Δh:

$$\Delta h = f(\Delta L_1, \Delta L_2), \quad (4)$$

где $\Delta L_1, \Delta L_2$ — погрешности определения наклонной дальности на точки донной поверхности, соответствующие началу и концу акустической тени.

На рисунке 3 показана зависимость ошибки определения относительной глубины точки поверхности на дне по акустической тени при рабочей глубине L в диапазоне от 2 до 60 метров, и дальности, выраженной в относительных глубинах, в диапазоне от L до $6L$.

Основную погрешность в определение пространственного положения объекта вносит ошибка определения высоты гидролокатора над дном: в комплексе вычисление высотного положения приемоизлучателя сводится к определению глубины под гидролокатором с помощью эхолота. Для случая, результат которого показан на рисунке 3, ошибка определения высоты объекта на дне вследствие ошибки эхолота в один отсчет дискретизации составляет 0,06-0,11 метра. Таким образом, при такой ошибке точность детектирования сигналов в режиме ГБО достаточна для определения глубины, исходя из регламентов точности проведения работ на дне, как при использовании идеального, так и восстановленного сигнала после сжатия сигнала.

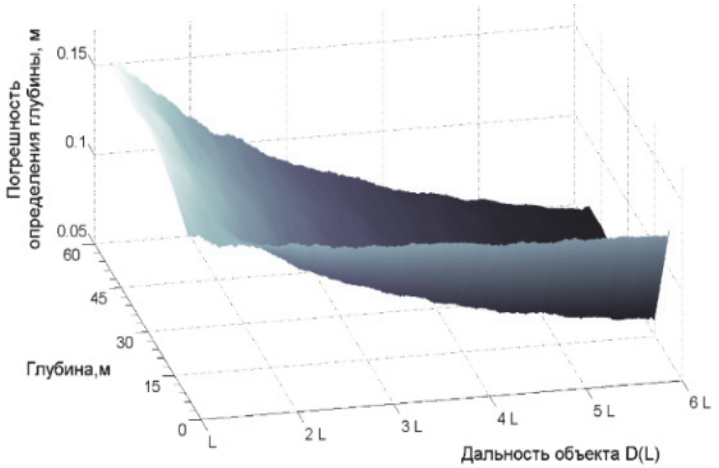


Рис. 3. График зависимости погрешности определения глубины от погрешности детектирования сигнала приемником, по тени от объекта на гидроакустическом изображении (ГБО)

Методы формирования батиметрической карты дна с использованием ИГБО основаны на обработке фазовой разницы сигналов, принимаемых на разнесенные в пространстве приемники в составе комплекса. Величина разнесения двух или более приемников называется базой интерферометра. Фиксирование на приемниках отраженных от одного объекта разрешения сигналов с различной фазой позволяют определить пространственное положение точки поверхности дна в широкой полосе обзора. Разрешающая способность по дальности ИГБО определяется длиной волны, базой и точностью измерения разности фаз. Для интерферометров в общем случае [20-21] справедлива формула зависимости ошибки определения глубины (относительной высоты объекта от дна) σ_h от ошибки определения разности фаз σ_φ, которая, в свою очередь, определяется как ошибка детектирования принимаемых сигналов на разнесенные в пространстве приемники:

$$\sigma_h = -\frac{r \sin\alpha}{B} \frac{\lambda}{4\pi} \sigma_\varphi, \tag{5}$$

где r — наклонная дальность до точки поверхности дна, α – угол визирования, B — база интерферометра, λ — длина волны излученного сигнала.

Согласно формуле (5) наблюдается зависимость точности определения глубин интерферометрическим гидролокатором бокового обзора от фазовой разницы хода лучей. Разница фаз $\partial\varphi$ определяется по временной разнице детектирования сигнала каждым приемником, что позволяет вычислить угол на объект или точку донной поверхности [22-23]:

$$\partial\varphi = \frac{2\pi B}{\lambda}\cos(\beta + \alpha), \tag{6}$$

где β — угол поворота базы интерферометра. Угол визирования (прихода отраженного сигнала) α определяется соотношением:

$$\alpha = \arccos(\frac{2H}{ct}), \tag{7}$$

где H — глубина элемента разрешения дна, c — скорость звука в воде, t — время прохождения сигнала от излучателя до дна и обратно.

Зависимость максимальной погрешности определения глубин интерферометрическим способом при точности определения моментов регистрации сигналов приемником два отсчета дискретизации приведена на рисунке 4.

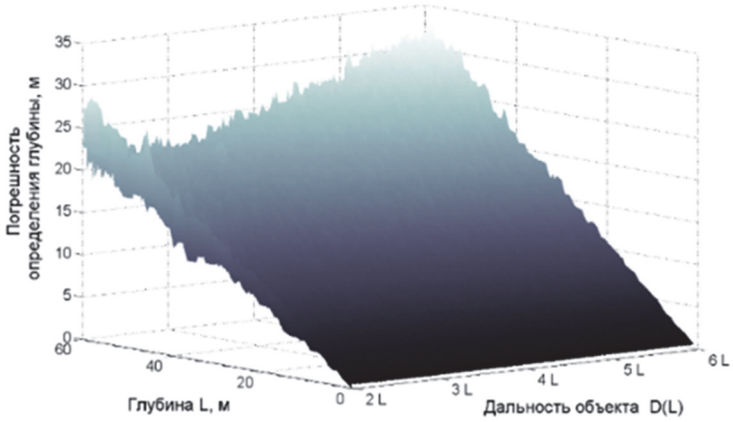


Рис. 4. График зависимости погрешности определения глубины от погрешности детектирования сигнала приемником при формировании данных о глубине водоема по фазоразностной информации

4. Обработка тональных гидроакустических сигналов. В гидроакустических комплексах для обнаружения в канале отраженного сигнала применяется способ на базе спектрально-корреляционного анализа временных рядов (СКАВР) [24]. СКАВР основывается на равносильности представления функции во временной и частотной областях с помощью преобразования Фурье. При обнаружении отраженного зондирующего импульса данным алгоритмом выделяются локальные экстремумы взаимокорреляционной функции принимаемого сигнала и зондирующего импульса.

Для оценки применимости данного способа была проведена серия вычислительных экспериментов. В результате представлена оценка ошибки детектирования тональных сигналов с разным показателем сигнал-шум. При обработке реальных гидроакустических сигналов следует учитывать, что их распространение сопровождается случайными аддитивными помехами, мешающими сигналами, а при отражении волн от поверхности параметры принимаемых сигналов флуктуируют [25]. Была рассмотрена модель гидроакустического сигнала при величине шума в канале от 0 до 50 дБ.

Допустимая точность обнаружения сигнала была принята в один дискретный отсчет. Оценка вероятности достоверного обнаружения момента приема отраженного сигнала (при условии отсутствия наложения отраженных компонент сигнала), а также корректности определения начальной фазы сигнала для метода СКАВР была проведена при доверительной вероятности $Q = 0,9$ и на доверительном интервале $\varepsilon = 0,05$, согласно формуле Бернулли [26]. На рисунке 5 приведена зависимость количества правильно определенных моментов приема эхо-импульсов методом СКАВР от различного соотношения сигнал-шум для отношения $f_d / f_н = 4$ для идеального и восстановленного сигналов.

Гидроакустический сигнал, регистрируемый на приемнике гидролокатора, складывается из суммы эхо-сигналов, отраженных от каждого элемента разрешения дна по мере движения фронта акустической волны. Принимаемый сигнал во временной области можно описать следующей формулой:

$$S_t(t) = S_g(t) + \sum_{n=1}^{N} k_n S_g(t - \tau_n) + e(t), \qquad (8)$$

где $S_g(t)$ — поверхностная составляющая, k_n — коэффициент амплитуды n-ой отраженной составляющей, τ_n — задержка n-ой отраженной составляющей, $e(t)$ — шумовая компонента.

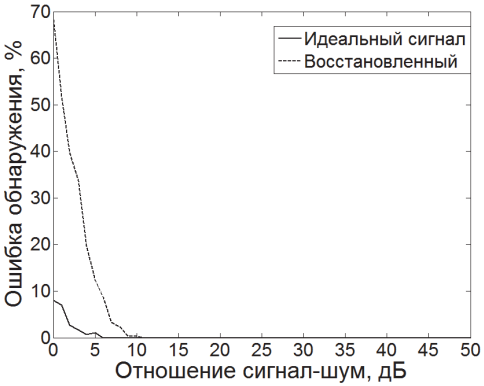


Рис. 5. Оценка помехоустойчивости метода СКАВР

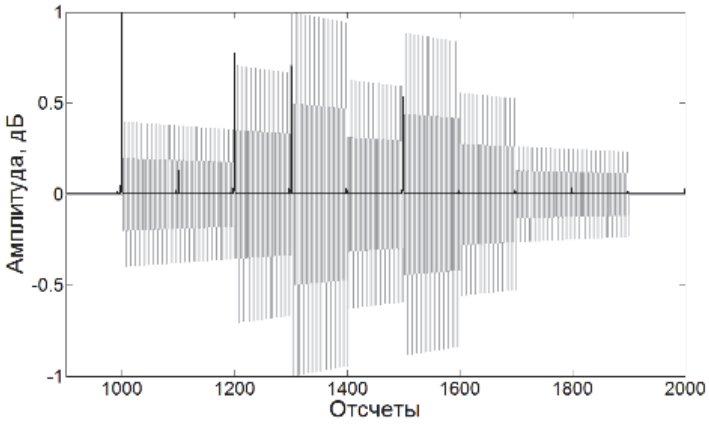
Проведенные ранее исследования [27] показывают, что в случае частичного или полного наложения эхо-сигналов от точек освещенной гидролокатором полосы метод СКАВР не применим при решении задачи их разрешения и обнаружения.

В радиотехнике для обнаружения наложенных отраженных составляющих отраженного сигнала успешно используется метод деления спектров (далее ДС) [28]. Сущность метода заключается в делении спектра регистрируемого сигнала на спектр эталона, в качестве которого принимается сигнал с огибающей формой функции Гаусса. Обратное преобразование Фурье над результатом деления позволяет получить пики в виде дельта-функции в моменты фиксирования эхо-сигналов (рисунок 6а). Следует отметить, что метод деления спектров в цифровых системах может успешно применяться при условии, что величина ошибки регистрации начальной фазы сигнала на АЦП не превышает 13°.

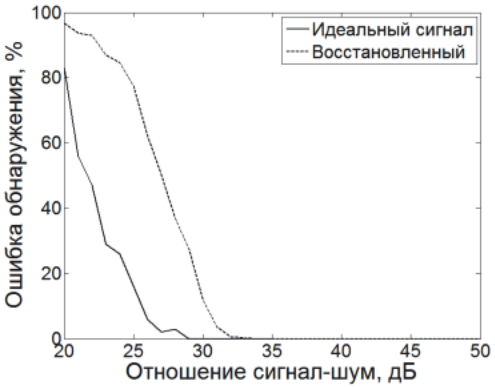
Для оценки применимости метода ДС была проведена серия вычислительных экспериментов при величине шума в канале от 50 до 20 дБ и начальной фазе регистрируемого сигнала $\varphi_0 = 0$ с допустимой точностью обнаружения сигнала в один дискретный отсчет. На рисунке 6б приведено отношение частоты корректно определенных моментов приема эхо-импульсов методом ДС от присутствующего в канале шума для отношения $f_d / f_н = 4$.

Из рисунка 6б видно, что метод деления спектров эффективен при работе с идеальными и с восстановленными сигналами. Но в случае с восстановленным сигналом помехозащищенность существенно меньше. Разница при сравнении с идеальным сигналом

составляет 3 дБ. Для повышения помехоустойчивости системы при работе с восстановленным сигналом можно применить комбинированный способ, основанный на совмещении работы методов ДС и СКАВР.



а)



б)

Рис. 6. Результаты моделирования метода деления спектров: а) обнаружение отраженных составляющих в гидроакустическом канале; б) оценка помехоустойчивости метода

В случае погрешности обнаружения тонального сигнала методом деления спектров на величину, меньшую, чем период зондирующего импульса, авторами предлагается комбинированный метод, основанный на корректировке времени прихода сигнала

уточнением мгновенной фазы для определения «истинного момента» прихода сигнала на приемную антенну.

Для решения данной задачи необходимо вычислить сдвиг фаз между пришедшим сигналом и квадратурными массивами отсчетов, что можно сделать при известных коэффициентах мнимой части сигнала A_k (квадратурной составляющей) и реальной части B_k (синфазной составляющей). При использовании комбинированного метода ошибка обнаружения сигнала будет не хуже, чем один отсчет дискретизации. В рассматриваемом случае для восстановленного сигнала значение соотношения сигнал-шум при заданной погрешности обнаружения составляет 34 дБ при использовании только метода ДС (рисунок 6б); при использовании комбинированного метода значение величины соотношения сигнал-шум составляет 28 дБ. Применимость метода СКАВР в дополнение к ДС допустимо, так как изначальная помехоустойчивость метода СКАВР выше чем у метода ДС (рисунок 5).

На рисунке 7 показан результат работы комбинированного метода при детектировании восстановленного сигнала.

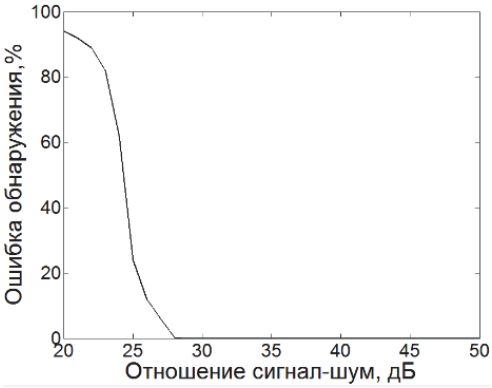


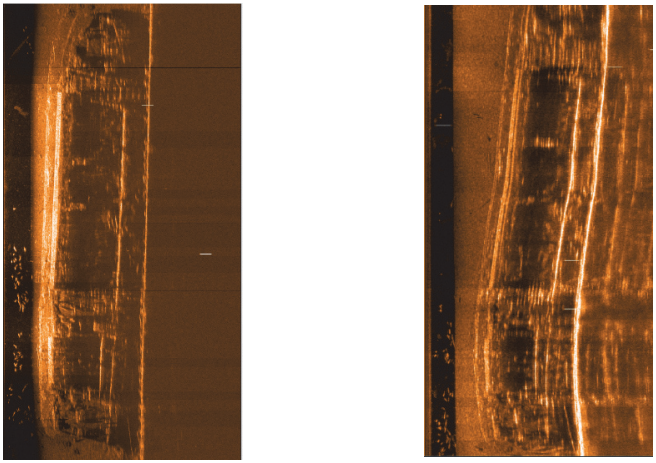
Рис. 7. Оценка помехоустойчивости комбинированного метода обнаружения отраженных сигналов в восстановленном сигнале — с точностью в один отсчет дискретизации

Метод деления спектров, используемый совместно со СКАВР, предлагается как базовый при обнаружении отраженных составляющих, однако он крайне чувствителен к фазовой ошибке при регистрации сигнала, что требует для расширения области его применения увеличивать частоту дискретизации принимаемого

сигнала. В рассматриваемом случае величина f_d должна быть больше $f_н$ как минимум в 28 раз, то есть f_d = 7,3 МГц взамен используемых на данный момент в комплексе 1МГц.

5. Обработка ЛЧМ-сигналов. Использование сигналов с линейно-частотной модуляцией позволяет в более чем 2 раза увеличить дальность действия ГБО и ИГБО, сохраняя при этом высокое разрешение. Также к достоинствам использования ЛЧМ-зондирующих сигналов можно отнести повышение помехоустойчивости, что позволяет использовать гидроакустическое оборудование в более сложных и динамических условиях.

На рисунке 8 приведены фрагменты гидроакустической съемки гидролокатором бокового обзора с тональным и ЛЧМ-зондирующим импульсом. Условия проведения съемки в обоих случаях аналогичны, движение носителя ГБО не стабилизируется, траектория проложена на равном расстоянии от рассматриваемого объекта (затонувшая баржа). Съемка с тональным сигналом предоставляет при анализе оператору визуально более понятную информацию о форме, размерах и относительном положении объекта на дне. Однако в случае проведения модельного эксперимента разрешающая способность ЛЧМ-зондирующего сигнала выше, чем при использовании тонального [39-30].



а) *б)*

Рис. 8. Фрагменты гидроакустической съемки дна средствами ГБО, акватория р. Амур, 2015 год: а) использование тонального сигнала; б) использование ЛЧМ-сигнала в качестве зондирующего

Следует отметить, что «сырая» информация, предоставляемая пользователю при проведении съемки данным комплексом при зондировании сигналом с ЛЧМ, представляет собой огибающую корреляционной функции, при зондировании тональным сигналом — огибающую амплитуды.

В общем случае обнаружение ЛЧМ-сигналов в гидроакустическом канале с точностью не хуже, чем один отсчет, при частоте дискретизации, удовлетворяющей теореме Котельникова, можно свести к определению максимума корреляционной функции (рисунок 9).

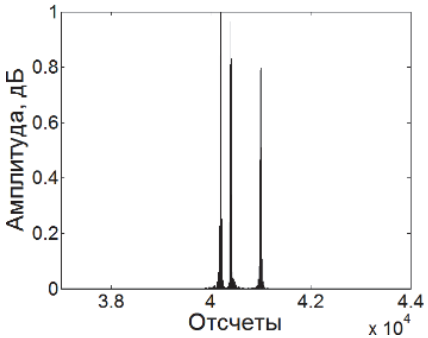
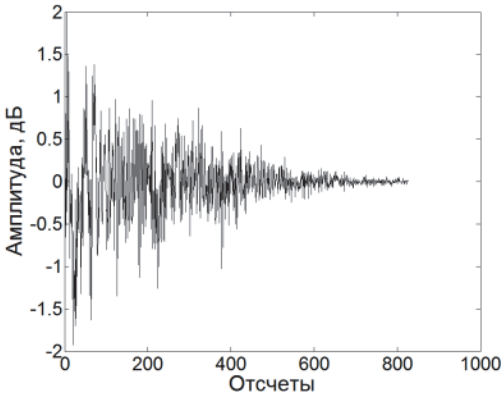


Рис. 9. Обнаружение трех отраженных копий ЛЧМ-зондирующего сигнала в канале методом общей корреляции

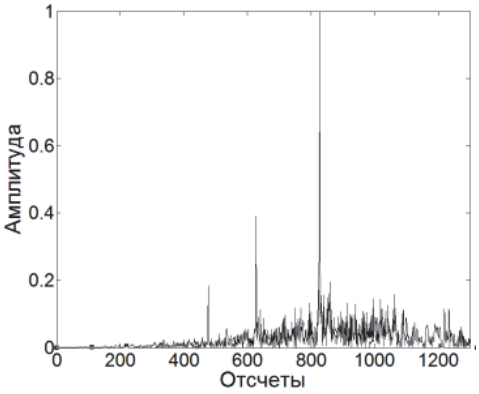
Рассматриваемый выше комплекс позволяет работать с несколькими конфигурациями ЛЧМ-зондирующих импульсов. Был промоделирован случай с частотами 295-335 кГц и частотой дискретизации 59 кГц (рисунок 10а) с тремя отраженными составляющими, смещенными друг от друга каждая на 200 отсчетов.

Данный сигнал затухает в условиях мелкого моря, отношение сигнал-шум — 0 дБ. Вид корреляционной функции, приведенный на рисунке 10б, позволяет сделать вывод о наличии трех отраженных составляющих и корректном (с точностью в один отсчет частоты дискретизации) определении их моментов фиксирования приемником по расположению пиков корреляционной функции.

При оценке обнаружения ЛЧМ-сигнала корреляционным методом были получены результаты погрешности обнаружения сигналов с точностью не хуже, чем два дискретных отсчета, представленные в таблице 1.



а)



б)

Рис. 10. Применение ЛЧМ-сигналов: а) ЛЧМ-сигнал, распространяющийся в условиях «мелкого моря» с тремя отраженными составляющими; б) взаимокорреляционная функция регистрируемого и излученного сигналов

Таблица 1. Моделирование определения начальной фазы восстановленного ЛЧМ-сигнала

Показатель	Отношение fd/fh			
	100	*10*	*4*	*2*
СКО, (мкс)	93	95,7	97,9	124,1
MIN, (мкс)	86	88	92,6	113
MAX, (мкс)	98	98,3	148	157

Результаты, представленные в таблице 1, могут быть уточнены корректировкой по фазе, рассчитанной через наклон скорости изменения частоты ЛЧМ-сигнала [31].

Эффективность алгоритма была оценена по следующим показателям:

1) максимальное значение определенной погрешности вычисления (MAX);

2) минимальное значение погрешности(MIN);

3) среднеквадратичное отклонение значения (СКО).

Сжатие ЛЧМ-сигналов в рассматриваемом комплексе подразумевает использование зондирующих импульсов с величиной $f_d / f_н \le 2$. Такая дискретизация не позволяет проводить корректировку фазы, так как не представляется возможным провести анализ спектра сигнала. Зависимость ошибки определения положения объекта на дне водоема от ошибки обнаружения ЛЧМ сигнала в один дискрет для различных глубин и дальностей приведена на рисунке 11.

Как видно, при той частоте семплирования, которая используется в комплексе на данный момент, такая погрешность будет приводить к ошибке вычисления глубины водоема до 1,76 метра при небольших углах обзора и иметь меньшую величину на большей дальности при использовании ЛЧМ сигналов в качестве зондирующих в интерферометрическом гидролокаторе.

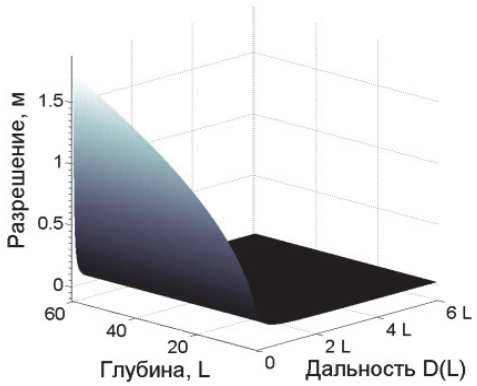


Рис. 11. График зависимости погрешности определения глубины при использовании зондирующего ЛЧМ-сигнала при ошибке обнаружения в один отсчет дискретизации

Чтобы оценить применимость корреляционного метода для разрешения ЛЧМ-составляющих в гидроакустическом канале, была проведена серия вычислительных экспериментов при величине шума от 0 до -50 дБ и начальной фазе регистрируемого сигнала φ_0=0, с

допустимой точностью обнаружения сигнала в дискретный отсчет. Результат моделирования ЛЧМ-сигнала с конфигурацией, представленной выше, приведен на рисунке 12.

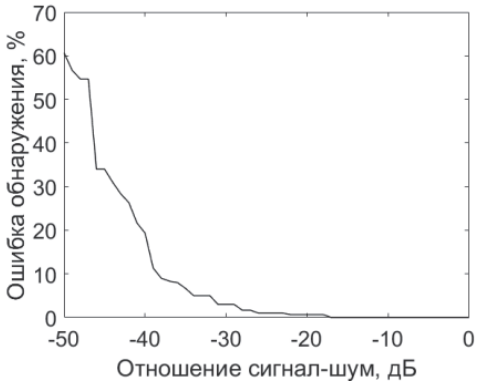


Рис. 12. Оценка помехоустойчивости метода корреляционной обработки для обнаружения ЛЧМ-отраженных составляющих в гидроакустическом канале

Как видно по результатам моделирования, ЛЧМ-сигналы обладают большей помехозащищенностью перед тональными.

7. Заключение. Получаемые данные в гидроакустических комплексах зачастую не отражают реальную обстановку на дне акватории, так как используемые методы сжатия-восстановления первичной информации имеют ряд недостатков, которые ведут к потере информации и неоднозначности восстановления сигнала. Широко используемый в гидроакустике метод СКАВР не позволяет обнаруживать отраженные эхо-сигналы в гидроакустическом канале в случае их наложения друг на друга при использовании тональных импульсов в качестве зондирующих. Использование комбинированного метода, предлагаемого авторами, основанного на дополнении метода деления спектров информацией, полученной в результате спектрально-корреляционного анализа, позволяет повысить точность получаемых данных. Применение данного метода для разрешения гидроакустических сигналов с необходимой частотой дискретизации способствует проведению гидроакустической съемки с требуемым для работ на дне разрешением в 0,1 метра. Достижение такого разрешения способно привести к большей различимости малоразмерных объектов на дне и увеличить точность определения их размеров и расположения. Результаты численного моделирования показывают, что

использование комбинированного способа определения момента прихода сигнала также способствует увеличению помехоустойчивости системы.

Использование ЛЧМ сигналов в качестве зондирующих позволяет эффективно применять комплекс в режиме гидролокатора бокового обзора. Проведение численного эксперимента позволило установить, что ЛЧМ сигналы имеют высокий показатель помехозащищенности.

Литература

1. *Болдинов Р.О., Скнаря А.В., Тощов С.А*. К вопросу о применении алгоритмов построения рельефа дна в интерферометрическом гидролокаторе бокового обзора «Неман ИГБО-500» // Журнал радиоэлектроники. 2017. № 2. С. 1–9.
2. *Болдинов Р.О., Баскаков А.И., Скнаря А.В.* Потенциальная точность интерферометрического гидролокатора бокового обзора//Вестник Московского энергетического института. 2016. № 3. С. 67–72.
3. *Каевицер В.И. и др.* Результаты применения многофункционального гидролокационного комплекса с ЛЧМ сигналами при инженерных обследованиях подводных сооружений // XIII Всероссийская конференция «Прикладные технологии гидроакустики и гидрофизики (ГА-2016)». 2016. С. 126–129.
4. *Каевицер В.И., Кривцов А.П., Смольянинов И.В., Элбакидзе А.В.* Опыт проведения исследований дна и донных отложений арктических морей гидролокационными комплексами с ЛЧМ зондирующими сигналами // Известия ЮФУ. Технические науки. 2017. № 8. С. 6–16.
5. *Кривцов А.П., Смольянинов И.В., Элбакидзе А.В., Степанов А.В.* Оценка сходимости глубин при площадной съемке рельефа дна многолучевым эхолотом и интерферометрическим гидролокатором бокового обзора // Журнал радиоэлектроники. 2017. № 4. С. 1–8.
6. *Матвиенко Ю.В. и др.* Пути совершенствования гидроакустических технологий обследования морского дна с использованием автономных необитаемых подводных аппаратов // Подводные исследования и робототехника. 2010. № 2. С. 14–15.
7. *Матвиенко Ю.В. и др.* Комплекс робототехнических средств для выполнения поисковых работ и обследования подводной инфраструктуры на шельфе // Подводные исследования и робототехника. 2015. № 1. С. 4–15.
8. *Ковтанюк А.Е., Сущенко А.А., Агафонов И.Б., Золотарев В.В.* Интерполяционные методы в задаче улучшения качества гидроакустических изображений // Технические проблемы освоения мирового океана. Материалы 4-й Всероссийской научно-технической конференции. 2011. С. 264–288.
9. *Ковтанюк А.Е., Сущенко А.А., Агафонов И.Б., Золотарев В.В.* Улучшение качества гидроакустических изображений методом двойной фильтрации // Подводные исследования и робототехника. 2011. № 2. С. 31–37.
10. РД 51-3-96. Регламент по техническому обслуживанию подводных переходов магистральных газопроводов через водные преграды // М.: РАО «Газпром». 2008. 73 с.

11. СП 46.13330.2012. Мосты и трубы. Свод правил // М.: Министерство регионального развития Российской Федерации. 2012. 144 с.
12. КВВТ РФ N 24-ФЗ. Кодекс внутреннего водного транспорта РФ. Правила содержания судовых ходов и судоходных гидротехнических сооружений // М.: Минтранс России. 2017. 83 с.
13. *Сажнева А.Э.* Технологии выявления скрытой информации изображений (на основе гидролокационных исследований) // М.: Научный мир. 2013. 85 с.
14. *Фирсов Ю.Г.* Основы гидроакустики и использования гидрографических сонаров // СПб: Нестор-История. 2010. 303 с.
15. *Lurton X., Lamarche G.* Backscatter measurements by seafloor-mapping sonars: Guidelines and Recommendations // A collective report by members of the GeoHab Backscatter Working Group. 2015. 200 p.
16. *Healy C.A., Schultz J.J., Parker K., Lowers B.* Detecting submerged bodies: Controlled research using side-scan sonar to detect submerged proxy cadavers // Journal of forensic sciences. Technical Note. 2015. vol. 3. pp. 743–752.
17. *Lubis M.Z., Kausarian H., Anurogo W.* Seabed Detection Using Application Of Image Side Scan Sonar Instrument (Acoustic Signal) // Journal of geoscience engineering, environment, and technology. 2017. vol. 2. no. 3. pp. 230–234.
18. *Grzadziel A., Felski A., Waz M.* Experience with the use of a rigidly-mounted side-scan sonar in a harbour basin bottom investigation // Ocean Engineering. 2015. vol. 109. pp. 439–443.
19. *Kumar N., Mitra U., Narayanan Sh.S.* Robust Object Classification in Underwater Sidescan Sonar Images by Using Reliability-Aware Fusion of Shadow Features // IEEE Journal of oceanic engineering. 2015. vol. 40. no. 3. pp. 592–606.
20. *Нестеров И.М., Трунов А.Н.* Влияние сжатия данных на ошибку определения высоты в радиолокационной интерферометрии РСА космического базирования // Журнал радиоэлектроники. 2015. № 6. С. 1–16.
21. *Pepe A., Salo F.* A Review of Interferometric Synthetic Aperture RADAR (InSAR) Multi-Track Approaches for the Retrieval of Earth's Surface Displacements // Applied Sciences. 2017. vol. 7. pp. 1–40.
22. *Pujol G.L.* Improving direction-sensing by multibeam sonar // The Journal of the Acoustical Society of America. 2013. vol. 134. 1–28 p.
23. *Saucan A.-A., Chonavel Th.* Model-based adaptive 3d sonar reconstruction in reverberating environments// IEEE transactions on image processing. 2015. vol. 24. no. 10. pp. 2928–2940.
24. *Бурдинский И.Н., Миронов А.С.* Цифровая система обработки гидроакустических навигационных сигналов // Электронные средства и системы управления. 2007. С. 296–299.
25. *Филлипов Б.И., Чернецкий Г.А.* Анализ статистических характеристик каналов и помех в гидроакустических каналах связи // Вестник АГТУ. Управление, вычислительная техника и информатика. 2015. № 3. С. 78–84.
26. *Феллер В.* Ведение в теорию вероятностей и ее приложения // М.: Мир. 1984. 738 с.
27. *Миронов А.С., Фомина Е.С.* Методы обработки простых сигналов в гидролокаторах бокового обзора // Информационные технологии XXI века. 2017. С. 51–59.
28. *Зверев В.А.* Временное разрешение в радио-, сейсмо- и акустической локации // Известия вузов. РАДИОФИЗИКА. 2000. С.402–412.

29. *Шостак С.В.*, *Бакланов Е.Н, Стародубцев А.П., Шевченко А.П.* Решение задачи «обнаружение – измерение дальности» для малоподвижных объектов методом активной корреляции // Журнал Радиоэлектроники. 2015. № 3. С. 1–14.
30. *Черниховская Г.Л.* Особенности применения сложных сверхширокополосных сигналов в гидроакустике // Радиофизические методы в дистанционном зондировании сред. Муром: Изд. - полиграфический центр МИ ВлГУ. 2012. С. 1–6.
31. *Кучеренко И.А.* Применение сверхширокополосных сигналов с линейной частотной модуляцией в запреградной радиолокации // Инженерный вестник Дона. 2016. № 1. С. 1–14.

Миронов Андрей Сергеевич — к-т техн. наук, доцент кафедры вычислительной техники факультета автоматизации информационных технологий, Тихоокеанский Государственный Университет (ТОГУ). Область научных интересов: подводная робототехника, обработка сигналов, аппаратные и программные средства определения координат в морской среде. Число научных публикаций — 40. andrei.s.mironov@yandex.ru; ул. Тихоокеанская, 136, Хабаровск, 680035; р.т.: +74212224356.

Фомина Екатерина Сергеевна — аспирант кафедры вычислительной техники факультета автоматизации информационных технологий, Тихоокеанский Государственный Университет (ТОГУ). Область научных интересов: программные средства определения координат в морской среде. Число научных публикаций — 8. fominaekt@gmail.com; ул. Тихоокеанская, 136, Хабаровск, 680035; р.т.: +79990828010.

DOI 10.15622/sp.59.6

A.S. MIRONOV, E.S. FOMINA

METHODS OF SONAR SIGNAL PROCESSING TO SOLVE THE SENSING BOTTOM SURFACE PROBLEM

Mironov A.S., Fomina E.S. **Methods of Sonar Signal Processing to Solve the Sensing Bottom Surface Problem.**

Abstract. The paper deals with the processing of hydroacoustic data recorded with help of hydroacoustic research complexes. Particular attention to classic and interferometric sonars is paid. In accordance to the regulatory documentation, the minimum permissible measurement errors for the formation of bottom surface maps for various economic sectors are determined.

As one of the important problems affecting the effectiveness of survey work with sonar complexes, the authors determine the problem of primary data compression, which, as a rule, leads to information loss without the possibility of its recovery. These drawbacks of the methods of primary information compression-recovery and processing of hydroacoustic data used in complexes reduce the overall effectiveness of the complexes usage both with the use of sidescan sonar and with the use of an interferometric side-scan sonar.

In the framework of a numerical experiment, it has been shown that the use of chirp signals as probing pulses makes it possible to effectively apply the complex in the survey sonar mode.

The results of the numerical experiment for estimating the spatial position of the object at the bottom of the sonar images using the phase difference information of the received signals using an interferometric sonar are presented. Based on the results of the experiment, the requirements for recording quality of reflected signals of various types in interferometric side-scan sonar are determined.

A method of resolving the reflected (with partial overlap and overlay) hydroacoustic tones, based on the method of dividing the spectra is proposed by the authors. To improve the efficiency of the chirp signal processing, the authors suggest to improve the accuracy of the detection of the signal detection time due to the phase correction calculated through the slope of the frequency change rate of the chirp signal.

Keywords: phase different sonar, sidescan sonar, hydroacoustics, tone signal, LFM, signal processing.

Mironov Andrey Sergeevich — Ph.D., associate professor of computer engineering department of School of Automation and Informational Technologies (SAIT), Pacific National University. Research interests: underwater robotics, signal processing, hard-ware and software for positioning in the marine environment. The number of publications — 40. andrei.s.mironov@yandex.ru; 136, Tikhookeansky str., Khabarovsk, 680035, Russia; office phone: +74212224356.

Fomina Ekaterina Sergeevna — Ph.D. student of computer engineering department of School of Automation and Informational Technologies (SAIT), Pacific National University. Research interests: software for positioning in the marine environment. The number of publications — 8. fominaekt@gmail.com; 136, Tikhookeansky str., Khabarovsk, 680035, Russia; office phone: +79990828010.

References

1. Boldinov R.O., Sknarya A.V., Toschov S.A. [On the question of the application of algorithms for constructing the relief in the bottom of the interferometric side scan sonar "Neman ISSS-500"]. *Zhurnal radiojelektroniki – Journal of Radioelectronics.* 2017. vol. 2. pp. 1–9. (In Russ.).

2. Boldinov R.O., Baskakov A.I., Sknarya A.V. [Potential accuracy of interferometric sonar side scan]. *Vestnik Moskovskogo Energeticheskogo Instituta – Bulletin of the Moscow Power Engineering Institute*. 2016. vol. 3. pp. 67–72. (In Russ.).
3. Kaevitser V.I. et. al. [Results of application of a multifunctional sonar complex with chirp signals during engineering surveys of underwater structures]. *Trudy XIII Vserossiyskoi konferentsii «Prikladnye tekhnologii gidroakustiki i gidrofiziki»: Sb. nauch. tr.* [Proceedings of XIII All-Russian Conference "Advanced Technologies of Hydroacoustics and Hydrophysics": Collected papers]. SPb: SPbSC RAS. 2016. pp. 126–129. (In Russ.).
4. Kaevitser V.I., Krivtsov A.P., Smolyaninov I.V., Elbakidze A.V. [Experience in researching the bottom and bottom sediments of the Arctic seas with sonar complexes with chirp sounding signals]. *Izvestiya YuFU. Tehnicheskie nauki – News of SFedU. Technical science.* 2017. vol. 8. pp. 6–16. (In Russ.).
5. Krivtsov A.P., Smolyaninov I.V., Elbakidze A.V., Stepanov A.V. [An estimate of the convergence of the depths for an area survey of the bottom relief by a multi-beam echosounder and an interferometric sonar sonar]. *Zhurnal radiojelektroniki – Journal of Radioelectronics.* 2017. vol. 4. pp. 1–8. (In Russ.).
6. Matvienko Yu.V. et. al. [Ways of improving hydroacoustic technologies of seabed survey using autonomous uninhabited underwater vehicles]. *Podvodnyie issledovaniya i robototehnika – Underwater Researches and Robotics.* 2010. vol. 2. pp. 4–15. (In Russ.).
7. Matvienko Yu.V. et. al. [A complex of robotic means for carrying out prospecting and survey of underwater infrastructure on the shelf]. *Podvodnyie issledovaniya i robototehnika – Underwater Researches and Robotics.* 2015. vol. 1. pp. 4–15. (In Russ.).
8. Kovtanyuk A.E., Suschenko A.A., Agafonov I.B., Zolotarev V.V. [Interpolation methods in the problem of improving the quality of hydroacoustic images]. *Tehnicheskie problemyi osvoeniya mirovogo okeana. Materialyi 4-y Vserossiyskoy nauchno-tehnicheskoy konferentsii: Sb. nauch. tr.* [Technical problems of development of the World Ocean. Materials of the 4th All-Russian Scientific and Technical Conference: Collected papers].Vladivostok: Dal'nauka Publ. 2011. pp. 264–288. (In Russ.).
9. Kovtanyuk A.E., Suschenko A.A., Agafonov I.B., Zolotarev V.V. [Improving the quality of hydroacoustic images by the method of double filtration]. *Podvodnyie issledovaniya i robototehnika – Underwater Researches and Robotics*. 2011. vol. 2. pp. 31–37. (In Russ.).
10. RD 51-3-96. [Regulation on maintenance of underwater transitions of main gas pipelines through water barriers]. M.: RAO «Gazprom». 2008. 73 p. (In Russ.).
11. SP 46.13330.2012. [Bridges and pipes. Set of rules]. M.: Ministerstvo regional'nogo razvitija Rossijskoj Federacii. 2012. 144 p. (In Russ.).
12. KVVT RF, N 24-FZ. [The Code of inland water transport of the Russian Federation, the rules for the maintenance of ships and navigable hydraulic structures]. M.: Mintrans Rossii. 2017. 83 p. (In Russ.).
13. Sazhneva A.Je. *Tehnologii vyjavlenija skrytoj informacii izobrazhenij (na osnove gidrolokacionnyh issledovanij)* [Technologies for the detection of hidden image information (based on sonar studies)]. Moscow: Nauchnyj mir Publ. 2013. 85 p. (In Russ.).
14. Firsov Yu.G. *Osnovy gidroakustiki i ispol'zovanija gidrograficheskih sonarov* [Fundamentals of hydroacoustics and the use of hydrographic sonars]. SPb: Nestor-Istorija Publ. 2010. 303 p. (In Russ.).
15. Lurton X., Lamarche G. Backscatter measurements by seafloor-mapping sonars. A collective report by members of the GeoHab Backscatter Working Group. 2015. 200 p.
16. Healy C.A., Schultz J.J., Parker K., Lowers B. Detecting Submerged Bodies: Controlled Research Using Side-Scan Sonar To Detect Submerged Proxy Cadavers. *Journal of forensic sciences. Technical Note.* 2015. vol. 3. pp. 743–752.

17. Lubis M.Z., Kausarian H., Anurogo W. Seabed Detection Using Application Of Image Side Scan Sonar Instrument (Acoustic Signal). *Journal of geoscience engineering, environment, and technology.* 2017. vol. 2. no. 3. pp. 230–234.
18. Grzadziel A., Felski A., Waz M. Experience with the Use of A Rigidly-Mounted Side-Scan Sonar In A Harbour Basin Bottom Investigation. *Ocean Engineering.* 2015. vol. 109. pp. 439–443.
19. Kumar N., Mitra U., Narayanan Sh.S. Robust Object Classification In Underwater Sidescan Sonar Images By Using Reliability-Aware Fusion Of Shadow Features. *IEEE Journal of oceanic engineering.* 2015. vol. 40. no. 3. pp. 592–606.
20. Nesterov I.M., Trunov A.N. [The effect of data compression on the altitude error in radar interferometry of space-based SAR]. *Zhurnal radiojelektroniki – Journal of Radioelectronics.* 2015. vol. 6. p. 1–16. (In Russ.).
21. Pepe A., Salo F. A Review of Interferometric Synthetic Aperture Radar (INSAR) Multi-Track Approaches for the Retrieval of Earth's Surface Displacements. *Applied Sciences*. 2017. vol. 7. pp. 1–40.
22. Pujol G.L. Improving Direction-Sensing By Multibeam Sonar. *The Journal of the Acoustical Society of America.* 2013. vol. 134. 1–28 p.
23. Saucan A.-A., Chonavel Th. Model-Based Adaptive 3d Sonar Reconstruction In Reverberating Environments. *IEEE transactions on image processing.* 2015. vol. 24. no. 10. pp. 2928–2940.
24. Burdinskiy I.N., Mironov A.S. [Digital system for processing hydroacoustic navigation signals]. XIV Mezhdunarodnaja nauchno-prakticheskaja konferencija *«Elektronnyie sredstva i sistemyi upravleniya»: Sb. nauch. tr.* [XIV International Scientific and Practical Conference «Electronic means and control systems»: Collected papers]. Tomsk: V-Spectr Publ. 2007. pp. 296–299. (In Russ.).
25. Fillipov B.I., Chernetskiy G.A. [Analysis of statistical characteristics of channels and interference in hydroacoustic communication channels]. *Vestnik AGTU. Upravlenie, vyichislitelnaya tehnika i informatika – Bulletin of ASTU. Management, computer science and informatics.* 2015. vol. 3. pp. 78–84. (In Russ.).
26. Feller W. *An introduction to probability theory and its applications.* Wiley. 1965. 704 p. (Russ. ed.: Feller W. *Vvedenie v teoriju verojatnostej i ee prilozhenija.* M. Mir Publ. 1984. 738 p.).
27. Mironov A.S., Fomina E.S. [Methods for processing simple signals in sonar sonar]. *Informacionnye tehnologii XXI veka – Information technology of the XXI century.* 2017. pp. 51–59. (In Russ.).
28. Zverev V.A. [Time resolution in radio, seismic and acoustic locations]. *Izvestija vuzov. Radiofizika – Proceedings of high schools. Radiophysics.* 2000. vol. 5. pp. 402–412. (In Russ.).
29. Shostak S.V., Baklanov E.N., Starodubcev A.P., Shevchenko A.P. [The solution of the problem of "detection - ranging" for inactive objects by the active correlation method]. *Zhurnal radioehlektroniki – Journal of Radioelectronics.* 2015. vol. 3. pp. 1–14. (In Russ.).
30. Chernihovskaya G.L. [Features of the application of complex ultra-wideband signals in hydroacoustics]. *Radiofizicheskie metodyi v distantsionnom zondirovanii sred. Materialy V Vserossijskoj nauchnoj konferencii: Sb. nauch. tr.* [Radiophysical methods in remote sensing of media. Materials of the V All-Russian Scientific Conference: Collected papers]. Murom: MI VLSU Publ. 2012. pp. 1–6. (In Russ.).
31. Kucherenko I.A. [The use of ultra-wideband signals with linear frequency modulation in the forbidden radar]. *Inzhenernyiy vestnik Dona – The engineer's bulletin of the Don.* 2016. vol. 1. pp. 1–14. (In Russ.).

УДК 004.8 **DOI** 10.15622/sp.59.7

В.А. Степаненко, А.М. Кашевник, А.В. Гуртов

КОНТЕКСТНО-ОРИЕНТИРОВАННОЕ УПРАВЛЕНИЕ КОМПЕТЕНЦИЯМИ В ЭКСПЕРТНЫХ СЕТЯХ

Степаненко В.А., Кашевник А.М., Гуртов А.В. **Контекстно-ориентированное управление компетенциями в экспертных сетях.**

Аннотация. В настоящее время в условиях нестабильной экономики организациям крайне важно эффективно управлять кадровыми ресурсами и знаниями, которыми обладают сотрудники. Для управления знаниями кадровых ресурсов в последние годы широко применяются соответствующие информационные системы (системы управления компетенциями). Такие системы активно используются для автоматизации процесса поиска экспертов при совместном решении задач. Целью данной статьи является анализ существующих систем управления компетенциями: выявление основных сценариев использования таких систем и требований к ним, а также разработка концептуальной модели системы контекстно-ориентированного управления компетенциями в экспертных сетях. В результате анализа существующих систем был сформулирован список основных требований к системам управления компетенциями, разработана концептуальная модель системы контекстно-ориентированного управления компетенциями в экспертных сетях, а также произведена классификация видов контекста, используемого для формализации текущей ситуации в экспертной сети. В статье была предложена модель контекста в рамках которой различается: контекст участника, контекст актива и контекст проекта. Для оценки эффективности предложенной концептуальной модели системы контекстно-ориентированного управления компетенциями в экспертных сетях в статье была рассмотрена задача поиска группы экспертов с необходимым набором компетенций. Анализ показал, что при небольшом количестве экспертов в системе управления компетенциями эффективна будет классическая система, но с ростом количества экспертов предложенная система показывает лучшие результаты. Представ-ленная в статье концептуальная модель системы контекстно-ориентированного управления компетенциями является многообещающей для использования для современных организаций как в России, так и за рубежом.

Ключевые слова: системы управления компетенциями, экспертные сети, компетенции, знания.

1. Введение. В настоящее время особую ценность для компаний представляет собой интеллектуальный капитал, которым владеют сотрудники. Это делает процесс управления человеческими ресурсами одним из ключевых для предприятия любого рода, так как управляя человеческими ресурсами, организация управляет самым значимым ресурсом на сегодняшний день — знаниями. Управление человеческими ресурсами достаточно широкое понятие, включающее в себя различные процессы в компании [1-3]. Следует отметить, что под термином «управление компетенциями» подразумевается процесс менеджмента компетенций с организационной точки зрения (от англ. competence management).

Для того чтобы управлять некоторым процессом, необходимо его формализовать. Одним из возможных вариантов формализации процесса управления человеческими ресурсами является использова-

ние систем управления компетенциями как сотрудников организации, так и внешних экспертов. Таким образом, можно говорить об экспертной сети, в которой участвуют эксперты различного уровня и взаимодействуют для совместного решения задач.

В данной статье были проанализированы существующие системы управления компетенциями для производственных предприятий и образовательных учреждений. Каждая рассмотренная система служит для решения различных конкретных проблем пользователя, таких как: поиск исполнителя или группы исполнителей для выполнения проекта или отдельной задачи; помощь в развитии компетенций пользователя или поиск инвесторов для проекта. Такой спектр разнообразных систем позволяет выявить основные сценарии их использования, а также определить требования к таким системам. Выявленные общие требования и сценарии использования могут быть применены как при разработке новой системы управления компетенциями, так и при совершенствовании или внедрении уже существующей в организации.

Следует отдельно отметить термины, которые используются в статье. Под термином компетенция (competence) подразумевается совокупность знаний, навыков и коммуникативных способностей (knowledge, skill, attitude) с уровнем профессионального владения, применяемых в некотором контексте. Различают как минимум 2 вида компетенций: компетенции отдельного человека и компетенции организации в целом [4]. Компетенции отдельного человека мы будем называть «индивидуальные компетенции», компетенции всей организации — «бизнес-компетенции организации», а комбинацию различных ресурсов и навыков, которая выделяет организацию на рынке и обеспечивает ее конкурентное преимущество — «ключевая компетенция».

На основе выявленных требований и сценариев использования систем управления компетенциями была разработана концептуальная модель системы контекстно-ориентированного управления знаниями в экспертных сетях, а также классификация видов контекста, применяемого для формализации текущей ситуации в экспертной сети, разработанная на основе [5].

2. Существующие системы управления компетенциями. В этом разделе будут подробно рассмотрены системы управления индивидуальными компетенциями и компетенциями организации, такие как DeCom [4], Knome [6, 7] TENCompetence [8, 9]. Система Технопарка ИТМО [10, 11], IMPAKT [12-15].

DeCom — система управления компетенциями, предназначенная для производственных компаний. Модель системы состоит из 3-х модулей: модуль профиля пользователя, модуль компетенции и модуль контекста. Модуль профиля позволяет хранить информацию о пользовате-

лях и пользовательских настройках (интерфейс, безопасность и т.д.). В модуле компетенций хранится модель представления компетенций в виде иерархии, основанная на стандарте IEEE RCD (Reusable Competency Definitions). Создатели DeCom расширили данный стандарт и добавили в модель представления компетенций сущности «профессиональный уровень владения» и «значимость» (или weight, позволяет определить, что выбранная компетенция более значимая для должности или выполнения проекта/задачи). Модель представления компетенций также хранит описание проектов и должностей, которые связаны с требуемыми для их выполнения компетенциями. Модуль контекста представляет собой набор элементов, реализующий следующие функции: определение местоположения пользователя; определение текущего уровня каждой из компетенций; определение возможностей для развития компетенций пользователя: сотрудники с более высоким уровнем владения данных компетенций, которые могут стать наставниками и физически находятся рядом; ресурсы, находящиеся в компании (например, книги), а также события в компании, имеющие место в будущем (например, курсы по повышению квалификации).

DeCom была разработана для решения нескольких основных пользовательских задач. Первая задача — определение текущего уровня владения компетенциями пользователя, а также «пробелов» в своих компетенциях. DeCom помогает пользователю найти компетенции, которые ему необходимо развить для того, чтобы выполнять свою работу на высоком уровне. Система ранжирует искомые компетенции в порядке убывания приоритета, чтобы пользователь видел, на что ему стоит обратить внимание в первую очередь. Вторая задача — продвижение по карьерной лестнице. Система представляет пользователю компетенции, которыми он обладает, требуемые компетенции для должности, которая его интересует и выводит список недостающих компетенций. Третья задача — смена профиля работы. Система показывает текущий уровень компетенций пользователя и рейтинг должностей в компании, в которых разница в требуемых компетенциях минимальная. Из этого списка он может выбрать интересующую его новую сферу деятельности и развивать навыки в соответствии с информацией, данной приложением.

Требования, предъявляемые к системе DeCom авторами работы [4]:

– предоставление возможности добавления, редактирования и удаления компетенций пользователя и выявления «пробелов» в его навыках;

– предоставление возможности поиска пользователя по требуемым компетенциям;

– предоставление возможности определения уровня профессионального владения компетенцией вручную;

– предоставление возможности определения значимости компетенции для конкретной должности вручную;

– использование контекстно-зависимой информации для поиска возможностей развития компетенций пользователя с использованием информации о ресурсах компании; информации о положении пользователя в физическом пространстве; информации о предстоящих событиях в сфере обучения: о курсах, семинарах, лекциях, конференциях и так далее.

Система DeCom реализована на языке C# с использованием технологии ASP.NET, которая позволяет системе работать как на стационарных, так и на мобильных устройствах и быть независимой от используемой операционной системы. Адаптация интерфейса на устройствах обеспечивается с помощью HTML и CSS технологий.

Система управления компетенциями KnoMe используется для нахождения соответствий между запросами пользователя системы и компетенциями сотрудников, которыми они обладают в данный момент либо будут обладать в будущем. Система легко масштабируема, имеет мобильную и веб-версию.

Создатели системы указывают, что помимо концепций, приведенных в статье [6], при разработке системы KnoMe они руководствовались трёхмерной каркасной моделью целей компании (hedgehog concept): компетенции (необходимо концентрироваться на своих сильных сторонах), покупательский спрос (необходимо выстраивать экономику компании так, чтобы она приносила максимум пользы), энтузиазм (необходимо учитывать интересы сотрудников компании).

В системе приведенные выше концепты реализованы следующим образом:

– компетенции — хранение информации по компетенциям каждого сотрудника или партнера в профиле: персональные данные, данные о сертификатах и пройденных курсах, методологических и технологических навыках;

– покупательский спрос — хранение информации обо всей истории работы с покупателями (пользователями) и внутренних проектах. Информация включает в себя как описание каждого покупателя (пользователя), так и описание выполненного проекта. Проект связан с каждым сотрудником, который принимал в нем участие. Здесь же описывается его роль в проекте, и требуемые технологические навыки для выполнения задач по проекту;

– энтузиазм — хранение оценок по 2-м шкалам для каждого отдельному навыка: уровень навыка (skill level) и интерес к исполь-

зованию (interest to use it) в личном профиле. Генерирование отчетов и визуализация данных в виде облаков навыков на уровне отдельной группы сотрудников (tribes) либо компании в целом на основании данной информации.

Требования, предъявляемые к системе KnoMe авторами работы [6]:

– редактирование профиля (общей информации, информации об имеющихся сертификатах и пройденных курсах, информации о технических навыках);

– поиск информации по сотрудникам или компетенциям;

– создание отчетов по компетенциям или группам;

– аутентификация для внешних пользователей (например, через LinkedIn).

Система разработана на JavaScript. Само приложение реализовано на Node.js и REST, пользовательский интерфейс — на Angular.js, а база данных использует СУБД CoachDB и поисковый механизм ElasticSearch.

TENCompetence — это система управления компетенциями сотрудника, которая помогает ему развивать собственные навыки. Система ориентирована на поддержание обучения и развитие пользователя на протяжении всей его жизни. Концептуальная модель TENCompetence включает в себя 4 концепции: действия пользователя, образовательная сеть (практикующее сообщество или группа обучающихся людей), модель представления компетенции и учебные материалы. Эти концепции детально раскрыты ниже.

Действия пользователя представляют собой шаги, которые он предпринимает для того, чтобы достичь своей главной цели обучения: повышать или поддерживать свой профессионализм, развивать компетенции и сравнивать профессиональный уровень владения с уровнем других пользователей. Последняя цель помогает раскрыть суть второй концепции — образовательная сеть. Образовательная сеть представлена в виде группы практикующего сообщества, которое применяет компетенции в своей деятельности. Сеть необходима для того, чтобы стимулировать пользователей к развитию и сотрудничеству во время обучения. Третья концепция — модель представления компетенций — включает в себя информацию о компетенциях, описание требуемого уровня профессионального владения компетенцией для выполнения задач или решения проблем и карты компетенций — набор компетенций определенной группы практикующего сообщества. Последняя концепция — образовательные материалы — представлена в виде источников информации, описания деятельности пользователя (оценка, обучение и другая активность), а также в виде персонализированных планов профессионального обучения пользователя.

Требования к системе, предъявляемые авторами работы [8]:

– определение целевой компетенции (пользователь имеет возможность создать профиль целевой компетенции, т.е. компетенции, которую он хотел бы развить. Это, в свою очередь, является основой для формирования персонализированного профессионального плана развития пользователя);

– соотнесение имеющихся компетенций с целевой (пользователь оценивает свои имеющиеся компетенции, а затем сравнивает их с теми, что он хотел бы развить);

– определение возможностей для развития компетенций (после определения пробелов в навыках пользователя, ему необходимо найти подходящие программы развития: курсы, документы, ресурсы, и выбрать какие-либо из них);

– формирование профиля компетенций (пользователь должен иметь возможность определять и описывать профили компетенций, а также интегрировать информацию о полученных им компетенциях из различных источников и документов);

– формирование персонализированного плана развития (пользователь должен иметь возможность получать какие-либо рекомендации, сформированные на основании информации об уже имеющихся в системе персонализированных планов профессионального развития других пользователей).

Система TENCompetence является клиент-серверным приложением. Клиентская часть разработана на платформе Eclipse Rich Client Platform, что дает возможность системе быть независимой от операционных систем. Сервер TENCompetence развернут на сервере приложений Tomcat, а база данных расположена на сервере MySQL.

Технопарк Университета ИТМО представляет собой объединение различных компаний, называемых резидентами, в одно сообщество при университете ИТМО. В университете существует единая система управления компетенциями резидентов Технопарка, реализованная для того, чтобы наглядно представлять компетенции резидентов потенциальным инвесторам либо заказчикам, которые хотят найти подходящего кандидата для выполнения поставленных задач. Система позволяет хранить информацию о резидентах в их личных профилях: общая информация, имеющиеся компетенции, профессиональный уровень владения компетенциями, свидетельства о получении компетенции. Компетенции в системе представлены в виде иерархии. Также в системе представлена возможность описывать задачи через требуемые для ее выполнения компетенции и профессионального уровня владения ими резидентом.

Требования к системе, предъявляемые авторами работы [10]:

– поиск резидентов по компетенциям, в результате которого будут найдены все похожие профили;

– «агрегация возможностей» — позволяет узнать все задачи, которые может выполнить искомый резидент;

– сравнение профилей задачи и резидента либо профилей двух резидентов;

– ранжирование профилей резидентов на основании наибольшего соответствия резидента задаче.

Система управления компетенциями технопарка университета ИТМО является клиент-серверным приложением. Серверная часть реализована на языке JAVA с использованием технологии Spring Framework. База данных расположена на сервере MySQL. Клиентская часть разработана с помощью технологий Spring Data JPA и Hibernate для извлечения данных и Spring MVC для представления пользовательского интерфейса.

IMPAKT — это интегрированная система управления кадровыми ресурсами предприятия, которая поддерживает выполнение 3-х бизнес-процессов компаний: извлечение ранжированного списка наиболее подходящих сотрудников для выполнения конкретных задач; формирование рабочей группы или команды для некоторой задачи или класса задач; и автоматическое извлечение ключевой компетенции компании. Авторы данной статьи определяют ключевую компетенцию организации как коллективный актив, являющийся результатом синергии всех человеческих ресурсов компании. Руководствуясь данным определением, исследователи представили алгоритм, который позволяет выявлять множество общих родовых объектов для сета, включающего в себя компетенции каждого сотрудника. Основной идеей данного алгоритма является выявление общей компетенции из сета профилей компетенций сотрудников компании. Для определения профилей сотрудников, которые могут войти в анализируемый сет, аналитик устанавливает соответствующий порог вхождения (например, рассматриваются только технические навыки в области информационных технологий). Более подробное описание алгоритма представлено в работе [12].

С помощью системы IMPAKT менеджер по персоналу описывает профиль кандидата; выполняет поиск кандидатов на должности, разделяя требуемые компетенции на обязательные и желаемые; получает ранжированную информацию по кандидатам, а также пояснения по полученной информации.

Система IMPAKT позволяет хранить профили сотрудников в формате, удобном для построения логических выводов с использованием SQL-запросов к реляционной базе данных отображенной в базу знаний IMPAKT. Система IMPAKT основывается на использовании разработанной авторами [12] онтологии, которая включает в себя около 5000 концептов, отображающих как технические, так и дополнительные компетенции сотрудника или кандидата. Под техническими компетенциями подразумеваются знания сотрудника/кандидата на должность о конкретных технологиях и инструментах, в то время как к дополнительным навыкам относятся способности к взаимодействию и коммуникации.

Подбор сотрудника с учетом обязательных и желаемых требований (matchmaking) проводится в два этапа: сначала поиск сотрудников, полностью удовлетворяющих обязательным требованиям (Strict Match), а затем на основании полученных результатов поиск по желаемым требованиям (Soft Match).

Требования, предъявляемые к системе IMPAKT авторами работы [12]:

– хранение информации о компетенциях сотрудников;

– предоставление возможности поиска кандидатов рекрутером (с учетом обязательных и желаемых требований);

– поиск и ранжирование кандидатов по наилучшему соответствию запросу;

– просмотр профиля каждого предложенного сотрудника;

– пояснение результата ранжирования;

– назначение более чем одной задачи группе сотрудников;

– определение ключевой компетенции компании (по любому критерию, определенному в онтологии).

Каждое описание задачи состоит из трех элементов: знания, требуемые для выполнения задачи, набор временных ограничений и число членов команды. Процесс создания команды рассматривает все возможные варианты компоновки/создания/сочетания членов команд как равновозможные. В случае, если найти команду, полностью удовлетворяющую запросу, невозможно, то система возвращает результат с командой, которая наиболее полно удовлетворяет запросу.

Система IMPAKT реализована на языке JAVA и использует JENA API для доступа к онтологии и Pellet Reasoner. Для хранения используется БД PostgreSQL.

Выявленные в процессе анализа рассмотренных систем управления компетенциями были систематизированы в виде сводной табли-

цы (таблица 1), в которой показаны основные сценарии использования системы управления компетенциями, соответствующие им требования, которые должны быть учтены для поддержки этих сценариев, а также выделенные сущности, которые должны быть отражены в концептуальной модели управления компетенциями.

Таблица 1. Соответствие выявленных требований сценариям использования

Сценарии использования	Требования к системе	Сущности концептуальной модели
1. Управление профилем пользователя / организации. 2. Управление компетенциями пользователя / организации в профиле.	–Хранение информации о пользователе / организации и его / ее компетенциях. –Управление информацией профиля. –Формирование персонализированного плана профессионального развития пользователя. –Выявление ключевой компетенции организации.	Пользователь; компетенция (с атрибутами навыки, знания, коммуникативные способности, профессиональный уровень владения), план профессионального развития.
3. Управление проектами.	–Хранение описания задач и компетенций в единой онтологии. –Разграничение прав доступа. –Поиск команды или отдельных пользователей во внешней среде.	Проект, задача (с атрибутами: требуемая обязательная компетенция, требуемая желаемая компетенция), компетенция.
4. Определение текущего профессионального уровня владения компетенциями пользователя / организации.	–Хранение информации о пользователе / организации и его / ее компетенциях. –Периодическая переоценка компетенций пользователя / организации. –Хранение онтологии компетенций вместе с описанием бизнес-процессов организации. –Выявление компетенций пользователя на основании бизнес-процессов организации и выполненных ранее им задач.	Пользователь, компетенция (с атрибутом «уровень профессионального владения»), сертификат (подтверждающий владение компетенцией)

Продолжение Таблицы 1.

5. Определение недостающих компетенций. 6. Переоценка компетенций назначенного на конкретную должность пользователя. 7. Отслеживание профессионального развития сотрудника (по изменениям имеющихся компетенций, отображенных в системе).	–Хранение информации о пользователе и его компетенциях. –Хранение информации о минимальном наборе компетенций, необходимом для конкретной должности, задачи, рабочей группы. –Хранение описания задач и компетенций в единой онтологии. –Определение «пробелов» в компетенциях. –Формирование кадрового резерва.	Пользователь, компетенция (с атрибутом «уровень профессионального владения»), сертификат (подтверждающий владение компетенцией), задача, проект
8. Поиск подходящих исполнителей для задач/проектов по заданным компетенциям, необходимым для выполнения проекта. 9. Создание ранжированных списков сотрудников, подходящих для выполнения задачи/проекта.	–Хранение информации о пользователе и его компетенциях. –Поиск подходящих исполнителей для выполнения задач/проектов по компетенциям. –Хранение описания задач и компетенций в единой онтологии. –Хранение стандарта или матрицы компетенций.	Пользователь, задача, проект, компетенция (с атрибутом «уровень профессионального владения»), матрица компетенций

В таблице 2 приведен сравнительный анализ рассмотренных систем управления компетенциями. В качестве показателей сравнения были выбраны основные требования, приведенные для каждой из систем авторами рассмотренных работ, а также требования, выявленные в результате анализа архитектуры других систем управления компетенциями (которые, однако, не имеют на сегодняшний день рабочего прототипа) [16-19].

Таблица 2. Сравнительный анализ систем управления компетенциями

Критерий сравнения	Система управления компетенциями				
	DeCom	KnoMe	IMPAKT	TENCompetence	Система Технопарка ИТМО
Требования к системам управления индивидуальными компетенциями					
Хранение информации о пользователе и его компетенциях	+	+	+	+	-
Формирование персонализированного плана профессионального развития пользователя	+	-	-	+	-
Периодическая переоценка компетенций пользователя	+	-	-	+	-
Выявление компетенций пользователя на основании бизнес-процессов организации и выполненных ранее им задач	-	-	-	-	-
Требования к системам управления бизнес-компетенциями организации					
Хранение информации об организации и ее компетенциях	-	-	+	-	+
Выявление ключевой компетенции организации	-	-	+		
Хранение онтологии компетенций вместе с описанием бизнес-процессов организации	(автоматически)	-	+		
Формирование кадрового резерва	(вручную)				
Общие требования					
Поиск подходящих исполнителей для выполнения задач/проектов по компетенциям.	+	+	+	+	+
Управление информацией профиля	+	+	+	+	+
Хранение стандарта или матрицы компетенций	+	+	-	-	-
Хранение описания задач и компетенций в единой онтологии	+	+	+	-	+

Продолжение таблицы 2.

Разграничение прав доступа	+	+	+	+	+
Определение «пробелов» в компетенциях	+	-	-	+	-
Поиск команды или отдельных пользователей во внешней среде	-	+	-	-	-
Модель компетенций, поддерживающая стандарт IEEE RCD	+	-	-	-	-

Из таблицы 2 видно, что самым мощным инструментом управления компетенциями как отдельных пользователей/сотрудников, так и компаний в целом является система IMPAKT, которая позволяет выполнять такие задачи, как: выявление ключевой компетенции компании на основании информации о компетенциях сотрудников организации, создание команды для выполнения задач (в нескольких вариантах), назначение нескольких задач одному сотруднику, поиск сотрудников с учетом обязательных и необязательных требований.

3. Основные сценарии использования и спецификация требований для автоматизации процесса поиска экспертов. Каждая из рассмотренных выше систем была создана для решения разных задач в области управления компетенциями. Системы DeCom, KnoMe и TENCompetence решают задачи отдельного пользователя: хранение и оценка имеющихся компетенций, создание персонализированного плана развития и предоставление обучающих материалов. Наряду с этим IMPAKT и Система управления компетенциями Технопарка Университета ИТМО позволяют искать целые команды или организации для выполнения задач или проектов, а также выявлять компетенции организации.

На основании анализа систем управления компетенциями были выявлены основные сценарии использования для автоматизации процесса поиска экспертов, представленные ниже.

– управление профилем пользователя (добавление, редактирование, удаление общей информации о пользователе, такой как имя, фамилия или название и тому подобное, связывание компетенциями);

– управление компетенциями пользователя в профиле пользователя (добавление, редактирование, удаление имеющихся компетенций);

– управление проектами организации (добавление, редактирование, удаление, создание связей с компетенциями);

– определение текущего профессионального уровня владения имеющимися компетенциями пользователя;

– определение недостающих компетенций (для выполнения задачи/проекта, получения должности и т.п.);

– поиск подходящих исполнителей для задач/проектов по заданным компетенциям, необходимым для выполнения проекта;

– создание ранжированных списков сотрудников, подходящих для выполнения задачи/проекта;

– периодическая переоценка компетенций назначенного на конкретную должность сотрудника;

– отслеживание профессионального развития сотрудника (по изменениям имеющихся компетенций, отображенных в системе).

Нетипичными сценариями использования (уникальные для каждой отдельной системы), рассмотрены более подробно:

– формирование персонализированного плана профессионального развития пользователя. В данном сценарии использования пользователь получает рекомендации по совершенствованию своих компетенций;

– поиск информации для смены профиля работы или продвижения по карьерной лестнице. Пользователь имеет текущий список с уровнем его компетенций и рейтинг должностей в компании, разница в требуемых компетенциях с которыми минимальная. Из этого списка он может выбрать интересующую его должность и получить список навыков/компетенций, которые ему необходимо развить;

– онлайн-обучение. В данном сценарии использования пользователь имеет доступ к различным обучающим материалам (книги, электронные журналы, статьи, аудио и видео материалы, вебинары, советы профессионалов и так далее), а также методам контроля (различные тесты), что позволит ему развивать компетенции в соответствии со сформированным персонализированным планом профессионального развития, а также отслеживать свой прогресс;

– поиск сотрудника по компетенциям с учетом обязательных и желаемых требований. Другими словами, поиск должен быть гибким. Он должен позволять пользователю указывать, какие из искомых компетенций являются обязательными, а какие опциональными. Данный сценарий использования является достаточно распространенным, так как весьма сложно найти исполнителя, чей набор компетенций абсолютно точно соответствует компетенциям, необходимым для выполнения задачи;

– поиск похожей компетенции. В случае, если для развития компетенции не нашлось походящих ресурсов — экспертов или объектов изучения, — то поиск продолжается по похожим компетенциям и связанным с ними ресурсам.

– распределение кадровых ресурсов в зависимости от типа задач: назначение одного человека на одну задачу; назначение нескольких человек на одну задачу; назначение нескольких задач на одного человека. Необходимость в таком сценарии использования продиктована следующими выявленными нюансами: (1) полное совпадение

между компетенциями сотрудников и компетенциями, требуемыми для выполнения задачи, случается крайне редко; (2) существуют такие задачи, результаты выполнения которых влияют на другие задачи, то есть выходные данные одной задачи являются входными для другой. Такие задачи лучше всего решать одному человеку. И, наконец, существуют задачи, требующие командной работы;

Аналогично на основании анализа работ в области управления компетенциями и выявленных сценариев использования были выделены следующие основные требования к системам управления индивидуальными компетенциями и компетенциями организации.

Основными требованиями к системе управления компетенциями являются следующие:

– *обеспечивать возможность управления информацией о пользователе*. Система должна обеспечивать добавление, редактирование, удаление общей информации о пользователе, такой как: личная информация, список имеющихся компетенций;

– *обеспечивать хранение следующей информации о пользователях*: профессиональные навыки; профессиональный уровень владения навыками; навыки, которые необходимо развить; пройденные программы повышения квалификации; характеристики как участника команды; результаты, достигнутые на предыдущих проектах;

– *хранить информацию о минимальном наборе компетенций, необходимом для конкретной должности, задачи, рабочей группы (стандарт или матрицу компетенций)*. На основании данных стандартов или матриц система будет иметь возможность выявлять навыки, которые необходимо развить пользователю;

– *хранить описание компетенций и задач для выполнения в единой онтологии*. Это требование является предпосылкой к реализации функции поиска исполнителей на задачи. Выполнение данного требования необходимо для того, чтобы не допустить ситуации при поиске, когда под двумя разными терминами подразумевается одно понятие или, наоборот, под одним термином подразумеваются различные понятия;

– *обеспечивать возможность поиска подходящих исполнителей для выполнения задач/проектов по компетенциям*. В системе должна быть реализована функция поиска исполнителя на задачу по заданным параметрам (например, поиск сотрудника, имеющего заданный набор компетенций с определенным уровнем профессионального владения; поиск сотрудника, чей профессиональный уровень владения конкретной компетенцией наивысший; или поиск не одного. А нескольких исполнителей на одну задачу, набор задач или целый проект);

– *Обеспечивать разграничение доступа к информации в зависимости от прав пользователя в системе*. Данное требование является стандартным и означает, что в системе должна быть реализована

функция разделения пользователей на группы и присвоения им определенных прав доступа, например: группа администраторов, группа исполнителей, группа работодателей (руководителей проектов, которые имеют права на размещение задач для исполнителей) и так далее.

К нестандартным требованиям к системе управления компетенциями можно отнести следующие:

– *определять «пробелы» в компетенциях пользователей на основании стандарта или матрицы компетенций (для конкретной должности или задачи)*. Реализация данного требования необходима для систем, целью которых является не только обычный поиск исполнителей на задачу, но и создание возможности формирования персонализированных планов развития пользователя в интересующих его сфере или направлении деятельности;

– *формировать персонализированный план профессионального развития пользователя и список необходимых для этого ресурсов для сокращения «пробелов» в его компетенциях*. Данное требование также в основном применимо к системам управления компетенциями, приоритетом которых является обеспечение возможности профессионального развития пользователя с помощью средств, которыми располагает организация;

– *периодически переоценивать компетенции пользователя и отслеживать прогресс их профессионального развития*. Данный функционал позволит хранить актуальную информацию о компетенциях пользователя, так как всегда существует вероятность того, что пользователь утратил компетенцию или приобрел новую (например, пользователь когда-то знал разговорный немецкий язык на уровне B1, но не использовал его в течение долгого периода, благодаря чему забыл множество слов и утратил уровень B1);

– *обеспечивать возможность искать команду или отдельных специалистов из внешней среды для привлечения их в организацию*. Данное требование актуально для систем, которые нацелены не только на создание команд из имеющихся пользователей/сотрудников, но и поиска новых ресурсов в случае, если располагаемые как-либо не удовлетворяют требованиям;

– *поддерживать стандарт IEEE RCD*. Использование уже готового описания компетенций позволит облегчить возможность интеграции имеющейся системы с другими системами;

– *хранить онтологию компетенций вместе с описанием бизнес-процессов и потоков данных компании*. Выполнение данного требования необходимо для того, чтобы иметь возможность связывать их друг с другом и облегчить выявление компетенций пользователя (см. следующий пункт);

– выявлять компетенции пользователя на основании бизнес-процессов организации, а также выполненных ранее пользователем задач, их степени сложности и шагов, предпринятых пользователем для их выполнения. Выполнение данного требования позволит наиболее точно оценивать компетенции пользователя и держать эти оценки в актуальном состоянии;

– обеспечивать возможность выявлять ключевые компетенции организации. Реализация данного требования необходима для того, чтобы организация могла понять свои сильные и слабые стороны и на основе этой информации создавать планы стратегического развития.

4. Концептуальная модель системы управления компетенциями участников экспертной сети. На основе выявленных сценариев использования и требований к автоматизации процесса поиска экспертов в экспертной сети для совместного решения ими задач была разработана концептуальная модель системы управления компетенциями в экспертной сети, представленная на рисунке 1. Основными сущностями данной концептуальной модели являются: участник экспертной сети, компетенция, компетентность, проект, задача и контекст.

Рассмотрим каждую из сущностей более детально.

Участник экспертной сети представляет собой как отдельного человека (эксперта), так и целую экспертную группу (резидента). У каждого участника есть профиль, который представляет собой модель участника в экспертной сети и содержит: личную информацию, контекст и имеющиеся компетенции.

Компетенция является совокупностью знаний, навыков, коммуникативных способностей в определенном контексте и характеризуется уровнем профессионального владения участником экспертной сети. Ее наличие может быть подтверждено свидетельством. При этом набор компетенций определяет *компетентность*, которая также может быть подтверждена свидетельством.

Задача имеет свой профиль, который представляет собой ее описание и список требуемых компетенций, необходимых для ее выполнения. Требуемые компетенции могут быть разделены на две категории: обязательные и желаемые. Обязательные компетенции — это те компетенции, без которых выполнение задачи не представляется возможным. Желаемые, в свою очередь, являются опциональным списком компетенций для данной задачи. Это означает, что при наличии всех обязательных компетенций, наличие компетенций из списка желаемых создаст претенденту на выполнение задачи конкурентное преимущество. Задача характеризуется контекстом и в зависимости от текущей ситуации в экспертной сети может иметь различный список требуемых и желательных компетенций для ее выполнения. Совокупность задач, объединенных общей тематикой, представляет собой *проект*.

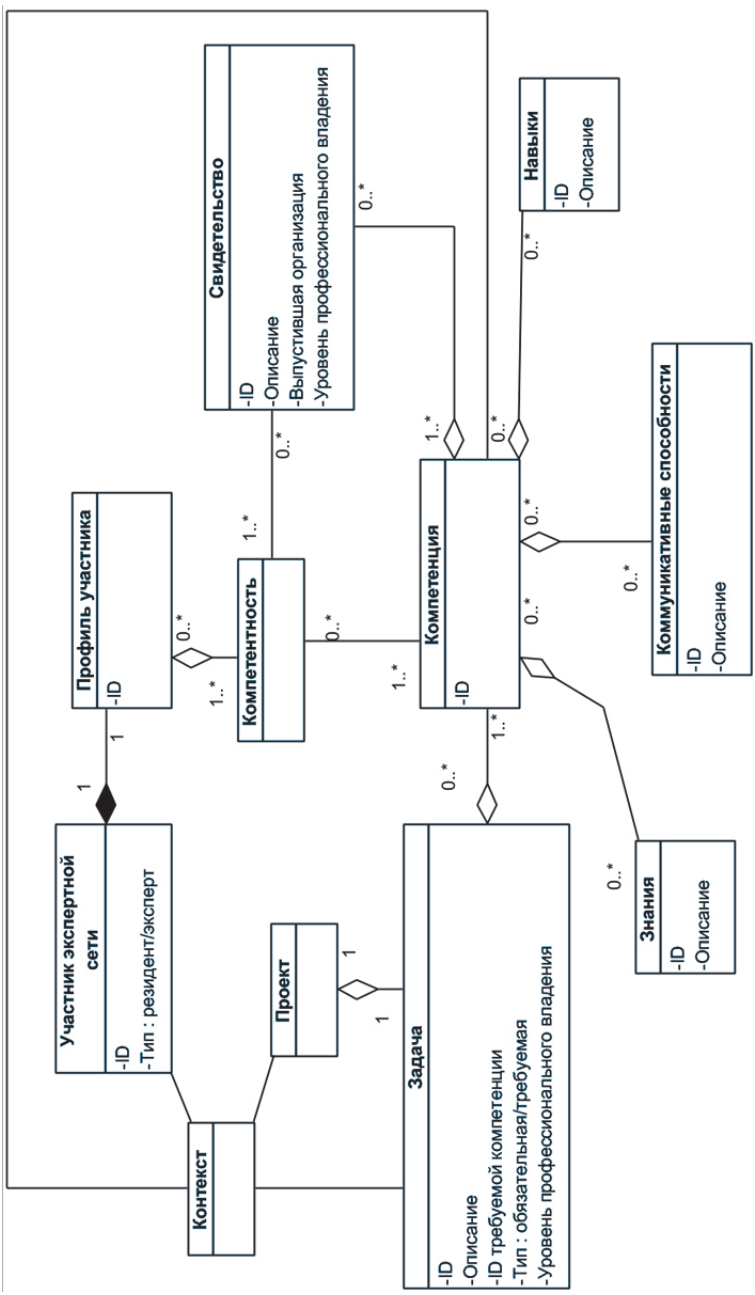


Рис. 1. Концептуальная модель системы управления компетенциями участников экспертной сети

Контекст. Сам термин контекст имеет множество определений. Согласно работе [20], самым распространенным из них является следующий: контекст — это любая информация, которая может быть использована для описания состояния сущности. При этом существует множество различных классификаций контекста, каждая из них имеет свои преимущества и недостатки, однако ни одна из них не может в полной мере удовлетворить всем требованиям, предъявленным к системе поиска экспертов в экспертных сетях.

Согласно работе [5], контекст разделяется на следующие классы:

– пространственно-временной контекст — описывает различные аспекты, связанные с пространством и временем. Включает в себя такие атрибуты, как время, местоположение, скорость, социальную сферу и так далее;

– контекст окружения — описывает сущности, которые окружают пользователя, а именно: сервисы, температуру, свет, влажность и так далее;

– индивидуальный контекст — описывает физическое состояние пользователя (пульс, давление, вес, цвет волос, настроение, предпочтения и т.д.);

– контекст задачи — описывает задачу, которую необходимо выполнить пользователю;

– социальный контекст — содержит информацию о социальной сфере пользователя, то есть соседях, друзьях, коллегах и родственниках, а также информацию о социальной роли пользователя, например, как начальника или исполнителя, студента или преподавателя и так далее.

Основываясь на данной классификации были выделены основные сущности классификации контекста экспертной сети (рисунок 2):

– контекст участника экспертной сети: пространственно-временной контекст, индивидуальный контекст, контекст окружения и социальный контекст;

– контекст актива: пространственно-временной контекст и контекст информации;

– контекст проекта и задачи: пространственно-временной контекст и контекст информации.

Контекст участника (экспертной сети) делится на две категории: контекст эксперта и контекст резидента. Контекст эксперта включает в себя информацию об его местоположении в физическом пространстве, статусе (доступен или не доступен для работы), сфере личных интересов, устройстве доступа (например, компьютер или телефон), а также его роль в системе, определяемую правами доступа. Контекст резидента включает в себя те же атрибуты, кроме сферы интересов. Вместо этого для резидента можно определить сферу деятельности. Кроме того, резидент может владеть активами, о которых будет сказано далее.

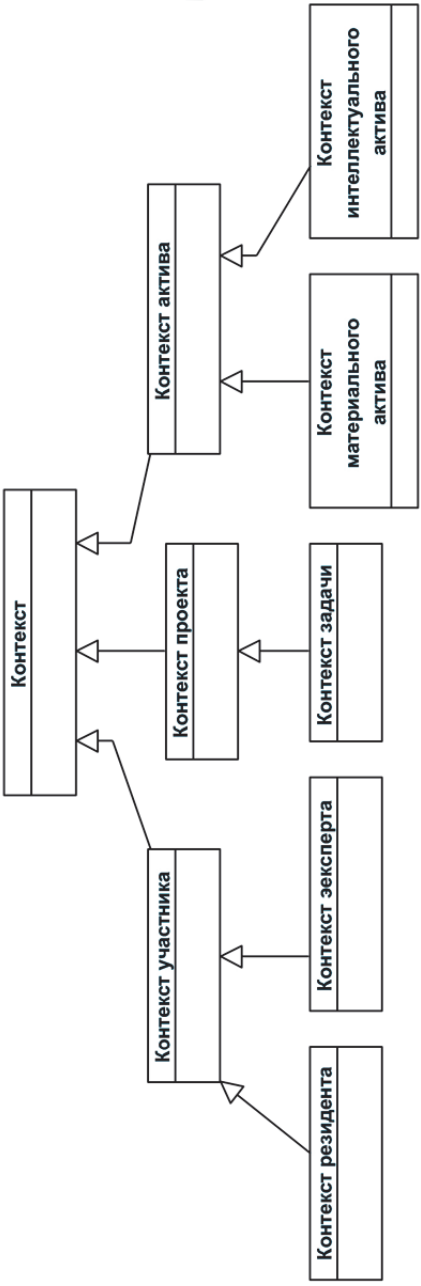


Рис. 2. Классификация видов контекста экспертной сети

Контекст участника (экспертной сети) делится на две категории: контекст эксперта и контекст резидента. Контекст эксперта включает в себя информацию об его местоположении в физическом пространстве, статусе (доступен или не доступен для работы), сфере личных интересов, устройстве доступа (например, компьютер или телефон), а также его роль в системе, определяемую правами доступа. Контекст резидента включает в себя те же атрибуты, кроме сферы интересов. Вместо этого для резидента можно определить сферу деятельности. Кроме того, резидент может владеть активами, о которых будет сказано далее.

Контекст актива представляет собой описание материальных или нематериальных ресурсов резидента. В данном случае материальные активы включают в себя предметы труда, здания, транспортные средства и так далее, а нематериальные активы представлены интеллектуальным капиталом, то есть экспертами и их компетенциями, а также сертификатами, подтверждающими наличие компетенций. Контекст интеллектуального актива может иметь атрибут «область применения». Например, участник экспертной сети, который имеет компетенцию «перевод текстов с английского языка», может переводить только технические тексты в области информационных технологий, а значит, областью применения будет «информационные технологии». Контекст свидетельства включает в себя описание времени и места выдачи данного свидетельства. Что касается материального актива, то он может быть описан такими атрибутами, как стоимость использования, местоположение, время использования (зима, лето и т.д.).

Контекст проекта наряду с *контекстом задачи* представляет собой описание области их применения (например, информационные технологии, лазерные технологии, пищевая промышленность и т.п.), а также дату начала и окончания их выполнения.

5. Оценка эффективности. Для оценки эффективности предложенной концептуальной модели системы управления компетенциями была рассмотрена задача поиска группы экспертов с требуемым набором компетенций с использованием обычной и предложенной в статье системы управления компетенциями. Критерием оценки эффективности является снижение времени поиска группы экспертов при использовании предложенной системы по сравнению с обычной. Таким образом, показателем эффективности в рассматриваемой задаче будет время поиска группы экспертов.

Экспертная сеть представлена в виде множества компетенций, которыми обладают эксперты или резиденты сети:

$$Network = (c_1, c_2, \ldots, c_N),$$

где N — количество компетенций в экспертной сети.

Каждая задача, поступающая для решения в экспертную сеть, описывается в следующем виде:

$$Task = (c_1, c_2, \ldots, c_M),$$

где M — количество компетенций, которыми должна обладать группа экспертов для решения задачи. Общее количество компетенций в системе всегда будет сильно больше, чем набор компетенций, требуемый для решения задачи, поэтому $N >> M$.

На рисунках 3 и 4 показан процесс поиска экспертов и резидентов в системе управления компетенциями для задачи. На рисунке 3 используется система управления компетенциями без учета контекста, а на рисунке 4 используется разработанная контекстно-ориентированная система управления компетенциями. В первом случае необходимо перебрать всех экспертов, зарегистрированных в системе управления компетенциями, в то время как во втором случае рассматриваются только те эксперты и резиденты, которые соответствуют контексту задачи.

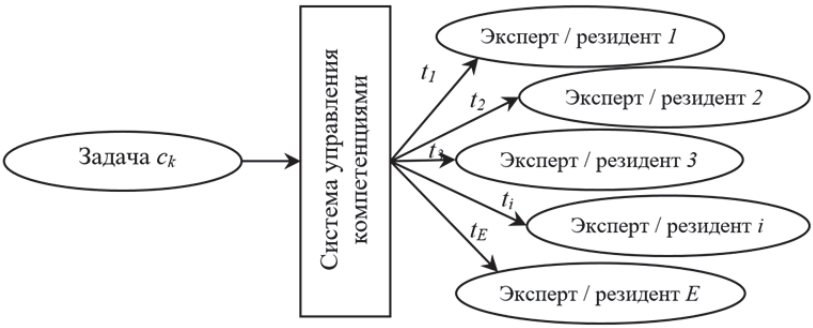


Рис. 3. Выбор экспертов для задачи c_k с использованием системы управления компетенциями без учета контекста

Время поиска группы экспертов / резидентов для задачи c_k в общем случае в системе управления компетенциями без использования контекста будет складываться из времени, затраченного на перебор всех экспертов и резидентов:

$$T_k = \sum_{i=1}^{E} t_i;$$

где t_i — время, затрачиваемое на проверку соответствия компетенций эксперта i для задачи c_k, а E — количество зарегистрированных экспертов / резидентов.

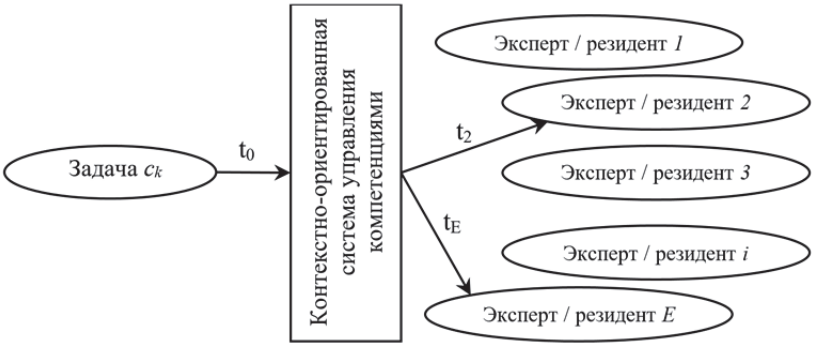


Рис. 4. Выбор экспертов для задачи c_k с использованием контекстно-ориентированной системы управления компетенциями

В случае использования контекстно-ориентированной системы управления знаниями время группы экспертов / резидентов для задачи c_k (T'_k) в общем случае будет складываться из времени формирования группы экспертов / резидентов, подходящих с учетом контекста (t_0) и времени, затраченного на перебор всех экспертов и резидентов из этой группы:

$$T'_k = t_0 + \sum_{i=1}^{E'} t_i,$$

где k — номер рассматриваемой задачи, t_i — время, затрачиваемое на проверку соответствия компетенций эксперта i для задачи c_k, t_0 — времени формирования группы экспертов / резидентов, подходящих с учетом контекста, а E' — количество экспертов / резидентов, подходящих для решения задачи c_k с учетом контекста.

В общем случае существует ситуация, при которой $E = E'$, тогда время поиска группы экспертов без использования контекста в системе управления компетенциями будет меньше, чем с использованием контекста. Такая ситуация может возникнуть в том случае, когда для решения задачи c_k необходимо привлечение всех доступных экспертов / резидентов. В реальной жизни такая ситуация маловероятна, и $E' << E$.

На рисунке 5 показаны графики зависимостей времени поиска группы экспертов для решения задачи от количества доступных экс-

пертов / резидентов с использованием и без использования контекста в системе управления компетенциями. При построении для наглядности было сделано допущение, что время, затрачиваемое на отбор каждого из экспертов, одинаковое и равно $t_{ср}$, тогда время поиска группы экспертов / резидентов для задачи c_k без использования контекста в системе управления компетенциями T будет равно:

$$T = t_{ср} E .$$

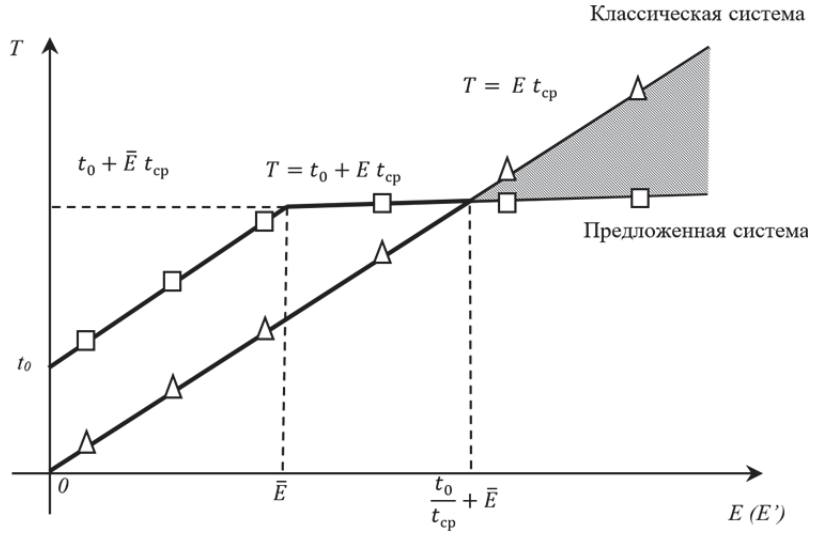


Рис. 5. Зависимость времени поиска группы экспертов для решения задачи от количества доступных экспертов / резидентов с использованием и без использования контекста в системе управления компетенциями

В случае использования контекстно-ориентированной системы управления компетенциями для задачи c_k будет сформирована группа из E' экспертов / резидентов за время t_0, и дальнейший отбор будет осуществляться из экспертов / резидентов этой группы. Причем:

$$E'\left[1, \overline{E}\right],$$

где $\overline{E}$ — это количество экспертов, участвующих в решении задачи. Причем, чем точнее контекст описывает текущую ситуацию, тем

меньше будет величина $\overline{E}$. Тогда для $E' < \overline{E}$ время взаимодействия участников с использованием контекста в системы управления знаниями будет определяться по формуле:

$$T = t_0 + E' t_{cp},$$

а для $N' > \overline{E}$, по формуле:

$$T = t_0 + t_{cp}.$$

6. Заключение. В статье представлен обзор существующих систем управления компетенциями в различных предметных областях, выявлены основные сценарии их использования и сформированы требования для класса систем управления компетенциями, ориентированных на автоматизацию процесса поиска группы экспертов для решения ими поставленной задачи. Сформулированные требования позволяют реализовать данные сценарии, что свидетельствует о достаточности определенного в статье набора требований для рассматриваемого класса систем. Самыми распространенными сценариями использования систем управления компетенциями являются следующие: поиск необходимого сотрудника; выявление компетенции организации; оценка имеющихся индивидуальных компетенций; выявление недостающих индивидуальных компетенций; построение индивидуального плана развития сотрудника; выявление требуемых индивидуальных компетенций; описание компетенций сотрудника и задач организации, используя единую терминологию и так далее. На основе выявленных требований была разработана концептуальная модель системы контекстно-ориентированного управления знаниями в экспертных сетях, которая объединяет выявленные положительные аспекты рассмотренных ранее моделей. Основными отличиями разработанной модели являются: поддержка требуемых и желательных компетенций при описании задачи и учет текущей ситуации в экспертной сети с использованием предложенной классификации видов контекста. При этом в рамках разработанной классификации видов контекста работе различается контекст участника, контекст актива и контекст проекта для формализации текущей ситуации в экспертной сети. Для оценки эффективности предложенной концептуальной модели системы управления компетенциями была рассмотрена задача поиска группы экспертов с требуемым набором компетенций с использованием предложенной контекстно-ориентированной системы управления компетенциями и с использованием системы управления компетенциями без использова-

ния контекста. Анализ показал, что при небольшом количестве экспертов в системе управления компетенциями эффективна будет классическая система, но с ростом количества экспертов предложенная система показывает лучшие результаты.

В качестве дальнейшей работы в данной области авторами планируется разработка архитектуры системы управления компетенциями на основе выявленных технологий и разработанной концептуальной модели, а также ее реализация и апробация.

Литература

1 *Miranda S., Orciuoli F., Loia V. Sampson D*. An ontology-based model for competence management // Data & Knowledge Engineering. 2017. vol. 107. pp. 51–66.

2 *Орешин А.Н., Лысанов И.Ю.* Новый метод автоматизации процессов аутентификации персонала с использованием видеопотока // Труды СПИИРАН. 2017. Вып. 54. С. 35–56.

3 *Бирюков Д.Н., Ломако А.Г., Жолус Р.Б.* Пополнение онтологических систем знаний на основе моделирования умозаключений с учетом семантики ролей // Труды СПИИРАН. 2016. Вып. 47. С. 105–129.

4 *Luis J. et al*. DeCom: A model for context-aware competence management // Computers in Industry. 2015. vol. 72. pp. 27–35.

5 *Krogstie J.* Requirement Engineering for Mobile Information Systems // Proceedings of 7th International Conference on Requirements Specification as a Foundation for Software Quality (REFSQ'01). 2001. 7 p.

6 *Niemi E., Laine S.* Designing a Competence Management System 'Knome' for a Knowledge-Intensive Project Organization // Proceedings of International Conference on Design Science Research in Information Systems (DESRIST 2016). 2016. vol. 7. pp. 217–222.

7 *Niemi E., Laine S.* Competence Management as a Dynamic Capability: A Strategic Enterprise System for a Knowledge-Intensive Project Organization // Proceedings of 49th Hawaii International Conference on System Sciences (HICSS 2016). 2016. pp. 4252–4261.

8 *Kew C*. The TENCompetence Personal Competence Manager. 2007. 6 p. URL: www.ceur-ws.org/Vol-280/p08.pdf (дата обращения: 04.04.2018).

9 *Vogten H., Koper R., Martens H., Bruggen J*. Using the Personal Competence Manager as a complementary approach to IMS Learning Design authoring // Interactive Learning Environments. 2008. vol. 16. no. 1. pp. 83–100.

10 *Smirnov A. et al*. Competency Management System for Technopark Residents: Smart Space-Based Approach // Internet of Things, Smart Spaces, and Next Generation Networks and Systems. 2016. LNCS 9870. pp. 15–24.

11 *Gordeev B., Baraniuk O., Kashevnik A*. Web-Based Competency Management System for Technopark of ITMO University // Proceedings of the 18th Conference of FRUCT association. 2016. pp. 463–466.

12 *Colucci S., Tinelli E., Di Sciascio E., Doninia F.M*. Automating competence management through non-standard reasoning // Engineering Applications of Artificial Intelligence. 2011. vol. 24. no. 8. pp. 1368–1384.

13 *Colucci S. et al.* Measuring core competencies in a clustered network of knowledge // Knowledge Management: Innovation, Technology and Cultures. 2007. vol. 6. pp. 279–291.

14 *Tinelli E. et al*. Embedding semantics in human resources management automation via SQL // Applied Intelligence. 2016. vol. 46(4). pp. 952–982.

15 *Tinelli E. et al*. I.M.P.A.K.T.: an innovative, semantic-based skill management system exploiting standard SQL // Proceedings of the 11th International Conference on Enterprise Information Systems (ICEIS 2009). 2009. pp. 224–229.

16 *Miranda S., Orciuoli F., Loia V., Sampson D*. An Ontology-based Model for Competence Management // Data & Knowledge Engineering. 2017. vol. 107. pp. 51–66.

17 *Draganidis F., Chamopoulou P., Mentzas G*. An Ontology Based Tool for Competency Management and Learning Paths // Proceedings of 6th International Conference on Knowledge Management (I-KNOW 06). 2006. pp. 1–10.

18 *Tripathi K., Agrawal M*. Competency Based Management In Organizational Context: A Literature Review // Global Journal of Finance and Management. 2014. vol. 6. no. 4. pp. 349–356.

19 *Hintringer S., Nemetz M*. Process driven Competence Management: A Case Study at Hilti Corporation // Proceedings of 6th Conference on Professional Knowledge Management: From Knowledge to Action. 2011. pp. 287–294.

20 *Alegre U., Augusto J.K., Clark T*. Engineering Context-Aware Systems and Applications: A survey // The Journal of Systems & Software. 2016. vol. 117. pp. 55–83.

Степаненко Виктория Александровна — магистрант кафедры информационных систем, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО). Область научных интересов: бизнес-аналитика, системы управления компетенциями. Число научных публикаций — 1. viktory.stepanenko@gmail.com; Кронверкский пр., 49, Санкт-Петербург, 197101; р.т.: +7(812)328-8071, Факс: +7(812)328-0685.

Кашевник Алексей Михайлович — к-т техн. наук, старший научный сотрудник лаборатории интегрированных систем автоматизации, Федеральное государственное бюджетное учреждение науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: управление знаниями, управление компетенциями, облачные среды, человеко-машинное взаимодействие, робототехника, профилирование, онтологии, интеллектуальные пространства. Число научных публикаций — 200. alexey@iias.spb.su; 14-я линия, 39, Санкт-Петербург, 199178; р.т.: +7(812)328-8071, Факс: +7(812)328-0685.

Гуртов Андрей Валерьевич — Ph.D., профессор, профессор кафедры компьютерных и информационных технологий, Линчёпингский университет. Область научных интересов: сетевая безопасность, индустриальный интернет, кибер-физические системы. Число научных публикаций — 200. andrei.gurtov@liu.se; SE-581 83, Линчёпинг, Эстергётланд, Швеция; р.т.: +46 13 28 47 02.

Поддержка исследования. Работа выполнена при финансовой поддержке РФФИ (проект № 16-29-12866), бюджетной темы № 0073-2018-0002 и гранта Университета ИТМО (проект № 617038).

DOI 10.15622/sp.59.7

V.A. STEPANENKO, A.M. KASHEVNIK, A.V. GURTOV

CONTEXT-ORIENTED COMPETENCE MANAGEMENT IN EXPERT NETWORKS

Stepanenko V.A., Kashevnik A.M., Gurtov A.V. **Context-Oriented Competence Management in Expert Networks.**

Abstract. Nowadays it is highly important for any organization to manage its resources effectively because of an unstable economy. There are two main resources of an organization: human resources and knowledge, which humans have. One of the ways for knowledge management is formalization of the competence management process by means of information systems. The choice of system depends on future use cases and system requirements. The purpose of this research is to analyze the competence management systems based on revealed common use cases and requirements. The result of the paper is a list with revealed common use cases and requirements, which could be useful for developing a new competence management system or for improving and modification an existing one. Based on the determined use cases and requirements the reference model of context-oriented competence management system in expert networks and context classification for current situation formalization have been developed. Developed reference model is oriented to take into account the current situation in the expert network. For this purposes a context model has been proposed that distinguishes participant context, active context, and project context. For the reference model efficiency estimation task for expert group search with needed competence set has been considered in the paper. In case of small amount of experts in expert network the classical system shows the better results but in case of large amount of experts the proposed system is better.

Keywords: competence management system, expert networks, competency, competence, common use cases.

Stepanenko Viktoriia Aleksandrovna — master student of information systems department, ITMO University (Saint Petersburg National Research University of Information Technologies, Mechanics and Optics). Research interests: business analysis, competence management systems. The number of publications — 1. viktory.stepanenko@gmail.com; 49, Kronverksky pr., Saint-Petersburg, 197101, Russia; office phone: +7(812)328-8071, Fax: +7(812)328-0685.

Kashevnik Alexey Mihajlovich — Ph.D., senior researcher of computer aided integrated systems laboratory, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS). Research interests: knowledge management, competence management, cloud computing, human-computer interaction, robotics, user profiling, ontologies, smart spaces. The number of publications — 200. alexey@iias.spb.su; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328-8071, Fax: +7(812)328-0685.

Gurtov Andrei Valer'evich — Ph.D., professor, professor of department of computer and information science, Linköping University (LIU). Research interests: network security, industrial Internet, cyber physi-cal systems, mobile networks, sensor networks. The number of publications — 200. andrei.gurtov@liu.se; 581 83 Linköping, Sweden; office phone: +46 13 28 47 02.

Acknowledgements. This research is supported by RFBR (grant 16-29-12866), State Research # 0073-2014-0005 and ITMO University (Project № 617038).

References

1. Miranda S., Orciuoli F., Loia V. Sampson D. An ontology-based model for competence management. *Data & Knowledge Engineering*. 2017. vol. 107. pp. 51–66.

2. Oreshin A.N., Lisanov I.Yu. [A New Method for Automation of the Personnel Authentication Process Using a Video Stream]. *Trudy SPIIRAN – SPIIRAS Proceedings.* 2017. vol. 54. pp. 35–56. (In Russ.).
3. Biryukov D.N., Lomako A.G. Zholus R.B. [Ontological Knowledge System Completion Based on Modeling Inferences Taking into Account Role Semantics]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2016. vol. 47. pp. 105–129. (In Russ.).
4. Luis J. et al. DeCom: A model for context-aware competence management. *Computers in Industry*. 2015. vol. 72. pp. 27–35.
5. Krogstie J. Requirement Engineering for Mobile Information Systems. Proceedings of 7th International Conference on Requirements Specification as a Foundation for Software Quality (REFSQ'01). 2001. 7 p.
6. Niemi E., Laine S. Designing a Competence Management System 'Knome' for a Knowledge-Intensive Project Organization. Proceedings of International Conference on Design Science Research in Information Systems (DESRIST 2016). 2016. vol. 7. pp. 217–222.
7. Niemi E., Laine S. Competence Management as a Dynamic Capability: A Strategic Enterprise System for a Knowledge-Intensive Project Organization. Proceedings of 49th Hawaii International Conference on System Sciences (HICSS 2016). 2016. pp. 4252–4261.
8. Kew C. The TENCompetence Personal Competence Manager. 2007. 6 p. Available at: www.ceur-ws.org/Vol-280/p08.pdf (accessed: 04.04.2018).
9. Vogten H., Koper R., Martens H., Bruggen J. Using the Personal Competence Manager as a complementary approach to IMS Learning Design authoring. *Interactive Learning Environments*. 2008. vol. 16. no. 1. pp. 83–100.
10. Smirnov A. et al. Competency Management System for Technopark Residents: Smart Space-Based Approach. Internet of Things, Smart Spaces, and Next Generation Networks and Systems. 2016. LNCS 9870. pp. 15–24.
11. Gordeev B., Baraniuk O., Kashevnik A. Web-Based Competency Management System for Technopark of ITMO University. Proceedings of the 18th Conference of FRUCT association. 2016. pp. 463–466.
12. Colucci S., Tinelli E., Di Sciascio E., Doninia F.M. Automating competence management through non-standard reasoning. *Engineering Applications of Artificial Intelligence.* 2011. vol. 24. pp. 1368–1384.
13. Colucci S. et al. Measuring core competencies in a clustered network of knowledge. Knowledge Management: Innovation, Technology and Cultures. 2007. vol. 6. pp. 279–291.
14. Tinelli E. et al. Embedding semantics in human resources management automation via SQL. *Applied Intelligence*. 2016. vol. 46(4). pp. 952–982.
15. Tinelli E. et al. I.M.P.A.K.T.: an innovative, semantic-based skill management system exploiting standard SQL. Proceedings of the 11th International Conference on Enterprise Information Systems (ICEIS 2009). 2009. pp. 224–229.
16. Miranda S., Orciuoli F., Loia V., Sampson D. An Ontology-based Model for Competence Management. *Data & Knowledge Engineering*. 2017. vol. 107. pp. 51–66.
17. Draganidis F., Chamopoulou P., Mentzas G. An Ontology Based Tool for Competency Management and Learning Paths. Proceedings of 6th International Conference on Knowledge Management (I-KNOW 06). 2006. pp. 1–10.
18. Tripathi K., Agrawal M., Competency Based Management In Organizational Context: A Literature Review. *Global Journal of Finance and Management*. 2014. vol. 6. no. 4. pp. 349–356.
19. Hintringer S., Nemetz M. Process driven Competence Management: A Case Study at Hilti Corporation. Proceedings of 6th Conference on Professional Knowledge Management: From Knowledge to Action. 2011. pp. 287–294.
20. Alegre U., Augusto J.K., Clark T. Engineering Context-Aware Systems and Applications: A survey. *The Journal of Systems & Software*. 2016. vol. 117. pp. 55–83.

DOI 10.15622/sp.59.8

M. SEČUJSKI, S. OSTROGONAC, S. SUZIĆ, D. PEKAR

LEARNING PROSODIC STRESS FROM DATA IN NEURAL NETWORK BASED TEXT-TO-SPEECH SYNTHESIS

Sečujski M., Ostrogonac S., Suzić S., Pekar D. **Learning Prosodic Stress from Data in Neural Network based Text-to-Speech Synthesis.**

Abstract. Naturalness is one of the most important aspects of synthesized speech, and state-of-the-art parametric speech synthesizers require training on large quantities of annotated speech data to be able to convey prosodic elements such as pitch accent and phrase boundary tone. The most frequently used framework for prosodic annotation of speech in American English is Tones and Break Indices – ToBI, which has also been adapted for use in a number of other languages. This paper presents certain deficiencies of ToBI when applied in synthesis of speech in American English, which are related to the absence of tags specifically intended to mark differences in the level of prosodic stress (emphasis) related to a particular sentence constituent. The research presented in the paper proposes the introduction of a set of tags intended for explicit modeling of the degree of prosodic stress. Namely, a certain sentence constituent can be particularly emphasized, when it is the intended focus of the utterance, or it can be de-emphasized, as is commonly the case with phrases reporting direct speech or with comment clauses. Through several listening tests it has been shown that learning such prosodic events from data has distinct advantages over approaches attempting to exploit the existing ToBI tags to convey the degree of emphasis in synthesized speech. Namely, speech synthesized by a neural network trained on data tagged for the level of prosodic stress appears more natural, and the listeners are more successful in locating the sentence constituent carrying prosodic stress.

Keywords: American English, prosodic stress, speech synthesis, ToBI.

1. Introduction. The quality of text-to-speech (TTS) synthesis systems is generally rated in terms of the intelligibility and the naturalness of the speech they produce. The intelligibility of synthesized speech is a well-defined concept, which is also easily evaluated through measures such as tests based on semantically unpredictable sentences (SUS) [1]. On the other hand, naturalness is a less defined concept, but it has nevertheless been widely used as a measure of TTS quality at events such as Blizzard challenges [2, 3]. The perceived feeling of naturalness of synthetic speech is based on a number of parameters that are difficult to identify and enumerate, and consequently, listeners are unable to tell what exactly contributes to naturalness [4]. Although there is no general consensus as to what naturalness is, a number of parameters related to it have been proposed, ranging from the ease of comprehension to the internal coherence of the acoustics of the utterance [5]. In many studies

the general quality of speech, or its similarity to natural human speech, is the only concept of naturalness that is evaluated. Ultimately, a successful text-to-speech (TTS) system should be able to convince listeners that they are listening to actual human speech.

Although synthetic speech has reached the level of intelligibility needed for wide practical application a long time ago, there are still challenging problems that remain to be solved. The current focus of the TTS research community is the synthesis of expressive content, which includes emotional expressivity, synthesis of different speaking styles, but no less importantly, synthesis of prosodic elements that convey linguistic meaning. Namely, the prosodic features of a natural-sounding synthesized utterance (the fundamental frequency contour — f_0, durations of phonetic segments, as well as temporal changes in volume) should match the features in a possible rendition of the same utterance by an actual human speaker, having in mind that there are many possible renditions of a single utterance, but that some of them may indicate differences in meaning. From the point of view of the listener, the main purposes of prosody in synthetic speech is to indicate syntactic boundaries and reveal some of the underlying syntactic structure of the utterance, as well as to facilitate the recognition of sentence constituents by exploiting the linguistic function of intonation and stress through combining different prosodic variables – pitch, length, loudness and timbre (quality of sound). The variability of these factors in speech appears to be largely ignored by the listeners. However, when some of them are missing or are inadequate, this is perceived as unnatural, and can even impair the intelligibility of synthesized speech, particularly in languages with stress or accent minimal pairs (pro-*test* vs. *pro*-test in English).

Nowadays, users of state-of-the-art dialogue systems expect to interact along the same principles that they use when interacting with other human beings, and consequently, dialogue systems are expected to behave and speak like human beings [6]. There have been various directions of research into how synthesized speech can be made more human-like. For instance, adding non-verbal elements such as laughing, breathing and clicking noises has been shown to increase the user's perception of naturalness of synthetic speech [7]. There has also been significant research effort aimed at investigating the influence of the insertion of filled pauses [8] or other manifestations of hesitation disfluency [9]. However, much of the naturalness of synthetic speech is

ruled by factors with deeper linguistic roots. Namely, for the user of a speech synthesis system to receive information with minimum cognitive effort, it is important that the system should be able not only to provide basic prosodic cues such as word stress or pitch accent to the listener, but to be able to convey elements such as rising intonation that turns a statement into a yes/no question, or prosodic stress, i.e. placing of emphasis on particular words because of their relative importance in the sentence.

Prosodic stress is often used pragmatically to focus the attention of the listener on particular words or the ideas associated with them, thus changing or clarifying the meaning of a sentence:

- *John* met Iris today. (Iris wasn't met by someone else today.)
- John met *Iris* today. (John didn't meet someone else today.)
- John met Iris *today*. (John and Iris didn't meet on some other day.)

Prosodic stress typically manifests itself as an increase in the prominence of stressed syllables, in terms of one or more prosodic variables previously mentioned. Words associated with prosodic stress are usually pronounced with louder and longer stressed syllables, and their fundamental frequency (pitch) usually extends over a wider range [3]. Stressed vowels in words carrying prosodic stress are typically associated with a more prominent pitch or pitch movement, increased duration and loudness, and they tend to be more peripheral in quality then vowels which are not associated with prosodic stress, which are normally more centralized. Furthermore, the stress-related acoustic differences between the syllables of a word that is not prosodically stressed are generally small compared to the differences between the syllables of a word which carries prosodic stress (cf. e.g. *Iris* and *today* in the examples above). Another use of prosodic stress is related to stress patterns that can be typical of a certain language, e.g. in French prosodic stress is typically placed on the final syllable of a string of words. This research will principally deal with the pragmatic use of prosodic stress, which is also referred to as contrastive stress. In natural human speech, there are also words and entire phrases that are pronounced in a pitch range that is compressed, in order to indicate that they are less relevant or that they do not bring any new information to the listener. A speech dialogue system that aims at establishing effortless speech communication with a human user should be able to provide such linguistic cues as well.

Parametric speech synthesizers represent the most widely used speech synthesis technique today, owing to their capability to learn complex mappings from linguistic features to acoustic features from data. They usually require large quantities of speech data to learn from, and obtain best results if the speech data is properly annotated. The principal task of a parametric speech synthesis system is to convert the input text into the acoustic features of speech which will be produced by a vocoder. To make this task easier, the input text is usually accompanied by annotation at various levels, not only regarding the phonemic identity of phonetic segments, but also prosodic features, at the level of syllable, word, phrase, or the entire utterance. On the other hand, the annotation of speech corpora is known to be an extremely time consuming task, requiring a lot of human effort, and often requiring the engagement of expert linguists.

Phonetic annotation represents the marking of phoneme and word boundaries and it can be carried out automatically with relatively high accuracy, based on the alignment of phonetic transcriptions and speech data collected from the voice talent. In order to avoid possible training errors introduced by faulty phonetic transcription, manual verification of phone and word boundaries is usually performed, possibly aided by a suitable graphical user interface. On the other hand, prosodic annotation represents the marking of a range of prosodic events at different levels, and is most often entirely manual. Prosodic annotation is carried out according to a chosen intonational model, which attempts to describe the intonation and temporal structure of the sentence. Intonational models can be divided into two broad categories, depending on the way they treat the dynamic character of the speech signal [1]. *Phonetic* models of intonation attempt to provide an explanation of the intonational features of the speech signal, especially the fundamental frequency. However, they are principally based on physical features and as such are unable to provide a connection to a discrete set of linguistic features that have a great influence on the acoustics of the utterance. *Phonological* models, on the other hand, are directly relevant to the listeners and their perception of speech, as they establish the relationship between the acoustic features of the signal and a corresponding discrete set of linguistically motivated prosodic events. For these reasons phonological models are relevant to both automatic speech synthesis and recognition. The intonational model most often used for American English is the Tone and Break Indices (ToBI), which is based on indexing pitch accents, phrase accents as well as boundary tones [11].

The remainder of the paper is organized as follows. The next section gives a brief overview of the standard ToBI model for American English, followed by a discussion on some of its shortcomings related to the synthesis of expressive speech. The issue of prosodic stress as well as reproduction of utterances containing direct speech and reporting phrases are given particular attention. To overcome these shortcomings of ToBI, the study described in this paper proposes an extension to the standard set of ToBI tags, which consists of the introduction of explicit marking of the degree of emphasis that the speaker associates with particular sentence constituents. Section 3 will present an experiment involving a listening test performed by 20 listeners, which confirms that the use of the ToBI model extended in this way leads to an improvement in the naturalness of synthesized speech and allows the listener to estimate the relative importance of particular words or phrases more accurately. The following section discusses the results of the experiment, while the concluding section summarizes the paper and provides an overview of the directions of future research.

2. ToBI intonational model and its shortcomings. Tone and Break Indices (ToBI) is a high-level prosodic model that has firstly been developed for American English, and was later extended with a number of variants for other languages [12]. ToBI represents the intonation of an utterance as a linear concatenation of tonal events, and global intonational contours are explained as concatenations of local strings of events.

A ToBI prosodic transcription of a particular utterance describes its tonal events and internal phrase structure, and can also provide other information as well. The term *tonal event* includes pitch accents, phrase accents as well as boundary tones. Tonal events represent combinations of high and low tones that may be associated with stressed syllables. The pitch accent that will be used in a certain situation depends largely on the syntax of the utterance, but it can also depend on semantics as well as a specific intention of the speaker. Consequently, the confidence with which pitch accents can be predicted is much lower than e.g. the confidence with which one can predict stressed syllables within a word. Since within each pitch accent a stressed syllable can be assigned a high or a low tone, pitch accents are divided into two groups – high (such as H*) and low (such as L*), and various other combinations such as L+H* i L*+H, are also allowed, with asterisk indicating the stressed syllable. Since the speaker assigns pitch accents i.e. prosodic prominence only to words which he/she considers important in a given situation, it is also possible that a stressed syllable does not carry a pitch accent at all.

The ToBI model also uses appropriate tags to indicate the internal phrase structure of an utterance, although the model is still essentially linear. Phrase breaks are indicated with levels from 0 to 4, where e.g. the lowest-level break index (0) is defined in terms of connected speech processes (occurring at boundaries such as "*did you*"), 1 indicates the typical absence of break at most phrase-medial word boundaries, while 4 indicates the boundary between two full intonational phrases. Namely, the utterance is divided into intonational phrases, delineated by level 4 breaks, and within an intonational phrase it is possible to identify intermediate phrases, delineated by level 3 breaks. Break index 2 indicates a sense of disjuncture at a boundary between two words where there is no acoustic evidence of tonal events and thus break indices 3 and 4 are not suitable. Each intermediate phrase boundary (break index 3) is assigned a phrase accent (L-, !H- and H-, where the exclamation mark denotes a downstep related to the previous H), while each intonation phrase (break index 4) is assigned a boundary tone (L% and H%). As each intonational phrase consists of at least one intermediate phrase, each level 4 boundary represents at the same time a level 3 boundary, which means that there are 6 possible combinations of phrase accents and boundary tones that can appear at the end of an intonational phrase (L-L%, H-L%, !H-L%, L-H%, H-H% and !H-H%). Phrase accents are also used to indicate the beginnings of intermediate phrases (%H and %L). The standard ToBI system includes other tags, such as the diacritic '<', which is used in combination with a high pitch accent when the syllable that follows the stressed syllable is higher than the stressed syllable (delayed peak). Some of the tags used by standard ToBI have been ignored in this research for being irrelevant (e.g. the tags indicating disfluencies in spontaneous speech were not used since the speech corpora used for training contain only fluent speech), and optional ToBI tags were not used.

Local tonal events, i.e. pitch accents, phrase accents and boundary tones, are considered as targets along the global intonational contour, and standard ToBI assigns local tonal events to specific points in time. However, this relationship between ToBI tonal events and particular time instants should be considered rather loose, since any identification of temporal events in linguistically motivated abstract representations would essentially be meaningless. In order to emphasize the symbolic aspect of ToBI, as well as to further simplify both ToBI corpus annotation and prediction of ToBI tags in synthesis, in this research it was assumed that

ToBI tags are assigned to particular phones, or in some cases words, instead of being assigned to arbitrary points in time. Similar modifications to the standard ToBI framework have already been implemented in speech synthesis systems such as *Festival* [13].

The standard ToBI model possesses many advantages which make it the model of choice for use within speech technology systems, and it has been defined having in mind its possible use within such systems. Namely, prosodic events are clearly defined, in a way that can be easily interpreted by a computer, the model is easily extensible to other languages and linguistic phenomena, and it has been designed so as to minimize the degree of disagreement between different ToBI annotators [14]. A speech synthesis model such as a neural network, when trained on ToBI annotated speech, is able to learn to reproduce the acoustic features of speech from its ToBI annotation. However, it should be kept in mind that the conversion of an intonation contour into its ToBI representation is many-to-one, which means that a number of intonation contours, which can be vastly different among themselves in terms of absolute frequencies and temporal behaviour, can correspond to the same ToBI transcription. Consequently, even within a single speaker, a ToBI transcription cannot be uniquely mapped into a set of acoustic features, i.e. a parametric speech synthesizer could construct a number of different sets of acoustic features based on a single ToBI transcription. As regards speech synthesis, it is sufficient that a parametric speech synthesizer should produce a set of acoustic features which would yield speech that sounds acceptable in a particular context.

From the point of view of expressive speech synthesis, an important advantage of using ToBI for symbolic representation of prosody is that it is possible to control some of the prosodic features of synthesized speech by manipulating its ToBI transcription. For instance, by manually changing pitch accents, phrase accents and boundary tones, statements can be turned into yes/no questions, and it is also possible to direct the attention of the listener to a particular word in the utterance. On the other hand, the ToBI model also has a number of disadvantages. Firstly, even for a person with relevant linguistic knowledge, ToBI annotation is a rather complex process, which has been reported to last up to several hundred times more than the duration of the speech being annotated [15]. Furthermore, since ToBI annotation essentially relies on the annotator's tacit understanding of the relationship between the objective intonational contour and its symbolic representation, there

is a strong subjective component to it. Consequently, regardless of the original intention to minimize the inter-annotator disagreement, it is still reported to be relatively high [16]. Finally, due to the complexity of the ToBI tagset, some tags or tag combinations may be scarce or completely absent from speech corpora, which has a negative effect on training [14]. For that reason, common modifications of the standard ToBI model usually include merging some of its categories into one, as it was done e.g. in [17].

The weakness of the standard ToBI model which is of particular relevance for this research is that it is not quite suitable for conveying linguistically relevant prosodic features such as prosodic stress. Namely, the relationship between ToBI tags and the perception of importance by the listener is defined on a relative scale, which means that ToBI can convey that one word may be more prosodically prominent than another, but cannot convey the absolute degree of its prosodic prominence. The distinction that ToBI makes between words with pitch accents and words without pitch accents appears to be insufficient to indicate e.g. that, among the words with pitch accents, one is significantly more important than others.

As far as the prosodic stress (assigning particular prominence to a word which carries new or particularly important information) is concerned, as in:

*Sarah will go to **London** in September.* (1)

ToBI does not offer an explicit solution. Clearly, the novelty of the information conveyed is related to the ToBI tags used, and this relationship has been the topic of much research. For example, in [18] the use of H* and L+H* pitch accents is reported to be related to novelty, while given or available information is assigned other pitch accents, depending on the context. However, this relationship is not conclusive enough to serve as a basis for the reproduction of prosodic stress in speech synthesis. For example, an instance of prosodic stress indicated with a bitonal accent L+H* in the synthesis of expressive speech is not necessarily converted to an acoustic representation characterized by sufficient prominence of the stressed syllable so as to unambiguously indicate prosodic stress. The most common reasons for this are related to the lack of training data, as well as the fact that the acoustic realizations of prosodic stress may be highly variable, and

commonly affect not only the intonation contour, but also the duration of particular phonetic segments as well as the manner of their articulation. For all these reasons, in practice more reliable means for conveying emphasis are usually preferred. For instance, to indicate the prosodic prominence of a particular word, the IBM speech synthesizer [19] combines the pitch accent H* and the phrase accent L-. The motivation for introducing suck a one-to-one mapping between contrastive prosodic stress and particular ToBI tags came from the analysis of a very small corpus consisting of several declarative sentences spoken by 20 professional speakers. It was found that the contrastively-emphasized word consistently had at least intermediate prosodic phrase boundaries on each side of the word, accompanied by break indices of level at least 3. However, although such a representation may have provided an unambiguous cue to prosodic stress, a one-to-one mapping between prosodic stress and particular ToBI tags is not what happens in practice, and thus results in a certain loss of naturalness. The research described in this paper exploits the appearance of more powerful automatic learning algorithms which are able to establish a more sophisticated relationship between prosodic stress and its acoustic counterparts. For that to be possible, an explicit tag (E+) has to be introduced in order to indicate that the speaker has intentionally emphasized a particular word. By training on a speech corpus that contains words tagged with E+ it was made possible for the system to establish, by learning from data, the connection between the intention to emphasize a word and its acoustic realization.

Similarly, standard ToBI does not offer any possibility to explicitly mark content that is commonly de-emphasized, such as comment clauses or inquit formulas used to report direct speech:

It would be nice, ***I suppose****, if they keep their promise.* (2)

"You should have seen it coming," ***I replied****.* (3)

Such phrases are commonly pronounced in a compressed range of fundamental frequency, i.e. pitch, in order to convey their lower degree of importance or the fact that they are not a part of the main clause. The research presented in this paper also investigated the possibility of annotating deemphasized content with a specific tag (CF0 — compressed f_0), in order to allow the system to reach its own conclusions as to the relationship between

the intention to de-emphasize a clause and its acoustic realization. To the best of our knowledge, there has been no research effort to explicitly model this type of dependency or introduce reduced emphasis into synthesized speech. An example of a ToBI annotation following the guidelines modified so as to accommodate for the introduction of E+ and CF0 tags is given in Figure 1.

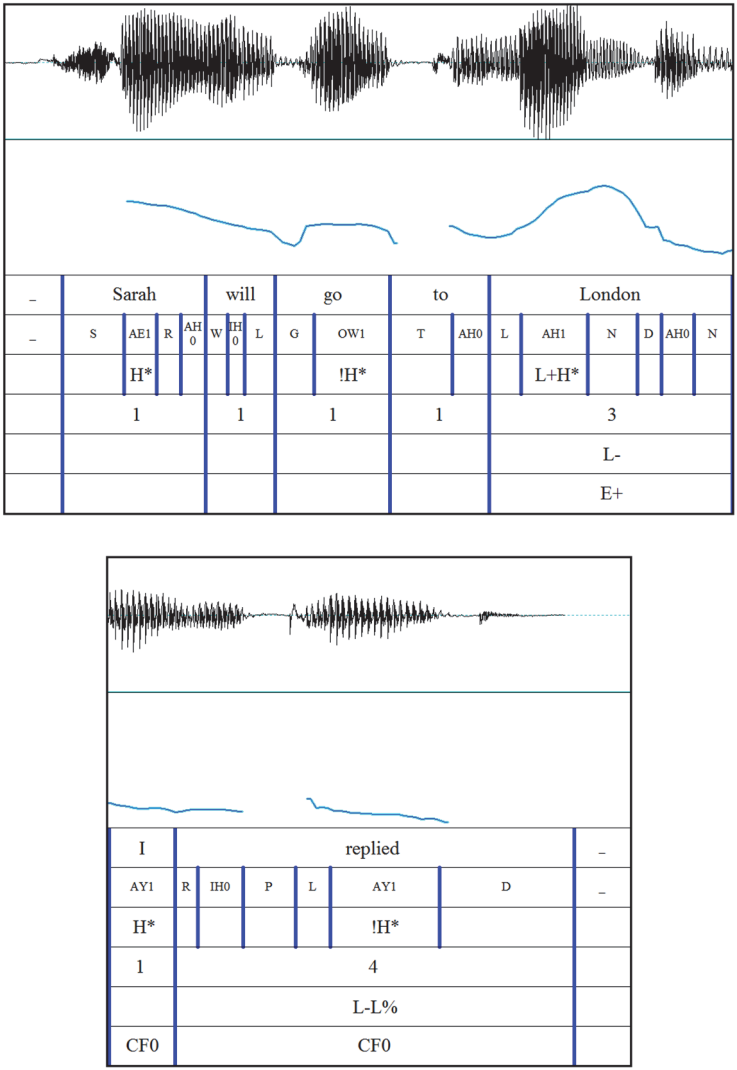


Fig. 1. Prosodic annotation of the sentence "*Sarah will go to London, I replied.*"

The same guidelines were used to annotate all speech data used for training in this research. Namely the annotators were instructed to do the following:

– Use the E+ tag on words whose prosodic features, including not only intonation but also the degree of articulation effort, seem to indicate that the speaker intended to assign particular importance to the word because it brings new information or is contrasted to an alternative word (stated or implied). This annotation was used on top of ToBI with no restrictions, in order to make it ToBI independent. For instance, if the articulation effort was strong enough, even the words regularly tagged with !H* could be assigned E+. Furthermore, while E+ was commonly indicated by higher pitch values in words with high ToBI pitch accents, it was also indicated by lower pitch values in words with low pitch accents. Such a use of E+ allowed it to be effectively excluded from some rounds of experiments, as it will be explained in the following section.

– Use the CF0 tag on clauses that are pronounced in a compressed pitch range, which seems to indicate that the speaker intended to assign to them a lower degree of emphasis than to the remainder of the utterance. These cases most notably included, but were not limited to, phrases reporting direct speech, comment phrases, asides and right dislocations related to afterthoughts. There is, however, a certain degree of dependence of ToBI annotation on the presence or absence of CF0. Namely, the clause under CF0 was ToBI annotated as if its pitch range was normal, which means that simple removal of CF0 from the speech corpus may not be adequate in all cases, unlike the case with E+.

3. The experiments. The experiments have been carried out on two speech corpora of American English, containing utterances provided by one male speaker (M) and one female speaker (F), both professional voice talents. The basic data related to the speech corpora is given in Table 1, including the data on the total number of E+ and CF0 tags. Both E+ and CF0 tags were used at word level, so it should be noted that the number of CF0 tags indicates the total number of *words* in clauses tagged with CF0. The numbers of E+ and CF0 tags are not the same across the two speakers, but this difference was disregarded in the experiment and two synthesizers, each trained on one of the corpora, were used in the listening tests in equal measure, i.e. the listeners were provided with examples of synthesized speech from both, male alternating with female for diversity. The results of the experiments were analyzed without regard

to the fact which of the corpora was used for training the system that provided a particular example of synthetic speech.

Table 1. Content of speech corpora

	M	F
Duration	3h 33min	4h 20min
# of utterances	3316	4556
# of words	43632	49580
# of E+	629	1162
# of CF0	2359	5522

The model used for synthesis of utterances in all experiments was based on deep neural networks (DNN), owing to the fact that they clearly outperform previous parametric approaches to speech synthesis [20]. The model is described in detail in [21], and it will be briefly presented here. It was developed using the *Merlin* toolkit [22] with some modifications, as well as the CNTK framework [23]. The WORLD vocoder [24] is used to convert the acoustic features provided by the model into a speech signal, and is also used to provide the acoustic feature vectors in the training phase.

In the synthesis phase, the input text is firstly processed to obtain linguistic features relevant for synthesis. The obtained linguistic features include phone identity and the identities of neighbouring phones, the phone position related to syllable/word/phrase boundary, word position related to phrase boundary, number of phones in syllable/word, number of words in phrase/utterance, part-of-speech information as well as prosodic information represented by ToBI transcription. After the linguistic features are obtained, the acoustic features are produced from the phonetic transcription of the text augmented with the obtained linguistic features. The segment of the speech synthesis system charged with the production of acoustic features from the phonetic transcription and linguistic features of input text consists of two deep neural networks — the duration network and the acoustic network, as shown in Figure 2.

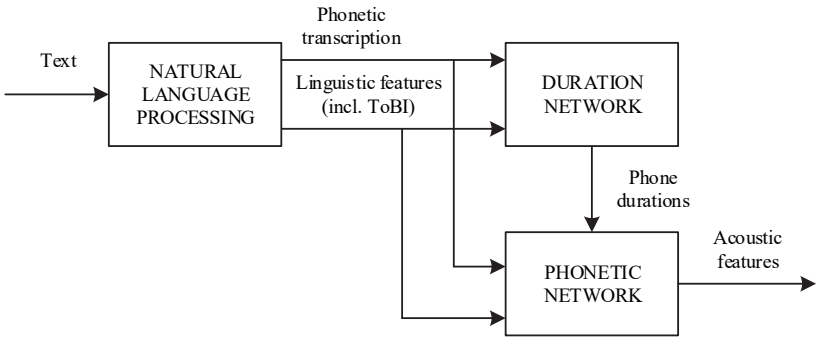


Fig 2. Neural network based model used for speech synthesis

The first network models phoneme durations and the second one models context-dependent acoustic features. The input for both networks is the phonetic transcription of the input text accompanied by linguistic features. In the training phase, the duration network adjusts its weight coefficients by minimizing the objective distance between the predicted values of HMM state durations of a phoneme and their actual durations in the training speech corpus. The actual values of HMM state durations of phonemes, as target features for the duration network, are extracted by forced alignment from training data, following the procedure proposed in the *Merlin* toolkit [22]. The inputs and outputs of the duration network are phone aligned. At synthesis phase, the duration network is required to predict the HMM state durations, and hence the durations of phones themselves, based on phone identity and linguistic context defined by features mentioned above. The HMM state durations obtained at the output of the duration network at synthesis time are used as additional inputs to the acoustic network. In the training phase, the acoustic network is trained to predict the relevant acoustic features given the phonetic transcriptions, linguistic context and HMM state durations. During the training, the acoustic network uses acoustic features extracted from speech recordings by the WORLD vocoder as target features. The acoustic features used include mel-generalised cepstral coefficients (MGCs), band aperiodicities (BAP) as well as log f_0, and they are further extended with their first and second derivatives as well as an additional flag indicating whether the current frame is voiced or unvoiced (V/UV). In all experiments in this paper 40 MGCs, 1 BAP, 1

log f_0 and 1 V/UV feature are used, yielding output feature vectors of length 127. Since the inputs and outputs to the acoustic network are frame aligned, the input feature vector of the acoustic network, in both training and synthesis phases, is extended by additional numeric features, including the index of the current frame in the state/phone as well as the index of the current state. Both networks consist of 4 hidden layers with 1024 neurons each. The first three have tangent hyperbolic as the activation function, while the fourth layer is recursive and uses long short-term memory (LSTM) neurons. The output layer is linear. The objective function used is mean squared distance between the predicted and the actual values in the training data. The input features are normalized to the interval [0.01, 0.99], while the output features are *z*-normalized. Each of the two networks is separately trained by backpropagation and stochastic gradient descent optimization. The smoothness of static features is achieved by using the maximum likelihood parameter generation algorithm [25], taking into account the predicted dynamic features. After the formants are further enhanced by postfiltering, the acoustic features are fed to the WORLD vocoder in order to generate speech waveforms.

As previously mentioned, two versions of the synthesizer were built, each trained on one of the two available speech corpora. Therefore, it was possible to synthesize sentences in either of the voices, M or F, based on specified phonetic transcription and ToBI annotation. This approach allowed the control over certain aspects of sentence intonation related to emphasis, as will be explained in more detail below.

The listening tests included 20 listeners who were not native speakers of English, but who professed to possessing good English language skills. The listeners had no or little previous experience with testing speech technology systems. The tests have been carried out in a relatively silent environment, using high-quality headphones. Nevertheless, it should be noted that the quality of the reproduction of synthesized speech is not of primary importance here because all experiments focus on prosodic features that are relatively robust to impairments in signal quality. Each of the listeners was required to evaluate 22 sentences, and each of the sentences was synthesized in 3 versions:

– Version A: Both ToBI tags E+ and CF0 were used both in training and in synthesis, as proposed by the research and described in the previous section.

– Versions B and C: Neither E+ nor CF0 were used in either training or synthesis, which corresponds to the standard ToBI model. In both cases, the effect of E+ was simulated by using either H* or L+H* in the ToBI transcription that is used as DNN input, as suggested by the findings of [18]. In the version B the effect of CF0 is ignored (i.e. the clause in a compressed f_0 range is annotated in the regular way, as if it was in no way different from the remainder of the utterance), while in the version C the pitch accents are removed from all words which were annotated with CF0 in version A. In this way the CF0 tag was equalized with the absence of a pitch accent. All of the aforementioned methods of simulating E+ or CF0 are in accordance with standard approaches based on the ToBI model.

The differences between versions A, B and C are conveniently summarized in Table 2.

Table 2. Versions of synthesis used in the experiments

<table>
<tr><th>A</th><th>B</th><th>C</th></tr>
<tr><td rowspan="2">E+ and CF0 used both in training and synthesis</td><td colspan="2">E+ and CF0 not used in either training or synthesis, E+ simulated using H* or L+H*</td></tr>
<tr><td>CF0 ignored</td><td>Pitch accents removed from words that have CF0 in version A</td></tr>
</table>

Experiment 1.

(a) In 10 sentences similar to the one from Example 1, with one word carrying the semantic focus of the sentence, the task of the listener was to determine, given 4 options, which word was assigned prosodic stress (E+) by the synthesizer, i.e. which of the words was intended to be emphasized. In none of the cases was it possible to determine the emphasized word solely on the basis of textual content of the utterance. The utterances were presented visually to the listeners, with available options indicated in boldface, as in:

Sarah talked *to her* ***neighbour*** *about a* ***problem***.

(b) In the second part of the experiment the same 10 sentences were used, but now the listeners were told which of the words was the intended focus of the utterance, and they were required to grade (on the scale from 1 to 5) how successfully this was conveyed in synthesized speech.

The aim of the Experiment 1 was to establish the effect of introducing E+ as opposed to signalling emphasis by rule-based methods. For that reason, the 10 utterances offered to the listeners included 5 utterances synthesized according to version A and 5 utterances synthesized according to version B. To minimize the influence of factors over which we had no control and which may have influenced the results of the listening tests, both the word which was assigned E+ and the order of presentation of the utterances were randomly varied across the listeners. For instance, if a word to which an E+ tag was assigned also happened to carry an L- phrase accent, the impression of emphasis was increased by the phrase accent, which would obscure the actual influence of E+. To mitigate this effect, versions where E+ was assigned to all 4 candidate words were used in the experiment in equal measure.

Experiment 2.

(a) In 12 utterances similar to those from Examples (2) and (3), including reporting clauses or comment clauses, which are commonly delivered in a compressed f_0 range, the listeners were required to grade (on the scale from 1 to 5) the general naturalness of intonation in synthesized speech.

(b) Each of the 12 utterances was presented to the listeners in all 3 versions, and they were required to select the version with most natural intonation.

The aim of the Experiment 2 was to establish the effect of introducing the CF0 tag on the naturalness of intonation, as opposed to signalling a lower degree of emphasis by excluding pitch accents or not signalling it at all. For that reason, both parts of the experiment included examples from all 3 synthesis versions in equal measure, in a random order unknown to the listeners. The listeners were unaware of the aim of the Experiment 2, but it was nevertheless possible for them to conclude that this experiment is related to a variable degree of emphasis associated with reporting or comment clauses.

4. Results and discussion. The results of all experiments are shown in Figure 3. The results of Experiment 1, concerned with E+, show that the listeners have been consistently identifying the sentence focus

most successfully in the version A of synthesis (76.0%, as opposed to 41.0% for version B, while 25.0% would correspond to a random choice in both cases). They were also consistent in assigning version A higher marks when judging how successfully the sentence focus was conveyed in synthesized speech (4.17 on average, as opposed to 3.35 for version B). As regards the CF0 tag, results are less conclusive because in some cases the difference between specific synthesis versions was almost negligible, as reported by a majority of listeners.

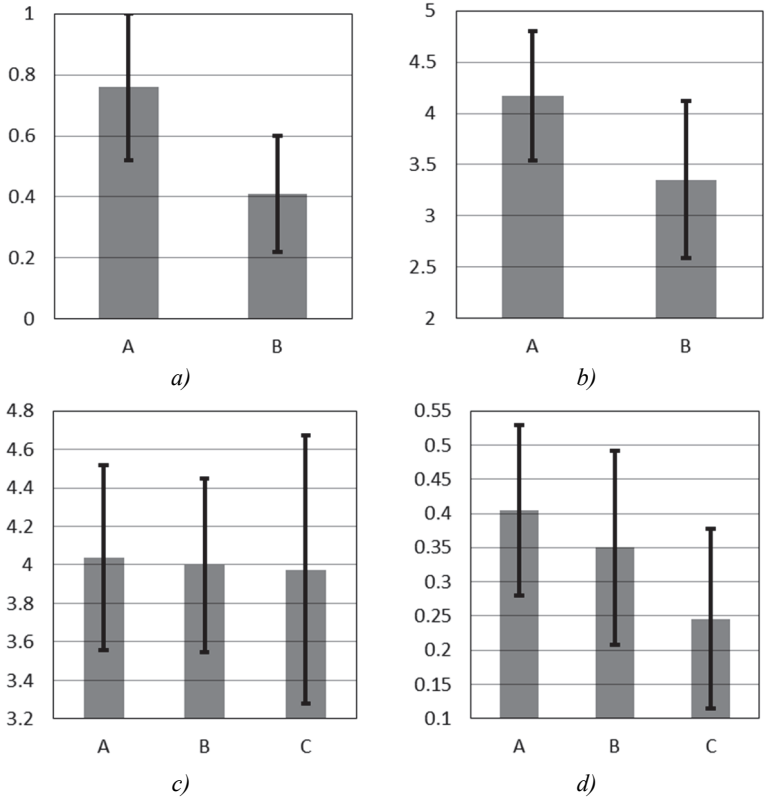


Fig. 3. Experiment results (mean value and standard deviation): a) Experiment 1a: percentage of correct identification of the emphasized word; b) Experiment 1b: average grade; c) Experiment 2a: average grade; d) Experiment 2b: relative frequency of a particular version being chosen as the most natural one

In the Experiment 2a, when evaluating utterances individually, the tendency towards assigning higher marks to the version A was practically

negligible (4.04, as opposed to 4.00 and 3.97 for versions B and C respectively). However, in direct comparison in Experiment 2b, the version A was noticeably more often identified as the most natural one (in 40.4% cases, as opposed to 35.0% and 24.6% for versions B and C respectively, while in this case 33.3% would correspond to a random choice). Furthermore, it can be noted that version C was least often recognized as the best one in direct comparison (Exp. 2b), although in individual evaluation (Exp. 2a) it received approximately the same marks as the version B.

Based on the results, it can be concluded that the initial hypothesis has been confirmed by the experiments, and it can also be noted that the variance between the answers given by particular listeners was significantly higher in case of CF0. A possible explanation of this fact is that the listeners may have had different expectations with respect to the delivery of reporting phrases, comment phrases or other content commonly delivered in a compressed f_0 range. For example, even when a reporting phrase is not synthesized within a compressed f_0 range, it can still sound quite acceptable to the listener, especially in a listening test, as opposed to actual speech communication. On the other hand, the expectations of listeners as regards prosodic stress are relatively clear and unambiguous. This may explain a considerably greater variance between the grades given by different listeners in Experiment 2 than in the Experiment 1. It should also be noted that the reproduction of E+ and particularly CF0 by the neural network based synthesizer in some cases was not entirely adequate. It can, thus, be concluded that of the reasons why the experiment results did not quite meet the expectations is certainly the inability of the DNN model to faithfully reproduce the E+ and CF0 tags after being trained on the available quantity of speech data.

5. Conclusion. The paper has presented a research aimed at increasing the quality of synthesis of expressive speech based on more adequate modeling of linguistically relevant prosodic features of speech, including prosodic stress and delivery of speech in a compressed f_0 range. In all cases of interest it has been shown that, if the standard ToBI model is augmented by tags aimed at reproduction of prosodic stress (E+) and content delivered in a compressed f_0 range (CF0), the target prosodic feature is more easily identified and there is an increase in overall naturalness.

Although the experiment was primarily concerned with synthesis of American English speech, the universality of the ToBI model suggests that

it would be possible to obtain the same results for other languages for which a ToBI model has been developed, and even for languages for which such a model could be developed in the future. The directions of our future research include the verification of the same hypotheses for Serbo-Croat, another language for which a ToBI model has been developed [26], as well as an investigation into the same phenomena in non-neutral speech styles. Since the range of fundamental frequency constitutes one of the most important features of a speech style or emotional state, it is an important research question to which extent the obtained results apply in case of different speech styles or emotional states.

It should be noted, however, that direct comparison of the results between different studies of this type is difficult because of their language dependence, dependence on corpus size as well as the differences in any of a number of varying parameters, starting from the choice of the system architecture or intonation model. Essentially, the question is to what extent linguistic phenomena should be explicitly modeled. Given a sufficiently complex system architecture and enough data, machine learning systems are able to learn surprisingly complex abstract linguistic concepts. However, as this study suggests, in case of relatively simple systems and a realistic amount of available data, explicit modeling of linguistic factors is still necessary to improve system performance.

References

1. Dall R., Yamagishi J., King S. Rating Naturalness in Speech Synthesis: The Effect of Style and Expectation. Proceedings of Speech Prosody. 2014. 5 p.
2. King S., Karaiskos V. The Blizzard Challenge 2016. Blizzard Challenge Workshop. 2016. 17 p.
3. King S., Wihlborg L., Guo W. The Blizzard Challenge 2017. Blizzard Challenge Workshop. 2017. 17 p.
4. Tatham M., Morton K. Developments in Speech Synthesis. John Wiley & Sons. 2005. 280 p.
5. Sluijter A. et al. Evaluation of speech synthesis systems for Dutch in telecommunication applications. Proceedings of the 3rd ESCA/COCOSDA Workshop (ETRW) on Speech Synthesis. 1998. 6 p.
6. Berg M. Modelling of Natural Dialogues in the Context of Speech-based Information and Control Systems. PhD Thesis. University of Kiel. 2014. 250 p.
7. Trouvain J. Laughing, Breathing, Clicking - The Prosody of Nonverbal Vocalisations. Proceedings of Speech Prosody. 2014. pp. 598–602.
8. Dall R. et al. Investigating Automatic & Human Filled Pause Insertion for Speech Synthesis. Proceedings of the Annual Conference of the ISCA. 2014. 5 p.
9. Székely É., Mendelson J., Gustafson J. Synthesising Uncertainty: The Interplay of Vocal Effort and Hesitation Disfluencies. 18th Annual Conference of the International

Speech Communication Association (INTERSPEECH 2017). 2017. vol. 2017. pp. 804–808.
10. Beckman M.E. Stress and Non-Stress Accent. Foris Publications. 1986. 241 p.
11. Silverman K. et al. ToBI: A standard for labeling English prosody. Proceedings of the 2nd International Conference on Spoken Language Processing. 1992. 4 p.
12. Beckman M.E., Hirschberg J., Shattuck-Hufnagel S. The original ToBI system and the evolution of the ToBI framework. Prosodic typology: The phonology of intonation and phrasing. 2006. 37 p.
13. Black A.W., Hunt A.J. Generating F0 contours from ToBI labels using linear regression. Proceedings of ICSLP. 1996. 4 p.
14. Wightman C.W. ToBI or not ToBI. Proceedings of the International Conference on Speech Prosody 2002. 2002. 5 p.
15. Syrdal A., Hirschberg J., McGory J., Beckman M. Automatic ToBI Prediction and Alignment to Speed Manual Labeling of Prosody. *Speech communication*. 2001. vol. 33. no. 1-2. pp. 135–151.
16. Syrdal A., McGorg J. Inter-Transcriber Reliability of ToBI Prosodic Labeling. Proceedings of the International Conference on Spoken Language Processing (ICSLP). 2000. 4 p.
17. Niemann H. et al. Prosodic processing and its use in Verbmobil. 1997 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP-97). 1997. vol. 1. pp. 75–78.
18. Pierrehumbert J., Hirschberg J.B. The meaning of intonational contours in the interpretation of discourse. Intentions in communication. 1990. pp. 271–311.
19. Hamza W. et al. The IBM Expressive Speech Synthesis System, Proceedings of the Eighth International Conference on Spoken Language Processing (ISCLP). 2004. 4 p.
20. Ze H., Senior A., Schuster M. Statistical parametric speech synthesis using deep neural networks. 2013 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). 2013. pp. 7962–7966.
21. Delić T., Sečujski M., Suzić S. A review of Serbian parametric speech synthesis based on deep neural networks. *Telfor Journal*. 2017. vol. 9. no. 1. pp. 32–37.
22. Wu Z., Watts O., King S. Merlin: An Open Source Neural Network Speech Synthesis System. Proceedings of the 9th ISCA Speech Synthesis Workshop. 2016. 6 p.
23. Seide F., Agarwal A. Cntk: Microsoft's open-source deep-learning toolkit. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. 2016. pp. 2135–2135.
24. Morise M., Yokomori F., Ozawa K. WORLD: a vocoder-based high-quality speech synthesis system for real-time applications. *IEICE Transactions on Information and Systems*. 2016. vol. 99. no. 7. pp. 1877–1884.
25. Tokuda K. et al. Speech parameter generation algorithms for HMM-based speech synthesis. Proceedings of the 2000 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'00). 2000. vol. 3. pp. 1315–1318.
26. Gođevac S. Transcribing Serbo-Croatian Intonation. Prosodic Typology: The Phonology of Intonation and Phrasing. 2005. 26 p.

Sečujski Milan — Ph.D., associate professor, head of Laboratory of Acoustics and Speech Technology of Faculty of Technical Sciences, University of Novi Sad. Research interests: digital signal processing, speech synthesis, natural language processing, dialogue systems, prosodic modelling, development of speech and language resources, machine learning, neural

networks. The number of publications — 160. secujski@uns.ac.rs; 6, Trg Dositeja Obradovića, 21000, Novi Sad, Serbia; office phone: +381-21-485-2533.

Ostrogonac Stevan — senior researcher, AlfaNum – Speech Technologies, software developer, AlfaNum – Speech Technologies. Research interests: text-to-speech synthesis, automatic speech recognition, natural language processing, dialogue systems, development of speech and language resources, machine learning, neural networks. The number of publications — 18. ostrogonac.stevan@alfanum.co.rs; 40, Bulevar Vojvode Stepe, 21000, Novi Sad, Serbia; office phone: +381-64-845-5302.

Suzić Siniša — researcher of Laboratory of Acoustics and Speech Technology of Faculty of Technical Sciences, University of Novi Sad. Research interests: expressive speech synthesis, digital signal processing, dialogue systems, machine learning, deep neural networks. The number of publications — 19. sinisa.suzic@uns.ac.rs; 6, Trg Dositeja Obradovića, 21000, Novi Sad, Serbia; office phone: +381-21-485-2521.

Pekar Darko — research assistant of the Department for Power, Electronic and Telecommunications Engineering of the Faculty of Technical Sciences, University of Novi Sad, CEO (Chief Executive Officer), AlfaNum Speech Technologies. Research interests: human-computer interaction, speech recognition and synthesis, speaker identification, emotion recognition, speech morphing, numerical simulations, artificial intelligence. The number of publications — 100. darko.pekar@alfanum.co.rs; 40, Bulevar Vojvode Stepe, 21000, Novi Sad, Serbia; office phone: +381-21-485-2521.

Acknowledgements. The research is supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia (grants TR32035 and OI178027). The authors are also grateful to the company Speech Morphing Inc. from Campbell, California, USA, for the permission to use their speech databases for this research.

УДК 004.5 **DOI** 10.15622/sp.59.8

М. Сечуйски, С. Острогонац, С. Сузич, Д. Пекар

ОБУЧЕНИЕ ПРОСОДИЧЕСКОЙ МОДЕЛИ ПО ДАННЫМ В НЕЙРОСЕТЕВОМ СИНТЕЗЕ РЕЧИ

Сечуйски М., Острогонац С., Сузич С., Пекар Д. **Обучение просодической модели по данным в нейросетевом синтезе речи.**

Аннотация. Естественность — один из важнейших аспектов синтезированной речи. Современные параметрические синтезаторы речи требуют обучения на большом количестве аннотированных речевых данных, чтобы иметь возможность передавать просодические элементы, такие как тоническое ударение и фразовый граничный тон. Наиболее часто используемый инструментарий для просодической аннотации речи в американском английском языке — Индексы Тонов и Просодических швов — ToBI, которые также были адаптированы для использования на других языках. В настоящей статье представлены некоторые недостатки ToBI в синтезе речи на американском английском языке, которые связаны с отсутствием тегов, специально предназначенных для обозначения различий в уровне просодии (акцента), связанной с конкретной частью предложения. В данном исследовании предлагается введение набора тегов, предназначенных для точного моделирования степени просодии, а именно определенная составляющая предложения может быть особо подчеркнута, если она является намеченным фокусом высказывания или ее роль преуменьшена, как это обычно бывает с фразами, сообщающими о прямой речи или комментариями.

С помощью нескольких аудирований было продемонстрировано, что изучение просодической модели на основе данных имеет определенные преимущества перед подходами, пытающимися использовать существующие теги ToBI для передачи степени акцента в синтезированной речи: речь, синтезированная нейронной сетью, обученной на данных с тегами уровня просодии, представляется более естественной, и слушатели могут с большим успехом отыскать просодическую составляющую предложения.

Ключевые слова: американский английский, просодическая модели, синтез речи, ToBI.

Сечуйски Милан — к-т техн. наук, доцент, заведующий лабораторией акустики и речи факультета технических наук, Нови-Садский университет. Область научных интересов: обработка цифровых сигналов, синтез речи, обработка естественного языка, диалоговая система, моделирование интонаций, разработка речевых и языковых ресурсов, машинное обучение, нейронные сети. Число научных публикаций — 160. secujski@uns.ac.rs; Трг Доситейа Обрадовича, 6, 21000, Нови Сад, Сербия; р.т.: +381-21-485-2533.

Острогонац Стеван — старший научный сотрудник, AlfaNum – Speech Technologies Ltd, разработчик программного обеспечения, AlfaNum – Speech Technologies Ltd. Область научных интересов: синтез речи, автоматическое распознавание речи, обработка естественного языка, диалоговая система, разработка речевых и языковых ресурсов, машинное обучение, нейронные сети. Число научных публикаций — 18. ostrogonac.stevan@alfanum.co.rs; бул. Войводе Степе, 40, 21000, Нови Сад, Сербия; р.т.: +381-64-845-5302.

Сузич Синиша — научный сотрудник лаборатории акустики и речи факультета технических наук, Нови-Садский университет. Область научных интересов: синтез выразительной речи, обработка цифровых сигналов, диалоговая система, машинное обучение, глубокие нейронные сети. Число научных публикаций — 19. sinisa.suzic@uns.ac.rs; Трг Доситейа Обрадовича, 6, 21000, Нови Сад, Сербия; р.т.: +381-21-485-2521.

Пекар Дарко — младший научный сотрудник департамента энергетики, электроники и телекоммуникационного инжиниринга факультета технических наук, Нови-Садский университет, главный исполнительный директор, AlfaNum Speech Technologies. Область научных интересов: человеко-машинное взаимодействие, распознавание и синтез речи, идентификация диктора, морфинг речи, статистический анализ, искусственный интеллект. Число научных публикаций — 100. darko.pekar@alfanum.co.rs; бул. Войводе Степе, 40, 21000, Нови Сад, Сербия; р.т.: +381-21-485-2521.

Поддержка исследований. Работа выполнена при финансовой поддержке Министерства образования, науки и технологического развития Республики Сербия (проекты TR32035 и OI178027). Авторы также благодарны компании Speech Morphing Inc., г. Кэмпбелл, Калифорния, США, за разрешение использовать свои речевые базы данных для этого исследования.

Литература

1. *Dall R., Yamagishi J., King S.* Rating Naturalness in Speech Synthesis: The Effect of Style and Expectation // Proceedings of Speech Prosody. 2014. 5 p.
2. *King S., Karaiskos V.* The Blizzard Challenge 2016 // Blizzard Challenge Workshop. 2016. 17 p.
3. *King S., Wihlborg L., Guo W.* The Blizzard Challenge 2017 // Blizzard Challenge Workshop. 2017. 17 p.
4. *Tatham M., Morton K.* Developments in Speech Synthesis // John Wiley & Sons. 2005. 280 p.
5. *Sluijter A. et al.* Evaluation of speech synthesis systems for Dutch in telecommunication applications // Proceedings of the 3rd ESCA/COCOSDA Workshop (ETRW) on Speech Synthesis. 1998. 6 p.
6. *Berg M.* Modelling of Natural Dialogues in the Context of Speech-based Information and Control Systems // PhD Thesis. University of Kiel. 2014. 250 p.
7. *Trouvain J.* Laughing, Breathing, Clicking - The Prosody of Nonverbal Vocalisations // Proceedings of Speech Prosody. 2014. pp. 598–602.
8. *Dall R. et al.* Investigating Automatic & Human Filled Pause Insertion for Speech Synthesis // Proceedings of the Annual Conference of the ISCA. 2014. 5 p.
9. *Székely É., Mendelson J., Gustafson J.* Synthesising Uncertainty: The Interplay of Vocal Effort and Hesitation Disfluencies // 18th Annual Conference of the International Speech Communication Association (INTERSPEECH 2017). 2017. vol. 2017. pp. 804–808.
10. *Beckman M.E.* Stress and Non-Stress Accent // Foris Publications. 1986. 241 p.
11. *Silverman K. et al.* ToBI: A standard for labeling English prosody // Proceedings of the 2nd International Conference on Spoken Language Processing. 1992. 4 p.
12. *Beckman M.E., Hirschberg J., Shattuck-Hufnagel S.* The original ToBI system and the evolution of the ToBI framework // Prosodic typology: The phonology of intonation and phrasing. 2006. 37 p.
13. *Black A.W., Hunt A.J.* Generating F0 contours from ToBI labels using linear regression // Proceedings of ICSLP. 1996. 4 p.
14. *Wightman C.W.* ToBI or not ToBI // Proceedings of the International Conference on Speech Prosody 2002. 2002. 5 p.
15. *Syrdal A., Hirschberg J., McGory J., Beckman M.* Automatic ToBI Prediction and Alignment to Speed Manual Labeling of Prosody // Speech communication. 2001. vol. 33. no. 1-2. pp. 135–151.

16. *Syrdal A., McGorg J.* Inter-Transcriber Reliability of ToBI Prosodic Labeling // Proceedings of the International Conference on Spoken Language Processing (ICSLP). 2000. 4 p.
17. *Niemann H. et al.* Prosodic processing and its use in Verbmobil // 1997 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP-97). 1997. vol. 1. pp. 75–78.
18. *Pierrehumbert J., Hirschberg J.B.* The meaning of intonational contours in the interpretation of discourse // Intentions in communication. 1990. pp. 271–311.
19. *Hamza W. et al.* The IBM Expressive Speech Synthesis System // Proceedings of the Eighth International Conference on Spoken Language Processing (ISCLP). 2004. 4 p.
20. *Ze H., Senior A., Schuster M.* Statistical parametric speech synthesis using deep neural networks // 2013 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). 2013. pp. 7962–7966.
21. *Delić T., Sečujski M., Suzić S.* A review of Serbian parametric speech synthesis based on deep neural networks // Telfor Journal. 2017. vol. 9. no. 1. pp. 32–37.
22. *Wu Z., Watts O., King S.* Merlin: An Open Source Neural Network Speech Synthesis System // Proceedings of the 9th ISCA Speech Synthesis Workshop. 2016. 6 p.
23. *Seide F., Agarwal A.* Cntk: Microsoft's open-source deep-learning toolkit // Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. 2016. pp. 2135–2135.
24. *Morise M., Yokomori F., Ozawa K.* WORLD: a vocoder-based high-quality speech synthesis system for real-time applications // IEICE Transactions on Information and Systems. 2016. vol. 99. no. 7. pp. 1877–1884.
25. *Tokuda K. et al.* Speech parameter generation algorithms for HMM-based speech synthesis // Proceedings of the 2000 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'00). 2000. vol. 3. pp. 1315–1318.
26. *Gođevac S.* Transcribing Serbo-Croatian Intonation // Prosodic Typology: The Phonology of Intonation and Phrasing. 2005. 26 p.

Signed to print 25.07.2018
Printed in Publishing center GUAP, 67, B. Morskaya, St. Petersburg, 190000, Russia

The journal is registered in Russian Federal Agency for Communications
and Mass-Media Supervision, certificate ПИ № ФС77-41695 dated August 19, 2010 г.
Subscription Index П5513, Russian Post Catalog

Подписано к печати 25.07.2018. Формат 60×90 1/16. Усл. печ. л. 13,5. Заказ № 298.
Тираж 150 экз., цена свободная.
Отпечатано в Редакционно-издательском центре ГУАП, 190000, Санкт-Петербург, Б. Морская, д. 67

Журнал зарегистрирован Федеральной службой по надзору в сфере связи
и массовых коммуникаций,
свидетельство ПИ № ФС77-41695 от 19 августа 2010 г.

Подписной индекс П5513 по каталогу «Почта России»

РУКОВОДСТВО ДЛЯ АВТОРОВ

Взаимодействие автора с редакцией осуществляется через личный кабинет на сайте журнала «Труды СПИИРАН» http://www.proceedings.spiiras.nw.ru. При регистрации авторам рекомендуется заполнить все предложенные поля данных.

Подготовка статьи ведется с помощью текстовых редакторов MS Word 2007 и выше. Объем основного текста – от 15 до 25 страниц включительно. Формат страницы документа – A5 (148 мм ширина, 210 мм высота); ориентация – портретная; все поля – 20 мм. Верхний и нижний колонтитулы страницы – пустые. Основной шрифт документа – Times New Roman, основной кегль (размер) шрифта – 10 pt. Переносы разрешены. Абзацный отступ устанавливается размером в 10 мм. Межстрочный интервал – одинарный. Номера страниц не проставляются.

В основную часть допускается помещать рисунки, таблицы, листинги и формулы. Правила их оформления подробно рассмотрены на нашем сайте в разделе «Руководство для авторов».

AUTHOR GUIDELINES

Interaction between each potential author and the Editorial board is realized through the personal account on the website of the journal "Proceedings of SPIIRAS" http://www.proceedings.spiiras.nw.ru. At the registration the authors are requested to fill out all data fields in the proposed form.

The submissions should be prepared using MS Word 2007 text editor or higher versions, at that, only manuscripts in *.docx format will be considered. The text of the paper in the main part of it should be from 15 – 25 pages of A5 size that is 210 X 148 mm; orientation – portrait; all margins – 20 mm. The font of the main paper text is Times New Roman of 10 pt font size. The pages' headers and footers should be empty; indention – 10 mm; line spacing – single; pages are not numbered; hyphenations are allowed.

Certain figures, tables, listings and formulas are allowed in the main section, and their typography is considered by the paper template in more detail in journal web.

ISSN 2078-9181

Вып. 4(59)

ТРУДЫ СПИИРАН
proceedings.spiiras.nw.ru

С-Пб
2018